(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 986 323**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.03.2021 PCT/EP2021/056482**

(87) Fecha y número de publicación internacional: **30.09.2021 WO21190969**

(96) Fecha de presentación y número de la solicitud europea: **15.03.2021 E 21715153 (9)**

(97) Fecha y número de publicación de la concesión europea: **15.05.2024 EP 4097948**

(54) Título: **Procedimiento de transmisión de datos y sistema de comunicación**

(30) Prioridad:

27.03.2020 DE 102020204023

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.11.2024

(73) Titular/es:

SIEMENS MOBILITY GMBH (100.0%)
Otto-Hahn-Ring 6
81739 München, DE

(72) Inventor/es:

JÄHN, MARCEL;
LORENZ, MATTHIAS y
SCHILLING, BENJAMIN

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Procedimiento de transmisión de datos y sistema de comunicación

Se especifica un procedimiento de transmisión de datos con los pasos:

A) establecimiento de una conexión de datos con una clave de conexión entre un primer interlocutor de comunicación y un segundo interlocutor de comunicación,
B) cifrado de la clave de conexión para la conexión de datos por parte del primer interlocutor y/o del segundo interlocutor con una clave adicional,
C) envío de un mensaje que contiene una parte no cifrada y una parte cifrada con la clave de conexión desde el primer interlocutor de comunicación al segundo interlocutor de comunicación,
donde la parte no cifrada del mensaje es la que contiene la clave de conexión cifrada con la clave adicional.

Además, se especifica un sistema de comunicación.

Se conocen procedimientos genéricos para la transmisión de datos de las publicaciones DE 101 21 819 A1 y US 2009/157551 A1.

Además, por la publicación WO 00/29962 A1 se conoce un sistema y un procedimiento para instalar una red segura auditable.

Una tarea por resolver es especificar un procedimiento para la transmisión de datos con el que un tercero pueda registrar y verificar de manera eficiente un flujo de datos con comunicación cifrada.

Esta tarea se resuelve, entre otras cosas, mediante un procedimiento para la transmisión de datos y un sistema de comunicación con las características de las reivindicaciones independientes de la patente. La formación adicional preferida es el objeto de las reivindicaciones dependientes.

Por consiguiente, en un procedimiento con las características del preámbulo de la reivindicación 1, según la invención está previsto que un tercer interlocutor en la comunicación participe como oyente en la conexión de datos,

donde la clave adicional es conocida por el tercer interlocutor, y
en una etapa D) el tercer interlocutor de comunicación descifra la clave de conexión cifrada con la clave adicional de la parte no cifrada del mensaje, de modo que el tercer interlocutor de comunicación puede leer la parte cifrada del mensaje.

El tercer interlocutor, que debe es un oyente en la conexión de datos, también puede denominarse abreviadamente tercero. Esto significa que el tercer interlocutor es incluido específicamente en la conexión de datos por el primer y/o el segundo interlocutor.

El tercer interlocutor conoce la clave adicional. Esto se puede lograr transmitiendo la clave adicional en forma cifrada en la parte no cifrada del mensaje, o dando a conocer la clave adicional fuera de este procedimiento, o haciendo que la clave adicional sea la parte pública de un par de claves asimétricas que se asigna al tercer interlocutor, por ejemplo, la clave pública de su certificado X.509.

En el paso D), el tercer interlocutor descifra la clave de conexión cifrada con la clave adicional de la parte no cifrada del mensaje. Esto hace posible que el tercer interlocutor descifre y, por tanto, lea la parte cifrada del mensaje en tiempo real o con un retardo de tiempo.

En el procedimiento aquí descrito la comunicación se realiza entre dos interlocutores, estando asegurada criptográficamente una conexión de datos entre los interlocutores. Uno de los dos interlocutores comunica una clave para descifrar los paquetes de datos transmitidos a un tercer interlocutor, como centro de archivo o centro de inspección, para poder archivar los paquetes de datos y/o comprobar si contienen malware.

Los términos clave de conexión y clave adicional no se refieren necesariamente solo a una única parte de clave, sino que también incluyen opcionalmente pares de claves. La clave de conexión y/o la clave adicional son, por tanto, una parte de clave simétrica o asimétrica de una conexión criptográfica o también un par de claves formado por partes de clave simétricas o asimétricas.

Los términos clave de conexión y clave adicional no se refieren necesariamente solo a una única parte de clave, sino que también incluyen opcionalmente pares de claves. La clave de conexión y/o la clave adicional son, por tanto, una parte de clave simétrica o asimétrica de una conexión criptográfica o también un par de claves formado por partes de clave simétricas o asimétricas.

La mayoría de las comunicaciones digitales están cifradas. Esto generalmente se logra usando TLS, donde se usan claves asimétricas para acordar una clave simétrica que ambos interlocutores utilizan para el cifrado y descifrado. Esta clave también se conoce como *session key*. La clave se acuerda, en particular, mediante un

intercambio de claves Diffie-Hellman o un intercambio de claves Diffie-Hellman-Merkle, en breve intercambio de clave DHM o, protocolo DHM. TLS significa *transport layer security,* o sea, seguridad de la capa de transporte. Con este enfoque, incluso si se intercepta la comunicación que incluye la clave acordada, no es posible que un espía descifre la comunicación de datos. La clave simétrica acordada puede ser diferente para cada nueva conexión de comunicación.

En algunos casos, como cuando se opera una red de señalización o para transacciones financieras, las comunicaciones digitales deben archivarse por razones legales. Esto normalmente lo logra un tercero que, por ejemplo, registra y guarda la comunicación de datos mediante un puerto de monitor en un conmutador. Si la comunicación de datos está cifrada, los datos archivados no se pueden utilizar inmediatamente para auditorías y ya no se pueden cumplir los requisitos legales y/o de cumplimiento.

Por razones de seguridad de TI, a menudo es necesario inspeccionar la comunicación de datos para ver si contiene malware o si el flujo de datos está comprometido para detectar ataques. Esto se hace, por ejemplo, utilizando un *deep packet inspection algorithmus* y/o utilizando un NIDS, es decir, utilizando un *network intrusión detection-system*. También en este caso la comunicación de datos se controla a menudo a través de un *monitor port*. Sin embargo, con la comunicación cifrada, la *Deep packet inspection* ya no es posible y la capacidad de detectar ataques se reduce.

Las formas alternativas de permitir que un tercero archive o inspeccione datos incluyen almacenar una clave a través de un canal de comunicación separado. Esto significa que un interlocutor envía la clave simétrica utilizada para el cifrado al tercero. Sin embargo, se requiere una conexión de datos adicional.

Otra opción alternativa es simplemente verificar la integridad mediante un cifrado, *cipher* en inglés. Sin embargo, esto no es una opción si se transmiten datos confidenciales, como por ejemplo información personal. Además, esto ya no es compatible con los cifrados existentes actualmente en TLS 1.3.

Otra opción alternativa es utilizar cifrado simétrico con una clave conocida. Sin embargo, esto ya no se corresponde con el estado de la técnica en conexiones protegidas criptográficamente.

Finalmente, una opción alternativa es utilizar un enfoque de intermediario y/o un *proxy*.

Todas las conexiones se realizan a través del tercero y el tercero interrumpe la conexión directa entre los interlocutores de comunicación. Ambos interlocutores de comunicación están conectados directamente con el tercero y sólo se cifra la conexión directa con el tercero, de modo que ya no existe un cifrado de extremo a extremo.

El procedimiento aquí descrito comprende preferentemente los siguientes pasos, en particular en el orden indicado:

1. Se acuerda una clave de conexión, en particular una clave de sesión, por ejemplo, mediante un intercambio de claves, como por ejemplo un intercambio de claves Diffie-Hellman.

2. Un interlocutor cifra la clave de sesión de modo que sólo pueda ser descifrada por un tercero, por ejemplo, utilizando una clave asimétrica con una clave pública del tercero. El tercero es, por ejemplo, un centro de archivo. Opcionalmente, se utiliza la clave de un certificado X.509 del tercero. Esto tiene la ventaja adicional de que, además del primer y segundo interlocutor como emisor/receptor, sólo el tercero como oyente puede descifrar el tráfico de datos.

3. La clave de sesión cifrada se comunica de forma transparente con el siguiente mensaje dentro de la conexión de datos en una parte no cifrada del protocolo de comunicación subyacente, por ejemplo, en una opción TCP. Opcionalmente, el certificado X.509 del tercero también se envía en las opciones TCP para que el interlocutor de comunicación que no envió la clave de sesión pueda decidir si se puede confiar en el tercero.

4. En el caso de un punto de archivo, el tercero preferentemente almacena, registra y/o archiva todas las comunicaciones de datos, en particular la opción TCP. Opcionalmente, todo se almacena de forma cifrada para que los datos contenidos no sean procesados. Como opción adicional, la clave de sesión se extrae y almacena y/o procesa por separado.

5. Opcionalmente, el tercero descifra la comunicación de datos en tiempo real, también llamado sobre la marcha, y almacena y/o procesa los datos descifrados.

Como se describió al principio, el tercero no sólo puede ser un organismo de archivo, sino también un organismo de control para comprobar el flujo de datos en busca de ataques.

El proceso aquí descrito ofrece en particular las siguientes ventajas:

- El cifrado de extremo a extremo entre los interlocutores de comunicación sigue intacto.

- Sólo un interlocutor debe apoyar el procedimiento, el procedimiento puede ser transparente para el otro interlocutor.

- Casi no se requiere ningún flujo de datos adicional ni gastos generales, por lo que el ancho de banda se utiliza poco más y apenas es necesario realizar pasos de proceso adicionales.

- El proceso se puede utilizar inmediatamente, por ejemplo, con sistemas de archivo existentes, ya que todos los datos adicionales se transfieren dentro de la conexión de datos, también llamada *inline*.

- No se requiere ningún canal adicional para la transmisión de claves al tercero.

- Sólo terceros de confianza pueden descifrar el tráfico.

- Opcionalmente, el descifrado por parte del tercero sólo se produce en casos justificados, por ejemplo, en caso de una auditoría.

- Los datos archivados y guardados se pueden almacenar sin cambios y cifrados.

- Para el interlocutor que no transmite la clave de conexión al tercero, opcionalmente queda claramente visible que la clave de conexión fue comunicada al tercero. Sin embargo, este no es el caso cuando se utilizan enfoques de intermediario o enfoques fuera de línea, también conocidos como *out-of-band*.

- Con el procedimiento aquí descrito es más fácil cumplir con normas como el GDPR, *general data privacy regulation*.

- Es posible lograr un almacenamiento de datos que cumpla con los requisitos legales incluso para el tráfico de datos cifrados.

- La *Deep packet inspection* y NIDS son compatibles con el procedimiento aquí descrito.

- Una gran aceptación del procedimiento aquí descrito para conexiones criptográficas es posible porque para ambos interlocutores resulta evidente que en la comunicación interviene un tercero como oyente y quién es el tercero. Esto es particularmente cierto si en el mensaje se envía un certificado X.509 del tercero. Por el contrario, los enfoques anteriores que involucran a un tercero para una conexión criptográfica generalmente no se aceptan porque, a diferencia del procedimiento descrito aquí, el espionaje secreto es difícil de prevenir.

- Es posible conceder licencias del proceso a usuarios que, en particular, deben cumplir requisitos legales para el archivo de comunicaciones, como en el sector financiero.

Según al menos una forma de realización, el tercer interlocutor de comunicación registra y/o inspecciona el mensaje, en particular en nombre del primer interlocutor de comunicación y/o del segundo interlocutor de comunicación. De este modo, el tercer interlocutor cumple otra función en la conexión de datos según lo previsto, en particular el archivo y/o la protección contra ataques.

Según al menos una forma de realización, el tercer interlocutor almacena la parte cifrada del mensaje y/o la clave de conexión descifrada y/o la clave de conexión todavía cifrada con la clave adicional. Es posible que el tercer interlocutor descifre la parte cifrada del mensaje en un momento posterior.

En particular, el tercer interlocutor descifra la parte cifrada del mensaje sólo si así lo solicita, por ejemplo, una autoridad de control externa. La entidad de control puede ser el primer o el segundo interlocutor de comunicación o incluso otra entidad.

Según al menos una forma de realización, el tercer interlocutor descifra la parte cifrada del mensaje en tiempo real utilizando la clave de conexión. En tiempo real significa en particular que no existe un retraso de tiempo o no existe un retraso de tiempo significativo en comparación con un descifrado del mensaje por parte del primer y/o del segundo interlocutor comunicador. Esto proporciona una protección eficaz contra ataques con la ayuda del tercer interlocutor. Es posible que un descifrado por parte del tercer interlocutor para detectar ataques preceda a un descifrado del mensaje por parte del destinatario. Esto significa que el descifrado, por ejemplo, por parte del segundo interlocutor, sólo se realiza una vez que el tercer interlocutor haya dado su permiso.

Según al menos una forma de realización, la clave adicional es una clave pública de un certificado del tercer interlocutor de comunicación o la clave adicional contiene dicha clave. El certificado es en particular un certificado X.509.

Según al menos una forma de realización, la parte no cifrada del mensaje con la clave de conexión forma parte de una cabecera de protocolo de control de transmisión autodefinida, en particular, por un operador de la

conexión de datos. Por ejemplo, esta parte del mensaje es una opción autodefinida en un *TCP-Header*. TCP significa *Transmission Control Protocol*.

Según al menos una realización, la clave de conexión es una clave de sesión de la conexión de datos. Esto significa que la clave de conexión sólo es válida para una única sesión y/o sólo durante un tiempo determinado. Por lo tanto, el paso A) se puede realizar varias veces, incluso varias veces mientras exista la conexión de datos.

Además, se especifica un sistema de comunicación. El sistema de comunicación está configurado para un procedimiento como se describe en relación con una o más de las realizaciones mencionadas anteriormente. Por lo tanto, también se describen características del sistema de comunicación para el procedimiento y viceversa.

En al menos una realización, el sistema de comunicación lleva a cabo un procedimiento descrito anteriormente al menos temporalmente durante el funcionamiento. La conexión de datos aquí es parcial o completamente inalámbrica o por cable.

Según al menos una realización, el sistema de comunicación forma parte de una infraestructura de red ferroviaria. El primer interlocutor de comunicación y/o el segundo interlocutor de comunicación se seleccionan preferentemente del siguiente grupo: una caja de señales, una central de rutas como por ejemplo una central de rutas ETCS, un contador de ejes, una señal de ruta, un interruptor de agujas, un vehículo ferroviario.

Esto significa que el primer y/o segundo interlocutor de comunicación puede ser un RBC, *Radio Block Centre*, es decir, una central de rutas ETCS, donde ETCS significa *European Train Control System*.

Las propiedades, características y ventajas de la invención mencionadas anteriormente y la manera en que se logran se explican con más detalle mediante la siguiente descripción de las realizaciones ejemplares de la invención junto con las figuras correspondientes, donde:

la figura 1 muestra una representación esquemática de una realización ejemplar de un sistema de comunicación descrito aquí,

la figura 2 es un diagrama de flujo esquemático de una realización ejemplar que muestra un procedimiento descrito aquí,

la figura 3 muestra una representación esquemática de un mensaje para realizaciones ejemplares de los procedimientos descritos aquí, y

la figura 4 muestra una representación esquemática de una realización ejemplar de un sistema de comunicación aquí descrito en una infraestructura de red ferroviaria.

En la figura 1 se muestra una realización ejemplar de un sistema de comunicación 10. El sistema de comunicación 10 incluye un primer interlocutor de comunicación 11 y un segundo interlocutor de comunicación 12. Entre los interlocutores de comunicación 11, 12 existe una conexión de datos 3 como emisores y receptores para el intercambio de mensajes 5, preferentemente bidireccional y cifrado.

Además, el sistema de comunicación 10 incluye un tercer interlocutor de comunicación 13. El tercer interlocutor de comunicación 13 participa en la conexión de datos 3 a través de un componente de conexión 8. El componente de conexión 8 es, por ejemplo, un *monitor port* de un *router*. El tercer interlocutor de comunicación 13 archiva y/o inspecciona los mensajes 5 intercambiados. Esto significa que el tercer interlocutor de comunicación 13 preferentemente no participa directamente en la comunicación entre los interlocutores 11, 12 de comunicación y es un oyente.

Es posible que los interlocutores de comunicación 11, 12, 13 funcionen de forma automática o semiautomática. Esto significa que no es necesariamente necesario que el personal operativo intervenga en la comunicación. Los interlocutores de comunicación 11, 12, 13 son, por ejemplo, ordenadores o sensores o incluso actuadores.

En la figura 2 se describe un procedimiento operativo para un sistema comunicativo 10. En una primera etapa S1 del procedimiento se acuerda una clave de conexión 2 entre el primer y el segundo interlocutor 11, 12 de comunicación, por ejemplo, mediante un intercambio de claves Diffie-Hellman. La clave de conexión 2 es en particular una clave de sesión.

En un paso de procedimiento opcional S2, el primer interlocutor de comunicación 11 recibe una clave 4 adicional. Por ejemplo, la clave 4 adicional se transmite desde el tercer interlocutor de comunicación 13 al primer interlocutor de comunicación 11. La clave adicional 4 es, por ejemplo, una clave pública de un certificado X.509 del tercer interlocutor de comunicación 13.

En el paso del procedimiento S3, la clave de conexión 2 es cifrada por el primer interlocutor de comunicación 11 utilizando la clave adicional 4.

A continuación, el mensaje 5 se envía al segundo interlocutor de comunicación 12 en el paso del procedimiento S4. El mensaje 5 contiene la clave de conexión 2 cifrada con la clave adicional 4. La clave de conexión cifrada 2 está contenida en una parte no cifrada del mensaje 5, véase también la figura 3. Las partes cifradas 52 del mensaje están cifradas con la clave de conexión 2.

Como se ilustra en la figura 1, el mensaje 5 también va al tercer interlocutor de comunicación 13. Después de recibir el mensaje 5, el tercer interlocutor de comunicación 13, el oyente, puede llevar a cabo uno o más pasos del procedimiento S5, S6, S7, S8, S9.

En la etapa S5 del procedimiento opcional, el mensaje 5 y la clave de conexión 2 se guardan cifrados o descifrados. Preferiblemente, al menos el mensaje 5 simplemente se archiva en forma cifrada y no se procesa en este paso S5. Dado que la clave de conexión 2 también se almacena al menos de forma cifrada, el mensaje 5 se puede descifrar más tarde.

El mensaje 5 se descifra especialmente en una etapa posterior del procedimiento, S6. Es posible que el paso del procedimiento S6 se lleve a cabo sólo después de recibir una solicitud 6. La solicitud 6 pasa en un paso de procedimiento S7 a través de una entidad de control externa 7, por ejemplo, a diferencia de la representación en la figura 2, la entidad de control 7 también puede ser implementada por el primer y/o el segundo interlocutor de comunicación 11, 12. Opcionalmente, el tercer interlocutor de comunicación 13 devuelve entonces información 9, por ejemplo, a la autoridad de control 7. Esta información 9 puede proporcionarse dentro del paso procesal 7.

En el paso S8 del procedimiento opcional, el tercer interlocutor de comunicación 13 comprueba el mensaje 5 en busca de ataques. Esta verificación se puede realizar en tiempo real.

Además, en la figura 2 se ilustra un paso opcional S9. En el paso del procedimiento S9, el tercer interlocutor de comunicación 13 proporciona retroalimentación al primero y/o al segundo interlocutor de comunicación 12. La retroalimentación puede contener, por ejemplo, que el mensaje 5 se recibió correctamente del tercer interlocutor de comunicación 13 y que desde el punto de vista del tercer interlocutor de comunicación 13 no es necesario volver a enviar el mensaje 5. Alternativa o adicionalmente, la respuesta indica que el mensaje 5 no contiene ningún ataque y/o que el mensaje 5 puede ser descifrado de forma segura por el segundo interlocutor de comunicación 12 como destinatario del mensaje 5.

En la figura 3 una construcción ejemplar ilustrado del mensaje 5. El mensaje 5 comprende N paquetes de datos 50.1, 50.2 a 50.N, donde N es un número natural mayor o igual a uno. Preferiblemente, cada paquete de datos contiene una parte no cifrada 51 y una parte cifrada 52. A diferencia de la representación en la figura 3, también es posible que sólo el primer paquete de datos 50.1 o sólo una parte de los paquetes de datos contenga una parte no cifrada 51. Cada una de las partes cifradas 52 contiene una carga útil del paquete de datos en cuestión, cada una de las partes no cifradas 51 representa preferiblemente una cabecera en inglés *Overhead* o *Header*.

En particular, la clave de conexión 2 cifrada con la clave adicional 4 está contenida en la parte no cifrada 51 sólo del primer paquete de datos 50.1. Esta zona de la parte no cifrada 51 es en particular una opción TCP autodefinida. A diferencia de la representación de la figura 3, la clave de conexión cifrada 2 también se puede transmitir varias veces.

Puesto que la clave adicional 4 es conocida por el tercer interlocutor de comunicación 13 y la clave de conexión 2 se encuentra en la parte no cifrada 51, el tercer interlocutor de comunicación 13 puede descifrar la clave de conexión 2 y así acceder también a las partes cifradas 52 del mensaje 5.

En la figura 4 se ilustra una infraestructura ferroviaria 100. La infraestructura de red ferroviaria 100 incluye el sistema de comunicación 10 y una red ferroviaria 107. Los primeros, segundos y/o terceros interlocutores de comunicación se encuentran en la infraestructura de red ferroviaria 100 en particular a través de cajas de señales 101, a través de una central de ruta ETOS 102, a través de contadores de ejes 103, a través de señales de ruta 104, a través de interru 105 y/o formados por vehículos ferroviarios 106.

Gracias al tercer interlocutor de comunicación 13, se puede protocolizar y registrar el tráfico de datos entre los componentes de la infraestructura de red ferroviaria 100. La conexión de datos entre los componentes de la infraestructura de la red ferroviaria 100 es cableada o inalámbrica.

Aunque la invención se ha ilustrado y descrito en detalle utilizando realizaciones ejemplares, la invención no se limita a las realizaciones ejemplares divulgadas ni a las combinaciones específicas de características explicadas en ellas. Un experto en la técnica puede obtener variaciones adicionales de la invención sin apartarse del alcance de la invención reivindicada.

Lista de símbolos de referencia

2	claves de conexión para la conexión de datos.
3	conexión de datos
4	llaves adicionales
5	mensaje
50.1, 50.2, 50.N	paquete de datos del mensaje
51	parte no cifrada del mensaje
52	parte cifrada del mensaje
6	solicitud para descifrar el mensaje
7	instancia de control
8	componentes de conexión
9	información sobre el mensaje
10	sistema de comunicación
11	primer interlocutor de comunicación (remitente)
12	segundo interlocutor de comunicación (receptor)
13	tercer interlocutor de comunicación (oyente)
100	infraestructuras de red ferroviaria
101	caja de señal
102	central de ruta ETCS
103	contadores de ejes
104	señal de ruta
105	interruptor de agujas
106	vehículo ferroviario
107	red ferroviaria
S1 – S9	etapas de procedimiento

REIVINDICACIONES

1. Procedimiento de transmisión de datos con los pasos:

A) establecer una conexión de datos (3) con una clave de conexión (2) entre un primer interlocutor de comunicación (11) y un segundo interlocutor de comunicación (12),
B) cifrado de la clave de conexión (2) para la conexión de datos (3) por parte del primer interlocutor (11) y/o del segundo interlocutor (11, 12) con una clave adicional (4),
C) envío de un mensaje (5), que contiene una parte no cifrada (51) y una parte (52) cifrada con la clave de conexión (2), desde el primer interlocutor de comunicación (11) al segundo interlocutor de comunicación (12), donde la parte no cifrada (51) del mensaje (5) contiene la clave de conexión (2) cifrada con la clave adicional (4), caracterizado porque en la conexión de datos (3) interviene un tercer interlocutor (13) en calidad de oyente, donde la clave adicional (4) es conocida por el tercer interlocutor de comunicación (13), y
en un paso D) el tercer interlocutor (13) descifra la clave de conexión (2) cifrada con la clave adicional (4) de la parte no cifrada (51) del mensaje (5), de modo que el tercer interlocutor (13) está habilitado para leer la parte cifrada (52) del mensaje (5).

2. Procedimiento según la reivindicación 1,

en el que el tercer interlocutor de comunicación (13) registra y/o inspecciona el mensaje (5) en nombre del primer interlocutor de comunicación (11) y/o del segundo interlocutor de comunicación (12).

3. Procedimiento según una de las reivindicaciones 1 o 2,

en el que el tercer interlocutor (13) de comunicación almacena la parte cifrada (52) del mensaje (5) y la clave de conexión (2) descifrada y/o la clave de conexión (2) todavía cifrada con la clave adicional (4),
en el que el tercer interlocutor de comunicación (13) solo descifra la parte cifrada (52) del mensaje (5) si una entidad de control (7) realiza una solicitud (6) para hacerlo.

4. Procedimiento según una de las reivindicaciones 1 o 2, en el que el tercer interlocutor de comunicación (13) descifra la parte cifrada (52) del mensaje (5) en tiempo real mediante la clave de conexión (2).

5. Procedimiento según una de las reivindicaciones 1 a 4, en el que la clave adicional (4) es una clave pública de un certificado (8) del tercer interlocutor de comunicación (13) o contiene dicha clave.

6. Procedimiento según una de las reivindicaciones 1 a 5,

en el que la parte no cifrada (51) del mensaje (5) con la clave de conexión (2) forma parte de un encabezado de protocolo de control de transmisión autodefinido por un operador de la conexión de datos (3).

7. Procedimiento según una de las reivindicaciones 1 a 6,

en el que la clave de conexión (2) es una clave de sesión de la conexión de datos (3).

8. Sistema de comunicación (10) configurado según un procedimiento según una de las reivindicaciones 1 a 7, en el que la conexión de datos (3) es al menos parcialmente inalámbrica o por cable.

9. Sistema de comunicación (10) según la reivindicación 8,

que forma parte de una infraestructura de red ferroviaria (100),
donde el primer interlocutor de comunicación (11) y/o el segundo interlocutor de comunicación (12) se selecciona del siguiente grupo: caja de señales (101), central de ruta ETCS (102), contador de ejes (103), señal de ruta (104), interruptor de agujas (105), vehículo ferroviario (106).

FIG 1

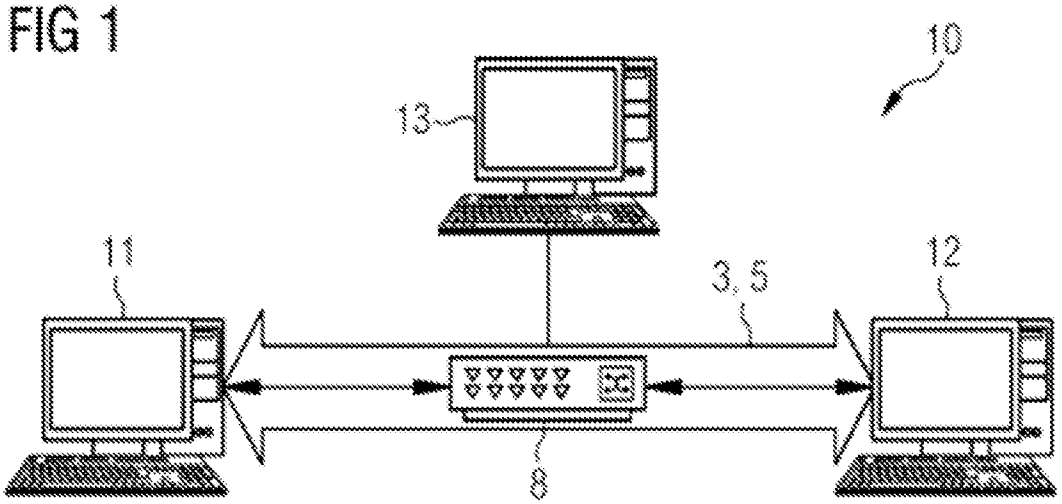


FIG 2

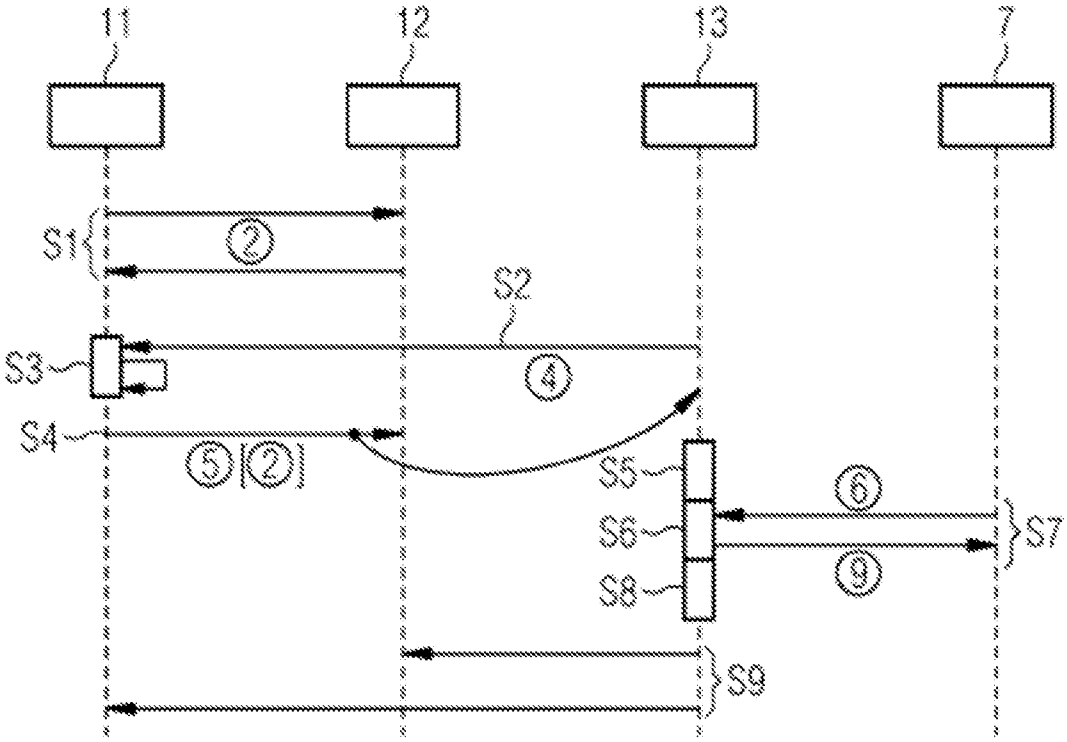


FIG 3

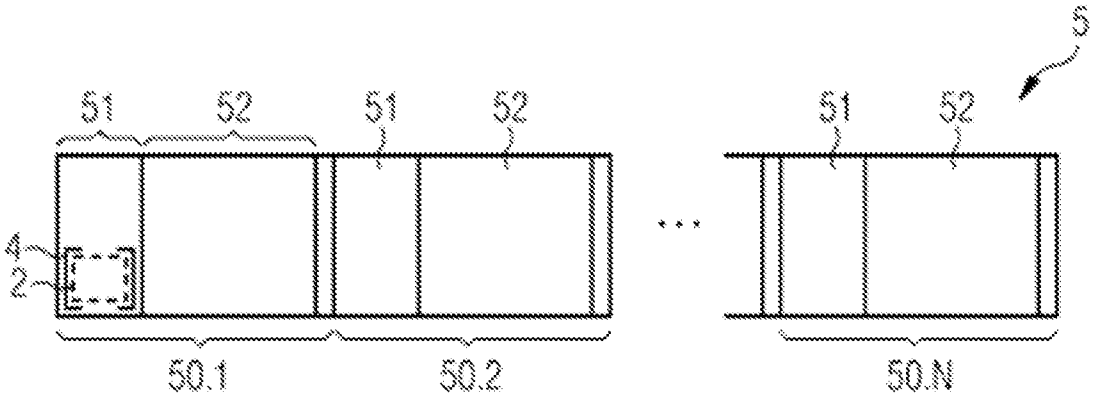
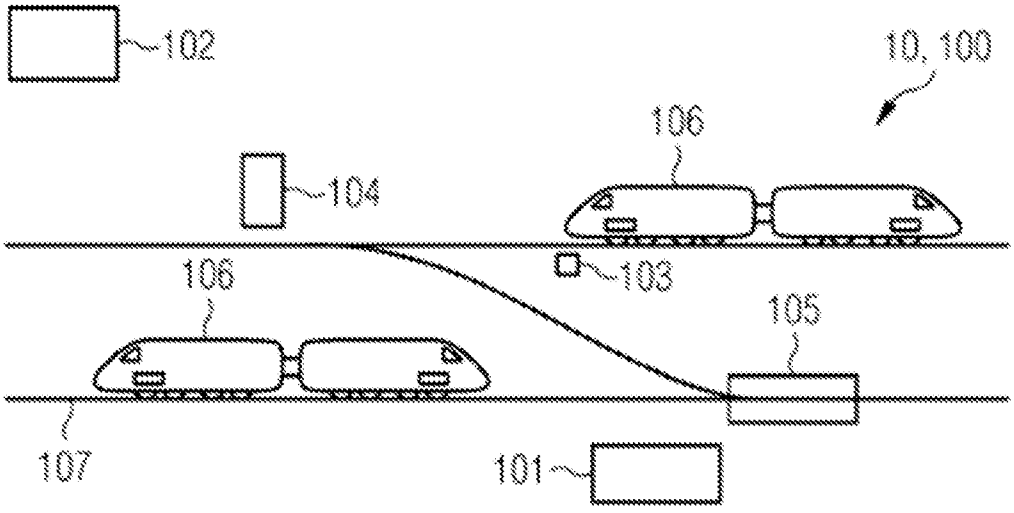

5
51
52
51
52
51
52
4
2
50.1
50.2
50.N

FIG 4


102
10, 100
106
104
103
106
105
107
101