(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 627 976**

(51) Int. CI.:

G07B 15/00 (2011.01)
G07B 15/06 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **19.04.2013 E 13164396 (7)**

(97) Fecha y número de publicación de la concesión europea: **15.03.2017 EP 2793194**

(54) Título: **Procedimiento para la carga de una unidad de a bordo con un tique electrónico**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.08.2017

(73) Titular/es:

KAPSCH TRAFFICCOM AG (100.0%)
Am Europlatz 2
1120 Wien, AT

(72) Inventor/es:

POVOLNY, ROBERT y
NAGY, OLIVER

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para la carga de una unidad de a bordo con un tique electrónico

La presente invención se refiere a un procedimiento para la carga y canjeo de tiques electrónicos en un sistema telemático de transporte.

Los sistemas telemáticos de transporte se usan para una multiplicidad de diferentes aplicaciones, sea para la identificación electrónica de un vehículo o para el pago de carreteras, peaje de acceso, por zonas o de ciudad, para el pago de tasas de aparcamiento, para el control de accesos (p. ej. instalaciones de barrera), para el registro electrónico del vehículo (electronic vehicle registration, EVR) etc. y así sucesivamente. Con esta finalidad se usan con frecuencia unidades de a bordo (On-Board-Units, OBUs) con un módulo de comunicación de corto alcance según el estándar DSRC (dedicated short range communication), a fin de poder localizarlas sobre la zona de cobertura de radio local de una radiobaliza que consulta.

A este respecto, en las unidades de a bordo se pueden cargar tiques electrónicos y luego usarse para el canjeo en los tipos más diferentes de radiobalizas, por ejemplo para pagar un peaje de carretera en una radiobaliza ("tique de peaje"), pagar una tasa de aparcamiento ("tique de aparcamiento"), pagar una tasa de entrada ("tique de entrada") o para saldar la adquisición de una mercancía o servicio, p. ej. para un servicio meteorológico, servicio de datos, servicio de información o entretenimiento o similares.

Para garantizar la integridad de un tique electrónico semejante en el recorrido de transmisión entre p. ej. una central que expide el tique, una unidad de a bordo que transporta el tique y una radiobaliza que canjea el tique, en sistemas telemáticos de transporte conocidos se usan actualmente pares de claves simétricos, que deben intercambiar los participantes en la comunicación antes de la comunicación. Esto requiere un procedimiento de distribución de claves asegurado, con consumo de tiempo, organización y costes correspondientemente elevado.

El documento WO 2009/082748 A1 describe un sistema de pago en un vehículo, en el que una unidad de a bordo se comunica con un comerciante a través del trasmisor-receptor. Para realizar una transacción, un lector de la unidad de a bordo reconoce p. ej. un teléfono móvil, que accede a una "Online Account" a través de una conexión de internet, con lo cual la transacción se lleva a cabo a través de la "Online Account" y/o la unidad de a bordo envía informaciones de pago (p. ej. números de tarjetas de crédito) al comerciante. La comunicación por radio entre la unidad de a bordo y el comerciante o entre la unidad de a bordo y teléfono móvil puede estar asegurada p. ej. a través de un sistema de encriptación mediante claves privadas y públicas.

El documento WO 2005/109348 A1 describe un procedimiento para el encargo de un código para la visualización de una estancia de aparcamiento válida, en donde un teléfono móvil solicita el código de una central y envía el código obtenido de la central a una etiqueta electrónica para la visualización en el vehículo. A este respecto, según el procedimiento conocido se encripta de nuevo la comunicación entre la central y el equipo móvil, por un lado, y entre el equipo móvil y la etiqueta electrónica, por otro lado.

El documento WO 03/042225 A2 muestra una encriptación de tiques con la ayuda de claves públicas y privadas: los tiques se encriptan por una central con una clave pública p. ej. de un teléfono móvil, con lo cual el tique encriptado se le envía al teléfono móvil. El teléfono móvil puede desencriptar a continuación el tique con su clave privada y canjearlo en un sistema de canjeo.

La invención se plantea el objetivo de superar las desventajas del estado de la técnica expuesto y crear un procedimiento de expedición y canjeo de tiques mejorado para tiques electrónicos en un sistema telemático de transporte.

Este objetivo se consigue en un primer aspecto de la invención con un procedimiento del tipo mencionado al inicio con las características de la reivindicación 1.

En la presente descripción, bajo DSRC y una interfaz DSRC se entiende una comunicación de corto alcance sobre un alcance por radio de cómo máximo algunos metros, algunas decenas de metros o algunos cientos de metros, tal y como se implementa, por ejemplo, mediante los estándares DSRC (dedicated short range communication), CEN-DSRC, UNI-DSRC, IEEE 802.11p o WAVE (wireless access for vehicular environments) o ITS-G5, inclusive WLAN y Wifi®, Bluetooth® o también tecnologías RFID activas y pasivas (radio frequency identification).

La invención se basa en el uso de procedimientos de encriptación asimétricos ("public/private key encryption") y de una interfaz separada, apropiada para esta encriptación de la unidad de a bordo, a través de la que se puede intercalar (cargar) el tique en la unidad de a bordo. La encriptación asimétrica ahorra la necesidad de un procedimiento asegurado de distribución de claves, según se requiere en el caso de claves simétricas. Así cada unidad de a bordo se puede equipar con su propio par de claves a partir de clave de unidad de a bordo pública y privada, por ejemplo durante la fabricación, sin que las claves de unidad de a bordo privadas tengan que ser conocidas durante el funcionamiento por los otros interlocutores en la comunicación, p. ej. el expedidor del tiques.

El uso de un teléfono móvil, en particular de un teléfono móvil apto para NFC y una interfaz NFC entre el teléfono

móvil y la unidad de a bordo DSRC, facilita en este caso la manipulación y la transferencia del tique asegurada, encriptada de la central a la unidad de a bordo con la ayuda de una red móvil (public land mobile network, PLMN), por un lado, y una interfaz inalámbrica o NFC, por otro lado.

Por ello es especialmente favorable cuando la segunda interfaz es una interfaz inalámbrica, preferentemente una interfaz NFC, lo que simplifica esencialmente la manipulación de la carga de una unidad de a bordo con un tique electrónico. La NFC (near field communication) es una tecnología de comunicación por radio sobre alcance por radio extremadamente corto de cómo máximo algunos centímetros o algunas decenas de centímetros y por ello requiere una cercanía estrecha a la unidad de a bordo para establecer la comunicación e intercalar el tique en la unidad de a bordo, lo que le da al usuario la seguridad de dirigirse exactamente a esta unidad de a bordo.

Una forma de realización preferida de la invención se destaca porque la radiobaliza se equipa con una clave electrónica pública y una privada de la radiobaliza o de una central del sistema telemático de transporte, y que en la unidad de a bordo, el tique desencriptado o el tique derivado de él se encripta nuevamente con la clave de radiobaliza pública o clave de central pública antes del envío a la radiobaliza. Preferiblemente a continuación en la radiobaliza se desencripta el tique o tique derivado con la clave de radiobaliza privada o clave de central privada.

Esta forma de realización se basa en una unidad de a bordo (“trusted”) digna de confianza, en la que se realiza un cambio de clave de una primera encriptación entre la central que expide el tique y unidad de a bordo que transporta el tique, por un lado, a una segunda encriptación entre la unidad de a bordo que transporta el tique y radiobaliza que canjea el tique, por otro lado. De este modo los expedidores de tiques (p. ej. central) y canjeadores de tiques (radiobaliza) no precisan tener uno de otro un conocimiento de claves privadas, lo que facilita esencialmente la manipulación de la distribución de claves.

En otro aspecto el procedimiento según la invención también comprende la expedición del tique en una central del sistema telemático de transporte, central equipada con una clave electrónica pública y una privada, y a saber con la etapa:

firma del tique con la clave de central privada.

Preferiblemente en la unidad de a bordo se valida el tique con la ayuda de la clave de central pública y sólo luego, cuando es válido, el tique o tique derivado de él se envía a la radiobaliza para el canjeo. De este modo en el entorno (trusted) digno de confianza de la unidad de a bordo se puede realizar no sólo el cambio de la encriptación, sino también una verificación de seguridad adicional de la validación del tique, si se desea.

Alternativamente o adicionalmente en la radiobaliza también se puede validar el tique o tique derivado de él con la ayuda de la clave de central pública y sólo luego, si es válido, se puede canjear.

La clave de radiobaliza pública o clave de central pública (según cuál de estas claves se requiera) se puede almacenar, por ejemplo, durante la fabricación en la unidad de a bordo. Alternativamente o preferiblemente esto también se puede realizar “on the fly”, es decir, preferiblemente se envía la clave de radiobaliza pública o clave de central pública de la radiobaliza a través de la interfaz DSRC a la unidad de a bordo.

Pero la clave de central pública también se puede enviar respectivamente con el tique o tique derivado.

Según otra característica preferida de la invención, en la central se provee el tique con una identificación unívoca y en la unidad de a bordo se verifica si la identificación de un tique recibido está contenida en una lista de identificaciones almacenadas y sólo luego, cuando no está contenida, el tique o tique derivado de él se envía a la radiobaliza para el canjeo.

Por consiguiente se garantiza que no se puedan realizar malversaciones durante el proceso de carga: un tique electrónico expedido por la central e intercalado en la unidad de a bordo tiene una identificación unívoca, que es “consumida” en cada proceso de carga, dado que ahora está almacenada en la lista de la unidad de a bordo y ya no es válida en el siguiente proceso de carga.

El tique electrónico se puede conservar en la unidad de a bordo, es decir, transportar por ésta y luego canjearse más tarde en esta forma en la radiobaliza. Alternativamente el tique se puede introducir en la unidad de a bordo en un monedero electrónico de la unidad de a bordo y luego opcionalmente de él se puede derivar el tique derivado. El tique derivado tiene, por ejemplo, una fracción o un múltiplo del valor monetario del tique electrónico original: a partir de un tique electrónico cargado en la unidad de a bordo se pueden generar varios tiques derivados “más pequeños” para el canjeo en la radiobaliza a través del monedero electrónico o varios tiques electrónicos cargados en el monedero electrónico pueden formar conjuntamente un tique derivado “más grande”. El monedero electrónico con el o los tique(s) electrónico(s) contenidos en él representa por tanto un “saldo” de lo que se puede “pagar” a través de la interfaz DSRC en las radiobalizas con la ayuda de los tiques derivados de él.

La identificación unívoca mencionada del tique puede ser una identificación de transacción o en el caso más sencillo también sólo un registro temporal.

La invención se explica a continuación más en detalle mediante ejemplos de realización representados en los dibujos adjuntos. En los dibujos muestra:

Fig. 1 una primera forma de realización del procedimiento según la invención mediante flujos de señales entre los componentes participantes en él;

Fig. 2 una segunda forma de realización del procedimiento según la invención en el mismo modo de representación que en la fig. 1; y

Fig. 3 una tercera forma de realización del procedimiento según la invención en el mismo modo de representación que en la fig. 1.

La fig. 1 muestra un sistema telemático de transporte 1, del que están representados una central 2 para la expedición de tiques electrónicos y – representativo de una multiplicidad de radiobalizas del sistema 1 – una radiobaliza 4 para el canjeo de un tique electrónico semejante. La central 2 puede ser, por ejemplo, un ordenador central de un sistema de peaje de carreteras, sistema de tasa de aparcamiento, sistema de comunicación o similares.

El tique electrónico 3 es un fichero que representa un valor real, por ejemplo, autorizado para la adquisición de un servicio, como la entrada a una zona o edificio (“tique de entrada”), para el uso de una plaza de aparcamiento (“tique de aparcamiento”), para la utilización de un tramo de carretera o zona (“tique de peaje”) o en general para la adquisición de una mercancía o servicio (“dinero electrónico”).

La radiobaliza 4 es una instalación electrónica en la que el tique electrónico 3 se puede canjear a fin de autorizar para la entrada, aparcamiento, utilización de carreteras o adquisición de mercancías o servicios. Por ejemplo, la radiobaliza 4 está colocada en una carretera (road side entity, RSE), para cobrar la utilización de su tramo de carretera mediante canjeo de un tique electrónico 3. Alternativamente la radiobaliza 4 es un parquímetro en el que se canjea un tique electrónico 3 para pagar por un estacionamiento. O la radiobaliza 4 es, según está representado de forma simbólica con 5, parte de una instalación de barrera que libera una barrera de entrada en el caso del canjeo de un tique electrónico 3, etc. y así sucesivamente.

La radiobaliza 4 está realizada según el estándar DSRC (dedicated short range communication) y configurada para llevar a cabo comunicaciones por radio RSRC a través de una interfaz DSRC 6 con las unidades de a bordo DSRC (Onboard-Units, OBUs) 7. Una OBU 7 semejante se lleva consigo, por ejemplo, por un vehículo (no representado), p. ej. montada en el lado interior del parabrisas, pero eventualmente también se puede llevar por el usuario.

En la presente descripción, bajo DSRC y una interfaz DSRC se entiende una comunicación de corto alcance a través de alcance por radio de cómo máximo algunos metros, algunas decenas de metros o algunas centenas de metros, tal y como se implementa, por ejemplo, mediante los estándares DSRC (dedicated short range communication), CEN-DSRC, UNI-DSRC, IEEE 802.11p o WAVE (wireless access for vehicular environments) o ITS-G5, inclusive WLAN y Wifi®, Bluetooth® o también tecnologías RFID activas y pasivas (radio frequency identification).

La unidad de a bordo DSRC 7 está equipada adicionalmente a su interfaz DSRC 6 con otra interfaz 8, preferiblemente una interfaz de radio según el estándar NFC (near field communication), a través de la que puede llevar a cabo comunicaciones con un teléfono móvil 9 (apto preferiblemente para NFC). El teléfono móvil 9 se puede comunicar, por su lado, a través de una red móvil (public land mobile network, PLMN) 10 y eventualmente otras redes de datos (no representadas), p. ej. el internet, con la central 2. Alternativamente la interfaz 8 también se puede realizar por WLAN, Bluetooth o también comunicación inalámbrica (p. ej. USB, tarjetas de memoria SD o similares).

Bajo el término “teléfono móvil” 9 entra aquí cualquier tipo de equipo de comunicación que se puede comunicar en una red móvil 10 y adicionalmente está equipado con la interfaz NFC 9, por ejemplo, un teléfono inalámbrico, Smartphone, ordenador portátil o tableta, asistente digital personal (PDA), etc. El alcance por radio de la interfaz NFC 8 está diseñado exclusivamente para el corto alcance, es decir, limitado a algunos centímetros o algunas decenas de centímetros, de modo que el teléfono móvil 9 se debe llevar al entorno inmediato de la unidad de a bordo DSRC 7, para poder realizar las comunicaciones por radio NFC a través de la interfaz NFC 8.

Para el procedimiento de carga, expedición y canjeo del tique representado a continuación, los componentes mencionados de central 2, radiobaliza(s) 4 y unidad(es) de a bordo DSRC 7 del sistema telemático de transporte 1 se equipan como sigue con pares de claves electrónicas a partir de respectivamente una clave pública (“public”) y una privada (“prívate”) de un procedimiento de encriptación de clave pública / privada. Según se conoce en la técnica, en el procedimiento de encriptación de clave pública / privada cada participante obtiene dos claves, y concretamente una clave pública, que se conoce por todos los otros participantes, y una clave privada, que mantiene en secreto. Un mensaje – como aquí el tique electrónico 3 – se puede encriptar por un emisor con la ayuda de la clave pública del receptor y luego ya sólo se puede desencriptar por el receptor con su clave privada. A la inversa un mensaje se puede firmar por un emisor con su clave privada. El receptor del mensaje puede comprobar éste con la clave pública del emisor respecto a la autenticidad de la firma por parte del emisor, es decir, validar la firma del emisor de esta manera.

La central 2 dispone para ello de una clave pública PubK.CS y una clave privada PrivK.CS; cada unidad de a bordo DSRC 7 dispone de una clave pública PubK.OBU y una clave privada PrivK.OBU y – al menos en una primera forma de realización del procedimiento, en las otras formas de realización del procedimiento esto no es obligatorio – cada radiobaliza 4 dispone de una clave pública PubK.TRX y una clave privada PrivK.TRX. La clave pública Pubk.TRX de la central 2 se pone a disposición de la radiobaliza 4 a través de un recorrido de datos 11 separado; o alternativamente cada vez se envía con un tique electrónico 3, según se explica todavía más tarde, en cuyo caso se puede suprimir el recorrido de datos 11. El recorrido de datos 11 puede ser, por ejemplo, internet, una intranet o una red móvil, o también un recorrido de transporte físico para un soporte de datos en el que se transporta la clave pública PubK.CS de la central 2 a la radiobaliza 4.

El procedimiento de carga, expedición y canjeo del tique representado en la fig. 1 trabaja como sigue. La carga del tique se inicia por el usuario en el teléfono móvil 9, para lo que maneja, por ejemplo, una aplicación correspondiente en su smartphone, tableta, etc. o desencadena y/o recibe mensajes SMS correspondientes (short message service) (etapa 12). Para la solicitación del tique 3 de la central 2, en una primera etapa 13 se solicita y recibe la clave pública PubK.OBU de la unidad de a bordo 7 a través de la interfaz 8, preferiblemente a través de NFC. El teléfono móvil 9 envía ahora un mensaje de solicitud de tique 14, que también contiene la clave pública PubK.OBU de la unidad de a bordo 7, a través de la red móvil 10 (y eventualmente otras redes de datos intermedias) a la central 2.

En la central 2 se genera un nuevo tique electrónico 3 y se provee, por ejemplo, con una identificación de tique TK unívoca, p. ej. una ID de transacción o un registro temporal. El tique 3 expedido se firma ahora en la central 2 con la clave de central privada PrivK.CS y se encripta con la clave de unidad de a bordo pública PubK.OBU recibida anteriormente en la solicitud del tique 14. El tique 3 firmado y encriptado, eventualmente junto con la clave de central pública PubK.CS, se envía de vuelta al teléfono móvil 9 a través de la red móvil 10 (etapa 18).

El teléfono móvil 9 envía el tique 3 recibido a través de la interfaz de red móvil 10, firmado y encriptado a través de la interfaz 8, preferiblemente a través de NFC, a la unidad de a bordo 7 (etapa 19). En la unidad de a bordo 7 se desencripta el tique 3 firmado y encriptado con la clave de unidad de a bordo privada PrivK.OBU (etapa 20). Opcionalmente el tique 3 ahora desencriptado, todavía firmado se puede validar con la ayuda de la clave de central pública PubK.CS, es decir, se verifica respecto a la autenticidad de la firma de la central 2 (etapa 21). Si falla la verificación, es decir, la firma no es auténtica y por ello el tique 3 no es válido, el tique 3 se puede rechazar y/o interrumpir el procedimiento.

A continuación la unidad de a bordo 7 encripta nuevamente el tique 3 desencriptado, firmado por la central y concretamente esta vez – en la forma de realización mostrada en la fig. 1 – con la clave de radiobaliza pública PubK.TRX (etapa 23). La clave de radiobaliza pública PubK.TRX puede haberse distribuido al comienzo del procedimiento en todas las unidades de a bordo 7 o la unidad de a bordo 7 solicita anteriormente en una etapa 22 la clave de radiobaliza pública PubK.TRX de la radiobaliza 4, en la que se querría canjear el tique 3, a través de la interfaz por radio DSRC 6. El tique 3 recién encriptado se envía a continuación a través de la interfaz DSRC 6 a la radiobaliza 4 para el canjeo (etapa 24).

En la radiobaliza 4 se desencripta el tique 3 recibido, firmado y recién encriptado con la clave de radiobaliza privada PrivK.TRX (etapa 25), y a continuación en la etapa 26 se verifica (valida) la autenticidad de su firma con la ayuda de la clave de central pública PubK.CS: cuando el tique 3 procede realmente de la central 2 (firma válida), entonces el tique 3 se canjea en una etapa 27. Según se debate el canjeo 27 puede tener como consecuencia una adquisición de mercancías o servicios correspondiente, una autorización de entrada, de tasa de aparcamiento o peaje o similares.

A este respecto, la clave de central pública PubK.CS se puede llevar consigo cada vez con el tique 3 en todas las etapas de transmisión 18, 19, 24 o alternativamente haberse transmitido una vez a través de la conexión 11 de la central 2 hacia la radiobaliza 4.

Se entiende que entre la recepción 19 del tique 3 firmado y encriptado por el teléfono móvil 9 en la unidad de a bordo 7 y el envío 24 del tique 3 recién encriptado y firmado de la unidad de a bordo 7 a la radiobaliza 27 que canjea el tique puede transcurrir algún tiempo, en el que el tique 3 está presente en la unidad de a bordo 7 y se transporta por ésta. A este respecto, en la unidad de a bordo DSRC 7 se realiza la desencriptación (etapa 20), la validación 21 (opcional) y el nuevo encriptación 23 en un entorno de hardware y/o software asegurado, por ejemplo, en un “trusted element” asegurado respecto al acceso de forma criptográfica y/o física en la unidad de a bordo 7, o la misma unidad de a bordo representa este “trusted element” digno de confianza. El sistema central 2 o los operadores del sistema telemático de transporte 1 pueden confiar en que el cambio de clave, es decir, la desencriptación y nueva encriptación del tique 3, se realiza correctamente en la unidad de a bordo 7. De este modo la expedición del tique de la central 2, el medio de comunicación de teléfono móvil 9 y la radiobaliza 4 que canjea el tique se desacoplan uno de otro en referencia a sus pares de claves correspondientes y no necesitan otras conexiones diferentes de las mencionadas; cuando también se prescinde del recorrido de datos 11 y la clave de central pública PubK.CS se transporta con el tique 3, en particular no hay una conexión directa entre central 2 que expide el tique y radiobaliza 4 que canjea el tique.

La fig. 2 muestra una forma de realización ligeramente modificada del procedimiento de la fig. 1. Las etapas 12 a 21

son iguales que en el procedimiento de la fig. 1. Para la nuevo encriptación del tique 3 en la unidad de a bordo 7, en esta forma de realización no se usa por el contrario la clave de radiobaliza pública PubK.TRX, sino la clave de central pública PubK.CS (etapa 28) y el tique 3 así firmado y encriptado se envía a través de la interfaz DSRC 6 a la radiobaliza 4 (etapa 29). En la radiobaliza 4, el tique 3 firmado y recién encriptado se desencripta ahora con la clave de central privada PrivK.CS (etapa 30) y luego se valida de nuevo la firma del tique 3 firmado con la ayuda de la clave de central pública PubK.CS (etapa 31), antes de que se realiza el canjeo (etapa 27).

La clave de central pública PubK.CS se puede transportar aquí de nuevo cada vez con el tique 3 o enviar una vez a través del recorrido de datos 11 de la central 2 a la radiobaliza 4. Además, la radiobaliza 4 también necesita aquí el conocimiento de la clave de central privada PrivK.CS, que se puede comunicar igualmente a través del recorrido de datos 11. Dado que la clave de central pública y la privada PubK.CS, PrivK.CS sólo se modifica raramente o no se modifica, aquí es suficiente una transmisión extraordinario o excepcional a través del recorrido de datos 11.

La fig. 3 muestra otra variante del procedimiento, en la que el tique 3 se introduce en primer lugar en un monedero electrónico 32 en la unidad de a bordo 7. Esta introducción puede consistir, por ejemplo, en la contabilización de una cantidad de dinero determinada en el monedero electrónico 32, en donde se puede tratar de un valor monetario estandarizado, predeterminado o un valor monetario que está indicado en el tique electrónico 3.

El procedimiento de la fig. 3 se desarrolla en las etapas 12 a 21 igual que en las fig. 1 y 2, en donde durante la expedición del tique 15 en la central 2 se provee el tique 3 en cualquier caso con una identificación TK unívoca, p. ej. una ID de transacción o un registro temporal. En la unidad de a bordo 7 está almacenada una lista 33 de identificaciones de tique TK de tiques electrónicos 3 recibidos hasta ahora y cada nuevo tique electrónico, que se intercala (19) de la central 2 a través del teléfono móvil 9 y la interfaz NFC 8 a la unidad de a bordo DSRC 7, en una etapa 34 se contraverifica respecto a su identificación de tique TK con la lista 33 de identificaciones de tique almacenadas: cuando la identificación de tique TK del tique electrónico 3 actual figura en la lista 33, luego el tique electrónico 3 ya se ha usado evidentemente una vez y se desecha o se interrumpe el procedimiento posterior. Cuando no está contenido en la lista 33, se introduce en el monedero electrónico 32 y simultáneamente la identificación de tique TK del tique electrónico 3 actual, recién canjeado se almacena en la lista 33 de identificaciones de tique almacenadas. El tique electrónico 3 se ha “consumido” por consiguiente.

Los tique 3 introducidos en el monedero electrónico 32, p. ej. en forma de un estado de saldo acumulado en su base del monedero electrónico 32, se pueden usar a continuación para llevar a cabo, por ejemplo, transacciones de tasas DSRC prepago convencionales con una radiobaliza 4, a fin de cargar o adeudar progresivamente el monedero electrónico 32 p. ej. mediante cada transacción DSRC a través de la interfaz DSRC 6. Alternativamente en la unidad de a bordo DSRC 7 se puede derivar del estado de saldo o el/los tique(s) 3 introducido(s) del monedero electrónico 32 uno o varios “nuevos” tiques electrónicos 3’, aquí también designado como tiques derivados 3’, que luego se pueden canjear según las variantes del procedimiento ilustradas en las fig. 1 y 2 (etapas 24 a 31) en una radiobaliza 4. A partir de un tique 3 introducido se pueden generar (derivar) así uno o varios tiques derivados 3’ a través del “buffer” del monedero electrónico 32, o a partir de uno o varios tiques 3 incorporados un tique derivado 3’.

Opcionalmente el tique 3, el estado de la cuenta del monedero electrónico 32 y/o el o los tique(s) derivado(s) 3’ se pueden firmar en la unidad de a bordo 7 con la clave de unidad de a bordo privada PrivK.OBU, sea para una transacción de peaje o tasa de aparcamiento DSRC convencionales o para la generación de tiques derivados 3’ firmados, que se canjean según las etapas 23 a 31 en una radiobaliza 4; la radiobaliza 4 que canjea puede validar luego la autenticidad de los tiques 3, 3’ mediante la clave de unidad de a bordo pública PubK.OBU.

La invención no está limitada a las formas de realización representadas, sino que comprende todas las variantes y modificaciones que están incluidas en el marco de las reivindicaciones conectadas.

REIVINDICACIONES

1. Procedimiento para la carga de una unidad de a bordo (7) con un tique electrónico (3) y canjeo del mismo o de un tique derivado del él (3') en una radiobaliza (4) de un sistema telemático de transporte (1), en donde la unidad de a bordo (7) tiene una interfaz DSRC (6) para la comunicación por radio con la radiobaliza (4) y una segunda interfaz (8) separada de la interfaz DSRC (6) para la comunicación por radio con un teléfono móvil (9), que comprende:

equipamiento de la unidad de a bordo (7) con una clave electrónica pública y una privada (PubK.OBU, PrivK.OBU) de la unidad de a bordo (7);

en el teléfono móvil (9), recepción (13) de la clave de unidad de a bordo pública (PubK.OBU) desde la unidad de a bordo (7),

en el teléfono móvil (9), envío (14) de un requerimiento de tique con la clave de unidad de a bordo pública (PubK.OBU) a través de una red móvil (10) a una central (2);

en la central (2), expedición (15) del tique (3),

en la central (2), encriptado (17) del tique con la clave de unidad de a bordo pública (PubK.OBU), y

en la central (2), envío (18) del tique (3) encriptado a la unidad de a bordo (7) a través de su segunda interfaz (8);

en el teléfono móvil (9), recepción de un tique (3) encriptado con la clave de unidad de a bordo pública (PubK.OBU) a través de la red móvil (10) de la central (2),

en el teléfono móvil (9), envío del tique (3) encriptado con la clave de unidad de a bordo pública (PubK.OBU) del teléfono móvil (9) a la unidad de a bordo (7);

en la unidad de a bordo (7), recepción del tique (3) encriptado con la clave de unidad de a bordo pública (PubK.OBU) a través de la segunda interfaz (8) de la unidad de a bordo (7),

en la unidad de a bordo (7), desencriptado (20) del tique (3) recibido con la clave de unidad de a bordo privada (PrivK.OBU), y

en la unidad de a bordo (7), envío (24) del tique (3) o de un tique derivado de él (3') a través de la interfaz DSRC (6) a la radiobaliza (4) para el canjeo.

2. Procedimiento según la reivindicación 1, **caracterizado porque** la segunda interfaz (8) es una interfaz inalámbrica, preferiblemente una interfaz NFC.

3. Procedimiento según la reivindicación 1 ó 2, **caracterizado porque** la radiobaliza (4) se equipa con una clave electrónica pública y una privada (PubK.TRX, PrivK.TRX) de la radiobaliza (4) y **porque** en la unidad de a bordo (7), el tique (3) desencriptado o el tique derivado de él (3') se encripta nuevamente (23) con la clave de radiobaliza pública (PubK.TRX) antes del envío a la radiobaliza (4).

4. Procedimiento según la reivindicación 3, **caracterizado porque** en la radiobaliza (4) se desencripta (25) el tique (3) o tique derivado (3') con la clave de radiobaliza privada (PrivK.TRX).

5. Procedimiento según la reivindicación 1 ó 2, **caracterizado porque** la radiobaliza (4) se equipa con una clave electrónica pública y una privada (PubK.CS, PrivK.CS) de la central (2) del sistema telemático de transporte (1) y **porque** en la unidad de a bordo (7), el tique (3) desencriptado o el tique derivado de él (3') se encripta nuevamente (23) con la clave de central pública (PubK.CS) antes del envío a la radiobaliza (4).

6. Procedimiento según la reivindicación 5, **caracterizado porque** en la radiobaliza (4) se desencripta (25) el tique (3) o tique derivado (3') con la clave de central privada (PrivK.CS).

7. Procedimiento según una de las reivindicaciones 1 a 6, que comprende además en la central (2) del sistema telemático de transporte (1), central equipada con una clave electrónica pública y una privada (PubK.CS, PrivK.CS):

firma (16) del tique con la clave de central privada (PrivK.CS).

8. Procedimiento según la reivindicación 7, **caracterizado porque** en la unidad de a bordo (7) se valida (21) el tique (3) con la ayuda de la clave de central pública (PubK.CS) y sólo luego, cuando es válido, el tique (3) o tique derivado de él (3') se envía (24, 29) a la radiobaliza (4) para el canjeo.

9. Procedimiento según la reivindicación 7 u 8, **caracterizado porque** en la radiobaliza (4) se valida (26) el tique (3) o tique derivado de él (3') con la ayuda de la clave de central pública (PubK.CS) y sólo luego, cuando es válido, se canjea.

10. Procedimiento según una de las reivindicaciones 7 a 9, **caracterizado porque** la clave de radiobaliza pública o

clave de central pública (PubK.TRS, PubK.CS) se envía (22) de la radiobaliza (4) a través de la interfaz DSRC (6) a la unidad de a bordo (7).

11. Procedimiento según una de las reivindicaciones 7 a 10, **caracterizado porque** la clave de central pública (PubK.CS) se envía (18, 19, 24, 29) cada vez junto con el tique (3) o tique derivado (3').

12. Procedimiento según una de las reivindicaciones 7 a 11, **caracterizado porque** en el central (2) el tique (3) se provee de una identificación (TK) unívoca y **porque** en la unidad de a bordo (7) se verifica si la identificación (TK) de un tique (3) recibido está contenido en una lista (33) de identificaciones (TK) almacenadas y sólo luego, cuando no está contenida, el tique (3) o tique derivado de él (3') se envía a la radiobaliza (4) para el canjeo.

13. Procedimiento según la reivindicación 12, **caracterizado porque** el tique se introduce en la unidad de a bordo en un monedero electrónico (32) de la unidad de a bordo (7), en donde preferiblemente el tique derivado (3') luego se deriva de él.

14. Procedimiento según la reivindicación 13, **caracterizado porque** en la unidad de a bordo (7) se valida (21) la firma del tique (3) con la ayuda de la clave de central pública (PubK.CS) y sólo luego, cuando ésta es válida, el tique (3) se introduce en el monedero electrónico (32).

15. Procedimiento según una de las reivindicaciones 12 a 14, **caracterizado porque** la identificación (TK) unívoca es un registro temporal.

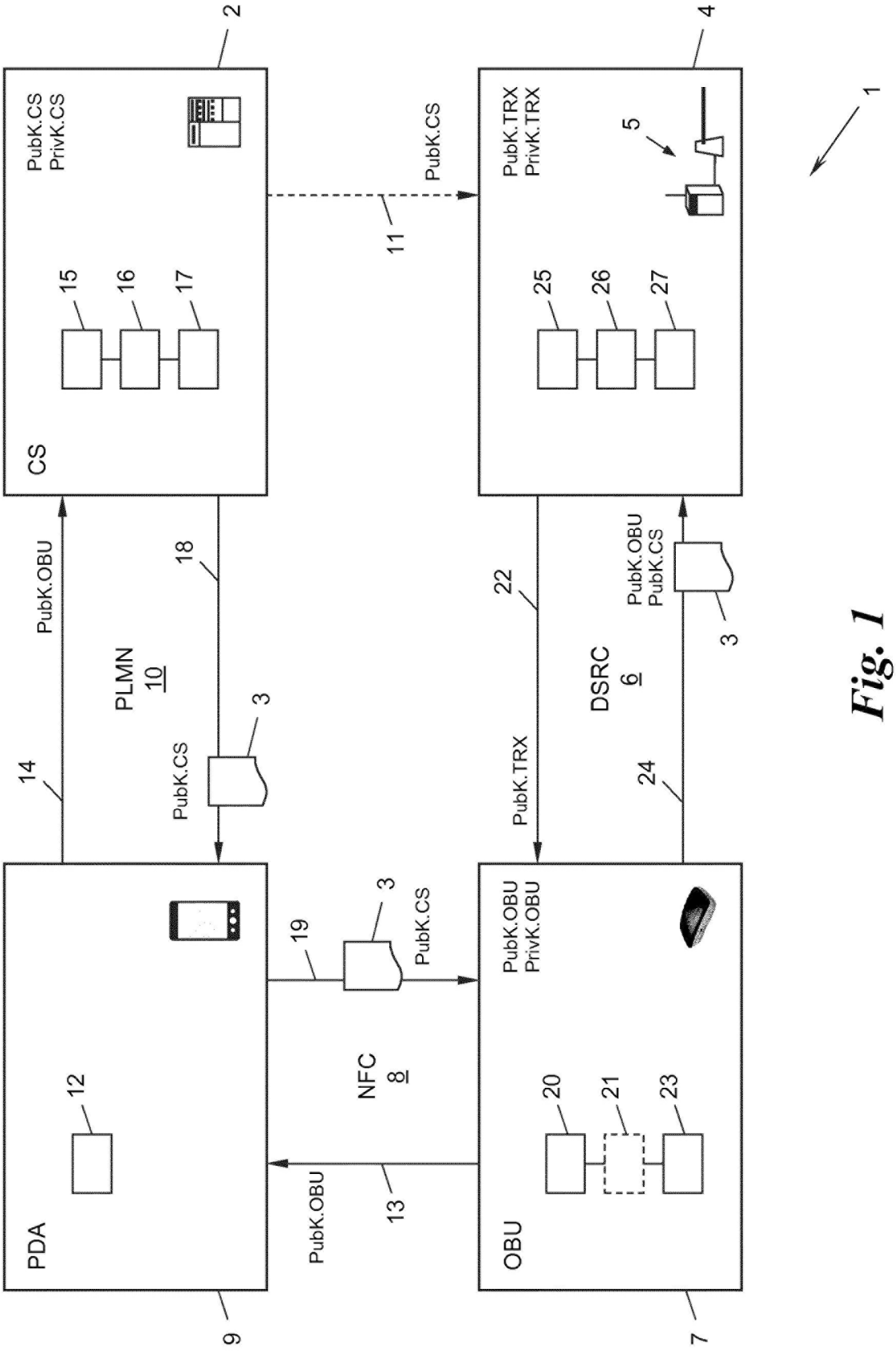
2
4
1
PubK.CS
PrivK.CS
PubK.CS
PubK.TRX
PrivK.TRX
5
11
15
16
17
25
26
27
CS
PubK.OBU
18
22
PubK.OBU
PubK.CS
PLMN
10
DSRC
6
3
3
14
PubK.CS
PubK.TRX
24
19
3
PubK.CS
PubK.OBU
PrivK.OBU
NFC
8
12
20
21
23
PDA
PubK.OBU
13
OBU
9
7

Fig. 1

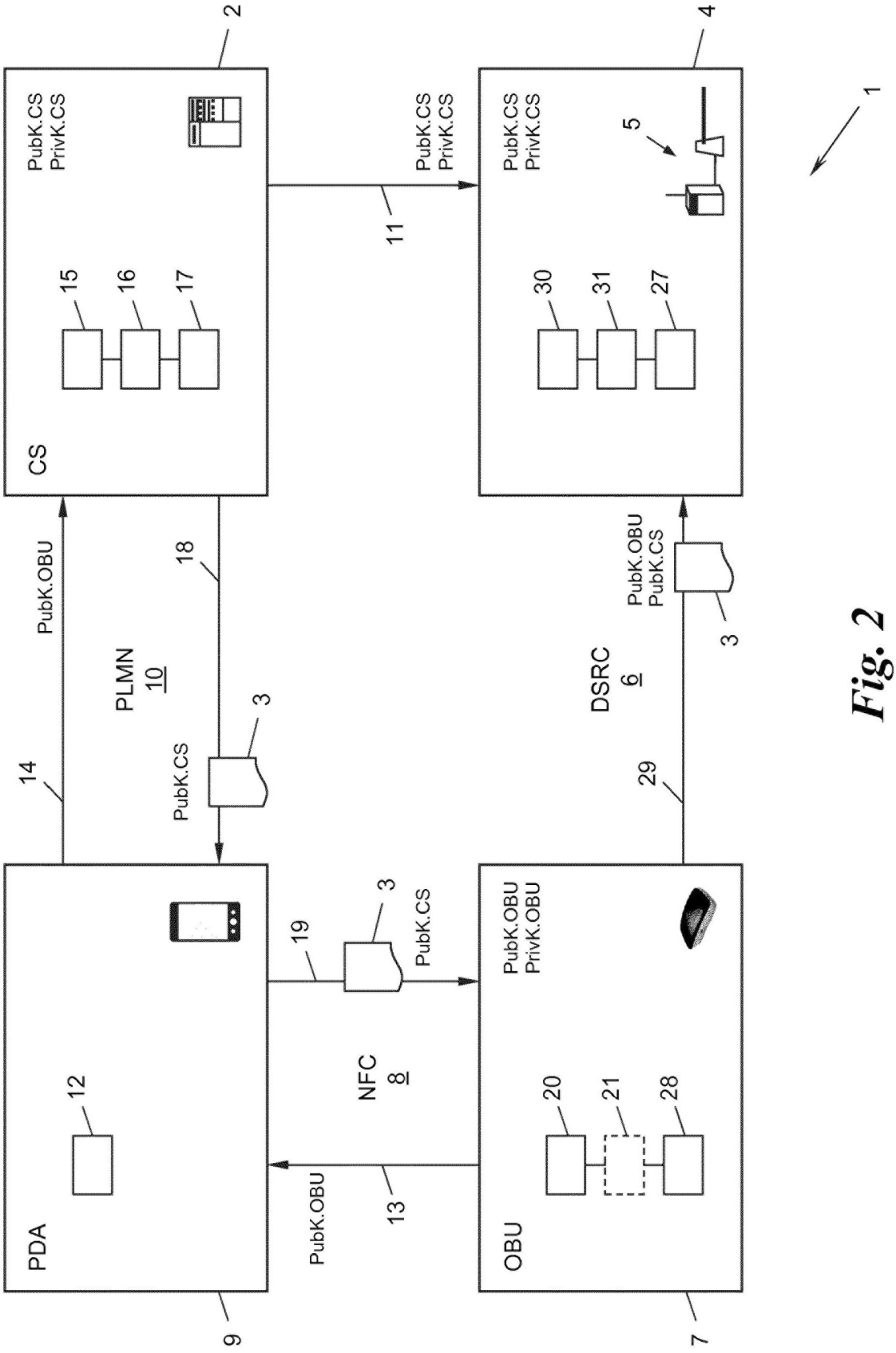
2
4
1
PubK.CS
PrivK.CS
5
11
15
16
17
30
31
27
CS
PLMN
10
DSRC
6
PubK.OBU
18
PubK.OBU
PubK.CS
3
14
29
PubK.CS
19
PubK.OBU
PrivK.OBU
12
NFC
8
20
21
28
PDA
OBU
PubK.OBU
13
9
7

Fig. 2

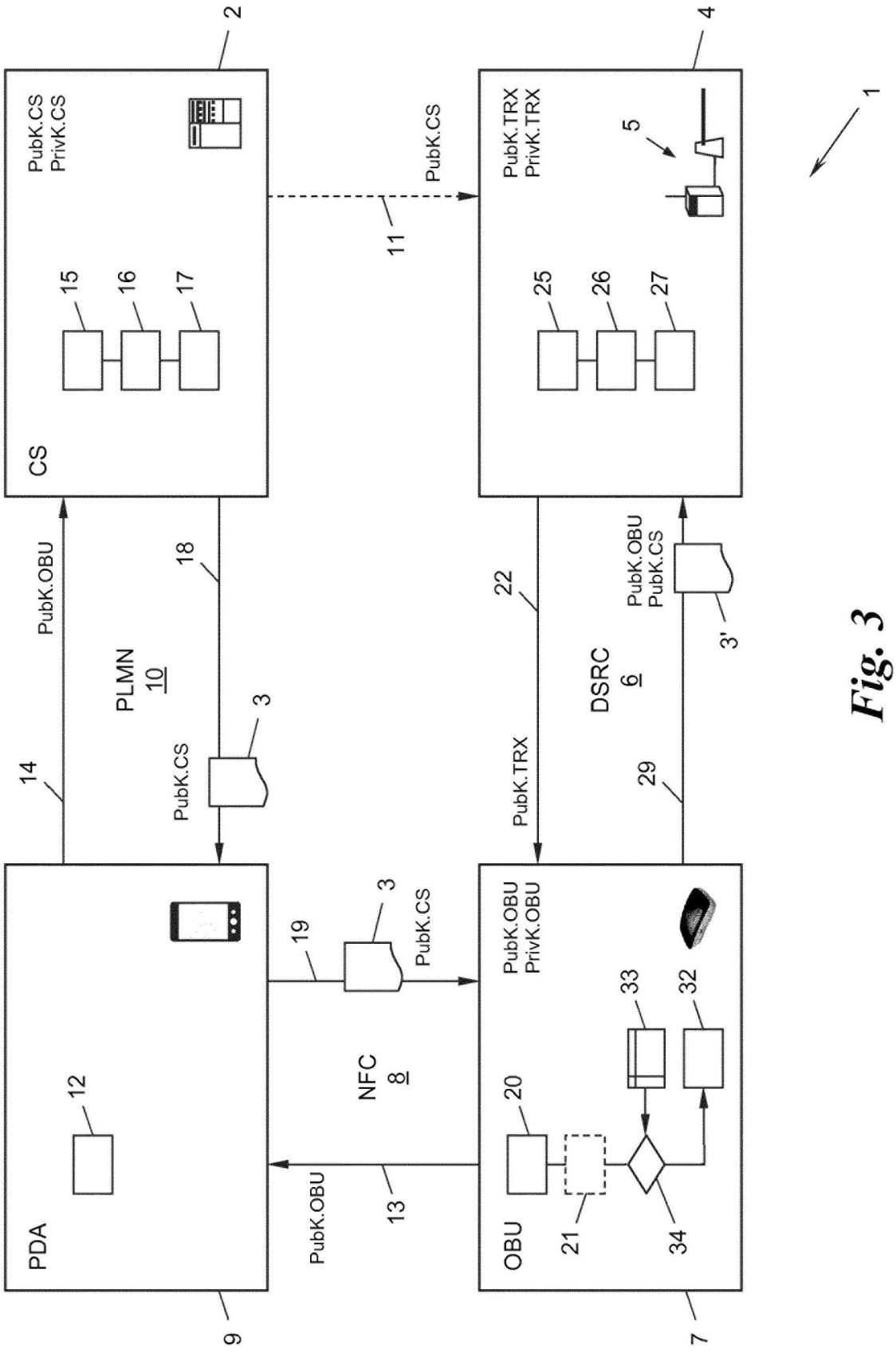
2
4
1
PubK.CS
PrivK.CS
PubK.CS
PubK.TRX
PrivK.TRX
5
11
15
16
17
25
26
27
CS
PubK.OBU
18
22
PubK.OBU
PubK.CS
PLMN
10
DSRC
6
3'
14
PubK.CS
3
PubK.TRX
29
19
3
PubK.CS
PubK.OBU
PrivK.OBU
33
32
NFC
8
12
20
PubK.OBU
13
21
34
PDA
OBU
9
7

Fig. 3