(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 024 757**

(51) Int. CI.:

H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **07.12.2021 E 21212698 (1)**

(97) Fecha y número de publicación de la concesión europea: **29.01.2025 EP 4016918**

(54) Título: **Procedimiento para la distribución inicial de datos protegidos en un sistema de protección de trenes ETCS**

(30) Prioridad:

18.12.2020 DE 102020216277

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.06.2025

(73) Titular/es:

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

(72) Inventor/es:

DÄGELE, ELMAR y
STEIN, FABRICE

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento para la distribución inicial de datos protegidos en un sistema de protección de trenes ETCS

La invención se refiere a un procedimiento para la distribución inicial de datos que requieren protección tales como, por ejemplo, al menos una clave, un certificado o una contraseña, en un sistema de protección de trenes ETCS entre al menos un centro de datos y al menos un dispositivo ETCS como, por ejemplo, una unidad a bordo (On-Board Unit, OBU) en el vehículo o un centro de bloqueo de radio (Radio Block Center, RBC) en la vía. Además, la invención también se refiere a un sistema de protección de trenes ETCS correspondiente.

En el sistema europeo de control de trenes (European Train Control System, ETCS), se utilizan claves criptográficas secretas para la comunicación segura entre los trenes con sus dispositivos ETCS a bordo (On-Board Unit, OBU) y las estaciones centrales ETCS o estaciones centrales de vía (Radio Block Center, RBC). Para cada una de estas relaciones de comunicación entre una unidad a bordo del vehículo y un centro de bloqueo de radio en tierra, se almacena una clave de comunicación (KMAC) en cada unidad a bordo y en cada centro de bloqueo de radio, de las cuales se deriva una clave de sesión secreta para la duración de una conexión de datos.

Un centro de datos (KMC), también conocido como centro de distribución de claves, es responsable de la generación y distribución de las claves criptográficas secretas (KMAC) en un entorno seguro de la instalación ferroviaria. La distribución de las claves secretas (KMAC) a los dispositivos ETCS, como la unidad a bordo y el centro de bloqueo de radio, puede realizarse tanto en línea como fuera de línea. La distribución fuera de línea puede realizarse, por ejemplo, mediante el intercambio de soportes de datos, y para la transmisión en línea puede utilizarse, por ejemplo, una conexión de telefonía móvil.

Los detalles exactos, como las interfaces y los procesos asociados, se especifican de manera uniforme en un conjunto de normas que se establece de manera uniforme en Europa a través de UNISIG, en particular UNISIG SUBSETS 114 y 137. UNISIG es un consorcio de empresas industriales que desarrollan las especificaciones técnicas de ETCS.

En la distribución de claves fuera de línea, se utilizan claves de transporte secretas adicionales (KTRANS) para garantizar la confidencialidad de las claves criptográficas. Con las claves de transporte secretas (KTRANS), se cifran las claves secretas (KMAC) para el transporte a las unidades ETCS. Las claves de transporte son generadas y emitidas por el centro de datos (KMC). La confidencialidad de las claves de transporte (KTRANS) es tan crítica para la seguridad como la confidencialidad de las claves (KMAC). Por lo tanto, primero deben almacenarse las claves de transporte (KTRANS) en las unidades ETCS para que luego sea posible la distribución de claves fuera de línea.

En la distribución de claves en línea, en cambio, se utilizan certificados raíz/cliente y contraseñas para transmitir en forma segura las claves criptográficas secretas. Estos certificados y contraseñas también deben mantenerse en secreto y debe garantizarse su autenticidad, y deben introducirse de manera segura en los dispositivos ETCS para poder iniciar la distribución de claves en línea.

Por ejemplo, en el documento WO 2009/027380 A1, se describe un procedimiento para la gestión de claves en línea ETCS.

Para poder llevar a cabo los dispositivos ETCS para la distribución de claves ETCS especificada de manera fuera de línea o en línea, es necesario un procedimiento para la distribución inicial de datos que merezcan protección, en particular claves. Un procedimiento de este tipo de acuerdo con el estado de la técnica consiste, por ejemplo, en que la introducción de las claves de transporte secretas (KTRANS) solo puede ser realizada por personas especialmente fiables de la empresa ferroviaria. Estas personas de confianza también se denominan gestores de claves. Todos los dispositivos, medios y procesos para el transporte, almacenamiento y procesamiento de las claves desprotegidas están sujetos a requisitos de seguridad especialmente estrictos. Por ejemplo, debe introducirse un ordenador especial que solo sea manejado por el gestor de claves. Este ordenador debe estar especialmente protegido contra ciberataques, lo que limita considerablemente su conectividad. Además, se aplican requisitos especiales de gestión y almacenamiento a todos los soportes de datos y ordenadores con material de claves no protegido, por ejemplo, para no poner en peligro el funcionamiento del sistema de protección de trenes ETCS por la vulneración de las claves, es decir, por la puesta en peligro de las claves secretas.

Sin embargo, el procedimiento descrito con anterioridad con los gestores clave presenta el problema de que, en especial en el caso de los operadores ferroviarios con grandes flotas de vehículos, puede suponer un considerable esfuerzo técnico y organizativo que también puede conllevar escasez de personal. Por ejemplo, en el trabajo del gestor clave, debe garantizarse que no haya otras personas presentes al mismo tiempo en el equipo ETCS en cuestión. El esfuerzo aumenta aún más si, por ejemplo, es necesario cambiar el hardware o el software de los equipos ETCS, como ocurre tras fallos de hardware o al actualizar el software. Por lo tanto, se necesitan procedimientos y sistemas simplificados o alternativos para la distribución inicial de datos que requieren protección en el sistema de protección de trenes ETCS.

La invención se basa, por lo tanto, en la tarea de proporcionar un procedimiento y un sistema de protección de trenes del tipo mencionado al principio que sean menos costosos y, por lo tanto, mejores.

De acuerdo con la invención, la tarea se resuelve mediante el procedimiento de la reivindicación de patente 1 y el sistema de protección de trenes ETCS de la reivindicación de patente 11.

En particular, la tarea se resuelve en el procedimiento de la invención de la siguiente manera: se generan determinados datos que deben protegerse para al menos un dispositivo ETCS en un entorno seguro en el centro de datos, se genera con los datos que deben protegerse al menos un paquete de transporte destinado al menos a un dispositivo ETCS en un entorno seguro, se asegura el paquete de transporte en el entorno seguro, el paquete de transporte seguro se transmite al dispositivo ETCS, el paquete de transporte seguro se desbloquea en un área segura del dispositivo ETCS y los datos que deben protegerse se almacenan en el área segura del dispositivo ETCS. La protección puede consistir, por ejemplo, en un cifrado y/o una firma digital. La desprotección puede consistir, por ejemplo, en un descifrado y/o una comprobación de la autenticidad mediante una firma digital.

Además, la solución de la invención se refiere a un sistema de protección de trenes ETCS para la distribución inicial de datos que requieren protección como, por ejemplo, al menos una clave, un certificado o una contraseña, entre al menos un centro de datos y al menos un dispositivo ETCS como, por ejemplo, una unidad a bordo (OBU) o un centro de bloqueo de radio (RBC) en tierra, con la que al menos un centro de datos, que está diseñado en un entorno seguro y para generar los datos que requieren protección, con al menos un centro de distribución de datos, que también está diseñada en un entorno seguro y para generar y proteger al menos un paquete de transporte con los datos que requieren protección, y con al menos un dispositivo ETCS, que tiene al menos un área segura y está diseñado para desbloquear el paquete de transporte cifrado y almacenar los datos que requieren protección en el área segura.

De acuerdo con la invención, los datos que deben protegerse para al menos una instalación ETCS se generan en un entorno seguro en el centro de datos. El centro de datos, que ya es conocido por el estado de la técnica como centro de distribución de claves (KMC), puede estar configurado, por ejemplo, en un ordenador en un entorno de oficina seguro. Esto es importante porque, en esta primera fase del procedimiento de la invención, los datos que deben protegerse aún no están protegidos. La generación de los datos protegidos puede ser realizada, por ejemplo, por una persona de confianza como el gestor de claves.

En este contexto, los datos que requieren protección pueden ser, por ejemplo, datos confidenciales o datos no confidenciales cuya integridad debe garantizarse como, por ejemplo, los certificados. La distribución inicial de los datos que requieren protección también puede incluir una actualización.

En el siguiente paso del procedimiento descrito, se genera un paquete de transporte específico para el dispositivo ETCS que contiene los datos que deben protegerse. En este caso, el paquete de transporte se genera específicamente para el dispositivo ETCS. Por supuesto, durante el funcionamiento, se generan varios paquetes de transporte para los diferentes dispositivos ETCS.

A continuación, de acuerdo con el procedimiento de la invención, el paquete de transporte se asegura en un entorno seguro, por ejemplo, cifrándolo o firmándolo. Aquí se puede utilizar, por ejemplo, un cifrado criptográfico y/o una firma digital.

En el siguiente paso, el paquete de transporte seguro se transmite al dispositivo ETCS correspondiente. Esto puede hacerse de la manera habitual, ya sea en línea o fuera de línea. La ventaja de esto es que los datos confidenciales están ahora protegidos, es decir, pueden ser transmitidos sin conexión por cualquier persona o en línea a través de cualquier medio, incluso “inseguro”, como la telefonía móvil, WLAN, 5G o Internet. Los datos confidenciales están protegidos contra el acceso no autorizado en el paquete de transporte.

En el último paso del procedimiento descrito, el paquete de transporte protegido se desbloquea en un área segura del dispositivo ETCS y los datos que requieren protección se almacenan en el área segura del dispositivo ETCS. El área segura del dispositivo ETCS es un almacenamiento protegido en el que se pueden almacenar datos que requieren protección, como claves ETCS no protegidas. Esta zona segura es, por ejemplo, un hardware especial, como un chip Trusted Platform Module (TPM), y, en su caso, una aplicación especial en forma de firmware que controla el acceso a los datos y su procesamiento. A menudo, las claves secretas solo pueden almacenarse para su seguridad, pero no leerse. Esto significa que solo pueden utilizarse en la zona segura. En la empresa, los datos útiles pueden transferirse a este hardware especial y, a continuación, cifrarse y/o descifrarse y/o firmarse electrónicamente y/o verificarse utilizando las claves secretas almacenadas. En el área segura del sistema ETCS, por ejemplo, la clave de transporte (KTRANS) se almacena de manera segura para la distribución de claves fuera de línea. Para la distribución de claves en línea, por ejemplo, se almacenan de manera segura al menos el certificado de cliente y la frase de contraseña.

La seguridad del paquete de transporte se garantiza, por ejemplo, con una clave (KP_{ENC}), mientras que para la firma del paquete de transporte se utiliza otra clave (KP_{SIG}). Con la clave privada (KP_{SK3}), se genera una firma digital del paquete de transporte que puede enviarse al dispositivo ETCS en el paquete de transporte. En este

caso, la firma también forma parte del paquete, ya que garantizar la autenticidad puede tener la misma prioridad que mantener la confidencialidad de las claves. De acuerdo con la invención, la clave o las claves necesarias para cifrar y/o firmar el paquete de transporte se almacenan en el centro de datos o en el centro de distribución de datos y en el dispositivo ETCS.

Una vez generados los paquetes de transporte cifrados y firmados en el centro de distribución de datos, se procede al transporte al dispositivo ETCS. Para ello, se pueden utilizar las vías habituales no protegidas, como el transporte manual mediante soporte de datos o la transmisión por correo electrónico.

En este ejemplo, cuando el paquete de transporte llega al dispositivo ETCS, se verifica la autenticidad del paquete mediante la firma suministrada con la clave pública (KP_{SIG}). Una vez autenticado, el paquete de transporte se descifra con la clave privada (KP_{ENC}). Los datos contenidos en el paquete de transporte, que incluyen, por ejemplo, solicitudes de claves, se procesan en el sistema ETCS en el orden correcto y, por ejemplo, se actualiza la memoria de claves. Para cada solicitud de clave procesada, el sistema ETCS puede generar un mensaje de confirmación (notificación KMC), cuyo contenido y formato también está definido en el estándar UNISIG y que se devuelve sin cambios al centro de datos.

En el dispositivo ETCS, la lectura del paquete de transporte se realiza, por ejemplo, con la ayuda de un ordenador de servicio. La comprobación y el descifrado del paquete de transporte se realizan únicamente en el área segura del dispositivo ETCS, de modo que, en ningún momento, existen datos no protegidos que deban protegerse fuera del área segura del dispositivo ETCS. El área segura dentro del sistema ETCS puede estar formada, por ejemplo, por un módulo de hardware especial o una tarjeta con chip adecuada. Una vez que el paquete de transporte ha sido verificado con éxito, su contenido se transfiere y se procesa.

Para permitir el bloqueo y desbloqueo del paquete de transporte según la invención, ya existen herramientas adicionales, como llaves y/o certificados, en el centro de distribución de datos y en el dispositivo ETCS. En el caso de las claves privadas, además, se garantiza su confidencialidad en forma permanente. Dado que, según la invención, el centro de distribución de datos se encuentra en un entorno seguro, no existe ningún nuevo requisito de seguridad. Los dispositivos ETCS conocidos también cuentan con zonas seguras, por lo que el esfuerzo adicional es mínimo.

El procedimiento según la invención y el sistema de protección de trenes según la invención tienen la ventaja de que simplifican la distribución del paquete de transporte protegido a los dispositivos ETCS. En lugar de un gestor de claves, la transmisión puede ser realizada por otras personas o por medios técnicos sin mayores requisitos de seguridad. Por ejemplo, esto puede ser realizado por el personal de mantenimiento de un tren, que puede llevar a cabo la instalación de las claves. El paquete de transporte también puede transferirse a los dispositivos ETCS a través de la telefonía móvil. Esto permite automatizar completamente la distribución de claves, de modo que ya no se requiere personal in situ para la instalación de las claves. En lugar de realizar muchas transacciones individuales, se pueden introducir varias solicitudes de claves y otros datos que requieren protección en un paquete de transporte en el dispositivo ETCS. Las notificaciones posteriores de las solicitudes de claves realizadas en los dispositivos ETCS también pueden generarse y almacenarse automáticamente uno tras otro. Esto reduce significativamente el tiempo necesario para la gestión de claves y la puesta en marcha inicial en los dispositivos ETCS.

De acuerdo con la invención, en el paquete de transporte se transmite una gran cantidad de datos que deben protegerse, incluyendo varias claves, certificados, contraseñas y/o solicitudes de claves. Esto tiene la ventaja de que, al agrupar los datos que deben protegerse en el paquete de transporte, se reduce considerablemente el trabajo y el número de paquetes de transporte que deben enviarse. Además de la clave de transporte (KTRANS) y la clave de comunicación (KMAC) mencionadas con anterioridad, el paquete de transporte también puede contener otras claves ETCS específicas del fabricante. Por ejemplo, las claves de personalización (KPERS) o los sellos de software (SEAL) también pueden integrarse como componentes en el paquete de transporte, lo que aumenta aún más la eficiencia del procedimiento descrito. Además, también se pueden incluir actualizaciones de claves en el paquete de transporte. En este caso, las nuevas claves se sustituyen en el dispositivo ETCS después de que el paquete de transporte haya sido verificado con éxito, por ejemplo, después de un ciclo determinado. Además de las claves para la gestión de claves fuera de línea, el paquete de transporte también puede utilizarse para distribuir los datos que deben protegerse para la gestión de claves en línea. Por ejemplo, pueden ser los certificados raíz/cliente y la frase de contraseña que se utilizan habitualmente para la gestión de claves en línea (OKM). La instalación y el procesamiento de estos datos se realiza de forma análoga a los datos de la gestión de claves fuera de línea en el dispositivo ETCS. Además de los datos de clave que deben protegerse, en el paquete de transporte se pueden almacenar otros parámetros necesarios para la puesta en marcha del dispositivo ETCS como, por ejemplo, el ID ETCS del dispositivo ETCS y el ID ETCS correspondiente del centro de datos. Al procesar el paquete de transporte en el dispositivo ETCS, todos los parámetros almacenados en el paquete de transporte se introducen automáticamente en el dispositivo ETCS en el orden correcto.

El procedimiento descrito puede mejorarse mediante modificaciones ventajosas, como se describe a continuación.

En una configuración ventajosa, para desbloquear al menos un paquete de transporte en el dispositivo ETCS, se puede utilizar al menos una herramienta, como una llave o un certificado, que se haya grabado en forma inamovible durante la fabricación del dispositivo ETCS. Esto tiene la ventaja de que la herramienta necesaria para desbloquear el paquete de transporte en el dispositivo ETCS puede almacenarse fácilmente durante la fabricación del dispositivo ETCS y, por lo tanto, no es necesario almacenar manualmente esta herramienta en la instalación ferroviaria. Esto puede ser especialmente ventajoso cuando se recibe el primer paquete de transporte. Después, la herramienta puede actualizarse.

Para garantizar la máxima calidad posible del paquete de transporte seguro, se puede utilizar un cifrado criptográfico simétrico o asimétrico o una combinación de estos procedimientos. Por ejemplo, se puede utilizar un procedimiento de cifrado asimétrico con claves públicas y privadas. La integridad y confidencialidad de los datos que requieren protección se garantizan mediante el cifrado criptográfico, mientras que, para proteger la autenticidad, se genera y comprueba la firma digital. Además, también se puede utilizar un cifrado híbrido que emplee adicionalmente AES (Advanced Encryption Standard). La clave AES, a su vez, está cifrada con una clave pública y almacenada en el paquete de datos. AES es un estándar de cifrado avanzado que incluye un procedimiento de cifrado simétrico.

Para reducir los datos que se van a transferir, especialmente para la transmisión en línea, el paquete de transporte se puede comprimir antes de la transmisión y expandir después de la transmisión.

Además, el paquete de transporte puede descifrarse en el dispositivo ETCS si el momento de la desactivación cae dentro de un período de tiempo predeterminado y/o si se ha introducido una contraseña predeterminada. Esto tiene la ventaja de que se implementa una seguridad adicional. De este modo, se limita el intervalo de tiempo permitido para el procesamiento del paquete de transporte en el dispositivo ETCS, es decir, una vez transcurrido o antes de que comience la validez, se bloquea la lectura y el procesamiento en el dispositivo ETCS. Mediante la contraseña predeterminada necesaria, se puede restringir el círculo de personas que pueden iniciar el procesamiento del paquete de transporte en el dispositivo ETCS. En este caso, se asume que la contraseña predeterminada solo se entrega a un grupo restringido de personas. De manera alternativa o adicional, se pueden establecer otras restricciones en el procesamiento del paquete de transporte: por ejemplo, se pueden restringir las funciones de modo que, por ejemplo, el desbloqueo del software en el dispositivo ETCS esté bloqueado, mientras que el bloqueo del software esté desbloqueado. Además, el paquete de transporte puede utilizarse en el momento oportuno para habilitar temporalmente determinadas funciones tales como, por ejemplo, para permitir la eliminación de todas las claves en el dispositivo ETCS. Este tipo de especificaciones de configuración pueden integrarse en el paquete de transporte, por ejemplo, al generarlo mediante un archivo XML. A continuación, en la configuración ETCS, estas especificaciones de configuración suministradas se evalúan y aplican durante el procesamiento del paquete de transporte.

Para que el procesamiento de los datos confidenciales sea especialmente seguro, la generación del paquete de transporte puede ser iniciada por una persona de confianza. Para lograr la misma ventaja, la generación de los datos confidenciales también puede ser iniciada por una persona de confianza. Una persona de confianza de este tipo puede ser, por ejemplo, el gestor de claves descrito con anterioridad. Dado que la generación del paquete de transporte y/o la generación de los datos que requieren protección puede tener lugar en forma centralizada, por ejemplo, en un entorno de oficina de confianza, el esfuerzo para el gestor de claves es mínimo.

La invención también se refiere a un procedimiento implementado por ordenador que está diseñado de acuerdo con una realización mencionada con anterioridad.

Además, la invención también se refiere a un dispositivo para el procesamiento de datos que, según la invención, está diseñado para llevar a cabo el procedimiento de acuerdo con una de las realizaciones mencionadas con anterioridad.

En una configuración ventajosa del sistema de protección de trenes ETCS según la presente invención, el centro de datos y el centro de distribución de datos pueden estar diseñados en el mismo entorno seguro, en particular, en un ordenador. Esto tiene la ventaja de que se necesita menos hardware y de que en ningún momento se utilizan datos no protegidos y dignos de protección fuera de dicho entorno seguro. Además, el centro de datos también puede diseñar el centro de distribución de datos.

A continuación, se explica la invención con referencia a los dibujos y a los ejemplos de realización que se muestran en ellos.

En ellos:

La Figura 1 muestra una representación esquemática de una instalación ferroviaria con un ejemplo de realización de un sistema de protección de trenes ETCS según la presente invención;

La Figura 2 muestra una representación esquemática del sistema de protección de trenes ETCS de la invención de la Figura 1;

La Figura 3 muestra otra representación esquemática del sistema de protección de trenes ETCS de la invención de las Figuras 1 y 2.

A continuación, se explica la invención con referencia a las formas de ejecución ejemplificadas en las Figuras 1 a 3.

Un sistema 1 ferroviario representado en la Fig. 1 presenta un vehículo 3 que circula a lo largo de una vía 2 y un sistema 4 de protección de trenes ETCS según la invención. El sistema 4 de protección de trenes ETCS comprende un centro 8 de control con un centro 5 de datos y un centro 6 de distribución de datos, así como varios dispositivos 7 ETCS. Aunque, en la Figura 1, se muestra de otra manera, el centro 5 de datos (KMC) y el centro 6 de distribución de datos (KDC) pueden estar muy separados físicamente y, en su caso, ser operados por diferentes edificios y/o empresas.

Los dispositivos ETCS, en su forma de ejecución mostrada en las Figuras 1-3, están diseñadas, por ejemplo, como un centro de bloqueo de radio RBC, que también podría denominarse central de línea ETCS, y como una unidad a bordo OBU, que también puede denominarse unidad de control del vehículo. El centro de bloqueo de radio RBC está dispuesto a lo largo de la ruta 2 de conducción y la unidad a bordo OBU está dispuesta en el vehículo 3. Para simplificar, en la Fig. 1, solo se muestran un vehículo 3 y un centro de bloqueo de radio RBC.

El centro 8 de control está diseñado para funcionar en algún lugar alejado de los dispositivos 7 ETCS, por ejemplo, en un entorno de oficina. En el funcionamiento del sistema 1 ferroviario, que está diseñado para ETCS, se utilizan claves de comunicación almacenadas en los dispositivos 7 ETCS para la comunicación entre la unidad a bordo OBU en el vehículo 3 y el centro de bloqueo de radio RBC. Estas claves de comunicación secretas y también las claves de transporte necesarias KTRANS deben almacenarse inicialmente de manera segura en los dispositivos ETCS. Esto se hace mediante el procedimiento de la invención y se explica a continuación, en particular con referencia a las Figuras 2 y 3.

En el centro 5 de datos, también denominado KMC (Key Management Center) en las Figuras, se generan primero los datos 9 que requieren protección. Estos datos que requieren protección o confidenciales son la clave de comunicación KMAC, la clave de transporte KTRANS, los certificados raíz OKM y una frase de contraseña OKM. Estos datos 9 que requieren protección se transmiten al centro 6 de distribución de datos después de su generación.

En las Figuras, el centro 6 de distribución de datos también se denomina KDC (Key Distribution Center). De acuerdo con la invención, en el centro 6 de distribución de datos, se genera y se guarda un paquete 10 de transporte individual para cada dispositivo 7 ETCS.

El centro 6 de distribución de datos, al igual que el centro 5 de datos, está diseñado en un entorno seguro, de modo que los datos que requieren protección pueden procesarse aquí sin protección y sin que exista ningún riesgo. El entorno 11 más seguro se muestra esquemáticamente en la Figura 1. En el ejemplo de realización de las Figuras, una parte de los datos 9 que requieren protección está cifrada. Estos datos 12 cifrados se muestran enmarcados con una línea discontinua. En el ejemplo de realización de las Figuras, estos datos cifrados 12 están cifrados con una clave KP_{ENC}.

Cada paquete de transporte con todos los datos 9 que requieren protección se firma en el paquete 10 de transporte con la clave KP_{SIG}. En esta forma, el paquete de transporte queda firmado para su seguridad, pero no completamente cifrado. Todos los datos confidenciales están cifrados en el paquete 10 de transporte. Los datos no confidenciales no están cifrados, sino firmados, para protegerlos contra la falsificación no autorizada. KP_{ENC} y KP_{SK3} forman parte de un procedimiento de cifrado asimétrico, como RSA. KP_{ENC} y KP_{SIG} se denominarán en lo sucesivo también clave 15 de paquete de transporte.

En el centro 6 de distribución de datos, se crea un paquete 10 de transporte individual para cada dispositivo ETCS. Esto se muestra, a modo de ejemplo, en la Fig. 2, en la que se crea el paquete 10 de transporte superior para el centro de bloqueo de radio RBC y el paquete 10 de transporte inferior para la unidad a bordo OBU. En el ejemplo de las Figuras, los paquetes 10 de transporte incluyen especificaciones 13 de configuración adicionales que determinan el procesamiento posterior de los datos 9 que requieren protección en los dispositivos 7 ETCS. Esto puede afectar, por ejemplo, a la validez del paquete 10 de transporte correspondiente. Así, el paquete 10 de transporte en el dispositivo 7 ETCS solo puede descifrarse, por ejemplo, si el momento del descifrado cae dentro de un período de tiempo predeterminado. De manera alternativa o adicional, el círculo de personas puede restringirse mediante la asignación de una contraseña. De este modo, el paquete 10 de transporte solo puede descifrarse en el dispositivo ETCS si se introduce una contraseña predeterminada que solo conoce el círculo de personas. Además, es posible restringir o habilitar funciones adicionales como especificaciones de configuración: por ejemplo, el procesamiento del paquete 10 de transporte en el dispositivo 7 ETCS solo puede realizarse para funciones habilitadas o, por ejemplo, el desbloqueo del software del dispositivo 7 ETCS está bloqueado, mientras que el bloqueo del software está habilitado. Alternativamente, el paquete 7 de transporte también puede utilizarse, si es necesario, durante un tiempo limitado para activar determinadas funciones como, por ejemplo, para permitir la eliminación de las claves en el dispositivo ETCS.

En el siguiente paso del procedimiento descrito, los paquetes 10 de transporte asegurados se transmiten desde el centro 6 de distribución de datos a los respectivos dispositivos 7 ETCS. Esto puede hacerse de varias maneras, como es sabido por el estado de la técnica, por ejemplo, mediante transmisión en línea, por correo electrónico o por conexión de datos. Por supuesto, también es posible la transmisión fuera de línea, por ejemplo, a través de un soporte de datos que es entregado por una persona.

Cada uno de los dispositivos 7 ETCS tiene un área 14 segura en la que se descifra el paquete 10 de transporte recibido. Para ello, se utilizan de nuevo como herramientas las claves del paquete de transporte KP_{ENC} y KP_{SIG}. Estas claves 15 de paquete de transporte están disponibles tanto en el centro 6 de distribución de datos como en los respectivos dispositivos ETCS. Cada dispositivo 7 ETCS tiene una clave de paquete de transporte individual o claves 15 de paquete de transporte individuales. En el ejemplo de la ilustración, las claves 15 de paquete de transporte ya han sido introducidas por el fabricante en el área 14 segura del dispositivo 7 ETCS durante la producción del hardware. Esto puede hacerse, por ejemplo, mediante un proceso de impresión. Las claves 15 de paquete de transporte pueden actualizarse y sustituirse después de la puesta en servicio del dispositivo 7 ETCS correspondiente, pero la introducción original por parte del fabricante en la producción de hardware garantiza que siempre haya una clave 15 de paquete de transporte en el dispositivo 7 ETCS correspondiente.

En la representación esquemática de la Fig. 3, además de la representación de la Fig. 2, también se muestra con flechas un flujo de datos desde el centro 5 de datos a través del centro 6 de distribución de datos hasta los dispositivos 7 ETCS, y viceversa. En la representación de ejemplo de la Fig. 3, a diferencia de la representación de la Fig. 2, se muestran tres unidades a bordo OBU diferentes, pero no un centro de bloqueo de radio RBC. Sin embargo, el flujo de datos al centro de bloqueo de radio RBC se produce de la misma manera o de manera similar a como se produce en las unidades a bordo OBU. Las tres unidades a bordo OBU están, por ejemplo, dispuestas en tres vehículos 3 diferentes, que están aparcados en diferentes plazas de aparcamiento, por ejemplo, en un depósito.

El flujo de datos representado en la Fig. 3 comienza en el centro 5 de datos, que genera los datos 9 que requieren protección y los transmite, por ejemplo, al centro 6 de distribución de datos mediante las denominadas órdenes clave. Dado que, en el ejemplo de las Figuras, tanto el centro 5 de datos como el centro 6 de distribución de datos están ubicados en un entorno seguro, no es necesario tomar ninguna medida de seguridad especial para la transmisión de los datos 9 que requieren protección. Alternativamente, ambos pueden estar separados físicamente y ser gestionados, por ejemplo, por diferentes operadores. En este caso, estos tendrían que acordar un procedimiento de transmisión seguro entre el centro 5 de datos y el centro 6 de distribución de datos.

En el centro 6 de distribución de datos, se generan y se guardan los paquetes 10 de transporte, tal como se ha descrito con anterioridad, y se transmiten a los respectivos dispositivos 7 ETCS.

Opcionalmente, puede haber una persona 16 de apoyo en el vehículo que, por ejemplo, envíe los paquetes 10 de transporte correspondientes a los dispositivos 7 ETCS mediante transmisión de datos sin conexión. Sin embargo, esta persona 16 de apoyo no tiene acceso en ningún momento a los datos que requieren protección, por lo que debe ser menos fiable que el gestor de claves. La persona 16 de apoyo puede ser, por ejemplo, el personal de mantenimiento.

Como respuesta o confirmación, los dispositivos 7 ETCS devuelven las respuestas 17 a través del centro 6 de distribución de datos o directamente al centro 5 de datos.

Opcionalmente, los paquetes 10 de transporte también pueden ser creados y transmitidos por el centro 5 de datos que, de este modo, asume las tareas del centro 6 de distribución de datos y lo forma. Esta realización opcional se indica en la Figura 3 mediante el recuadro discontinuo entre el centro 5 de datos y el centro 6 de distribución de datos.

La transmisión de los paquetes 10 de transporte entre el centro 6 de distribución de datos y los dispositivos 7 ETCS y la de las respuestas 17 en la dirección opuesta pueden realizarse a través de cualquier canal de datos 18.

REIVINDICACIONES

1. Procedimiento para la distribución inicial de datos (9) que requieren protección tales como, por ejemplo, al menos una clave, un certificado o una contraseña, en un sistema (4) de protección de trenes ETCS entre al menos un centro (5) de datos y al menos un dispositivo (7) ETCS como, por ejemplo, una unidad a bordo - OBU en el vehículo o un centro de bloqueo de radio - RBC en la vía,

en el que determinados datos que requieren protección para al menos un dispositivo (7) ETCS se generan en un entorno (11) seguro en el centro (5) de datos,

en el que, con los datos (9) que requieren protección, se genera al menos un paquete (10) de transporte destinado a al menos un dispositivo (7) ETCS en un entorno (11) seguro,

en el que el paquete (10) de transporte se asegura en el entorno (11) seguro, en el que el paquete de transporte asegurado (10) se transmite al dispositivo (7) ETCS,

en el que el paquete (10) de transporte seguro se desbloquea en un área (14) segura del dispositivo (7) ETCS y los datos (9) que requieren protección se almacenan en el área (14) segura del dispositivo (7) ETCS, en donde, en el paquete (10) de transporte, se transmite una gran cantidad de datos (9) que requieren protección, que comprenden varias claves, certificados, contraseñas y/o solicitudes de claves.

2. Procedimiento de acuerdo con la reivindicación 1,

caracterizado porque,

para desbloquear al menos un paquete (10) de transporte en el dispositivo (7) ETCS, se utiliza al menos una herramienta que se ha incorporado en forma inseparable durante la fabricación del dispositivo (7) ETCS.

3. Procedimiento de acuerdo con una de las reivindicaciones anteriores,

caracterizado porque

se utiliza un cifrado criptográfico simétrico o asimétrico o una combinación de ambos procedimientos para asegurar el paquete (10) de transporte.

4. Procedimiento de acuerdo con una de las reivindicaciones anteriores,

caracterizado porque

el paquete (10) de transporte se comprime antes de la transmisión y se expande después de la transmisión.

5. Procedimiento de acuerdo con una de las reivindicaciones anteriores,

caracterizado porque

el paquete (10) de transporte solo se desbloquea en el dispositivo (7) ETCS si el momento del desbloqueo cae dentro de un tiempo predeterminado y/o si se ha introducido una contraseña predeterminada.

6. Procedimiento de acuerdo con una de las reivindicaciones anteriores,

caracterizado porque

la generación del paquete (10) de transporte es iniciada por un gestor de claves como persona de confianza.

7. Procedimiento de acuerdo con una de las reivindicaciones anteriores,

caracterizado porque

la generación de los datos (9) es iniciada por un gestor de claves como una persona de confianza.

8. Procedimiento implementado por ordenador,

caracterizado porque

el procedimiento está diseñado de acuerdo con una de las reivindicaciones anteriores.

9. Dispositivo para el procesamiento de datos,

caracterizado porque

el dispositivo está diseñado para llevar a cabo el procedimiento de acuerdo con una de las reivindicaciones

anteriores.

10. Sistema (4) de protección de trenes ETCS para la distribución inicial de datos (9) que requieren protección como, por ejemplo, al menos una clave, un certificado o una contraseña, entre al menos un centro (5) de datos y al menos un dispositivo ETCS como, por ejemplo, una unidad a bordo - OBU en el vehículo o un centro de bloqueo de radio - RBC en la vía, en donde el sistema (4) de protección de trenes ETCS comprende lo siguiente:

el al menos un centro (5) de datos, que está diseñado en un entorno (11) seguro y para generar los datos (9) que requieren protección,

al menos un centro (6) de distribución de datos, que también está diseñado en un entorno seguro y para generar y asegurar al menos un paquete (10) de transporte con los datos (9) que requieren protección,

y el al menos un dispositivo ETCS, que presenta al menos un área (14) segura y está diseñado para desbloquear el paquete (10) de transporte seguro y almacenar los datos (9) que requieren protección en el área (14) segura,

en donde se transmiten, en el paquete (10) de transporte, una gran cantidad de datos (9) que requieren protección, que comprenden varias claves, certificados, contraseñas y/o solicitudes de claves.

11. Sistema (4) de protección de trenes ETCS de acuerdo con la reivindicación 10,

caracterizado porque

el centro (5) de datos y el centro (6) de distribución de datos se configuran en el mismo entorno (11) seguro.

12. Sistema (4) de protección de trenes ETCS de acuerdo con la reivindicación 10,

caracterizado porque

el centro (5) de datos y el centro (6) de distribución de datos se configuran en un ordenador.

13. Sistema (4) de protección de trenes ETCS de acuerdo con la reivindicación 10, 11 o 12,

caracterizado porque

el centro (5) de datos constituye el centro (6) de distribución de datos.

DIBUJOS

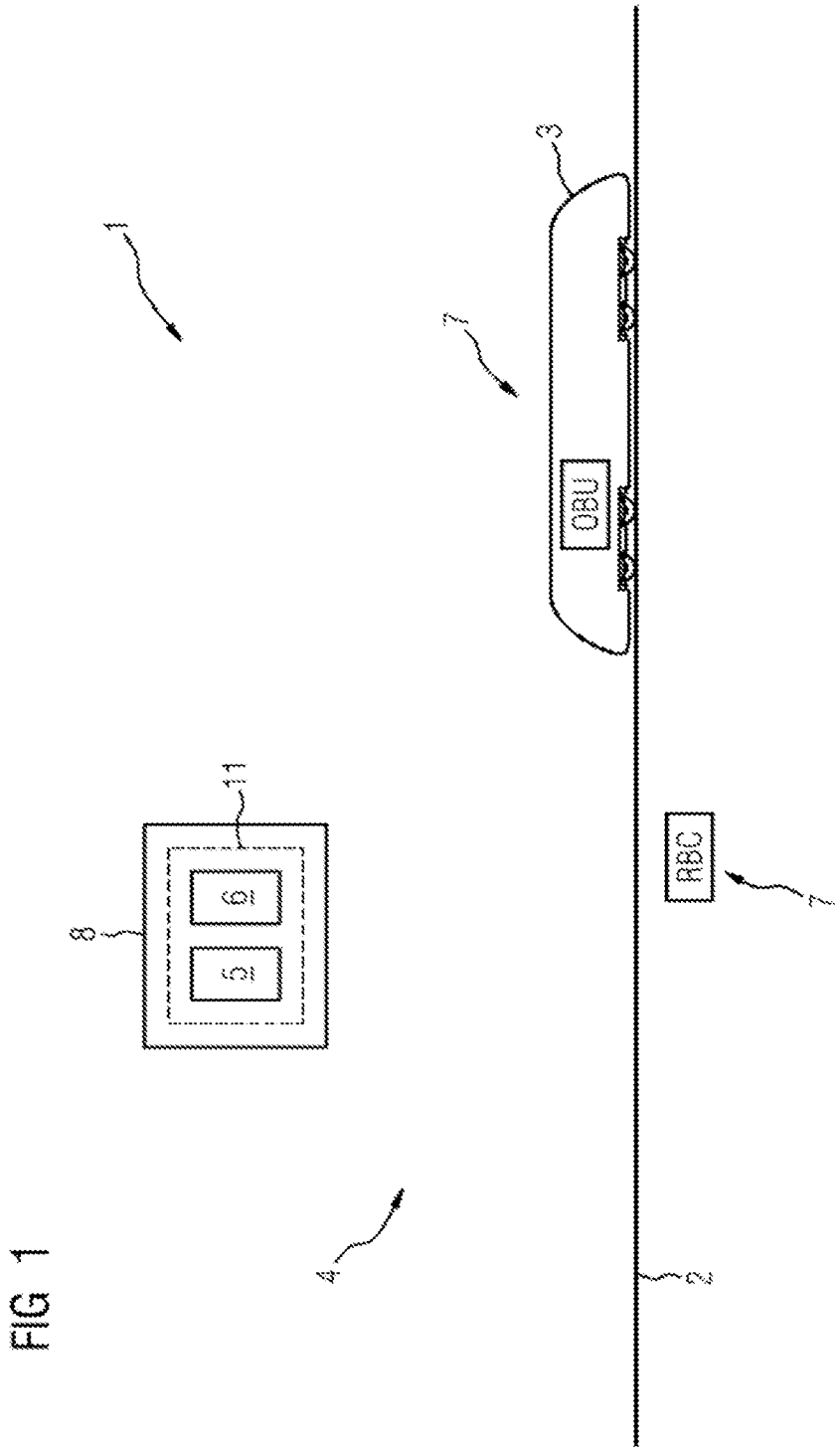
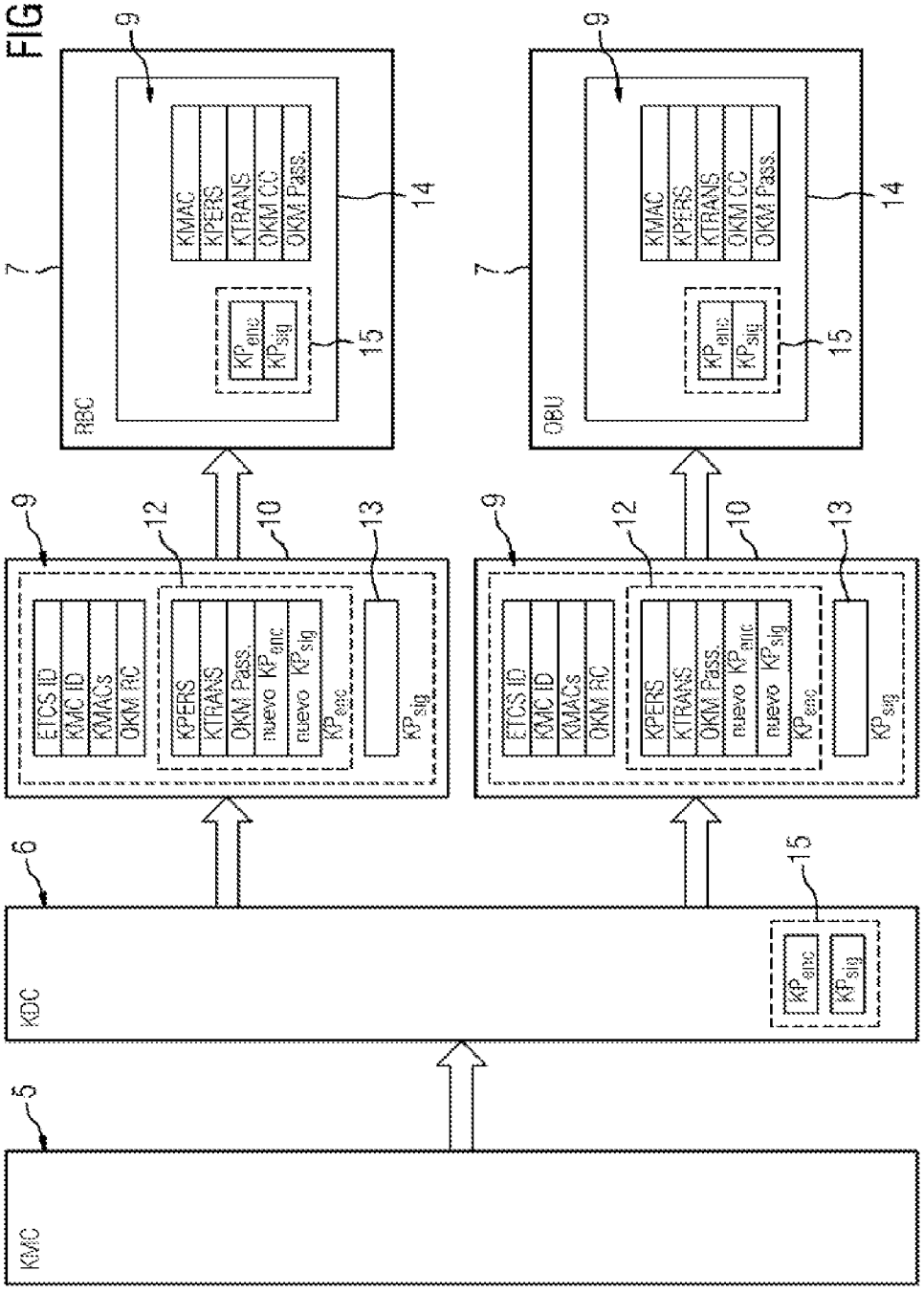


FIG 1

FIG 2


KMC
KDC
OBU
RSC
ETCS ID
KMC ID
KMACs
OKM RC
KPERS
KTRANS
OKM Pass.
nuevo KP enc
nuevo KP sig
KP enc
KP sig
KMAC
KPERS
KTRANS
OKM CC
OKM Pass.
5
6
7
9
10
12
13
14
15

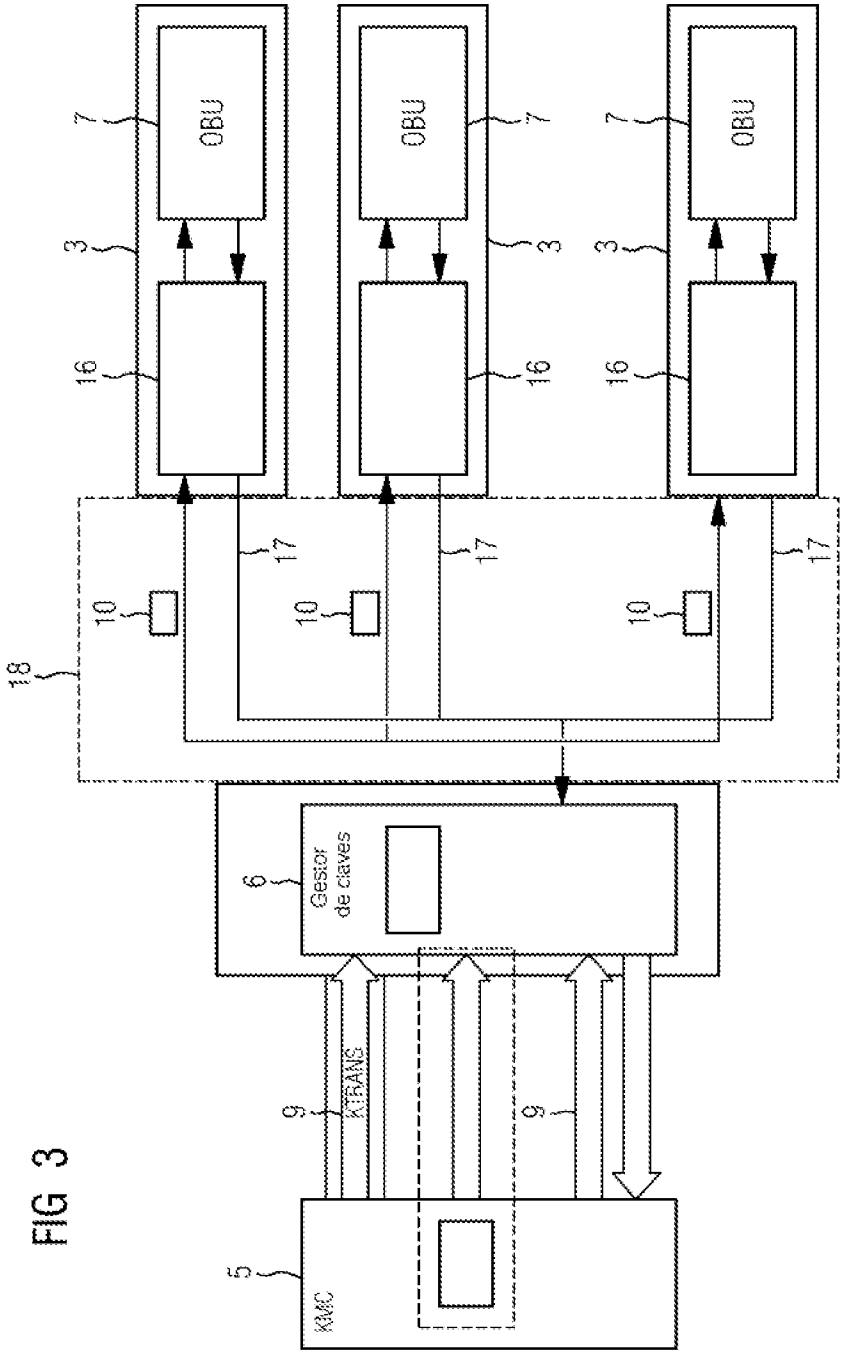

OBU
OBU
OBU
7
7
7
3
3
3
16
16
16
17
17
17
10
10
10
18
6
Gestor de claves
9
KTRANS
9
5
KMC

FIG 3