(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 909 011**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.10.2019 E 19204398 (2)**

(97) Fecha y número de publicación de la concesión europea: **22.12.2021 EP 3633952**

(54) Título: **Sistemas y métodos para recibir y transmitir señales de comunicación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.05.2022

(73) Titular/es:

XERTIFIED AB (100.0%)
Jumkilsgatan 7A
752 18 Uppsala, SE

(72) Inventor/es:

ERIKSSON, MARTIN y
ALM, JENS

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistemas y métodos para recibir y transmitir señales de comunicación

Campo de la invención

La presente invención se refiere en general recibir y transmitir señales de comunicación. Más específicamente, la presente invención se refiere a sistemas y métodos para recibir y transmitir señales de comunicación.

Antecedentes de la invención

El interés en dispositivos conectados e Internet de las cosas está incrementando constantemente dentro de prácticamente todos los campos, tal como en los campos de fabricación, medicina y finanzas. Aunque se debe priorizar la seguridad de red para muchas de estas aplicaciones, actualmente hay decenas o cientos de millones de dispositivos que se conectan a diferentes redes inseguras. Los dispositivos conectados, por ejemplo, pueden variar desde aparatos médicos, robots de fabricación, semáforos hasta impresoras y escáneres.

Las soluciones de seguridad existentes para redes y dispositivos conectados se basan principalmente en varios principios. Un principio para estas redes y dispositivos conectados puede comprender establecer la seguridad a un nivel de red, asumiendo de este modo que se puede confiar en todos los usuarios y dispositivos dentro de la red. Sin embargo, si un intruso compromete la red o si un dispositivo dentro de la red se conecta directamente a una red pública, se pueden comprometer todos los dispositivos en la red. Otro principio puede ser la agrupación de diferentes usos y/o tecnologías y entonces enfocarse en asegurar las agrupaciones. Sin embargo, el o los problemas se pueden dividir en un mayor número de problemas más pequeños, que reduce el umbral de seguridad. Un principio adicional es adaptar la seguridad para un hardware específico. Sin embargo, estas soluciones de seguridad adaptadas pueden no permitir que también se aseguren otros dispositivos. Además, un principio puede ser simplemente usar un nivel de seguridad relativamente bajo, tal como Secure Sockets Layer (SSL).

La solicitud de patente US 20030196084A1 divulga un sistema de dispositivos inalámbricos que participan en comunicaciones seguras con redes seguras sin almacenar información comprometedora en el dispositivo inalámbrico. Se puede permitir que el dispositivo inalámbrico participe en una llamada infraestructura de clave pública (PKI). Además, la solicitud divulga cómo se solicita a un usuario que proporcione un certificado digital para la autenticación antes de que se otorgue acceso. Sin embargo, un problema con el sistema divulgado en la presente es que no aborda completamente el riesgo de seguridad de la conexión entre un servidor de proxy y recursos. Por ejemplo, el sistema divulgado está en riesgo de un ataque de intermediario, es decir, interceptación de redes, entre el servidor de proxy y un recurso. Un problema adicional con el sistema divulgado en la presente es que si se compromete el servidor de proxy, entonces se pueden comprometer todos los recursos conectados.

La solicitud de patente US 2015/0271097 A1 divulga un sistema para permitir que los recursos se comuniquen de manera eficiente uno con otro a través de sus respectivos proxies.

Sumario de la invención

Es de interés proporcionar alternativas a las soluciones de seguridad de red de la técnica anterior a fin de mejorar su seguridad y capacidad de gestión. Adicionalmente, existe el deseo de hacer más fácil la protección de dispositivos en redes públicas y privadas, especialmente para dispositivos antiguos y dispositivos de diferentes fabricantes. Más específicamente, los sistemas de acuerdo con la técnica anterior pueden no ser suficientemente seguros, pueden requerir vastas combinaciones de diferentes tecnologías y/o técnicas, haciendo los sistemas complejos y/o difíciles de manejar. Adicionalmente, puede ser difícil expandir o reducir de manera segura las soluciones proporcionadas por la técnica anterior. Además, los sistemas de acuerdo con la técnica anterior pueden no ser suficientemente seguros con respecto a personas con intención maliciosa que ya tienen acceso a una red.

Por lo tanto, es un objeto de la presente invención proporcionar alternativas a las soluciones de seguridad de red de la técnica anterior a fin de mejorar su seguridad, capacidad de gestión, controlabilidad, capacidad de expansión y/o capacidad de reducción.

Este y otros objetos se logran al proporcionar un sistema de comunicación para controlar un sistema de comunicación que tiene las características en la reivindicación independiente 1. Las realizaciones preferidas se definen en las reivindicaciones dependientes.

Por lo tanto, de acuerdo con un primer aspecto de la presente invención, se proporciona un sistema de comunicación para recibir y transmitir señales de comunicación. El sistema de comunicación comprende una red de datos y al menos un dispositivo de proxy. El al menos un dispositivo de proxy se acopla a la red de datos. Además, el al menos un dispositivo de proxy se configura para la autenticación de certificado digital. El sistema de comunicación comprende además al menos un recurso. Cada dispositivo de proxy del al menos un dispositivo de proxy se acopla a un respectivo recurso del al menos un recurso. Además, el al menos un recurso se acopla de manera comunicativa a la red de datos mediante el al menos

un dispositivo de proxy. Además, el al menos un dispositivo de proxy se puede configurar para controlar una comunicación entre la red de datos y el al menos un recurso con base en la autenticación de certificado digital.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un arreglo de comunicación. El arreglo de comunicación comprende el sistema de comunicación de acuerdo con el primer aspecto de la presente invención. Además, el arreglo de comunicación comprende un sistema de gestión acoplado al por lo menos un dispositivo de proxy del sistema de comunicación. El sistema de gestión se puede configurar para comunicar datos de autenticación de certificado digital entre el al menos un dispositivo de proxy y el sistema de gestión.

De acuerdo con un tercer aspecto del presente concepto inventivo, se proporciona un método para controlar un sistema de comunicación. El método comprende un sistema de comunicación de acuerdo con al menos uno del primer aspecto y el segundo aspecto de la invención. El método comprende el paso de detectar una comunicación entre el al menos un dispositivo de proxy y al menos uno del al menos un recurso y la red de datos. Además, el método comprende el paso de realizar una autenticación de certificado digital. Adicionalmente, el método comprende el paso de controlar la comunicación detectada con base en la autenticación de certificado digital.

Por lo tanto, el primer, segundo y tercer aspecto de la presente invención se basan en el concepto o idea común de que uno o más recursos se acoplan de manera comunicativa a una red de datos mediante un respectivo dispositivo de proxy, y que el respectivo dispositivo de proxy se puede configurar para controlar una comunicación entre la red de datos y el al menos un recurso con base en la autenticación de certificado digital. De este modo, cada recurso se asegura por un respectivo dispositivo de proxy. Por lo tanto, incluso en el caso de que un recurso se comprometa, la red de datos aún estaría protegida. Además, en el caso de que la red de datos se comprometa, cada recurso aún está protegido por un respectivo dispositivo de proxy. Por lo tanto, la presente invención tiene un mayor nivel de redundancia, que incrementa el nivel de seguridad. De este modo, incluso si una persona comprometiera una red privada protegida o un servidor de proxy, los recursos acoplados de manera comunicativa seguirían protegidos por cada respectivo dispositivo de proxy.

El sistema de comunicación se puede configurar para recibir y transmitir señales de comunicación dentro del sistema y entre el sistema de comunicación y otros dispositivos y/o redes. El sistema de comunicación se puede configurar para recibir y transmitir señales de comunicación de manera segura. El sistema de comunicación comprende una red de datos, al menos un dispositivo de proxy acoplado a la red de datos y al menos un recurso. Por el término “red de datos” se quiere decir aquí al menos una de una red de datos segura individual, una red de datos no segura individual, una red de datos en la nube y una pluralidad de redes de datos auxiliares. Por el término “dispositivo de proxy”, se quiere decir aquí un dispositivo intermediario, configurado para controlar una comunicación entre la red de datos y el al menos un recurso. Más específicamente, el “dispositivo de proxy” puede constituir un dispositivo configurado para el control de acceso de comunicación.

El al menos un dispositivo de proxy se configura para la autenticación de certificado digital. Por el término “autenticación de certificado digital” se quiere decir aquí la autenticación o validación de comunicación segura, por ejemplo, con base en al menos uno de un documento electrónico, un certificado digital, una firma, una clave pública y/o una clave privada. Por el término “recurso” se quiere decir aquí sustancialmente cualquier dispositivo que se pueda acoplar de manera comunicativa a la red de datos, por ejemplo, un dispositivo electrónico. El al menos un dispositivo de proxy se configura para controlar una comunicación entre la red de datos y el al menos un recurso con base en la autenticación de certificado digital. Por el término “configurado para controlar una comunicación”, se quiere decir aquí que el dispositivo de proxy se configura para permitir o deshabilitar la comunicación.

De acuerdo con una realización de la presente invención, el al menos un dispositivo de proxy se puede configurar para almacenar al menos un certificado digital. Por el término “certificado digital” se quiere decir aquí al menos uno de un documento electrónico, un certificado de identidad, una firma, una clave pública y/o una clave privada. El al menos un dispositivo de proxy se puede configurar para controlar una comunicación entre la red de datos y el al menos un recurso con base en al menos el uno o más certificados digitales almacenados. Se debe señalar que el o los certificados almacenados se pueden generar por el sistema de comunicación. La presente realización es ventajosa ya que la seguridad del sistema de comunicación se puede incrementar aún más. Además, se puede incrementar la capacidad de gestión del sistema de comunicación. El al menos un dispositivo de proxy se puede configurar para almacenar al menos un certificado digital, que se puede referir como un primer modo. Se apreciará que un dispositivo de proxy que se configura para operar en un primer modo puede ser relativamente eficiente en consumo de energía, notablemente ya que puede necesitar una cantidad menor de energía de cálculo que un dispositivo de proxy configurado para generar al menos un certificado digital. Por lo tanto, el dispositivo de proxy configurado para operar en un primer modo puede consumir menos energía y además puede ser relativamente pequeño. Además, el dispositivo de proxy configurado para operar en un primer modo se puede arreglar de manera más conveniente en una proximidad cercana a su respectivo recurso.

De acuerdo con una realización de la presente invención, el al menos un dispositivo de proxy se puede configurar para generar al menos una de al menos una clave pública y al menos una clave privada. El al menos un dispositivo de proxy se puede configurar para operar en un segundo modo, que se puede referir como un modo activo. Un dispositivo de proxy configurado para operar en un segundo modo se puede configurar para generar una o más claves públicas y/o una o más claves privadas. El al menos un dispositivo de proxy se puede configurar para recibir un certificado digital con base en la

o las claves públicas y/o la o las claves privadas. Por lo tanto, la presente realización es ventajosa ya que la seguridad del sistema de comunicación se puede incrementar aún más.

De acuerdo con una realización de la presente invención, el al menos un dispositivo de proxy se puede configurar además para controlar la comunicación entre la red de datos y el al menos un recurso con base en al menos uno de un hardware de certificado, una contraseña, una dirección IP, un puerto IP y una dirección MAC. Por lo tanto, el al menos un dispositivo de proxy se puede configurar además para controlar la comunicación entre la red de datos y el o los recursos con base en la autenticación de certificado digital y uno o más de un hardware de certificado, una contraseña, una dirección IP, un puerto IP y una dirección MAC. Se apreciará que el nivel de seguridad del sistema se puede incrementar por cada una de estas características o funciones adicionales mencionadas, en las cuales se basa el control de la comunicación del sistema.

De acuerdo con una realización de la presente invención, el al menos un dispositivo de proxy puede comprender un primer puerto de comunicación acoplado al por lo menos un recurso, y un segundo puerto de comunicación acoplado a la red de datos. Por lo tanto, el uno o más recursos se pueden acoplar físicamente a la red de datos mediante el primer y segundo puerto de comunicación del uno o más dispositivos de proxy respectivos. Por lo tanto, la comunicación con el o los recursos solo es posible a través del dispositivo de proxy, o por un acoplamiento físico directamente al recurso mediante el primer y segundo puertos de comunicación. Se apreciará que un acoplamiento o conexión física directamente al o a los recursos requiere que haya acceso físico a uno o más recursos, que se pueden restringir. Por lo tanto, la seguridad del sistema de comunicación se puede incrementar aún más por la presente realización.

De acuerdo con una realización de la presente invención, al menos uno del al menos un dispositivo de proxy y el al menos un recurso puede comprender un identificador. El identificador se puede configurar para indicar al menos una de una identificación y una ubicación de al menos uno del al menos un dispositivo de proxy y el al menos un recurso. Por el término “identificador” se quiere decir aquí sustancialmente cualquier dispositivo, unidad o similar, que se configura para indicar una identificación o ubicación del o de los dispositivos de proxy y/o el o los recursos. Se debe señalar que la seguridad de un sistema puede ser dependiente de saber qué usuarios y/o dispositivos están en el sistema, y dónde están estos usuarios y/o dispositivos en el sistema. Por lo tanto, un sistema de comunicación, donde el al menos un recurso y/o el al menos un dispositivo de proxy se identifica y/o se ubica puede incrementar adicionalmente la seguridad del sistema de comunicación.

De acuerdo con una realización de la presente invención, el identificador puede comprender un receptor. El receptor se puede configurar para recibir una ubicación de al menos uno del al menos un dispositivo de proxy y el al menos un recurso. Por lo tanto, el o los dispositivos de proxy y/o el o los recursos se pueden ubicar geográficamente, que puede incrementar adicionalmente la controlabilidad y la seguridad del sistema.

De acuerdo con una realización de la presente invención, el sistema de gestión se puede configurar para almacenar al menos una de la al menos una clave pública y la al menos una clave privada. Se apreciará que si el sistema de gestión se configura para almacenar la o las claves públicas y/o la o las claves privadas, entonces el al menos un dispositivo de proxy puede no necesitar configurarse para almacenar estas claves públicas y/o claves privadas. La presente realización es ventajosa ya que el dispositivo de proxy puede ser menos complejo en su configuración. Por ejemplo, el dispositivo de proxy de acuerdo con la presente realización puede comprender menos hardware/circuitería (complejos) que un dispositivo de proxy que se configura para almacenar la o las claves públicas y/o la o las claves privadas. Por lo tanto, se puede reducir el consumo de energía del dispositivo de proxy. Además, se puede reducir el tamaño del dispositivo de proxy. Además, se puede reducir la cantidad de material (elementos) necesarios para producir este dispositivo de proxy, mejorando de este modo la rentabilidad del sistema.

De acuerdo con otra realización de la presente invención, el sistema de gestión se puede configurar para generar al menos una clave pública y al menos una clave privada. La gestión se puede configurar además para generar al menos un certificado digital con base en al menos una de la al menos una clave pública y la al menos una clave privada. Por lo tanto, el sistema de gestión se puede configurar para generar la o las claves públicas y/o la o las claves privadas y proporcionar esta clave o estas claves al o a los dispositivos de proxy. Por consiguiente, puede no ser necesario que el dispositivo de proxy se configure para generar esta clave o estas claves por sí mismo.

La presente realización es ventajosa ya que la eficiencia del sistema se puede mejorar aún más.

De acuerdo con una realización de la presente invención, el sistema de gestión se puede configurar para realizar al menos una de una identificación y una localización de al menos uno del al menos un dispositivo de proxy y el al menos un recurso con base en el identificador. En otras palabras, el presente arreglo de comunicación puede comprender un sistema de comunicación, donde el o los recursos y/o el o los dispositivos de proxy se identifican y/o se ubican con base en el identificador. La presente realización es ventajosa ya que la identificación y/o ubicación del o de los recursos y/o el o los dispositivos de proxy puede incrementar aún más la seguridad del arreglo de comunicación.

De acuerdo con una realización de la presente invención, el sistema de gestión se puede configurar además para realizar al menos uno de un análisis de al menos una de la identificación y la ubicación de al menos uno del al menos un dispositivo de proxy y el al menos un recurso, un seguimiento de al menos una de la identificación y la ubicación de al menos uno

del al menos un dispositivo de proxy y el al menos un recurso, y un control de al menos una de la identificación y la ubicación de al menos uno del al menos un dispositivo de proxy y el al menos un recurso. Se apreciará que el análisis, seguimiento y/o control de la identificación y/o la ubicación del o de los dispositivos de proxy y/o el o los recursos de la presente realización puede incrementar la transparencia del sistema de comunicación. Por lo tanto, por esta realización la seguridad y/o la controlabilidad del arreglo de comunicación se pueden incrementar aún más.

De acuerdo con una realización de la presente invención, al menos uno del sistema de gestión y el al menos un dispositivo de proxy se pueden configurar para registrar la comunicación de datos entre la red de datos y el al menos un dispositivo de proxy. Por lo tanto, el sistema de gestión y/o el o los dispositivos de proxy se pueden configurar para registrar la comunicación de datos entre la red de datos y el o los dispositivos de proxy, es decir, del dispositivo de proxy a la red de datos y de la red de datos al dispositivo de proxy, respectivamente. Por el término “configurado para registrar”, se quiere decir que el sistema de gestión y/o el o los dispositivos de proxy pueden registrar, catalogar y/o anotar la comunicación de datos entre la red de datos y el o los dispositivos de proxy. La comunicación de datos registrados por el arreglo de comunicación se puede usar para mejorar la controlabilidad de la comunicación e incrementar de este modo la seguridad del arreglo de comunicación.

La comunicación de datos registrados puede comprender al menos uno de una marca de tiempo, datos del al menos un recurso a la red, datos de la red de datos al por lo menos un recurso, un emisor de comunicación de datos, un receptor de comunicación de datos, una cantidad de la comunicación de datos, un tipo de la comunicación de datos, varios tiempos de espera de comunicación de datos, varios intentos de comunicación de datos y datos de certificado. En otras palabras, los datos registrados pueden comprender cualquiera de, o una combinación de, las formas de datos mencionadas como se ejemplifica. Por lo tanto, por la presente realización, la controlabilidad de la comunicación y por lo tanto, la seguridad del arreglo de comunicación, se pueden incrementar aún más.

De acuerdo con una realización de la presente invención, al menos uno del sistema de gestión y el al menos un dispositivo de proxy se pueden configurar además para controlar la comunicación entre la red de datos y el al menos un dispositivo de proxy con base en la comunicación de datos registrados. Por lo tanto, de acuerdo con la presente realización, el sistema de gestión y el o los dispositivos de proxy se pueden configurar para controlar la comunicación con base en la comunicación de datos registrados de acuerdo con una o más de las realizaciones previamente descritas. La presente realización es ventajosa ya que se incrementa el nivel de seguridad en el arreglo de comunicación.

De acuerdo con una realización de la presente invención, al menos uno del sistema de gestión y el al menos un dispositivo de proxy se pueden configurar para registrar datos de certificado digital entre la red de datos y el al menos un dispositivo de proxy. Los datos de certificado digital registrados pueden comprender al menos uno de una marca de tiempo, certificado digital transmitido del al menos un dispositivo de proxy a la red de datos, certificado digital transmitido de la red de datos al por lo menos un dispositivo de proxy, certificado digital recibido por el al menos un dispositivo de proxy, certificado digital recibido por la red de datos, varias solicitudes de certificado digital. Por lo tanto, por la presente realización, se puede mejorar la seguridad del sistema de comunicación.

Otros objetivos de, características de y ventajas de la presente invención llegarán a ser evidentes cuando se estudie la siguiente divulgación detallada, los dibujos y las reivindicaciones anexas. Aquellos expertos en la técnica se darán cuenta de que diferentes características de la presente invención se pueden combinar para crear realizaciones diferentes de aquellas descritas en lo siguiente.

Breve descripción de los dibujos

Este y otros aspectos de la presente invención se describirán ahora en más detalle, con referencia a los dibujos anexos que muestran la o las realizaciones de la invención.

Las figuras 1 a 4 muestran esquemáticamente los sistemas de comunicación de acuerdo con las realizaciones de ejemplificación de la presente invención, y
Las figuras 5 y 6 muestran esquemáticamente los arreglos de comunicación de acuerdo con las realizaciones de ejemplificación de la presente invención.

Descripción detallada

La figura 1 muestra esquemáticamente un sistema de comunicación 100 para recibir y transmitir señales de comunicación de acuerdo con una realización de ejemplificación de la presente invención. El sistema de comunicación 100 mostrado comprende una red de datos 110. Además, el sistema de comunicación 100 comprende un dispositivo de proxy 120 acoplado a la red de datos 110. Se muestra que el sistema de comunicación 100 comprende un recurso 130. El dispositivo de proxy 120 se acopla al respectivo recurso 130, es decir, cada dispositivo de proxy 120 del sistema de comunicación 100 se acopla a un respectivo recurso 130. El recurso 130 se acopla de manera comunicativa a la red de datos 110 mediante el dispositivo de proxy 120. El dispositivo de proxy 120 se configura para autenticación de certificado digital. El dispositivo de proxy 120 mostrado se configura además para controlar una comunicación entre la red de datos 110 y el recurso 130 con base en la autenticación de certificado digital.

Se debe señalar que el sistema de comunicación 100 como se ejemplifica no se limita por la ilustración en la figura 1. Por ejemplo, puede haber sustancialmente cualquier número de recursos 130 que se pueda acoplar de manera comunicativa a un respectivo número de dispositivos de proxy 120. El dispositivo de proxy 120 se puede acoplar de manera comunicativa a la red de datos 110 mediante cable o de manera inalámbrica. Adicionalmente, el dispositivo de proxy 120 se puede acoplar de manera comunicativa a la red de datos 110 mediante un conmutador y un enrutador (no mostrado). Además, el término “red de datos” se debe interpretar como al menos una de una red de datos segura individual, una red de datos no segura individual, una red de datos en la nube y una pluralidad de redes de datos auxiliares.

De acuerdo con un ejemplo, el dispositivo de proxy 120 en la figura 1 se puede configurar para almacenar al menos un certificado digital 410 (no mostrado), donde el al menos un certificado digital se puede usar para autenticación de certificado digital. Además, el dispositivo de proxy 120 se puede configurar para generar al menos una de al menos una clave pública y al menos una clave privada, donde la o las claves públicas y/o la o las claves privadas se pueden usar para autenticación de certificado digital. Además, el dispositivo de proxy 120 se puede configurar además para controlar la comunicación entre la red de datos 110 y el o los recursos 130 con base en uno o más de un dispositivo de certificado, una contraseña, una dirección IP, un puerto IP y una dirección MAC.

Aunque no se muestra explícitamente en la figura 1, se apreciará que la red de datos 110 puede comprender una pluralidad de redes de datos auxiliares, donde esta pluralidad de redes de datos auxiliares se puede interconectar de manera comunicativa. Por ejemplo, el recurso 130 se puede acoplar de manera comunicativa a una primera red de datos auxiliar mediante el dispositivo de proxy 120, y el dispositivo de proxy 120 se puede configurar para controlar una comunicación entre la primera red de datos auxiliar y el recurso 130 con base en la autenticación de certificado digital, por ejemplo, recibido de una segunda red de datos auxiliar.

La figura 2 muestra esquemáticamente un sistema de comunicación 100 para recibir y transmitir señales de comunicación de acuerdo con una realización de ejemplificación de la presente invención. Se debe señalar que la figura 2 comprende características, elementos y/o funciones como se muestra en la figura 1 y se describe en el texto asociado. Por lo tanto, también se refiere a esa figura y texto para un entendimiento incrementado.

En la figura 2, la red de datos 110 del sistema de comunicación 100 mostrado se acopla de manera comunicativa a un servidor de certificación digital 400. Aunque se dibuja por separado por razones de claridad, se va a entender que la red de datos 110 puede comprender el servidor de certificación digital 400. El servidor de certificación digital 400 se puede configurar para generar un certificado digital con base en una clave pública y/o una clave privada. El servidor de certificación digital 400 puede comprender un dispositivo de infraestructura de clave pública (PKI). Además, el dispositivo de PKI puede comprender un servidor de autenticación de red (NAS) o un servidor de red (NS). El sistema de comunicación 100 se puede configurar para autenticación de certificado digital con base en una comunicación con el servidor de certificación digital 400. El dispositivo de proxy 120 del sistema de comunicación 100 se puede acoplar de manera comunicativa al servidor de certificación digital 400. El acoplamiento comunicativo entre el dispositivo de proxy 120 y el servidor de certificación digital 400 se puede proporcionar mediante la red de datos 110. El dispositivo de proxy 120 se puede configurar para autenticación de certificado digital con base en una comunicación con el servidor de certificación digital 400. El dispositivo de proxy 120 se puede configurar para traducción de dirección de red (NAT).

En la figura 2 se ilustra una transmisión de un certificado digital 410 entre el dispositivo de proxy 120 y la red de datos 110. El dispositivo de proxy 120 se puede configurar para transmitir un certificado digital 410 si el respectivo recurso 130 intenta comunicarse mediante el dispositivo de proxy 120. El certificado digital 410 se puede transmitir mediante la red de datos 110 al servidor de certificación digital 400. El servidor de certificación digital 400 se puede configurar para autenticar el certificado digital 410. Se debe entender que el término “autenticar” comprende al menos validar, aprobar, certificar, confirmar y/o verificar. El dispositivo de proxy 120 se puede configurar para controlar una comunicación entre la red de datos 110 y el recurso 130 con base en una autenticación de certificado digital por un servidor de certificación digital 400. El dispositivo de proxy 120 se puede configurar además ya sea para otorgar o denegar la comunicación entre el recurso 130 y la red de datos 110 con base en la autenticación de certificado digital. Se debe señalar que el dispositivo de proxy 120 se puede configurar además para controlar la comunicación con base en uno o más de puertos IP, filtros IP y/o filtros de puerto.

De acuerdo con un ejemplo, el sistema de comunicación 100 se puede configurar para revocar, poner en cuarentena y/o desconectar el o los recursos 130 con base en un incidente de red de datos predeterminado. Por el término “incidente de red de datos” se quiere decir sustancialmente cualquier tipo de incidente, evento, cambio o similar en el sistema de comunicación 100 tal como una desconexión y/o un cambio en una transmisión entre la red de datos 110, el o los dispositivos de proxy 120, el o los recursos 130 y/o el servidor de certificación digital 400.

El dispositivo de proxy 120 mostrado en la figura 2 comprende además un primer puerto de comunicación 210 que se acopla de manera comunicativa al recurso 130. Además, el dispositivo de proxy 120 mostrado comprende un segundo puerto de comunicación 220 que se acopla de manera comunicativa a la red de datos 110. El dispositivo de proxy 120 se puede configurar para controlar una comunicación mediante el primer puerto de comunicación 210 y el segundo puerto de comunicación 220. Aquí, el recurso 130 solo se puede acoplar de manera comunicativa al dispositivo de proxy 120 mediante el primer puerto de comunicación 210. Por lo tanto, el único canal para comunicación con el recurso 130 puede

ser a través del respectivo dispositivo de proxy 120. Se apreciará que el primer y/o el segundo puerto de comunicación 210, 220 no se limitan a ningún tipo específico de puerto y/o interfaz. El primer y/o segundo puerto de comunicación 210, 220 puede comprender al menos uno de RJ45, inalámbrico, fibra, USB y RS232. El dispositivo de proxy 120 puede comprender un canal de comunicación (es decir, individual). El canal de comunicación puede comprender el primer puerto de comunicación 210 acoplado al recurso 130, y el segundo puerto de comunicación 220 acoplado a la red de datos 110. Por lo tanto, solo puede haber una forma de comunicación en el sistema de comunicación 100, específicamente, a través del dispositivo de proxy 120.

De acuerdo con el sistema de comunicación 100, como se ejemplifica en la figura 2, se muestra que el dispositivo de proxy 120 comprende un identificador 300. El identificador 300 se puede configurar para indicar una identificación y/o una ubicación del dispositivo de proxy 120. Se debe señalar que el recurso 130 puede comprender un identificador 300. Además, el identificador 300 mostrado comprende un receptor 310. El receptor 310 se puede configurar para recibir una ubicación del dispositivo de proxy 120. Además, el receptor 310 se puede configurar para transmitir la ubicación al dispositivo de proxy 120. A su vez, el dispositivo de proxy 120 se puede configurar para transmitir la ubicación a la red de datos 110. El receptor 310 se puede configurar para almacenar la ubicación. Además, el receptor 310 se puede configurar para recibir una ubicación de GPS.

El identificador 300 puede comprender un código leíble (no mostrado). El código leíble se puede configurar, por ejemplo, como un código de barras, un código QR o similares. El identificador 300 se puede configurar para que sea leíble y/o escaneable. Además, el identificador 300 se puede configurar para que se lea y/o escanee por un dispositivo portátil. La indicación de la identificación puede comprender uno o más de un número de identificación, un número de serie y un nombre de dispositivo. El identificador 300 puede estar en contacto (físico directo) con el dispositivo de proxy 120.

Adicionalmente, se apreciará que la indicación de identificación como se ejemplifica puede comprender una indicación digital de identificación, que se puede referir como una ID digital. La ID digital puede comprender al menos una de una dirección IP, un puerto IP, una ubicación dentro de una red de datos, datos de identificación de dispositivos conectados y una dirección MAC. Además, el dispositivo de proxy 120 y el recurso 130, y sus acoplamientos y/o conexiones dentro de y/o a la red de datos 110, se pueden indicar en detalle. Por lo tanto, se pueden rastrear y monitorear los cambios de uno o más dispositivos, conexiones, etc., del sistema de comunicación 100.

La indicación de una ubicación del dispositivo de proxy 120 y/o el recurso 130 puede comprender indicar una ubicación geográfica del dispositivo de proxy 120 y/o el recurso 130. De manera alternativa, la indicación de una ubicación del al menos un dispositivo de proxy 120 y/o el recurso 130 puede comprender indicar una ubicación de red del dispositivo de proxy 120 y/o el recurso 130. El sistema de comunicación 100 se puede configurar para recibir la indicación de la ubicación (geográfica y/o de red) del dispositivo de proxy 120 y/o el recurso 130.

Además, el sistema de comunicación 100 puede comprender planos. Se debe entender que el término “planos” comprende, por ejemplo, datos y/o archivos tal como dibujos, diseños y/o archivos de diseño asistido por computadora (CAD). Los planos pueden comprender información sobre el o los lugares geográficos donde se ubican el recurso 130 y/o el dispositivo de proxy 120. Además, los planos pueden comprender información y/o la o las indicaciones de dónde se ubica el recurso 130 y/o el dispositivo de proxy 120 en este o estos lugares geográficos.

La figura 3 muestra un sistema de comunicación 100 para recibir y transmitir señales de comunicación de acuerdo con una realización de ejemplificación de la presente invención. Se debe señalar que la figura 3 comprende características, elementos y/o funciones como se muestra y describe en relación con las figuras 1 y 2. Por lo tanto, también se refiere a aquellas figuras y textos asociados para un entendimiento incrementado.

El sistema de comunicación 100 ilustrado en la figura 3 es ejemplar por razones de entendimiento. Por ejemplo, puede haber sustancialmente cualquier número de recursos 130. Por consiguiente, el sistema de comunicación 100 puede comprender cualquier número de dispositivos de proxy 120 acoplados a la red de datos 110, donde cada dispositivo de proxy 120 se acopla a un respectivo recurso 130. La red de datos 110 del sistema de comunicación 100 se acopla de manera comunicativa a dos dispositivos de usuario 140a, 140b. Por el término “dispositivo de usuario” se quiere decir aquí sustancialmente cualquier dispositivo (electrónico) configurado para conectarse al recurso 130 mediante la red de datos 110, por ejemplo, una computadora. Se apreciará que puede haber sustancialmente cualquier número de dispositivos de usuario 140a, 140b acoplados a la red de datos 110 del sistema de comunicación 100, y que los dos dispositivos de usuario 140a, 140b se muestran como un ejemplo. De acuerdo con el ejemplo de la figura 3, la comunicación entre los dispositivos de usuario 140a, 140b acoplados a la red de datos 110 y el recurso 130 acoplado a la red de datos 110 mediante el respectivo dispositivo de proxy 120 se puede controlar por el dispositivo de proxy 120 con base en la autenticación de certificado digital. El o los dispositivos de usuario 140a, 140b solo se pueden comunicar con el recurso 130 mediante el dispositivo de proxy 120, donde el dispositivo de proxy 120 se configura para controlar la comunicación entre el o los dispositivos de usuario 140a, 140b y el recurso 130 con base en la autenticación de certificado digital. De este modo, solo un dispositivo de usuario autenticado 140a, 140b puede comunicarse con el recurso 130. Por lo tanto, una persona con intención maliciosa que usa el dispositivo de usuario 140a, 140b puede no ser capaz de conectarse al recurso 130, aunque la persona con intención maliciosa se puede conectar a la red de datos 110 por el dispositivo de usuario 140a, 140b.

La figura 4 muestra un sistema de comunicación 100 para recibir y transmitir señales de comunicación de acuerdo con una realización de ejemplificación de la presente invención. Se debe señalar que la figura 4 comprende características, elementos y/o funciones como se muestra y describe en relación con las figuras 1, 2 y/o 3. Por lo tanto, también se refiere a una o más de esas figuras y textos asociados para un entendimiento incrementado.

El sistema de comunicación 100 en la figura 4 muestra dos certificados digitales 410a, 410b. Los certificados digitales 410a, 410b se pueden transmitir entre un dispositivo de usuario 140a, 140b y la red de datos 110. Los certificados digitales 410a, 410b se pueden transmitir desde un dispositivo de usuario 140a, 140b al dispositivo de proxy 120, mediante la red de datos 110. El dispositivo de proxy 120, mediante el cual un recurso 130 se acopla de manera comunicativa a la red de datos 110, se puede configurar para controlar la comunicación entre un recurso 130 y un dispositivo de usuario 140a, 140b, con base en la autenticación de certificado digital, donde la autenticación de certificado digital se puede basar en uno o más de los certificados digitales 410a, 410b. Además, el o los certificados digitales 410a, 410b pueden comprender además una contraseña, una dirección IP, un puerto IP y/o una dirección MAC.

Además, de acuerdo con un ejemplo, el dispositivo de usuario 140b se muestra acoplado a un dispositivo de certificado 420. Además, el dispositivo de certificado 420 se puede acoplar de manera comunicativa al recurso 130. El dispositivo de certificado 420 se puede configurar para proporcionar al dispositivo de usuario 140b datos de certificado, donde los datos de certificado pueden comprender al menos uno de un certificado digital 410, una contraseña, una clave pública, una clave privada y un testigo (token). Adicionalmente, el dispositivo de proxy 120 se puede configurar para controlar la comunicación entre el recurso 130 y el dispositivo de usuario 140b con base en la autenticación de certificado digital, donde la autenticación de certificado digital se puede basar al menos en los datos de certificado. El dispositivo de certificado 420 se puede configurar para recibir una tarjeta inteligente, donde la tarjeta inteligente se puede configurar para proporcionar datos de certificado al dispositivo de certificado. Por el término “tarjeta inteligente” se quiere decir un dispositivo electrónico físico configurado para autenticación de certificado digital.

El dispositivo de proxy 120 mostrado en la figura 4 se acopla de manera comunicativa a un servidor de certificación digital 400. El servidor de certificación digital 400 puede comprender un dispositivo de infraestructura de clave pública (PKI). Además, el dispositivo de PKI puede comprender un servidor de autenticación de certificado (CAS) o un servidor de certificado (CS). Se debe señalar que el concepto inventivo no se limita a la realización mostrada en la figura 4. Por ejemplo, el o los dispositivos de proxy 120 se pueden acoplar de manera comunicativa al servidor de certificación digital 400 mediante la red de datos 110. El o los dispositivos de proxy 120 se pueden configurar para transmitir un certificado digital 410 a un servidor de certificación digital 400. El servidor de certificación digital 400 puede autenticar el certificado digital 410. De manera alternativa, el dispositivo de proxy 120 puede comprender una lista de certificados digitales. Un dispositivo de proxy 120 se puede configurar para autenticar un certificado digital 410 con base en la lista de certificados. Se apreciará que el o los dispositivos de usuario 140a, 140b solo se pueden comunicar con el recurso 130 mediante el dispositivo de proxy 120 con base en el o los certificados digitales 410a, 410b. Por lo tanto, una persona con intención maliciosa que usa el o los dispositivos de usuario 140a, 140b no es capaz de conectarse al recurso 130 sin proporcionar el o los certificados digitales 410a, 410b al dispositivo de proxy 120.

La figura 5 muestra un arreglo de comunicación 500 de acuerdo con un ejemplo de ejemplificación. El arreglo de comunicación 500 mostrado comprende un sistema de comunicación 100 de acuerdo con una realización de ejemplificación de la presente invención. Se debe señalar que la figura 5 comprende características, elementos y/o funciones como se muestra y describe en relación con las figuras 1 a 4. Por lo tanto, también se refiere a una o más de esas figuras y/o textos asociados para un entendimiento incrementado.

El arreglo de comunicación 500 mostrado en la figura 5 comprende un sistema de gestión 510. El sistema de gestión 510 se puede configurar para comunicar datos de autenticación de certificado digital entre un dispositivo de proxy 120 y el sistema de gestión 510. Además, la figura 5 muestra un dispositivo de usuario 140, acoplado de manera comunicativa al sistema de gestión 510 del arreglo de gestión 510. El recurso 130 se acopla de manera comunicativa al dispositivo de usuario 140 mediante el dispositivo de proxy 120 y el sistema de gestión 510.

El sistema de gestión 510 se puede configurar para almacenar una clave pública y/o una clave privada. El sistema de gestión 510 se puede configurar para comunicar un certificado digital a un dispositivo de proxy 120, y donde el dispositivo de proxy 120 se puede configurar para almacenar el certificado digital.

El sistema de gestión 510 y/o el o los dispositivos de proxy 120 se pueden configurar para registrar la comunicación de datos entre la red de datos 110 y el o los dispositivos de proxy 120. La comunicación de datos registrados puede comprender uno o más de una marca de tiempo, datos del o de los recursos 130 a la red de datos 110, datos de la red de datos 110 al o a los recursos 130, un emisor de comunicación de datos, un receptor de comunicación de datos, una cantidad de la comunicación de datos, un tipo de la comunicación de datos, varios tiempos de espera de comunicación de datos, varios intentos de comunicación de datos y datos de certificado. El sistema de gestión 510 y/o el o los dispositivos de proxy 120 se pueden configurar además para controlar la comunicación entre la red de datos 110 y el o los dispositivos de proxy 120. El control de la comunicación entre la red de datos 110 y el o los dispositivos de proxy 120 se puede basar en la comunicación de datos registrados. La comunicación de datos registrados puede comprender un incidente de red de datos. El sistema de gestión 510 y/o el dispositivo de proxy 120 se pueden configurar además para controlar la

comunicación entre la red de datos 110 y el dispositivo de proxy con base en una comunicación de datos registrados predeterminada. El sistema de gestión 510 y/o el dispositivo de proxy 120 se puede configurar además para realizar un control predeterminado de la comunicación entre la red de datos 110 y el dispositivo de proxy con base en una comunicación de datos registrados predeterminada. Un control de la comunicación por el sistema de gestión 510 puede comprender conectar un dispositivo de proxy 120, un recurso 130, un dispositivo de usuario 140 y/o la red de datos 110, desconectar un dispositivo de proxy 120, un recurso 130, un dispositivo de usuario 140 y/o la red de datos 110, re-encaminar un dispositivo de proxy 120, un recurso 130, un dispositivo de usuario 140 y/o la red de datos 110, revocar un certificado digital 410, alterar una lista de certificados, cerrar un puerto y/o cambiar el ancho de banda entre un dispositivo de proxy 120, un recurso 130, un dispositivo de usuario 140 y/o la red de datos 110 y un dispositivo de proxy 120, un recurso 130, un dispositivo de usuario 140 y/o la red de datos 110.

El dispositivo de usuario 140 solo se puede comunicar con el recurso 130 mediante el dispositivo de proxy 120 y/o el sistema de gestión 510. El dispositivo de proxy 120 y/o el sistema de gestión 510 se pueden configurar para controlar la comunicación entre el dispositivo de usuario 140 y el recurso 130 con base en la autenticación de certificado digital y/o comunicación de datos registrados.

La figura 6 muestra un arreglo de comunicación 500 de acuerdo con una realización de ejemplificación de la presente invención. Se debe señalar que la figura 6 comprende características, elementos y/o funciones como se muestra y describe en relación con las figuras 1 a 5. Por lo tanto, también se refiere a una o más de esas figuras y/o textos asociados para un entendimiento incrementado.

Adicionalmente, el arreglo de comunicación 500 mostrado en la figura 6 comprende un servidor de certificación digital 400. El servidor de certificación digital 400 mostrado se acopla de manera comunicativa al sistema de gestión 510 y al dispositivo de proxy 120. Además, el servidor de certificación digital 400 se puede acoplar de manera comunicativa al sistema de gestión 510 y/o el o los dispositivos de proxy 120 mediante la red de datos 110.

El arreglo de comunicación 500 puede comprender cualquier número de recursos 130, donde cada recurso 130 se acopla a una red de datos 110 mediante un respectivo dispositivo de proxy 120. Cada dispositivo de proxy 120 se configura para controlar una comunicación entre la red de datos 110 y su respectivo recurso 130 con base en la autenticación de certificado digital.

Por lo tanto, cada dispositivo de proxy 120 se puede configurar para controlar una comunicación de la red de datos 110 a su recurso respectivo 130, con base en la autenticación de certificado digital. Un dispositivo de usuario 140 se puede acoplar a la red de datos 110 del sistema de comunicación 100. De este modo, cada dispositivo de proxy 120 se puede configurar para controlar una comunicación entre un dispositivo de usuario 140 y el respectivo recurso 130 del dispositivo de proxy 120, con base en la autenticación de certificado digital. La autenticación de certificado digital puede comprender el dispositivo de proxy 120 que recibe un certificado digital 410 del sistema de gestión 510. El dispositivo de proxy 120 se puede configurar para comparar el certificado digital 410 recibido con una lista de certificados. El dispositivo de proxy 120 y/o el sistema de gestión 510 se puede configurar para autenticar el certificado digital 410 con base en la comparación entre el certificado digital 410 y la lista de certificados.

El sistema de gestión 510 se puede configurar para generar el certificado digital 410. Adicionalmente, el sistema de gestión 510 se puede configurar para generar una o más claves públicas y/o una o más claves privadas. Además, el sistema de gestión 510 se puede configurar para generar el certificado digital 410, con base en la o las claves públicas y/o la o las claves privadas, donde esta clave o estas claves se pueden generar por el sistema de gestión 510.

Adicionalmente, el sistema de gestión 510 se puede configurar para recibir el certificado digital 410 del servidor de certificación digital 400 con base en una transmisión de una o más claves públicas y/o una o más claves privadas del sistema de gestión 510 al servidor de certificación digital 400. El certificado digital 410 se puede generar durante la inscripción de un dispositivo de proxy 120. Por el término “inscripción” se quiere decir secuencia de arranque y/o instalación. Se puede generar una lista de certificados durante la inscripción de un dispositivo de proxy 120. La inscripción de un dispositivo de proxy 120 puede comprender acoplar un respectivo recurso 130 a la red de datos 110 mediante el dispositivo de proxy 120. La inscripción del dispositivo de proxy 120 puede comprender además generar un certificado digital 410 y/o una lista de certificados y/o almacenar el certificado digital 410 y/o la lista de certificados en el dispositivo de proxy 120. La generación de una lista de certificados puede comprender recibir una lista de certificados del sistema de gestión 510. La lista puede comprender el o los certificados digitales 410 relacionados con el o los recursos 130 comprendidos y/o el o los dispositivos de usuario 140 acoplados al sistema de comunicación 100. El sistema de gestión 510 se puede configurar para la revocación de un certificado digital 410. La revocación del o de los certificados digitales 410 se puede basar en un incidente de red de datos. El sistema de gestión 510 se puede configurar para alterar una lista de certificados de un dispositivo de proxy 120, donde la alteración de la lista de certificados se puede basar en un incidente de red de datos.

El dispositivo de proxy 120 se puede configurar para almacenar uno o más de los certificados digitales 410. El dispositivo de proxy 120 se puede configurar además para transmitir uno o más certificados digitales 410 a un servidor de certificación digital 400, donde el servidor de certificación digital 400 se puede configurar para autenticar el o los certificados digitales

410. El dispositivo de proxy 120 se puede configurar para transmitir un certificado digital 410 con base en un intento de comunicación de un recurso 130 acoplado a la red de datos 110 mediante el dispositivo de proxy 120.

El o los dispositivos de proxy 120 y/o el o los recursos 130 pueden comprender un identificador 300, que puede comprender un receptor 310. El sistema de gestión 510 se puede configurar para realizar una identificación y/o una ubicación del o de los dispositivos de proxy 120 y/o el o los recursos 130 con base en el identificador 300. El sistema de gestión 510 se puede configurar para enviar una solicitud de ubicación al dispositivo de proxy 120 y/o el o los recursos 130. Adicionalmente, el o los dispositivos de proxy 120 y/o el o los recursos 130 se pueden configurar para transmitir una ubicación al sistema de comunicación 100 y/o el sistema de gestión 510. Por lo tanto, si se cambia la ubicación del dispositivo de proxy 120 y/o el recurso 130, geográficamente o con respecto a la red de datos 110, el sistema de comunicación 100 y/o el sistema de gestión 510 puede registrar el cambio. El sistema de gestión 510 se puede configurar además para realizar un análisis de la identificación y/o la ubicación del o de los dispositivos de proxy 120 y el o los recursos 130, un seguimiento de la identificación y/o la ubicación del o de los dispositivos de proxy 120 y el o los recursos 130 y/o un control de la identificación y/o la ubicación del o de los dispositivos de proxy 120 y el o los recursos 130.

Además, el sistema de gestión 510 se puede configurar para recibir la indicación de la ubicación del o de los dispositivos de proxy 120 y/o el o los recursos 130. El sistema de gestión 510 se puede configurar para rastrear la indicación de la ubicación del o de los dispositivos de proxy 120 y/o el o los recursos 130. Por lo tanto, si la indicación de la ubicación del o de los dispositivos de proxy 120 y/o el o los recursos 130 cambia, entonces el sistema de gestión 510 se puede configurar para rastrear este cambio. Un cambio de la indicación de la ubicación se puede comprender por uno o más incidentes de red de datos. El sistema de gestión 510 se puede configurar para controlar la comunicación con base en un cambio de indicación de la ubicación. Además, el sistema de gestión 510 se puede configurar para generar datos de identificación con base en las identificaciones del identificador 300. El sistema de gestión 510 se puede configurar para identificar un comportamiento del o de los dispositivos de proxy 120 y/o el o los recursos 130 con base en los datos de identificación generados. Por el término “comportamiento” se quiere decir conexiones, desconexiones, identidad de usuario y/o acoplamientos/conexiones de la red de datos 110, el o los dispositivos de proxy 120, el o los recursos 130 y/o el o los dispositivos de usuario 140. El sistema de gestión 510 se puede configurar para usar estos datos para rastrear y/o mapear comportamientos del o de los dispositivos de proxy 120 y/o el o los recursos 130 con el paso del tiempo.

La persona experta en la técnica se da cuenta de que la presente invención de ninguna manera se limita a las realizaciones preferidas descritas anteriormente. Por el contrario, son posibles muchas modificaciones y variaciones dentro del alcance de las reivindicaciones anexas. Por ejemplo, cualquier dispositivo de proxy 120 y/o recursos 130 puede comprender un identificador 300. Además, cada identificador 300 puede comprender un receptor 310. Cada dispositivo de proxy 120 puede comprender un primer puerto de comunicación 210 y/o un segundo puerto de comunicación 220. Además, el o los dispositivos de proxy 120 y/o el sistema de gestión 510 se pueden acoplar de manera comunicativa al servidor de certificación digital 400 mediante la red de datos 110. Adicionalmente, el sistema de gestión 510 puede comprender uno o más dispositivos de certificación 420. En otras palabras, el o los recursos 130, el o los dispositivos de proxy 120 y/o el o los dispositivos de usuario 140 se pueden acoplar a un dispositivo de certificado 420.

REIVINDICACIONES

1. Un sistema de comunicación (100) para recibir y transmitir señales de comunicación, que comprende

una red de datos (110),
al menos dos dispositivos de proxy (120) acoplados a la red de datos,

donde los al menos dos dispositivos de proxy se configuran para autenticación de certificado digital al transmitir un certificado digital (410) a un servidor de certificación digital (400) configurado para autenticar el certificado digital, y al menos dos recursos (130), donde cada dispositivo de proxy de los al menos dos dispositivos de proxy (120) se acopla a un respectivo recurso de los al menos dos recursos (130), donde los al menos dos recursos (130) se acoplan de manera comunicativa a la red de datos (110) mediante los al menos dos dispositivos de proxy (120), donde un único canal de comunicación con los al menos dos recursos (130) es a través del respectivo dispositivo de proxy, y donde los al menos dos dispositivos de proxy (120) se configuran para permitir o deshabilitar una comunicación entre la red de datos (110) y los al menos dos recursos (130) con base en la autenticación de certificado digital.

2. El sistema de comunicación de acuerdo con la reivindicación 1, donde los al menos dos dispositivos de proxy se configuran para almacenar al menos un certificado digital.

3. El sistema de comunicación de acuerdo con la reivindicación 1 o 2, donde los al menos dos dispositivos de proxy se configuran para generar al menos uno de al menos una clave pública y al menos una clave privada.

4. El sistema de comunicación de acuerdo con cualquiera de las reivindicaciones anteriores, donde los al menos dos dispositivos de proxy se configuran además para controlar la comunicación entre la red de datos y los al menos dos recursos con base en al menos uno de un dispositivo de certificado, una contraseña, una dirección IP, un puerto IP y una dirección MAC.

5. El sistema de comunicación de acuerdo con cualquiera de las reivindicaciones anteriores, donde los al menos dos dispositivos de proxy comprenden un primer puerto de comunicación (210) acoplado a los al menos dos recursos, y un segundo puerto de comunicación (220) acoplado a la red de datos.

6. El sistema de comunicación de acuerdo con cualquiera de las reivindicaciones anteriores, donde al menos uno de los al menos dos dispositivos de proxy y los al menos dos recursos comprenden un identificador (300) configurado para indicar al menos uno de una identificación y una ubicación de al menos uno de los al menos dos dispositivos de proxy y los al menos dos recursos.

7. El sistema de comunicación de acuerdo con la reivindicación 6, donde el identificador comprende un receptor (310) para recibir una ubicación de al menos uno de los al menos dos dispositivos de proxy y los al menos dos recursos.

8. El sistema de comunicación de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además un sistema de gestión (510) acoplado a los al menos dos dispositivos de proxy, donde el sistema de gestión se configura para comunicar datos de autenticación de certificado digital entre los al menos dos dispositivos de proxy y el sistema de gestión.

9. El sistema de comunicación de acuerdo con la reivindicación 3 y 8, donde el sistema de gestión se configura para almacenar al menos una de la al menos una clave pública y la al menos una clave privada.

10. El sistema de comunicación de acuerdo con la reivindicación 8, donde el sistema de gestión se configura para generar al menos una clave pública y al menos una clave privada, y además que se configura para generar al menos un certificado digital con base en al menos una de la al menos una clave pública y la al menos una clave privada.

11. El sistema de comunicación de acuerdo con la reivindicación 6 o 7, y 8, donde el sistema de gestión se configura para realizar al menos una de una identificación y una ubicación de al menos uno de los al menos dos dispositivos de proxy y los al menos dos recursos con base en el identificador.

12. El sistema de comunicación de acuerdo con la reivindicación 11, donde el sistema de gestión se configura además para realizar al menos uno de un análisis de al menos una de la identificación y la ubicación de al menos uno de los al menos dos dispositivos de proxy y los al menos dos recursos, un seguimiento de al menos una de la identificación y la ubicación de al menos uno de los al menos dos dispositivos de proxy y los al menos dos recursos, y un control de al menos una de la identificación y la ubicación de al menos uno de los al menos dos dispositivos de proxy y los al menos dos recursos.

13. El sistema de comunicación de acuerdo con cualquiera de las reivindicaciones 8-12, donde al menos uno del sistema de gestión y los al menos dos dispositivos de proxy se configuran para registrar la comunicación de datos entre la red de datos y los al menos dos dispositivos de proxy.

14. El sistema de comunicación de acuerdo con la reivindicación 13, donde la comunicación de datos registrados comprende al menos uno de una marca de tiempo, datos de los al menos dos recursos a la red de datos, datos de la red de datos a los al menos dos recursos, un emisor de comunicación de datos, un receptor de comunicación de datos, una cantidad de la comunicación de datos, un tipo de la comunicación de datos, varios tiempos de espera de comunicación de datos, varios intentos de comunicación de datos y datos de certificado.

15. El sistema de comunicación de acuerdo con la reivindicación 13 o 14, donde al menos uno del sistema de gestión y los al menos dos dispositivos de proxy se configuran además para controlar la comunicación entre la red de datos y los al menos dos dispositivos de proxy con base en la comunicación de datos registrados.

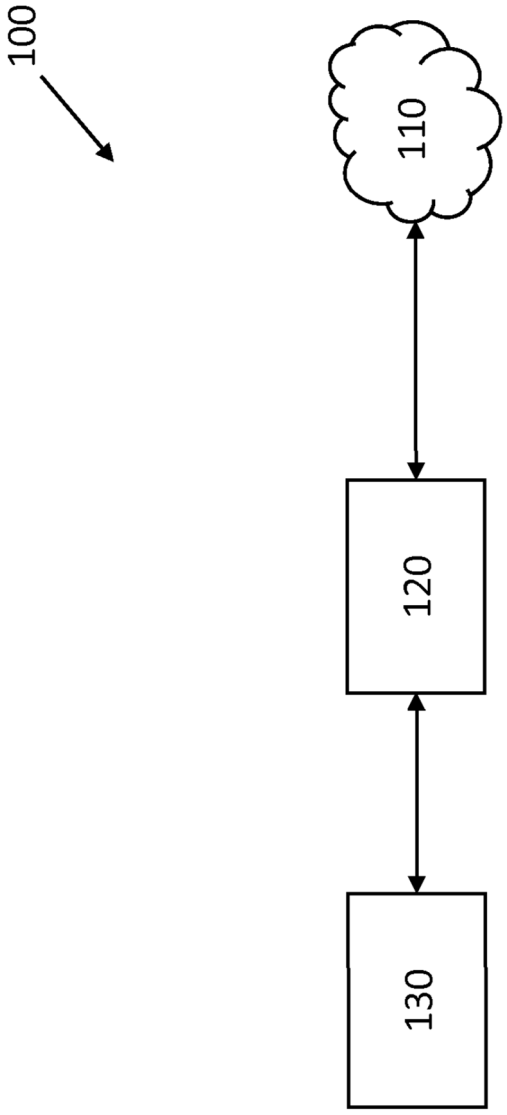

Fig. 1

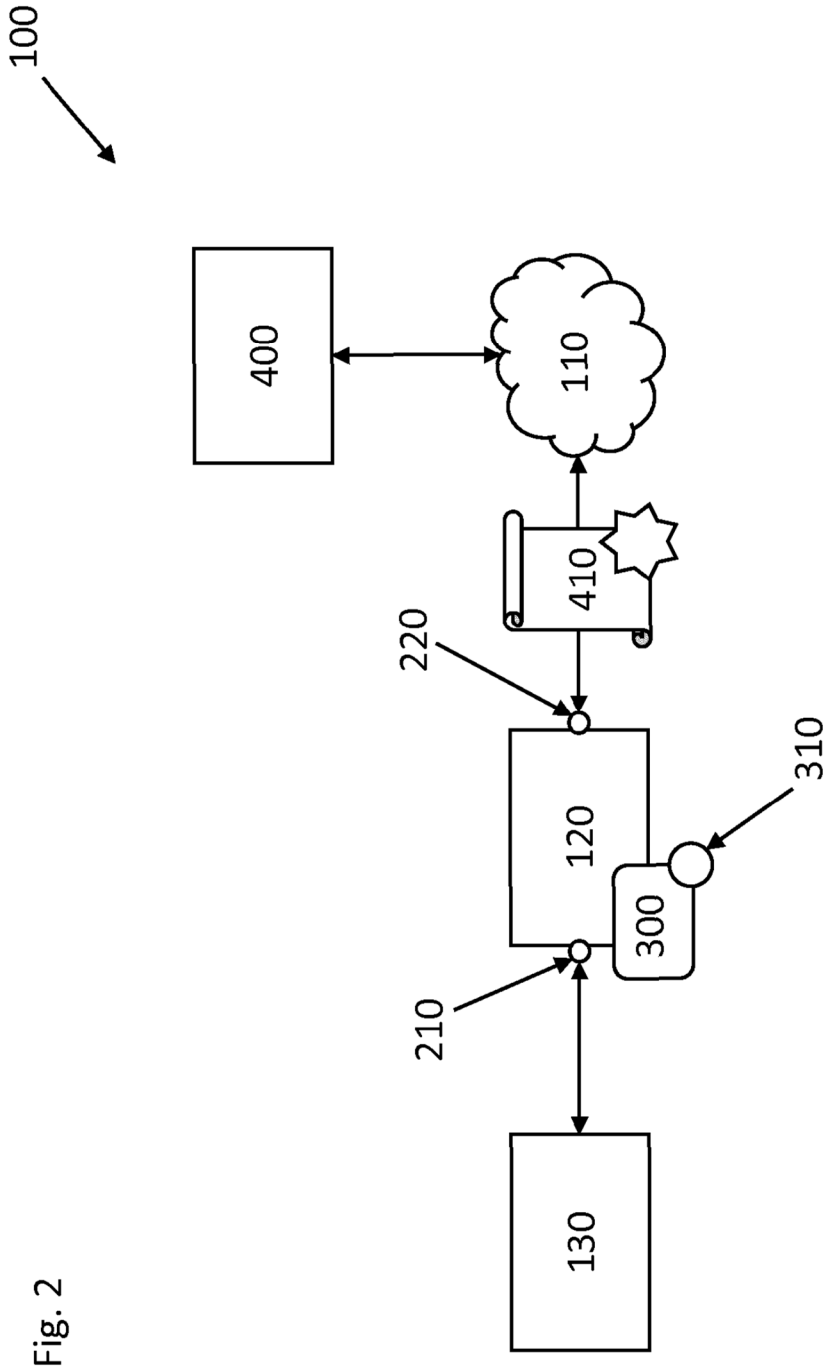

Fig. 2

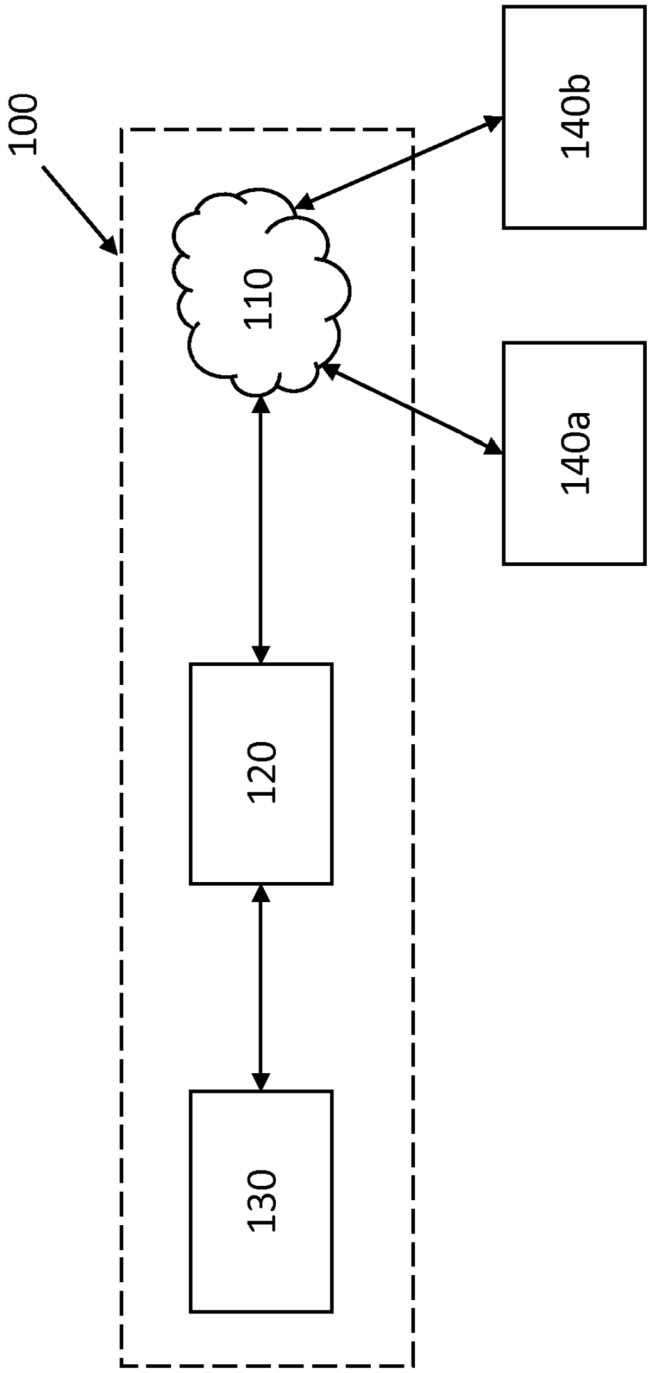

Fig. 3

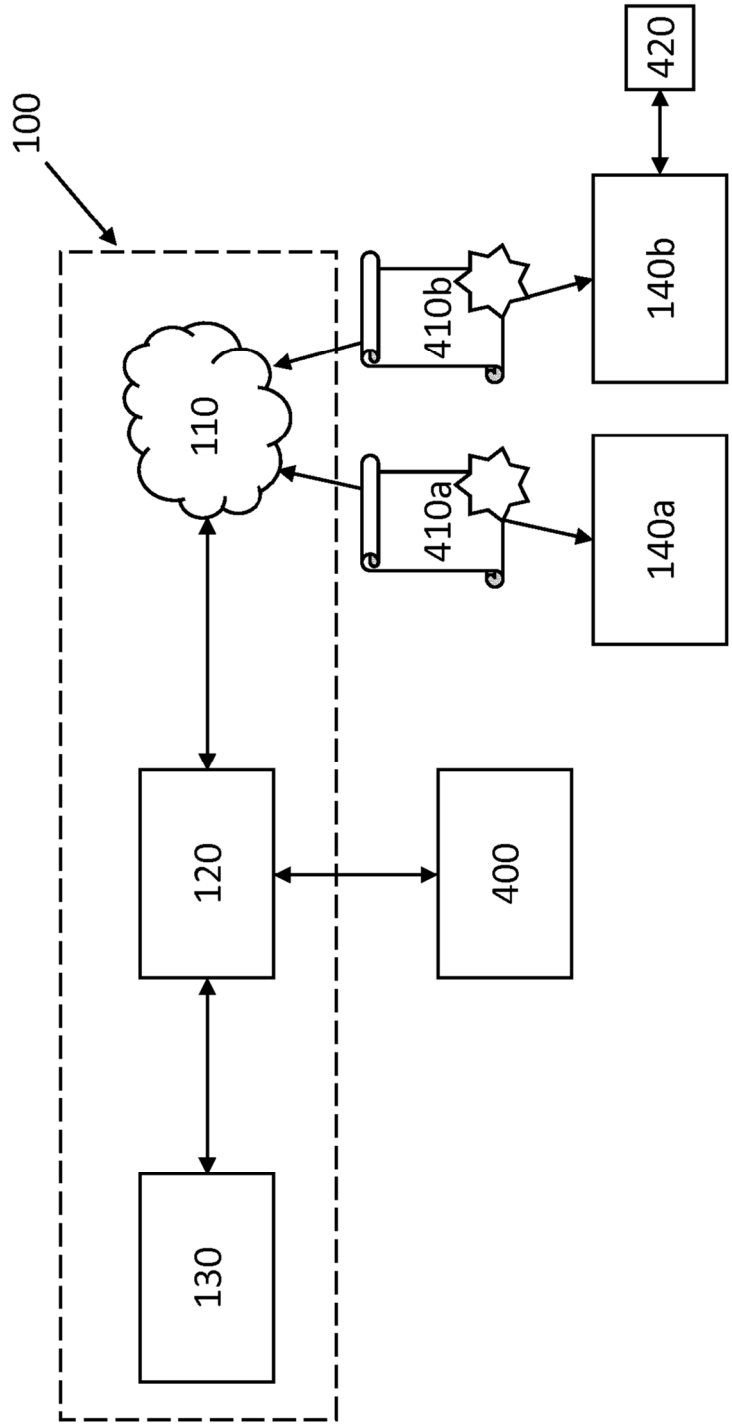

Fig. 4

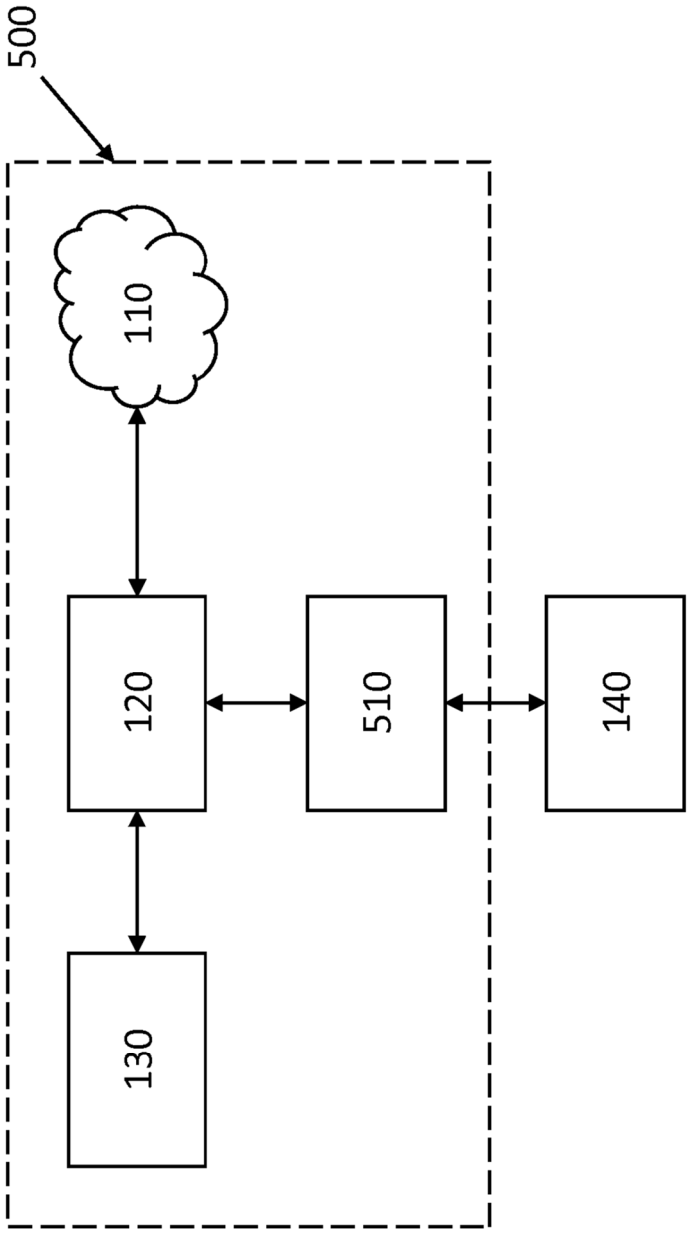

Fig. 5

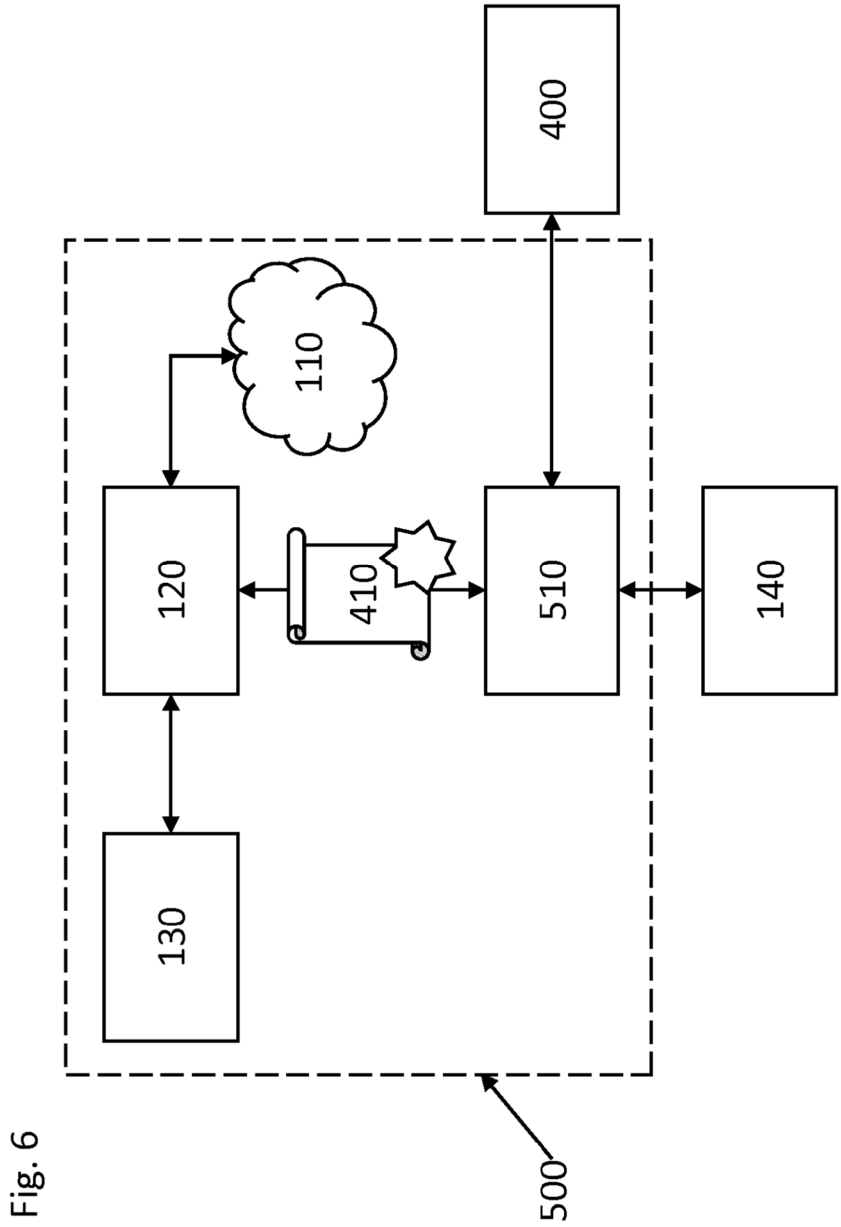

Fig. 6