(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 791 956**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.05.2016 PCT/EP2016/061073**

(87) Fecha y número de publicación internacional: **15.12.2016 WO16198241**

(96) Fecha de presentación y número de la solicitud europea: **18.05.2016 E 16723126 (5)**

(97) Fecha y número de publicación de la concesión europea: **22.04.2020 EP 3308516**

(54) Título: **Aparato y procedimiento de autorización para una emisión autorizada de un token de autenticación para un dispositivo**

(30) Prioridad:

11.06.2015 DE 102015210718

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.11.2020

(73) Titular/es:

SIEMENS AKTIENGESELLSCHAFT (100.0%)
Werner-von-Siemens-Straße 1
80333 München, DE

(72) Inventor/es:

BROCKHAUS, HENDRIK;
FRIES, STEFFEN;
MUNZERT, MICHAEL y
VON OHEIMB, DAVID

(74) Agente/Representante:

LOZANO GANDIA, José

DESCRIPCIÓN

Aparato y procedimiento de autorización para una emisión autorizada de un token de autenticación para un dispositivo

La invención se refiere a un aparato de autorización y a un procedimiento para la emisión autorizada de un token de autenticación para un dispositivo, que es, por ejemplo, parte de un sistema de automatización.

Los sistemas industriales actuales comprenden diversos tipos de dispositivos interconectados por una red de datos y transfiriendo datos entre ellos. Dichos sistemas de control industrial o SCADA (control de supervisión y adquisición de datos) se comunican cada vez más por medio de protocolos abiertos tales como IP (protocolo de Internet), TCP (protocolo de control de transmisión), UDP (protocolo de datagramas de usuario), HTTP (protocolo de transferencia de hipertexto) y CoAP (protocolo de aplicación restringido). En caso de que se deban usar protocolos de seguridad adicionales, estos protocolos de seguridad aplican típicamente criptografía, haciendo uso de tokens de autenticación tales como, por ejemplo, certificados con claves públicas y privadas respectivas, o contraseñas, etc.

Para obtener dicho token de autenticación, por ejemplo, un certificado, un dispositivo tiene que demostrar su identidad. Esto puede lograrse mediante el uso de un parámetro de autenticación establecido previamente, típicamente una contraseña de un solo uso o una clave privada, instalada, por ejemplo, durante el proceso de producción o durante el montaje, o durante el establecimiento anterior de un token de autenticación para el dispositivo o un componente del mismo.

Un token de autenticación contiene o hace referencia al parámetro de autenticación, así como a la información de identidad sobre el dispositivo y/o su componente, por ejemplo, el número de serie del dispositivo y/o el nombre del componente, y posiblemente información adicional como su período de validez y firma digital por parte de la entidad emisora.

El hardware, el software, las personas, las políticas y los procedimientos se especifican para una denominada infraestructura de clave pública (PKI) para crear, administrar, distribuir, usar, almacenar y revocar certificados digitales y administrar el cifrado de clave pública. Para asignar un token de autenticación a un dispositivo, por ejemplo, después de la instalación en un sistema de control industrial en una infraestructura de clave pública, el dispositivo envía una petición de token de autenticación, que es típicamente una petición de firma de certificado, un mensaje a una autoridad de registro fiable por la autoridad de certificación o directamente a la autoridad de certificación. La autoridad de registro verifica normalmente la identidad del dispositivo, por ejemplo, manualmente por un administrador o verificando el parámetro de autenticación, que puede ser una contraseña de un solo uso enviada por el dispositivo o una firma relacionada con un certificado preexistente emitido y firmado por una autoridad de certificación fiable. El certificado preexistente incluye información sobre el dispositivo en sí y/o uno de sus componentes, por ejemplo, una identificación del dispositivo, como un número de serie y/o una ID del componente, un período de validez del certificado y una clave pública que puede usarse para verificar la firma de la petición. Una vez que la autenticación del dispositivo se realiza correctamente, la autoridad de registro aceptará este mensaje de petición y lo pasará a una autoridad de certificación, que emite un token de autenticación.

El documento EP 2 120 392 divulga un procedimiento para transmitir una petición de emisión de certificado desde un dispositivo terminal a un aparato de emisión de certificado a través de una red.

Para mejorar la seguridad de las aplicaciones de sistemas industriales, los tokens de autenticación de dispositivos dedicados o uno de sus componentes solo se proporcionarán en un determinado entorno, por ejemplo, en secciones dedicadas de un sistema de control. La provisión de tokens de autenticación del dispositivo también estará restringida en el tiempo, por ejemplo, la comunicación a las autoridades de registro y certificación solo será posible durante un período de tiempo determinado. Esto también debería ayudar a evitar que un dispositivo o sus componentes de software sean utilizables fuera del sistema de control previsto, por ejemplo, para evitar el mal uso del dispositivo, por ejemplo, después del robo.

Por lo tanto, el objetivo de la presente solicitud es proporcionar un procedimiento y medios para controlar y limitar la emisión de token(s) de autenticación del dispositivo a localizaciones dedicadas, dominios organizacionales, períodos de tiempo y aplicaciones.

Este objetivo se logra mediante las medidas y los medios de las reivindicaciones independientes. Las reivindicaciones subordinadas proporcionan modos de realización ventajosos adicionales de la solución.

La presente invención se refiere a un procedimiento y a un aparato de autorización para una emisión autorizada de un token de autenticación para un dispositivo basándose en información de contexto.

De acuerdo con un modo de realización de la invención, un procedimiento para la emisión autorizada de un token de autenticación para un dispositivo comprende los pasos de

- pedir un token de autenticación para el dispositivo enviando un mensaje de petición y al menos un parámetro de autenticación a un aparato de autorización,

- verificar la autenticidad del mensaje de petición usando el parámetro de autenticación,

- verificar la autorización para la petición comparando la información sobre el dispositivo obtenida con el mensaje de petición en el aparato de autorización con la información de contexto para el dispositivo almacenado en una base de datos, y

- sobre el éxito de la verificación de la autenticidad y de la autorización, autorizar la emisión del token de autenticación pedido.

La comparación de la información sobre el dispositivo con la información de contexto para el dispositivo proporciona la posibilidad de verificar otras condiciones que deben cumplirse antes de aceptar el mensaje de petición en el aparato de autorización. Al verificar el al menos un parámetro de autenticación proporcionado con el mensaje de petición, se asegura que el mensaje realmente lo envía el dispositivo que pretende ser. Solo si ambas verificaciones proporcionan un resultado positivo, el token de autenticación pedido se emitirá por el propio aparato de autorización o, por ejemplo, por una autoridad de certificación que se informa por el aparato de autorización para emitir el token de autenticación pedido. Con estas medidas, por ejemplo, una inscripción automática de dispositivos puede restringirse a áreas o dominios específicos del sistema o a intervalos de tiempo y circunstancias específicos, como los procedimientos de servicio. Por ejemplo, los dispositivos, tales como los terminales de servicio, solo pueden acceder al sistema de automatización a intervalos de tiempo predefinidos. Esto implica también que los piratas informáticos que ataquen un proceso de inscripción automática pueden repelerse con alta probabilidad, ya que tendrían que cumplir con todas las condiciones implicadas en la información de contexto. El dispositivo puede proporcionar al menos un parámetro de autenticación junto con el mensaje de petición o puede proporcionarse por un tercero, por ejemplo, una persona de servicio que envíe una contraseña como parámetro de autenticación para probar la autenticación del dispositivo.

En un modo de realización del procedimiento, la información sobre el dispositivo (20) obtenida con el mensaje de petición (CSReq) y usada para verificar la autorización del mensaje de petición es al menos una de la información adicional incluida en el mensaje de petición, de la información generada en el aparato de autorización durante la recepción del mensaje de petición o de la información sobre el dispositivo enviado por otra parte al aparato de autorización.

La información adicional que se recibe como parte del mensaje de petición puede ser información que indique el dominio de un sistema de automatización en el que se debe instalar el dispositivo. La información generada en el aparato de autorización durante la recepción del mensaje de petición puede ser el momento en que el mensaje de petición se recibe en el aparato de autorización. La información sobre el dispositivo enviada por otra parte puede ser información enviada por un personal de servicio o un servidor de instalación. Por lo tanto, pueden establecerse diversas condiciones para emitir un token de autenticación.

De acuerdo con otro modo de realización del procedimiento, se genera al menos un parámetro de autenticación dependiendo de una clave privada relacionada con un certificado digital preinstalado específico del dispositivo.

Los certificados digitales específicos del dispositivo se emiten normalmente durante la instalación o la fabricación de un dispositivo y, por lo tanto, ya están disponibles en un dispositivo. Por lo tanto, no es necesario tomar medidas adicionales para proporcionar un parámetro de autenticación específico del dispositivo. Un certificado digital específico del dispositivo proporciona habitualmente un tema para el que se emite, aquí, por ejemplo, un número de serie del dispositivo, una clave pública y una firma digital. Se puede incluir información adicional típica como se especifica en la norma X.509. El parámetro de autenticación puede ser, por ejemplo, una firma digital generada aplicando la clave privada. Una clave pública relacionada exclusivamente con la clave privada se incluye en un certificado específico del dispositivo preexistente, y se conoce en el aparato de autorización. La autenticación se verifica positivamente cuando el aparato verifica la firma digital del mensaje de petición aplicando la clave pública del dispositivo.

En un modo de realización adicional del procedimiento, el token de autenticación es un certificado digital.

Esto significa que el dispositivo recibe un certificado digital después de la autorización de la emisión de un token de autenticación. El certificado digital se usa normalmente durante la configuración de una sesión con un compañero de comunicación para identificar y autenticar el dispositivo al compañero de comunicación. Por lo tanto, el certificado digital permite la comunicación del dispositivo con socios de comunicación arbitrarios.

En un modo de realización adicional del procedimiento, la información de contexto para el dispositivo almacenado en una base de datos es al menos uno de información de identificación, de información de organización, de información de localización, de información relacionada con el tiempo, de información de aplicación y de información de estado en el dispositivo y/o sus componentes.

Esto permite una variedad de condiciones que pueden verificarse. Por ejemplo, la información de identificación puede ser una dirección IP o un rango de direcciones IP. Aquí, la dirección IP del paquete de datos en que se transmite el mensaje de petición al identificar el dispositivo o su componente en una capa inferior de la pila de protocolos de transmisión puede compararse con una dirección IP predefinida o un rango de direcciones IP almacenado en la base de datos. La información de la organización puede ser, por ejemplo, una unidad de producción o un cliente al que está asignado el dispositivo. La información de localización puede ser la localización geográfica del dispositivo al enviar el mensaje de petición. Información relacionada con el tiempo que es, por ejemplo, un intervalo de tiempo en el que se permite la emisión de un certificado. La información de la aplicación podría distinguir la provisión de tokens para diferentes tareas, tales como aplicaciones de servicio, o para aplicaciones de mantenimiento. La información de estado puede identificar que un dispositivo o su componente está, por ejemplo, "en funcionamiento", "en mantenimiento", si, por ejemplo, se emite un token de autenticación respectivo. La información de estado puede expresar que un dispositivo o su componente está, por ejemplo, "en preparación", "en uso", "fuera de servicio", "reemplazado" o "robado".

La información sobre el dispositivo obtenida con el mensaje de petición y usada para verificar la autorización del mensaje de petición en el aparato de autorización puede ser el mismo tipo de información que la información de contexto descrita anteriormente.

En un modo de realización adicional del procedimiento, al menos parte de la información de contexto para el dispositivo almacenado en una base de datos predefinida se actualiza cuando se emite el token de autenticación.

Esto permite el seguimiento y el monitoreo del estado de un dispositivo o su componente.

En un modo de realización adicional del procedimiento, al menos parte de la información de contexto para los dispositivos almacenados en la base de datos predefinida puede actualizarse de manera segura por un tercero.

Esto permite cambiar la información de contexto, por ejemplo, por un personal de mantenimiento, por un controlador de supervisión u otros terceros fiables. Un tercero puede ser personal humano o un dispositivo de control. El acceso se proporciona de forma segura, por ejemplo, mediante mecanismos criptográficos usados para la autenticación del tercero y para las verificaciones de integridad de los datos transmitidos.

De acuerdo con un segundo modo de realización de la invención, se proporciona un aparato de autorización para una emisión autorizada de un token de autenticación para un dispositivo. El aparato comprende

- una unidad de almacenamiento configurada para proporcionar una base de datos que incluya información de contexto para el dispositivo,

- una unidad de interfaz configurada para recibir un mensaje de petición y al menos un parámetro de autenticación del dispositivo,

- una primera unidad de verificación configurada para verificar la autenticidad del mensaje de petición usando el parámetro de autenticación,

- una segunda unidad de verificación configurada para verificar la autorización de la petición comparando la información sobre el dispositivo obtenida con el mensaje de petición con la información de contexto para el dispositivo almacenado en una base de datos, y

- una unidad de autorización configurada para autorizar la emisión del token de autenticación pedido, si la primera y la segunda unidad de verificación indicaron un resultado positivo.

El aparato de autorización verifica no solo el dispositivo como tal, sino también otras condiciones previas establecidas por la información de contexto en una base de datos predefinida. Por lo tanto, el aparato de autorización acepta y reenvía un mensaje de petición solo si se cumplen las condiciones previas implicadas en el contenido de la base de datos predefinida. Esto permite evitar el uso o la aplicación de un dispositivo si no se cumplen las condiciones predefinidas.

En un modo de realización adicional del aparato de la invención, la unidad de almacenamiento está configurada para actualizarse cuando se emita el token de autenticación.

Esto permite monitorear y hacer un seguimiento, por ejemplo, del estado del dispositivo, por ejemplo, en diferentes aplicaciones. La base de datos predefinida indica, por ejemplo, cuándo se emitió o autorizó un token de autenticación y/o para qué aplicación se emitió el token.

En un modo de realización adicional, el aparato de la invención comprende una interfaz adicional configurada para proporcionar acceso seguro a la unidad de almacenamiento para que un tercero actualice la base de datos predefinida.

La interfaz adicional puede configurarse para proporcionar protocolos de seguridad como el protocolo de seguridad de capa de transporte (TLS) que proporciona verificaciones de autorización e integridad para los datos proporcionados a través de esta interfaz.

En un modo de realización adicional, el aparato de la invención comprende una unidad emisora configurada para emitir el token de autenticación pedido para el dispositivo.

En este caso, el aparato de autorización no solo autoriza la emisión del token de autenticación sino que también emite un token de autenticación. Esto cumple con una autoridad combinada de registro y certificación conocida por una infraestructura de clave pública PKI.

En un modo de realización adicional de la invención es un programa informático con medios de código programable, que realiza todos los pasos del procedimiento descritos anteriormente, cuando el programa se realiza en un ordenador programable y/o un procesador de señales digitales.

Un modo de realización adicional de la invención proporciona un medio de almacenamiento digital con señales de control legibles electrónicamente, que interactúan con un ordenador programable y/o un procesador de señales digitales de manera que pueden realizarse todos los pasos del procedimiento descrito.

Las ventajas de la invención descrita anteriormente, junto con otras ventajas, pueden entenderse mejor haciendo referencia a la siguiente descripción tomada junto con los dibujos adjuntos. Los dibujos no son necesariamente a escala, haciendo hincapié en su lugar en colocarse en general ilustrando los principios de la invención.

La Figura 1 es un diagrama de flujo de un modo de realización del procedimiento inventivo;

La Figura 2 muestra un flujo de mensajes de un modo de realización del procedimiento inventivo entre un dispositivo y un aparato de autorización; y

La Figura 3 muestra un diagrama de bloques de un modo de realización de un aparato de autorización construido de acuerdo con la invención.

En los dibujos, caracteres de referencia similares se refieren en general a las mismas partes en las diferentes vistas y figuras.

La Figura 1 es un diagrama de flujo de un modo de realización del procedimiento inventivo. El procedimiento puede aplicarse por un dispositivo que es, por ejemplo, un dispositivo de campo de un sistema de automatización industrial o un controlador de un sistema de generación de energía, por ejemplo, con funcionalidad SCADA. Los dispositivos se comunican, por ejemplo, por medio de protocolos abiertos tales como IP, TCP, UDP, http y CoAP. Para asegurar esta comunicación, se usan protocolos de seguridad adicionales como, por ejemplo, seguridad de capa de transporte (TLS) o protocolos de seguridad específicos del sistema de automatización adicionales que aplican típicamente funciones criptográficas asimétricas usando clave privada y pública.

En el estado inicial 10, el dispositivo obtiene o genera un parámetro de autenticación inicial específico del dispositivo, por ejemplo, una contraseña de un solo uso o una clave privada relativa a una clave pública del dispositivo, que se implementó durante la fabricación, el montaje o la configuración del dispositivo. Ya está disponible cuando el dispositivo se implementa en un sistema, donde los diversos dispositivos se comunican entre sí por medio de una red de comunicación.

En el paso 11, que puede repetirse cualquier número de veces, el dispositivo puede derivar de su(s) parámetro(s) de autenticación ya existente(s) cualquier número de parámetros de autenticación adicionales, que pueden ser específicos para el dispositivo o para cualquier componente del mismo. Para cualquiera de estos parámetros de autenticación, el dispositivo puede obtener, por cualquier medio seguro, un token de autenticación relacionado, por ejemplo, un certificado digital. Como se mencionó anteriormente, este token incluye información de identidad, por ejemplo, el número de serie del dispositivo y/o una ID de componente, el parámetro de autenticación o una referencia al mismo, y opcionalmente información adicional como el período de validez y la firma digital de la entidad emisora.

En el paso 12, el dispositivo pide un token de autenticación inicial, actualizado o adicional enviando un mensaje de petición usando cualquier parámetro(s) de autenticación válido(s) e incluyendo posiblemente el(los) token(s) de autenticación relacionado(s) y/u otra información sobre el dispositivo a un aparato de autorización.

En el aparato de autorización en un primer paso de verificación 13, se verifica la identidad del dispositivo y la autenticidad de su petición verificando el(los) parámetro(s) de autenticación proporcionado(s) y posiblemente el(los) token(s) de autenticación relacionado(s).

En un segundo paso de verificación 14, la información sobre el dispositivo se compara con la información de

contexto para el dispositivo almacenado en una base de datos predefinida. La base de datos predefinida es accesible por el aparato de autorización. La base de datos predefinida puede incluirse en el aparato de autorización o puede localizarse en un servidor externo o unidad de almacenamiento. En caso de éxito de ambos pasos de verificación, se acepta el mensaje de petición, lo que significa que se autoriza la emisión del token de autenticación pedido; véase el paso 15. Si el mensaje de petición se autoriza en el paso 15, se emite un token de autenticación, por ejemplo, por una Autoridad de Certificación y se envía de vuelta al dispositivo. El procedimiento termina en el estado 16.

En la Figura 2, se muestra un flujo de mensajes acorde entre un dispositivo 20 y un aparato de autorización 30 para el caso típico de pedir un nuevo token de autenticación, es decir, un nuevo certificado digital. El dispositivo 20 contiene un parámetro de autenticación, por ejemplo, en forma de una clave privada relacionada con un certificado de componente 21 que incluye el identificador del dispositivo y/o su componente, tal como un número de serie IDxn, así como una clave pública específica del dispositivo y típicamente una firma digital de una autoridad emisora para este certificado de componente. El aparato de autorización 30 comprende una base de datos predefinida 38 que incluye información de contexto para el dispositivo 20.

El dispositivo 20 pide emitir un nuevo token de autenticación, aquí un certificado $Cert_{op}$, para que el dispositivo se use luego en comunicación con los socios de comunicación en el sistema. Por lo tanto, el dispositivo envía un mensaje de petición CSReq que incluye la clave pública Kpub para la cual se emitirá el certificado e información adicional como un identificador IDxn, por ejemplo, el número de serie del dispositivo, que puede ser parte del certificado de componente. Información adicional como la dirección IP IPxn del dispositivo o componente puede ser parte del mensaje de petición CSReq. Opcionalmente, puede proporcionarse información adicional como información sobre el dominio en el cual está instalado el dispositivo Wx con un mensaje de petición CSReq. El mensaje de petición comprende además una firma digital generada usando cualquier parámetro de autenticación establecido antes, por ejemplo, la clave privada relacionada con el certificado de dispositivo, y opcionalmente también el certificado de dispositivo en sí.

Al recibir el mensaje de petición CSReq en el aparato de autorización 30, la firma digital proporcionada verifica la identidad del dispositivo y la autenticidad e integridad del mensaje de petición; véase el paso 13 en la Figura 1. Como segundo paso 14, ahora también se verifica la autorización para pedir el token de autenticación comparando información sobre el dispositivo y posiblemente más información, como el tiempo de recepción, con información de contexto para el dispositivo almacenado en la base de datos predefinida 38. La base de datos predefinida 38 debe proporcionarse de antemano, por ejemplo, mediante la puesta en marcha de información para un sistema de automatización o dominio del sistema. En la fase de preparación, un agente de montaje envía una lista con los identificadores de dispositivo IDxn que se instalarán, por ejemplo, en un parque eólico X a una administración central. En la administración central se genera la base de datos predefinida 38. La base de datos predefinida 38 incluye ahora todos los identificadores de dispositivo IDxn, así como información adicional, por ejemplo, sobre un rango de direcciones IP IPx1 a IPxn asignadas a los dispositivos que se instalarán en windpark X. Más información asignada al ID de dispositivo IDnx y almacenado en la base de datos predefinida 38 puede ser un período de tiempo en el cual los dispositivos pueden pedir un token o información sobre los componentes de los dispositivos autorizados para pedir tokens de autenticación. Información adicional sobre los dispositivos es, por ejemplo, información de estado con respecto a los dispositivos o asignaciones de token de autenticidad para el dispositivo.

Sólo si también la segunda verificación 14 tiene éxito, el aparato de autorización 30 autoriza a la CSReq el mensaje de petición para aceptarse y reenviarse a un organismo emisor para emitir el certificado $Cert_{op}$ pedido. En la Figura 2 se supone que el aparato de autorización 30 mostrado incluye también una autoridad de certificación. También es posible que el aparato de autorización 30 transfiera el mensaje de petición a un componente separado que emita el certificado pedido.

Como resultado, se envía un mensaje de respuesta de certificado CSRes al dispositivo 20 que incluye el token de autenticación pedido, en este caso el certificado. Este token de autenticación ahora se usa y almacena como certificado 22 en el dispositivo 20.

El aparato de autorización 30 notifica normalmente la autorización del mensaje de petición CSReq o la emisión del token actualizando la base de datos predefinida, por ejemplo, cambiando la información de estado. Esto da como resultado una base de datos 39 actualizada. La base de datos 39 actualizada puede incluir además otros parámetros modificados. En esta base de datos 39 modificada, por ejemplo, el estado del dispositivo ahora cambia de "sin token" a "token emitido". También puede incluirse información más dedicada, por ejemplo, la dirección IP asignada al dispositivo, que debería ser una de las direcciones IP desde el rango de direcciones IP predefinido para los dispositivos.

También puede incluirse en la base de datos información sobre aplicaciones o casos de uso, como "mantenimiento" o "funcionamiento normal". Por ejemplo, un caso de uso puede establecerse en "en mantenimiento" o el estado puede "desactivarse" cuando el dispositivo se pone fuera de servicio.

La Figura 3 muestra un aparato de autorización 30 conectado por cualquier tipo de red de comunicación alámbrica

o inalámbrica 42 con el dispositivo 20. El aparato de autorización 30 comprende una unidad de interfaz 31 que proporciona una interfaz al dispositivo 20. El aparato de autorización 30 comprende además unidades de almacenamiento 32 configuradas para proporcionar la base de datos 38, 39. El aparato de autorización 30 comprende además una primera unidad de verificación 31 que está configurada para verificar que el dispositivo y su mensaje de petición son auténticos. Una segunda unidad de verificación 34 está configurada para verificar su autorización comparando la información sobre el dispositivo y posiblemente más información con la información de contexto para el dispositivo almacenado en la base de datos 38, 39.

El aparato de autorización 30 también comprende una unidad de autorización 35 configurada para autorizar la emisión del token de autenticación pedido, si tanto la primera como la segunda unidad de verificación indican un resultado positivo. La autorización puede realizarse transfiriendo el mensaje de petición por medio de una conexión externa 41 a una entidad externa que emita el token y enviándolo al dispositivo 20. El aparato de autorización 30 también puede contener una unidad emisora 37 que emita el token de autenticación pedido. Aquí el token de autenticación se transmite desde el aparato de autorización 30 al dispositivo 20.

El aparato de autorización 30 también puede comprender una interfaz 36 adicional configurada para proporcionar acceso seguro a la unidad de almacenamiento 32 para terceros fiables. Por medio de esta interfaz 36, un tercero, como el personal operativo o los controladores de monitoreo o supervisión, pueden acceder a la unidad de almacenamiento 32 para proporcionar una base de datos predefinida o para modificar la base de datos o eliminarla. La interfaz puede soportar algoritmos criptográficos para realizar la autenticación del tercero que accede y proporcionar medidas para garantizar la integridad de los datos transferidos. También puede accederse a y cambiar la unidad de almacenamiento 32 y especialmente la base de datos 32 después de que se autorice un mensaje de petición y se actualice la base de datos 38 de acuerdo con el resultado de la verificación, véase la base de datos 39 en la Figura 2.

La descripción anterior de los diversos modos de realización de la invención se ha presentado con fines ilustrativos y descriptivos. No pretende ser exhaustiva ni limitar la invención a las formas precisas divulgadas. Muchas modificaciones y variaciones son posibles en vista de las enseñanzas anteriores. Por tanto, se pretende que el alcance de la invención no se limite con esta descripción detallada, sino que se determine a partir de las reivindicaciones adjuntas a la misma.

REIVINDICACIONES

1. Procedimiento para la emisión autorizada de un token de autenticación para un dispositivo (20), que comprende

- pedir (12) el token de autenticación para el dispositivo (20) enviando un mensaje de petición (CSReq) y al menos un parámetro de autenticación a un aparato de autorización (30), en el que el al menos un parámetro de autenticación se genera dependiendo de una clave privada relacionada con un certificado digital preinstalado del dispositivo (20),

- verificar (13) la autenticidad del mensaje de petición usando el parámetro de autenticación,

- verificar (14) la autorización del mensaje de petición comparando la información sobre el dispositivo (20) obtenida con el mensaje de petición en el aparato de autorización con la información de contexto para el dispositivo (20) almacenada en una base de datos (38, 39), en la que la información de contexto para el dispositivo (20) es al menos una de la información de identificación, de la información de organización, de la información de aplicación o de la información de estado del dispositivo, y

- en caso de éxito de la verificación de la autenticidad y la autorización (13, 14) del mensaje de petición, autorizar (15) la emisión del token de autenticación pedido, en el que el token de autenticación pedido es un nuevo certificado digital.

2. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que al menos parte de la información de contexto para el dispositivo (20) almacenado en la base de datos se actualiza cuando se emite el token de autenticación.

3. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que la información de contexto para el dispositivo (20) almacenada en la base de datos (38, 39) puede actualizarse de forma segura por un tercero.

4. Procedimiento de acuerdo con una de las reivindicaciones anteriores, en el que la información sobre el dispositivo (20) obtenida con el mensaje de petición (CSReq) y usada para verificar la autorización del mensaje de petición es al menos una de la información adicional incluida en el mensaje de petición, de la información generada en el aparato de autorización durante la recepción del mensaje de petición o de la información sobre el dispositivo enviada por otra parte al aparato de autorización.

5. Aparato de autorización (30) para una emisión autorizada de un token de autenticación (Certop) para un dispositivo, que comprende

- una unidad de almacenamiento (32) configurada para proporcionar una base de datos (38, 39) que incluye información de contexto para el dispositivo (20),

- una unidad de interfaz (31) configurada para recibir un mensaje de petición para el token de autenticación y al menos un parámetro de autenticación del dispositivo, en el que el al menos un parámetro de autenticación se genera dependiendo de una clave privada relacionada con un certificado digital preinstalado del dispositivo (20),

- una primera unidad de verificación (33) configurada para verificar la autenticidad del mensaje de petición usando el parámetro de autenticación,

- una segunda unidad de verificación (34) configurada para verificar la autorización del mensaje de petición comparando la información sobre el dispositivo (20) obtenida con el mensaje de petición con la información de contexto para el dispositivo (20) almacenada en una base de datos (38, 39), en la que la información de contexto para el dispositivo (20) es al menos una de la información de identificación, de la información de organización, de la información de localización, de la información relacionada con el tiempo, de la información de aplicación o de la información de estado del dispositivo, y

- una unidad de autorización (35) configurada para autorizar la emisión del token de autenticación pedido, si la primera unidad de verificación (33) indicó una verificación exitosa de la autenticidad del mensaje de petición y la segunda unidad de verificación (34) indicó una verificación exitosa de la autorización del mensaje de petición, en el que el token de autenticación pedido es un nuevo certificado digital.

6. Aparato de acuerdo con la reivindicación 5, en el que la base de datos contenida en la unidad de almacenamiento (32) está configurada para actualizarse cuando se emita el token de autenticación.

7. Aparato de acuerdo con la reivindicación 5 o 6, que comprende una unidad de interfaz adicional (36) configurada para proporcionar acceso seguro a la unidad de almacenamiento (32) para que un tercero actualice la base de datos (38, 39).

8. Aparato de acuerdo con una de las reivindicaciones 5 a 7, que comprende una unidad emisora (37) configurada para emitir el token de autenticación pedido para el dispositivo (20).

9. Programa informático con medios de código de programa, que realiza todos los pasos del procedimiento de cualquiera de las reivindicaciones 1 a 4, cuando el programa se realiza en un ordenador programable y/o en un procesador de señales digitales.

10. Medio de almacenamiento digital con señales de control legibles electrónicamente, que interactúan con un ordenador programable y/o un procesador de señales digitales de manera que pueden realizarse todos los pasos del procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 4.

FIG 1

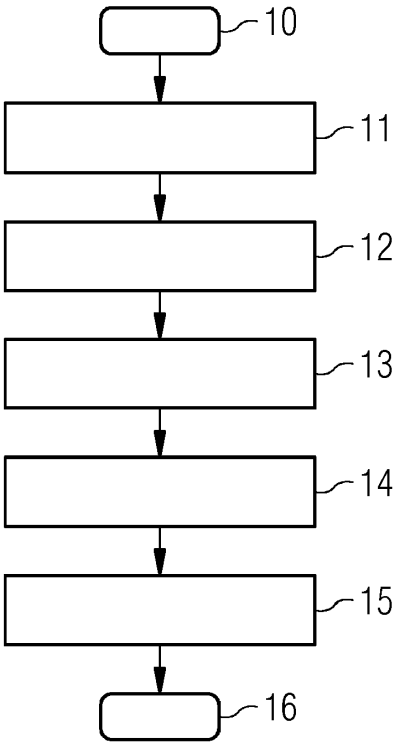


FIG 2

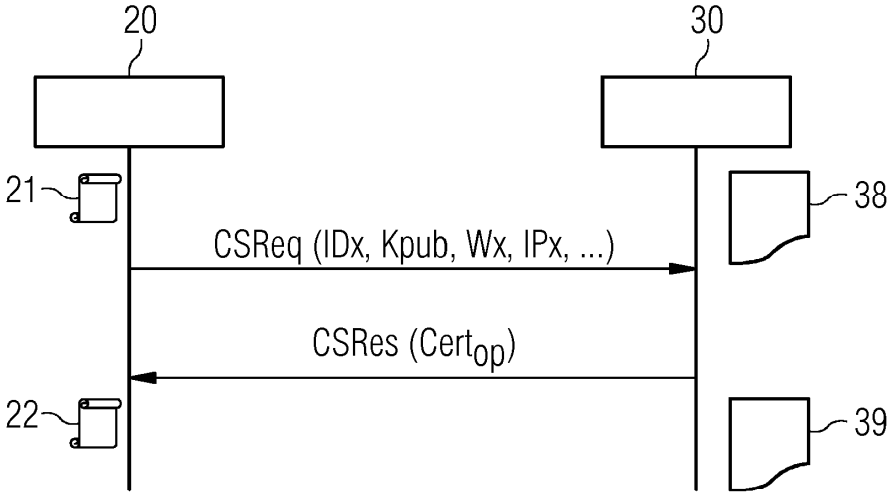
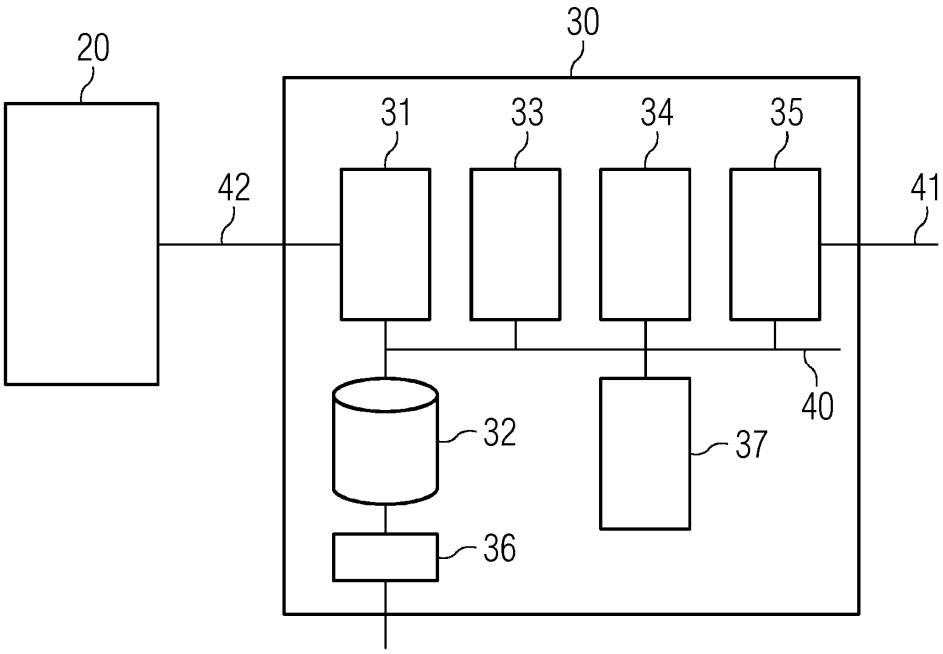

20
30
21
38
CSReq (IDx, Kpub, Wx, IPx, ...)
CSRes (Cert$_{op}$)
22
39

FIG 3


20
30
31
33
34
35
42
41
40
32
37
36