(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 015 933**

(51) Int. Cl.:

H04L 9/32 (2006.01)
G06F 21/64 (2013.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.05.2019 PCT/EP2019/062899**

(87) Fecha y número de publicación internacional: **28.11.2019 WO19224131**

(96) Fecha de presentación y número de la solicitud europea: **20.05.2019 E 19729618 (9)**

(97) Fecha y número de publicación de la concesión europea: **25.12.2024 EP 3794769**

(54) Título: **Modificación del contenido de un almacenamiento de certificados raíz**

(30) Prioridad:

24.05.2018 DE 102018208201

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.05.2025

(73) Titular/es:

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

(72) Inventor/es:

BOTH, THOMAS y
LÖFFLER, PHILIPP

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Modificación del contenido de un almacenamiento de certificados raíz

La invención se refiere a un procedimiento para operar un aparato técnico que tiene un almacenamiento de certificados en forma de un componente en tierra o a bordo de un sistema técnico ferroviario. Un procedimiento de este tipo se conoce por el documento de publicación alemana DE 10 2016 204 630 A1.

El documento US 6,816,900 B1 revela un procedimiento para actualizar un almacenamiento de certificados raíz con el fin de verificar la identidad del proveedor del sitio web cuando se comunica con sitios web de terceros.

El documento US 9,621,356 B2 divulga un procedimiento para revocar certificados almacenados. El procedimiento utiliza dos firmas para revocar la revocación de un certificado que se autentica a sí mismo y no puede ser autenticado externamente desde otra fuente.

La invención se basa en el objetivo de especificar un procedimiento para operar un componente en tierra o a bordo de un sistema ferroviario que sea particularmente a prueba de manipulaciones con respecto a un cambio en el software o los archivos.

La invención se basa en el problema de especificar un procedimiento para operar un componente de vía o de a bordo de un sistema ferroviario que sea particularmente a prueba de manipulaciones con respecto al cambio de software o archivos.

Este objetivo se logra de acuerdo con la invención mediante un procedimiento con las características de acuerdo con la reivindicación 1. Las configuraciones ventajosas del procedimiento de acuerdo con la invención se dan en las reivindicaciones dependientes.

La invención prevé además que el almacenamiento de certificados sea un almacenamiento de certificados raíz en el que se almacenan los certificados raíz considerados válidos, sobre cuya base el aparato puede comprobar si el software recién transferido o recién instalado o los archivos recién recibidos deben clasificarse como fiables y pueden utilizarse o ejecutarse, por lo que, para cambiar el contenido del almacenamiento de certificado raíz se procede de tal manera que se genera un contenedor de datos en el lado del operario, que contiene al menos lo siguiente: un comando para cambiar el contenido del almacenamiento de certificados raíz y, en caso de que se añada un nuevo certificado raíz al almacenamiento de certificados raíz, el certificado raíz respectivo, un certificado de firma del lado del operario que contiene una clave pública, un conjunto de datos de cadena de confianza que hace referencia a un certificado raíz base y permite una verificación del certificado de firma en el lado del operador y una firma generada con una clave privada del certificado de firma en el lado del operador, se comprueba la fiabilidad de la firma en el lado del dispositivo, específicamente sobre la base de la clave pública en el certificado de firma en el lado del operador, del conjunto de datos de la cadena de confianza y de al menos un certificado raíz básico que se almacena en el lado del aparato y se considera fiable en el lado del aparato, y en el caso de una verificación de firma que confirme la fiabilidad, el comando contenido en el contenedor de datos para cambiar el contenido del almacenamiento de certificados raíz se ejecuta en el lado del aparato.

Una ventaja significativa del procedimiento según la invención es que el acceso al almacenamiento de certificados raíz en el lado del aparato solo se produce cuando se alimenta o se transmite un contenedor de datos, lo que, utilizando un conjunto de datos de cadena de confianza y un certificado raíz base conocido en el lado del aparato, permite verificar una firma también contenida en el contenedor de datos. El uso del contenedor de datos previsto en la invención con el contenido descrito evita una situación en la que el personal operativo, que está autorizado a realizar cambios técnicos en el aparato técnico, también pueda acceder al almacenamiento de certificados raíz del aparato y manipularlo. Cambiar el almacenamiento de certificados raíz solo es posible si se ha creado un contenedor de datos que tenga un certificado de firma de confianza verificable por parte del operador. Solo se tendrán en cuenta aquellos contenedores de datos que cumplan las condiciones mencionadas. La verificabilidad de la autenticidad de los contenedores de datos permite que estos se transmitan a través de líneas de transmisión de datos no seguras, por ejemplo, o que sean implementados *in situ* por personal no autorizado para crear contenedores de datos.

Es ventajoso que el operador genere un contenedor de datos que también contenga una o más de las siguientes informaciones: una indicación de validez que indique la validez del contenedor de datos, una indicación de uso que indique el uso del nuevo certificado raíz en caso de añadir un nuevo certificado raíz, una indicación de afiliación que indique la afiliación del contenedor de datos al aparato técnico al que se dirige, y/o una indicación (indicación de aplicación) de una o más aplicaciones del aparato técnico que deben poder utilizar el nuevo certificado raíz en caso de que se añada un nuevo certificado raíz.

Como contenedor de datos, se genera preferiblemente un contenedor de datos con una sección de encabezado, una sección de carga útil y una sección de firma que contiene la firma.

En la última variante, el conjunto de datos de la cadena de confianza y el certificado de firma del operario se colocan preferiblemente en la sección de encabezado.

El comando para cambiar el contenido del almacenamiento de certificados raíz y, si se añade un nuevo certificado raíz al almacenamiento de certificados raíz, el certificado raíz respectivo se aloja preferiblemente en la sección de carga útil.

La indicación de validez y uso del certificado raíz en caso de que se añada un nuevo certificado raíz, la indicación de afiliación sobre el aparato técnico mencionado y/o la indicación de aplicación para una o más aplicaciones del aparato técnico que han de poder utilizar el nuevo certificado raíz en caso de que se añada un nuevo certificado raíz, se alojan preferiblemente en la sección de encabezado.

La firma se forma preferiblemente sobre el contenido de la sección de encabezado y la sección de datos de operario.

Se genera preferiblemente una firma del tipo RFC7515 como firma.

Se prefiere especialmente una firma web JSON como firma.

El procedimiento se prefiere especialmente para su uso con los siguientes componentes de ingeniería ferroviaria: contadores de ejes, sistemas de detección de vía libre, sistemas de comunicación, sistemas de radio móvil y/o sistemas de enclavamiento.

La invención también se refiere a un aparato ferroviario que es un componente de vía o de a bordo de un sistema ferroviario y está equipado con un almacenamiento de certificados.

Según la invención está previsto que el almacenamiento de certificados sea un almacenamiento de certificados raíz en el que se almacenen los certificados raíz considerados válidos, por medio de los cuales el componente puede verificar si el software recién transferido o recién instalado o los archivos recién recibidos deben clasificarse como confiables y pueden utilizarse o ejecutarse, y el componente tiene un sistema de prueba que puede procesar un contenedor de datos que contenga al menos lo siguiente: una instrucción para cambiar el contenido del almacenamiento de certificados raíz y, en caso de que se añada un nuevo certificado raíz al almacenamiento de certificados raíz, el certificado raíz respectivo, un certificado de firma del lado del servidor que contenga una clave pública, un conjunto de datos de cadena de confianza que haga referencia a un certificado raíz base y una verificación del certificado de firma del lado del servidor y una firma generada con una clave privada del certificado de firma del lado del servidor, y el sistema de prueba está diseñado de tal manera que comprueba la fiabilidad de la firma, es decir, sobre la base de la clave pública en el certificado de firma del lado del servidor, del conjunto de datos de la cadena de confianza y al menos un certificado raíz base almacenado del lado del aparato y considerado de confianza y, en el caso de una verificación de firma que confirme la fiabilidad, libera para su ejecución o ejecuta por sí mismo el comando contenido en el contenedor de datos para cambiar el contenido del almacenamiento de certificados raíz.

En cuanto a las ventajas del aparato técnico según la invención, se hace referencia a las declaraciones anteriores en relación con el procedimiento técnico según la invención.

La invención se explicará con más detalle a continuación sobre la base de ejemplos; en este contexto,

La figura 1 muestra una disposición con un ejemplo de realización de un aparato técnico según la invención y un sistema de parametrización conectado al aparato técnico, en una primera fase de un procedimiento para cambiar el contenido de un almacenamiento de certificados raíz del aparato técnico,

La figura 2 muestra la disposición según la figura 1 en una segunda fase del procedimiento para cambiar el contenido del almacenamiento de certificados raíz,

La figura 3 muestra un ejemplo de realización de un contenedor de datos según la invención, mediante el cual se puede realizar un cambio en el contenido del almacenamiento de certificados raíz en el aparato técnico según las figuras 1 y 2.

Las figuras 4-7 muestran otros ejemplos de realización de contenedores de datos para cambiar el contenido del almacenamiento de certificados raíz del aparato técnico según las figuras 1 y 2.

La figura 8 muestra un ejemplo de realización de un sistema de prueba que puede utilizarse con el aparato técnico de acuerdo con las figuras 1 y 2, y

La figura 9 muestra otro ejemplo de realización de un sistema de prueba que puede utilizarse con el aparato técnico de acuerdo con las figuras 1 y 2.

En las figuras se utilizan siempre los mismos signos de referencia para componentes idénticos o comparables en aras de la claridad.

La figura 1 muestra un aparato técnico 10 que está conectado a un sistema de parametrización externo 30 a través de una línea de transmisión de datos 20. La línea de transmisión de datos 20 puede ser una línea de transmisión de datos no segura, es decir, una que podría ser manipulada bajo ciertas circunstancias.

El aparato técnico 10 comprende un almacenamiento de certificados raíz 11 y un sistema de prueba 12. El sistema de parametrización externo 30 permite cambiar externamente el contenido del almacenamiento de certificados raíz 11 con la intervención del sistema de prueba 12 a través de la línea de transmisión de datos 20.

En el ejemplo de realización mostrado en la figura 1 se asume, por ejemplo, que un nuevo certificado raíz ZW debe ser añadido o almacenado en el almacenamiento de certificados raíz 11 del aparato técnico 10 utilizando el sistema de parametrización externo 30. Un comando B correspondiente para cambiar el contenido del almacenamiento de certificados raíz 11, en este caso el comando B para añadir el nuevo certificado raíz ZW, se aloja en un contenedor de datos DC, que se transmite al sistema de prueba 12 a través de la línea de transmisión de datos 20 una vez finalizado.

Además del certificado raíz ZW y del comando B para cambiar el contenido del almacenamiento de certificados raíz 11, el contenedor de datos DC también contiene un conjunto de datos de cadena de confianza VDS y un certificado de firma Z del lado del operador que contiene una clave pública OS de un operador autorizado para generar el contenedor de datos DC. El término "operador" debe entenderse aquí no solo como un operador humano, sino también como una máquina operativa autosuficiente, como un ordenador debidamente programado.

El conjunto de datos de la cadena de confianza VDS hace referencia a un certificado raíz básico ZWB y permite la verificación del certificado de firma 2 del lado del operador.

Además, el contenedor de datos DC contiene una firma SIG(PS(Z)), que se ha generado con una clave privada PS del certificado de firma 2 del lado del operador.

El sistema de prueba 12 del aparato 10 comprueba la fiabilidad del contenedor de datos DC verificando en un primer paso, sobre la base de la clave pública OS en el certificado de firma Z del lado del operador, del conjunto de datos de la cadena de confianza VDS y de un certificado raíz base ZWB almacenado en el almacenamiento de certificados raíz 11, si la firma SIG(PS(Z)) se basa en un certificado raíz base ZWB digno de confianza y, por lo tanto, ha sido generada por un operador considerado fiable.

La figura 2 muestra la disposición según la figura 1, después de que el sistema de prueba 12 haya establecido la fiabilidad del contenedor de datos DC y, por lo tanto, se considere legítimamente instruido para ejecutar el comando B para cambiar el contenido del almacenamiento de certificados raíz 11 y almacenar el certificado raíz ZW contenido en el contenedor de datos DC en el almacenamiento de certificados raíz.

En el ejemplo de realización según las figuras 1 y 2, se supone a modo de ejemplo que se va a almacenar un nuevo certificado raíz ZW en el almacenamiento de certificados raíz 11 y el comando B comprende una solicitud correspondiente para complementar el almacenamiento de certificados raíz 11. Alternativamente, el comando B también puede referirse a la eliminación de un certificado raíz ya almacenado en el almacenamiento de certificados raíz 11 o a cualquier otro cambio en el almacenamiento de certificados raíz 11; en este caso, el comando B también describe el cambio deseado en cada caso.

La figura 3 muestra un primer ejemplo de una estructura ventajosa para el contenedor de datos DC de acuerdo con las figuras 1 y 2. En el ejemplo de realización según la figura 3, el contenedor de datos DC tiene tres secciones, a saber, una sección de encabezado KA, una sección de carga útil NA y una sección de firma SA.

El conjunto de datos de la cadena de confianza VDS y el certificado de firma 2 del operador, que contiene la clave pública OS del operador, se almacenan preferiblemente en la sección de encabezado KA.

En la sección de carga útil NA se encuentra preferiblemente el comando B para cambiar el contenido del almacenamiento de certificados raíz 11 y el certificado raíz ZW que se ve afectado.

En la sección de firma SA se encuentra la firma SIG(PS(Z)), que ya se ha explicado y que, sobre la base del conjunto de datos de la cadena de confianza VDS, del certificado raíz base ZWB almacenado en el almacenamiento de certificados raíz 11 y de la clave pública OS en el certificado de firma 2, permite verificar la fiabilidad del contenedor de datos DC. La firma SIG(PS(Z)) se forma preferiblemente sobre el contenido de la sección de encabezado KA y la sección de datos NA.

Como firma, se genera preferiblemente una firma del tipo RFC7515, en particular una firma web JSON.

La figura 4 muestra un segundo ejemplo de realización de un diseño ventajoso para un contenedor de datos DC que puede utilizarse para cambiar el contenido del almacenamiento de certificados raíz 11 en el aparato técnico 10 según las figuras 1 y 2. A diferencia de la realización según la figura 3, el contenedor de datos DC

según la figura 4 comprende además una especificación de aplicación App que define una o más aplicaciones del aparato técnico 10 que deben poder utilizar el nuevo certificado raíz en caso de que se añada un nuevo certificado raíz ZW.

La figura 5 muestra un tercer ejemplo de realización de un diseño ventajoso para un contenedor de datos DC que puede utilizarse para cambiar el contenido del almacenamiento de certificados raíz 11 en el aparato técnico 10 según las figuras 1 y 2. A diferencia de los ejemplos de realización según las figuras 3 y 4, el contenedor de datos DC según la figura 5 comprende además una indicación de uso Vw que indica el uso de un nuevo certificado raíz ZW. Por ejemplo, la indicación de uso puede indicar que el nuevo certificado raíz ZW debe utilizarse para verificar la autenticidad de los módulos de software recién instalados.

La figura 6 muestra un cuarto ejemplo de realización de un diseño ventajoso de un contenedor de datos DC que puede utilizarse para cambiar el contenido del almacenamiento de certificados raíz 11 en el aparato técnico 10 según las figuras 1 y 2. A diferencia de los ejemplos de realización según las figuras 3 a 5, el contenedor de datos DC según la figura 6 tiene además una indicación de afiliación Zghk que confirma la afiliación del contenedor de datos DC al aparato técnico 10.

La figura 7 muestra un quinto ejemplo de realización para un diseño ventajoso de un contenedor de datos DC que puede utilizarse para cambiar el contenido del almacenamiento de certificados raíz 11 en el aparato técnico 10 según las figuras 1 y 2. A diferencia de los ejemplos de realización según las figuras 3 a 6, el contenedor de datos DC según la figura 7 tiene además una indicación de validez Tmax, que indica una validez temporal del contenedor de datos DC y, por lo tanto, permite una limitación temporal de la usabilidad del contenedor de datos DC, de modo que una vez expirado el período de validez, la utilización del contenedor de datos DC se bloquea automáticamente.

La figura 8 muestra un ejemplo de un sistema de prueba 12 que puede utilizarse con el aparato técnico 10 según las figuras 1 y 2. El sistema de prueba 12 comprende un ordenador 120 y una memoria 121. En la memoria 121 se almacena un programa de prueba PM que, cuando es ejecutado por el ordenador 120, permite a este funcionar como un sistema de prueba 12, como ya se ha explicado anteriormente en relación con las figuras 1 a 7.

La figura 9 muestra otro ejemplo de realización de un sistema de prueba 12 que puede utilizarse con el aparato técnico 10 según las figuras 1 y 2. En el ejemplo de realización según la figura 9, el sistema de prueba 12 está formado simplemente por un ordenador 120 que, programado por un programa de prueba PM almacenado en el almacenamiento de certificados raíz 11, es capaz de ejecutar el procedimiento de prueba descrito en relación con las figuras 1 y 2, es decir, de verificar la fiabilidad de los contenedores de datos recibidos DC y, si es necesario, ejecutar los comandos B contenidos en él para cambiar el contenido del almacenamiento de certificados raíz 11.

El contenedor de datos DC formado con el sistema de parametrización 30 no tiene que ser alimentado en el aparato técnico 10 a través de una línea de datos 30 o inmediatamente después de su generación. Alternativamente, puede almacenarse primero temporalmente e introducirse más tarde *in situ* por el personal de operación en una interfaz del aparato.

En la variante mencionada de último es posible realizar un control de seguridad en dos etapas: en primer lugar, se puede verificar si el personal operativo está autorizado a realizar cambios en el aparato técnico 10; si este es el caso, la fiabilidad del contenedor de datos 10 se puede verificar en un segundo paso. En este caso, las autorizaciones se pueden diseñar de manera diferente: por ejemplo, el personal operativo *in situ* no tiene que estar autorizado para generar contenedores de datos DC por sí mismo; basta con que el personal operativo *in situ* traiga un contenedor de datos DC válido generado por otro operador autorizado para cambiar el almacenamiento de certificados raíz 11.

Aunque la invención ha sido ilustrada y descrita en detalle por medio de ejemplos de realización preferidos, la invención no está limitada por los ejemplos divulgados y los expertos en la materia pueden derivar otras variaciones sin apartarse del alcance de la invención.

Lista de signos de referencia

10	Aparato técnico
11	Almacenamiento de certificados raíz
12	Sistema de prueba
20	Línea de transmisión de datos
30	Sistema de parametrización
120	Ordenador

121	Memoria
App	Indicación de aplicación/indicación de aplicación
B	Comando
DC	Contenedor de datos
KA	Sección de encabezado
NA	Sección de carga útil
OS	Clave pública
PM	Programa de prueba
PS	Clave privada
SA	Sección de firma
SIG(PS(Z))	Firma
Tmax	Indicación de validez
VDS	Conjunto de datos de confianza
Vw	Indicación de uso
2	Certificado de firma
Zghk	Indicación de afiliación
ZW	Certificado raíz
ZWB	Certificado raíz base

REIVINDICACIONES

1. Procedimiento para operar un aparato técnico que es un componente en tierra o a bordo de un sistema técnico ferroviario, en el que el aparato técnico está equipado con un almacenamiento de certificados,

caracterizado porque el almacenamiento de certificados es un almacenamiento de certificados raíz en el que se almacenan certificados raíz considerados válidos, mediante los cuales el aparato técnico puede verificar si el software recién transferido o instalado o los archivos recién recibidos deben clasificarse como fiables y pueden utilizarse o ejecutarse,

en cuyo caso para cambiar el contenido del almacenamiento de certificados raíz (11) se procede de tal modo que

- el operador genera un contenedor de datos (DC) que contiene al menos lo siguiente:

- un comando (B) para cambiar el contenido del almacenamiento de certificados raíz (11) y, en caso de que se añada un nuevo certificado raíz (ZW) al almacenamiento de certificados raíz (11), el certificado raíz (ZW) respectivo,

- un certificado de firma (Z) en el lado del operario que contiene una clave pública (OS),

- un conjunto de datos de cadena de confianza (VDS) que hace referencia a un certificado raíz base (ZWB) y permite una verificación del certificado de firma (Z) en el lado del operador, y

- una firma (SIG(PS(Z)) generada con una clave privada (PS(Z)) del certificado de firma (Z) en el lado del operador,

- la firma (SIG(PS(Z)) se comprueba para determinar su fiabilidad en el lado del aparato, basándose en la clave pública (OS) del certificado de firma del lado del servidor (Z), el conjunto de datos de la cadena de confianza (VDS) y al menos un certificado raíz base (ZWB) almacenado en el lado del aparato y considerado fiable en el lado del aparato, y

- en el caso de una verificación de firma que confirme la fiabilidad, en el lado del aparato se lleva a cabo el comando (B) contenido en el contenedor de datos (DC) para cambiar el contenido del almacenamiento de certificados raíz (11).

2. Procedimiento según la reivindicación 1,

caracterizado porque se genera un contenedor de datos (DC) en el lado del operario, que también contiene una o más de las siguientes indicaciones:

- una indicación de validez (Tmax) que indica la validez temporal del contenedor de datos (DC),

- una indicación de uso (Vw) que indica el uso del nuevo certificado raíz (ZW) en caso de que se añada un nuevo certificado raíz (ZW),

- una indicación de afiliación (Zghk) que indica la afiliación del contenedor de datos (DC) al aparato técnico (10) mencionado, y/o

- una indicación (App) de una o más aplicaciones del aparato técnico (10) que, en caso de que se añada un nuevo certificado raíz (ZW), deben poder utilizar el nuevo certificado raíz (ZW).

3. Procedimiento según una de las reivindicaciones anteriores,

caracterizado porque como contenedor de datos (DC) se genera un contenedor de datos (DC) con una sección de encabezado (KA), una sección de carga útil (NA) y una sección de firma (SA) que contiene la firma (SIG(PS(Z)).

4. Procedimiento según la reivindicación 3,

caracterizado porque el conjunto de datos de la cadena de confianza (VDS) y el certificado de firma (Z) en el lado del operario se alojan en la sección de encabezado (KA).

5. Procedimiento según una de las reivindicaciones anteriores 3 a 4,

caracterizado porque el comando (B) para cambiar el contenido del almacenamiento de certificados raíz (11) y, en caso de que se añada un nuevo certificado raíz (ZW) al almacenamiento de certificados raíz (11), el certificado raíz respectivo (ZW) se alojan en la sección de carga útil (NA).

6. Procedimiento según una de las reivindicaciones 3 a 5 anteriores,

caracterizado porque, en caso de que se añada un nuevo certificado raíz (ZW), una indicación de validez (Tmax) y una indicación de uso (Vw) del certificado raíz (ZW), una indicación de afiliación (Zghk) para el aparato técnico (10) mencionado y/o una indicación (App) de una o más aplicaciones del aparato técnico (10), que deberían poder utilizar el nuevo certificado raíz (ZW) en caso de que se añada un nuevo certificado raíz (ZW), se alojan en la sección de encabezado (KA).

7. Procedimiento según una de las reivindicaciones anteriores,

caracterizado porque la firma (SIG(PS(Z)) se forma sobre el contenido de la sección de encabezado (KA) y la sección de datos de operario (NA).

8. Procedimiento según una de las reivindicaciones anteriores,

caracterizado porque se genera una firma del tipo RFC7515 como la firma (SIG(PS(Z)).

9. Procedimiento según una de las reivindicaciones anteriores,

caracterizado porque se genera una firma web JSON como la firma (SIG(PS(Z)).

10. Procedimiento según una de las reivindicaciones anteriores,

caracterizado porque se modifica el contenido de un almacenamiento de certificados raíz (11) de uno de los siguientes sistemas ferroviarios: contador de ejes, sistema de detección de vía libre, sistema de comunicación, sistema de radio móvil y/o sistema de enclavamiento.

11. Aparato ferroviario que es un componente de vía o de a bordo de un sistema ferroviario y está equipado con un almacenamiento de certificados,

caracterizado porque

- el almacenamiento de certificados es un almacenamiento de certificados raíz en el que se almacenan certificados raíz considerados válidos, mediante los cuales el componente puede verificar si el software recién transmitido o instalado o los archivos recién recibidos deben clasificarse como fiables y pueden utilizarse o ejecutarse, y

- el componente tiene un sistema de prueba (12) que puede procesar un contenedor de datos (DC) que contiene al menos lo siguiente:

- un comando (B) para cambiar el contenido del almacenamiento de certificados raíz (11) y, en caso de que se añada un nuevo certificado raíz (ZW) al almacenamiento de certificados raíz (11), el certificado raíz (ZW) respectivo,

- un certificado de firma (Z), en el lado del operario, que contiene una clave pública (OS),

- un conjunto de datos de cadena de confianza (VDS) que hace referencia a un certificado raíz base (ZWB) y hace posible una verificación del certificado de firma (Z) en el lado del operario, y

- una firma (SIG(PS(Z)) generada con una clave privada (PS(Z)) del certificado de firma (Z) del lado del operario, y

- el sistema de prueba (12) está diseñado de tal manera que

- comprueba la fiabilidad de la firma (SIG(PS(Z)), más precisamente sobre la base de la clave pública (OS) en el certificado de firma (Z) del lado del operario, del conjunto de datos de la cadena de confianza (VDS) y al menos de un certificado raíz base (ZWB) almacenado del lado del aparato y considerado fiable, y

-en el caso de una comprobación de firma que confirme la fiabilidad, se autoriza el comando (B) contenido en el contenedor de datos (DC) para cambiar el contenido del almacenamiento de certificados raíz (11) para su ejecución o se ejecuta por sí mismo.

DIBUJOS

FIG 1

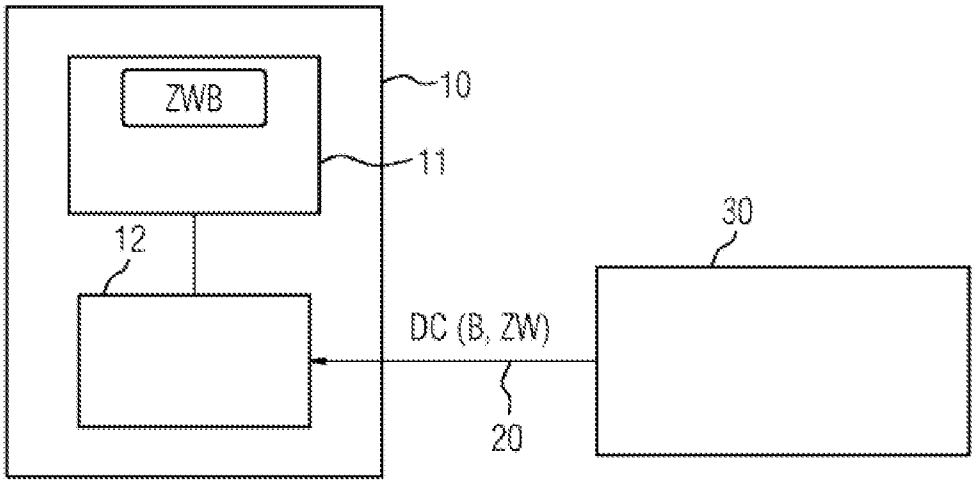

FIG 2

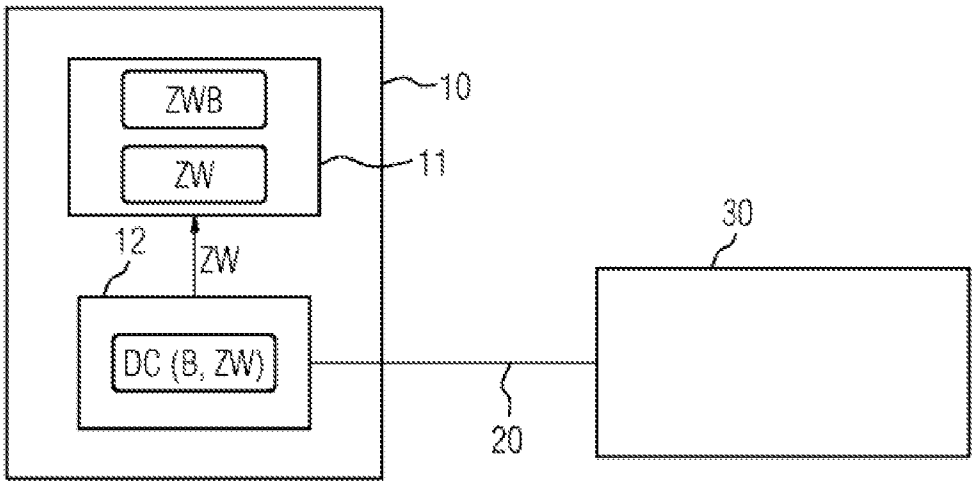

FIG 3

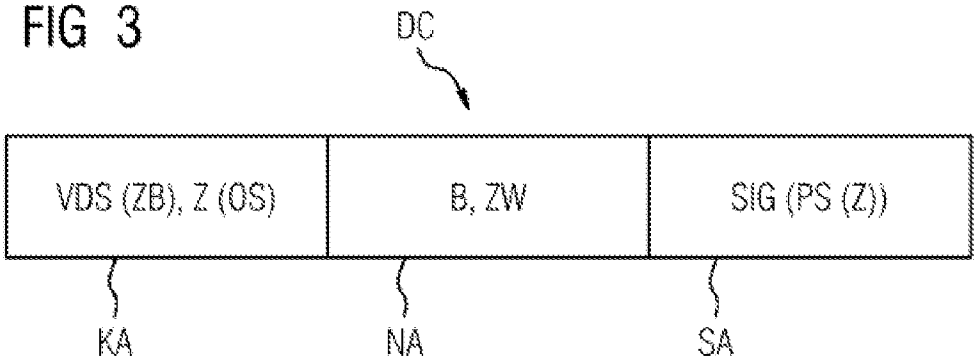

FIG 4

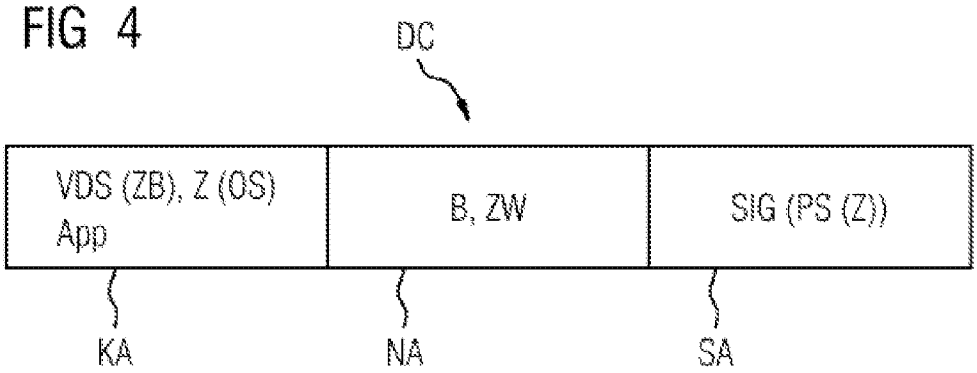

FIG 5

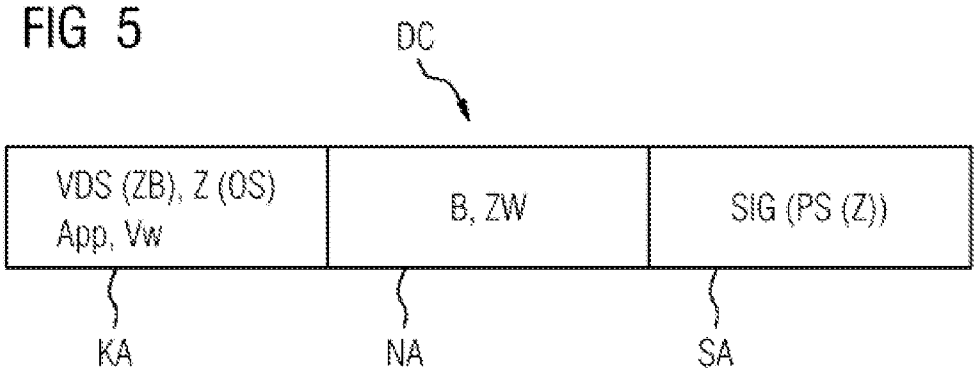

FIG 6

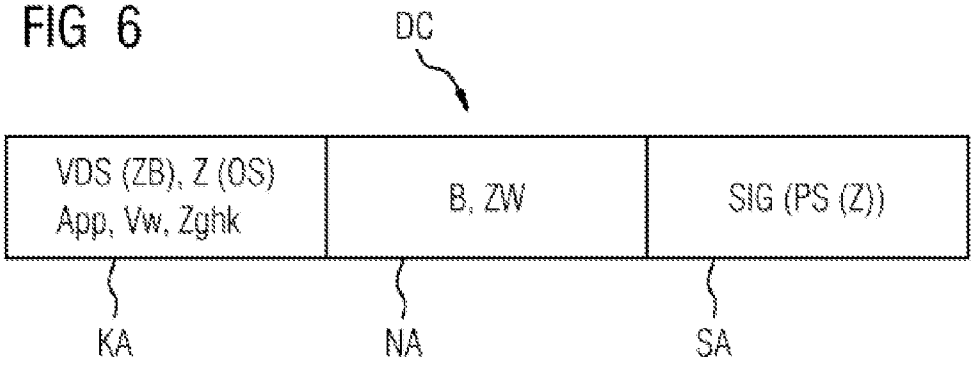
DC
VDS (ZB), Z (OS)
App, Vw, Zghk
B, ZW
SIG (PS (Z))
KA
NA
SA

FIG 7

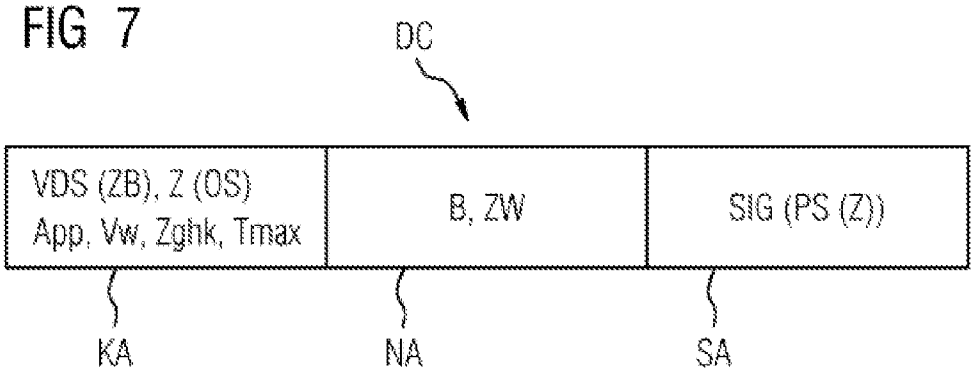
DC
VDS (ZB), Z (OS)
App, Vw, Zghk, Tmax
B, ZW
SIG (PS (Z))
KA
NA
SA

FIG 8

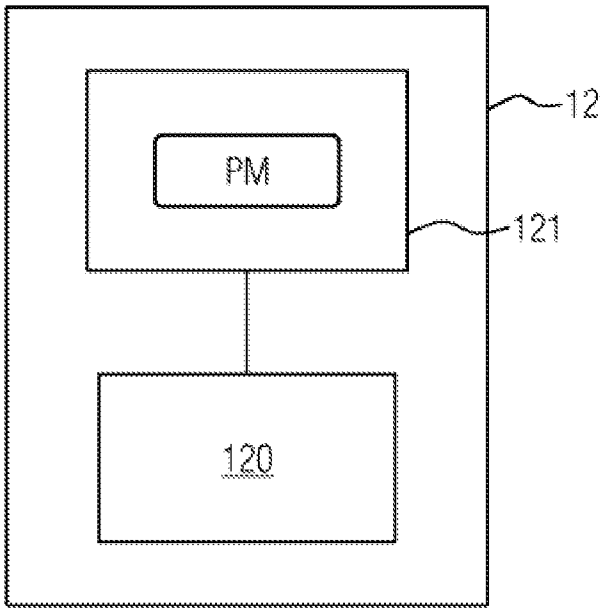

FIG 9