(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 587 283**

(51) Int. Cl.:

H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04N 21/214 (2011.01)
B64D 11/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.08.2012** **PCT/EP2012/066756**

(87) Fecha y número de publicación internacional: **06.03.2014** **WO14032707**

(96) Fecha de presentación y número de la solicitud europea: **29.08.2012** **E 12753715 (7)**

(97) Fecha y número de publicación de la concesión europea: **18.05.2016** **EP 2891289**

(54) Título: **Método y sistema para asociar contenidos de información**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.10.2016

(73) Titular/es:

SIEMENS CONVERGENCE CREATORS GMBH (100.0%)
Autokaderstrasse 29
1210 Wien, AT

(72) Inventor/es:

SCHREIBER, GERALD

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

ES 2 587 283 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Método y sistema para asociar contenidos de información

Área técnica

La presente invención hace referencia a un método para asociar contenidos de información en un medio de transporte, en particular en un avión. Los contenidos de información, en el medio de transporte, por ejemplo durante un viaje, son visualizados en una unidad de salida generalmente móvil, específica del usuario, como por ejemplo smartphones, ordenadores portátiles, tablets, etc. y son consumidos por un usuario de la unidad de salida. La presente invención hace referencia además a un sistema para ejecutar el método para asociar contenidos de información.

Estado del arte

En los medios de transporte de pasajeros, como por ejemplo aviones, trenes, autobuses o también barcos, actualmente se instalan sistemas de información. Mediante los sistemas de información mencionados, denominados también como sistemas de información y entretenimiento, pueden por ejemplo transmitirse datos hacia unidades de salida con el fin de informar y/o de entretener. Mediante los sistemas de información de esa clase, conocidos por ejemplo por la solicitud US 2005/0216938 A1, durante la utilización del respectivo medio de transporte (por ejemplo avión, barco, tren, etc.), a los pasajeros se proporcionan por ejemplo ofertas de información y/o programas de entretenimiento. Las unidades de salida para visualizar y consumir los contenidos de información pueden estar instaladas de forma fija en el medio de transporte por ejemplo como pantallas de salida o unidades de salida específicas del usuario (por ejemplo ordenador portátil, tablet, smartphone, etc.), que son puestas a disposición del pasajero o que son llevadas por el mismo en el medio de transporte.

Los sistemas de información - en particular en aviones - se han perfeccionado mucho en los últimos 25 años. En un inicio, esos sistemas estaban compuestos solamente por sistemas de audio, mediante los cuales a los pasajeros se les ofrecía información de audio y/o de datos de audio (por ejemplo música). A partir de los años '80, los sistemas de información se ampliaron a emisiones de información en video (por ejemplo cintas de video VHS), donde los contenidos de información podían verse por ejemplo mediante pantallas en grupo en la cabina del avión, etc. Desde los primeros años de la década del '90, los sistemas de información se ampliaron a los así llamados sistemas con pantallas individuales, donde por ejemplo videos, música u otra información podía ser seleccionada por un usuario en una pantalla perteneciente al asiento o en dispositivos de salida, mediante un dispositivo de mando, donde dicha información se visualizaba en el dispositivo de salida. Con el paso del tiempo, en particular en los vuelos, comenzó a proporcionarse a los pasajeros la así llamada infotainment - es decir, contenidos de información, como por ejemplo información sobre el vuelo en tiempo real, datos de video (por ejemplo noticias, películas), datos de audio, etc., con el fin de informar y de entretener - en unidades de salida específicas del usuario (por ejemplo tablets, smartphones, ordenadores portátiles, etc.). Las unidades de salida pueden ser puestas a disposición por la compañía operadora del medio de transporte o como unidad de salida se utilizan dispositivos móviles del pasajero. Junto con los aviones existen también otros medios de transporte, como por ejemplo barcos, trenes, autobuses, etc. que ofrecen a los pasajeros o viajeros contenidos de entretenimiento y/o de información.

En los aviones, los sistemas de información comprenden generalmente una unidad de servidor central desde la cual se comunica por ejemplo con unidades de salida, desde la cual se procesan entradas de pasajeros y la cual se encarga de una distribución de los contenidos de información. Generalmente, de manera adicional, se proporciona un sistema de datos que pertenece al sistema de información, en donde están almacenados por ejemplo contenidos de información (por ejemplo datos de video y/o de audio), y donde eventualmente pueden guardarse otros datos (por ejemplo datos de unidades de salida, etc.). Los contenidos de información seleccionados, por ejemplo mediante el así llamado streaming (emisión en directo), pueden ser transmitidos a las unidades de salida específicas del usuario, como por ejemplo a dispositivos de salida (tablet, smartphone, etc.) llevados por los pasajeros. Sin embargo, para ello, junto con un punto de acceso mediante el cual una unidad de salida puede establecer una conexión inalámbrica hacia el sistema de información del medio de transporte, es necesario un así llamado servidor de streaming, para una transmisión y salida de los contenidos de información (por ejemplo datos de audio y/o de video). Además, en ese servidor de streaming deben ser cargados nuevos contenidos de información actuales por la respectiva compañía operadora del medio de transporte. Lo mencionado exige ante todo una elevada inversión logística y una infraestructura generalmente costosa y de alta gama dentro del medio de transporte (por ejemplo dentro del avión). Además, para una actualización continua de los contenidos de información es necesaria una extensa cantidad de datos que debe ser transferida al servidor de streaming.

Sin embargo, para proporcionar a los pasajeros contenidos de información actuales, existe también la posibilidad de que una compañía operadora de un medio de transporte (por ejemplo una aerolínea, una compañía ferroviaria, etc.) ponga a disposición a modo de préstamo, de forma gratuita, o a cambio de un pago, unidades de salida, como por ejemplo tablets. En esas unidades de salida pueden estar cargados por ejemplo contenidos de información actuales (por ejemplo datos de video, películas, libros electrónicos). Al ser usada una unidad de salida durante la utilización

de un medio de transporte, un pasajero puede seleccionar contenidos de información actuales cargados previamente en los contenidos de salida. Los contenidos de información seleccionados pueden ser reproducidos en la unidad de salida, así como pueden ser visualizados por el usuario. Sin embargo, la utilización de unidades de salida con contenidos de información cargados previamente en la unidad de salida, presenta la desventaja de que es necesaria una elevada inversión logística, así como una cantidad correspondiente de unidades de salida. A modo de ejemplo, los contenidos de información deben ser cargados en las unidades de salida y deben ser actualizados. Generalmente, también las baterías de los dispositivos deben ser cargadas entre dos salidas. En particular, para una actualización de los contenidos de información son necesarias también extensas cantidades de datos que deben estar disponibles en una infraestructura correspondiente para cargar las unidades de salida.

Otra posibilidad para una utilización de contenidos de información dentro de un medio de transporte o viajando con dicho medio, consiste en vender contenidos de información (por ejemplo datos de video, libros electrónicos, etc.) a un usuario o pasajero. Dichos contenidos de información pueden ser cargados para el pasajero antes de un viaje en el respectivo dispositivo de salida (por ejemplo tablet, ordenador portátil, etc.). El pasajero puede llevar el dispositivo de salida en el medio de transporte y consumir allí el contenido de información previamente adquirido y cargado. Sin embargo, lo mencionado presenta la desventaja de elevados costes para adquirir una copia personal, no limitada temporalmente, de los contenidos de información. Esos costes resultan más elevados para el pasajero antes de la utilización del medio de transporte, donde los mismos son más reducidos en otro momento que durante la utilización del medio de transporte. Otra desventaja consiste en la escasa disponibilidad de nuevos contenidos de información actuales cuando los contenidos adquiridos o cargados han sido utilizados.

Descripción de la invención

Es objeto de la presente invención proporcionar un método, así como un sistema, a través del cual se posibilite un acceso a contenidos de información actuales en un medio de transporte, en especial en un avión, sin una gran inversión, así como sin una logística y/o infraestructura costosa y con una seguridad elevada.

Dicho objeto se alcanzará a través de un método, así como de un sistema de la clase mencionada en la introducción con las características según las reivindicaciones independientes. En las reivindicaciones dependientes se indican formas de ejecución ventajosas de la presente invención.

De acuerdo con la invención, el objeto se alcanzará mediante un método de la clase mencionada, en donde a cada medio de transporte - por ejemplo a cada avión, barco, etc. de una compañía operadora - mediante un primer par de claves que se compone de una primera clave secreta y de una primera clave pública, se asocia un servidor a bordo. La primera clave secreta es almacenada en el servidor a bordo. Antes de la utilización del medio de transporte, una aplicación se instala en una unidad de salida móvil, específica del usuario, y un segundo par de claves, compuesto por una segunda clave secreta y una segunda clave pública, es solicitado por la aplicación. La segunda clave secreta es transmitida a la aplicación en la unidad de salida, identificando de forma unívoca con ello por ejemplo la unidad de salida, así como a un pasajero. A continuación, los contenidos de información disponibles son visualizados por la aplicación. Para cada contenido de información seleccionado se crea una identificación única, mediante la cual los contenidos de información seleccionados son solicitados por la aplicación en la unidad de salida. De este modo, a la identificación única se asocia un tercer par de claves, con una tercera clave secreta y una tercera clave pública. Después, la tercera clave secreta se cifra con la segunda clave pública que está asociada a la unidad de salida, así como al pasajero y, seguidamente, con la primera clave pública a través de la cual se conoce el servidor a bordo correspondiente, y se asocia al servidor a bordo correspondiente del medio de transporte, así como se almacena en el mismo. Después, los contenidos de información seleccionados, cifrados con la tercera clave pública, son transmitidos a la unidad de salida y son almacenados allí.

El aspecto principal de la solución propuesta acorde a la invención, reside en el hecho de que los contenidos de información cifrados son transmitidos temporalmente separados de la (tercera) clave secreta necesaria para el descifrado. Un cifrado y una transmisión de los contenidos de información a la unidad de salida específica del usuario tienen lugar antes de una utilización del medio de transporte. Debido a ello, algoritmos de cifrado potentes y parcialmente también intensivos en cuanto al tiempo de cálculo pueden utilizarse para proteger los contenidos de información. Además, el cifrado de los contenidos de información tiene lugar en base a una identificación única que se asigna a un contenido de información seleccionado, de forma individual por usuario, donde la identidad del usuario, por ejemplo debido a una reserva - es conocida en particular mediante el segundo par de claves utilizado. De este modo, un robo de contenidos de información actuales, en particular legalmente protegidos (por ejemplo películas, libros electrónicos, etc.) puede comprobarse con mucha facilidad. De este modo, y debido a una utilización de algoritmos de cifrado seguros, el método acorde a la invención presenta una seguridad elevada.

La clave secreta para descifrar los contenidos de información se almacena con un doble cifrado en el servidor a bordo. Puesto que el servidor a bordo sólo proporciona claves no se necesita un rendimiento especial del ordenador para el servidor a bordo y, antes de una utilización del servidor a bordo durante un funcionamiento del medio de transporte, sólo deben cargarse posteriormente las claves necesarias correspondientes - es decir, las claves que se necesitan para contenidos de información que fueron seleccionadas por pasajeros. De este modo, tanto la inversión

para infraestructura, o la inversión en cuanto al hardware para el servidor a bordo, así como la inversión logística, continúa siendo reducida. Por ejemplo, para la carga posterior de las claves, debido a un ancho de banda requerido para ello y a una cantidad de datos, puede ser utilizada una conexión de telefonía móvil. Una transmisión de los contenidos de información extensos es realizada ya antes del uso del medio de transporte, por ejemplo por el pasajero, en la unidad de salida, donde las redes de comunicación pueden ser utilizadas con costes reducidos y con una velocidad de transferencia correspondiente (por ejemplo Internet, etc.). De este modo, se ponen a disposición de los pasajeros ofertas esencialmente más actuales y extensas de contenidos de información que en comparación con la utilización de por ejemplo un servidor a bordo del medio de transporte.

En el caso de una utilización del medio de transporte, de manera ideal, desde la unidad de salida específica del usuario se establece una conexión hacia el servidor a bordo. Antes de reproducir el contenido de información seleccionado, la tercera clave secreta que está almacenada en el servidor a bordo, es descifrada con la primera clave secreta que se encuentra en el servidor a bordo. A continuación, la tercera clave secreta cifrada aún con la segunda clave pública es transmitida desde el servidor a bordo en la aplicación hacia la unidad de salida, y allí es descifrada con la segunda clave secreta. Seguidamente, el contenido de información seleccionado que se encuentra en la unidad de salida se descifra con la tercera clave secreta y puede ser visualizado. A través de una transmisión de la tercera clave secreta necesaria para descifrar los contenidos de información seleccionados una vez comenzada la utilización del medio de transporte, una utilización ilegal de los contenidos de información se impide de forma sencilla. A través del primer y del segundo par de claves se asegura que la tercera clave secreta que se encuentra asociada a la identificación única del contenido de información seleccionado mediante el tercer par de claves, se encuentra disponible en el servidor a bordo correspondiente de aquel medio de transporte en el cual se encuentra también el pasajero, así como la unidad de salida correspondiente, que puede identificarse mediante el segundo par de claves, con los contenidos de información cifrados. Los contenidos de información pueden ser consumidos durante la utilización del medio de transporte y, de manera sencilla y sin una gran inversión, se impide un uso ilegal, así como un robo de los contenidos de información.

Se considera ventajoso que una asociación entre el servidor a bordo, la unidad de salida específica del usuario, contenidos de información seleccionados y/o el primer, el segundo y el tercer par de claves, sea almacenada en un banco de datos de inventario. Mediante un almacenamiento de esa asociación en el banco de datos de inventario, una compañía operadora del medio de transporte puede rastrear en qué medio de transporte y por qué pasajero han sido utilizados o son utilizados contenidos de información. De este modo, de forma muy sencilla y sin una gran inversión, es posible rastrear un robo o una utilización ilegal (por ejemplo un copiado ilegal, etc.). Asimismo, se considera conveniente que después de la instalación de la aplicación y de una transmisión de la segunda clave secreta en la aplicación, un registro de datos con información sobre una utilización del medio de transporte se transmita a la unidad de salida o a un pasajero. De este modo, desde la compañía operadora del medio de transporte (por ejemplo una compañía operadora de una aerolínea) a un pasajero en el registro de datos puede transmitirse una descripción sobre su viaje con el medio de transporte, así como una descripción unívoca sobre el mismo. El registro de datos mencionado, a modo de ejemplo, puede ser transmitido mediante un correo electrónico que eventualmente está cifrado y/o marcado, a un mensaje, por ejemplo a un número de llamada guardado al realizar una reserva, conocido por la compañía operadora o, por ejemplo en el caso de un vuelo, mediante un así llamado pasaporte de abordaje. Una aceptación del registro de datos puede tener lugar por ejemplo de forma automática a través de la aplicación en la unidad de salida específica del usuario o después de su instalación o de su inicio, mediante ese registro de datos, puede verificarse con facilidad si el usuario de la unidad de salida ha sido reservado como para pasajero para una utilización adecuada de un medio de transporte (por ejemplo vuelo, viaje en tren, etc.).

En un perfeccionamiento preferente del método acorde a la invención se prevé que los pares de claves sean generados por un servidor de claves. Además, se considera ventajoso que las claves públicas, en especial la primera y la segunda clave pública del primer y del segundo par de claves, sean almacenadas en un banco de datos de claves. De este modo, de manera sencilla, una creación de los pares de claves, así como de las claves, puede tener lugar de forma centralizada. También el almacenamiento o el almacenamiento intermedio para las claves públicas, en particular para aquellas claves públicas que se utilizan para cifrar la tercera clave secreta, puede realizarse de forma centralizada. Debido a ello, la inversión para la infraestructura, así como para logística, se reduce con facilidad.

En una variante ventajosa del método acorde a la invención se prevé que después de abandonar el medio de transporte la clave secreta, así como todos los contenidos de información seleccionados, sean borrados por la unidad de salida. A través de un borrado de los contenidos de información seleccionados se impide de forma sencilla una utilización ilegal, aumentado la seguridad, así como la protección, para los contenidos de información. Borrando las claves secretas a través del servidor a bordo, así como del servidor de claves, después de finalizar la utilización del medio de transporte, se impide adicionalmente una utilización y/o un acceso a los contenidos de información cifrados después de abandonar el medio de transporte o después de finalizado un viaje. De manera alternativa, a modo de ejemplo, las claves secretas pueden ser borradas por el servidor ya después de una transmisión confirmada - en el caso de la primera y de la tercera clave secreta en el servidor a bordo, y en el caso de la segunda clave secreta en la aplicación en la unidad de salida específica del usuario. Eventualmente, un borrado de los

contenidos de información seleccionados y de las claves secretas puede tener lugar con una demora temporal, para considerar retrasos o demoras que se produzcan de forma eventual durante el período de utilización del medio de transporte.

Se considera ventajoso que una identificación única sea adjudicada para cada contenido de información seleccionado por un servidor de catálogo. A través del servidor de catálogo, los contenidos de información disponibles pueden ser administrados centralmente de forma sencilla y pueden ser visualizados por la aplicación en la unidad de salida específica del usuario. A través de una adjudicación central de las identificaciones para un contenido de información seleccionado, el mismo puede ser asociado de forma unívoca a un determinado uso de un medio de transporte (por ejemplo vuelo, viaje en tren, etc.), así como a un pasajero.

En el caso de un perfeccionamiento preferente del método acorde a la invención, el tercer par de claves es generado al momento de una selección del contenido de información. De este modo, los pares de claves para el cifrado de contenidos de información son generados sólo en caso necesario y la cantidad de dichos pares de claves se mantiene reducida. El par de claves puede ser asociado de forma muy sencilla y unívoca al contenido de información seleccionado, así como a la respectiva identificación única correspondiente.

De manera alternativa, sin embargo, también puede ser ventajoso que una cantidad de terceros pares de claves sean generados previamente a la formación de una cantidad de reserva y que después sean transmitidos al servidor a bordo. De este modo, al momento de seleccionar un contenido de información, un tercer par de claves se extrae de la cantidad de reserva y entonces a ese tercer par de claves se asocia una identificación única del contenido de información seleccionado. El procedimiento mencionado presenta la ventaja de que los contenidos de información pueden ser seleccionados aún a muy corto plazo antes de una utilización de un medio de transporte, por ejemplo después de una transmisión de las claves en el servidor a bordo. Una transmisión de la tercera clave secreta (para descifrar el contenido de información seleccionado) tiene lugar previamente simplemente de forma cifrada con la primera clave pública que está asociada al servidor a bordo. La retransmisión de la tercera clave secreta a la unidad de salida es realizada por el servidor a bordo durante la utilización del medio de transporte, por ejemplo mediante un procedimiento seguro, por ejemplo mediante la segunda clave pública o mediante Secure Socket Layer (SSL, capa de puertos seguros).

De manera ideal, los contenidos de información seleccionados son marcados durante un cifrado. Un marcado de esa clase puede efectuarse por ejemplo de forma completamente visible, por ejemplo a través de una así llamada marca de agua o signo de agua, de forma audible o cubierta a través de una así llamada marca de agua forense o de un signo de agua digital en la señal de imagen, de video y/o acústica. Una marca de agua digital consiste en un marcado técnico en medios soporte, como por ejemplo datos de imagen, de video o de audio, o en textos referidos a la empresa y por lo general no perceptibles. Por consiguiente, una marca de agua digital se utiliza por ejemplo para introducir información del propietario de un derecho para un rastreo de violaciones de derechos de creación de una empresa. A modo de ejemplo, con las marcas de agua digitales puede verificarse con gran facilidad la autenticidad de un archivo y asegurar su rastreabilidad.

Además, el objeto se alcanzará a través de un sistema de la clase mencionada en la introducción, en donde se proporcionan un servidor a bordo para establecer una conexión con una unidad de salida específica del usuario, como por ejemplo una tablet, un smartphone, un ordenador portátil, etc., dentro de un medio de transporte, una aplicación que puede instalarse en la unidad de salida específica del usuario, un servidor de claves y un banco de datos de claves para generar y almacenar pares de claves - compuestos por una clave secreta y una clave pública - así como la clave y un servidor de catálogo para solicitar una oferta de contenidos de información disponibles y para otorgar identificaciones únicas para contenidos de información seleccionados. Además, el sistema acorde a la invención comprende un servidor de cifrado para cifrar contenidos de información seleccionados, un banco de datos de inventario para almacenar asociaciones entre el servidor a bordo, la unidad de salida específica del usuario, contenidos de información seleccionados y/o pares de claves respectivamente correspondientes, así como un banco de datos de información para almacenar contenidos de información disponibles y que pueden ser seleccionados. Además, al menos una red de comunicaciones se proporciona respectivamente para una comunicación dentro y para una comunicación fuera del medio de transporte.

El aspecto principal del sistema acorde a la invención reside en el hecho de que tiene lugar una separación entre una transmisión de los contenidos de información cifrados seleccionados y una transmisión de las claves correspondientes para un descifrado. A través de una estructura del sistema en un servidor a bordo, en donde se almacenan solamente las claves correspondientes - una primera clave secreta, que identifica el servidor a bordo, y una tercera clave secreta para descifrar los contenidos de información -, una aplicación que puede instalarse en una unidad de salida específica del usuario y que se encarga de una comunicación con los otros componentes del sistema, y unidades centrales del servidor y del banco de datos para regenerar y almacenar claves, para administrar los contenidos de información, etc., en particular la infraestructura, así como el hardware para una utilización de contenidos de información durante el uso de un medio de transporte, se mantiene de forma sencilla y conveniente en cuanto a los costes. Además, a través del sistema acorde a la invención los contenidos de información seleccionados pueden ser cifrados de forma segura y pueden ser asociados de forma unívoca a una utilización

determinada de un medio de transporte (por ejemplo de un avión, etc.) y a un pasajero correspondiente, debido a lo cual se dificulta o se impide un robo y/o una utilización ilegal de los contenidos de información. Además, en el caso de un sistema por fuera del medio de transporte, existe la posibilidad de poner a disposición una oferta de contenidos de información esencialmente mayor que en el caso de un servidor streaming o de un sistema streaming dentro del medio de transporte, ya que por fuera del medio de transporte puede utilizarse un sistema con una capacidad de almacenamiento esencialmente más grande.

Se considera ventajoso que el servidor de claves, el servidor de catálogo y el servidor de cifrado en un servidor y/o en un servidor y/o en un banco de datos de claves, en un banco de datos de inventario y en un banco de datos de información estén agrupados en un banco de datos. De este modo, pueden reducirse con mucha facilidad los costes para infraestructura, así como para el hardware.

De manera ideal, el servidor a bordo está realizado como una unidad móvil. De este modo, es posible que el servidor a bordo esté realizado como un dispositivo móvil, operado mediante batería, el cual se activa una vez iniciada la utilización en un medio de transporte - es decir, durante un vuelo o un viaje en tren, etc. De este modo, de manera ventajosa, durante la utilización en aviones no se requiere una aprobación aeronáutica, así como en el caso de una utilización en un tren no se requiere ninguna aprobación relativa a la tecnología ferroviaria, ya que el servidor a bordo no está conectado al medio de transporte. Además, a modo de ejemplo, el servidor a bordo - en correspondencia con la asociación a través del primer par de claves - puede ser utilizado de forma flexible en diferentes medios de transporte de la compañía operadora.

Sin embargo, también es posible que el servidor a bordo esté realizado como módulo de software. De este modo, el servidor a bordo puede ser utilizado con facilidad en instalaciones ya existentes que presentan sólo muy pocas memorias y/o recursos de procesamiento (por ejemplo unidad de cálculo, etc.), así como por ejemplo así llamados sistemas de conectividad, servidores web locales, etc.

De forma alternativa, también existe la posibilidad de que el servidor a bordo no esté colocado a bordo del medio de transporte, sino por fuera, en los componentes restantes del servidor y del banco de datos del sistema. De este modo, una comunicación con la unidad de salida durante la utilización del medio de transporte (por ejemplo vuelo, viaje en tren, etc.) puede tener lugar por ejemplo mediante el así llamado sistema de conectividad o, a modo de ejemplo, la tercera clave secreta para descifrar los contenidos de información seleccionados es transmitida inmediatamente antes de la utilización del medio de transporte - por ejemplo inmediatamente antes de la salida del avión, por ejemplo al registrarse o al abordar. Eventualmente, puede realizarse una determinación de la posición de la unidad de salida, para determinar si la misma se encuentra cerca del medio de transporte (por ejemplo en las puertas de embarque, en el caso de un avión, etc.). Debido a ello, la infraestructura en el medio de transporte se mantiene reducida y, de forma adicional, se asegura que el contenido de información no sea utilizado por personas no autorizadas.

Breve descripción del dibujo

A modo de ejemplo, la presente invención se explicará a continuación mediante la figura añadida. La figura muestra:

Figura 1: a modo de ejemplo y de forma esquemática, el sistema acorde a la invención, así como el desarrollo del método acorde a la invención para asociar contenidos de información.

Ejecución de la invención

La figura 1, a modo de ejemplo y de forma esquemática, muestra el sistema acorde a la invención para asociar contenidos de información IN que pueden ser visualizados y consumidos durante la utilización de un medio de transporte BF, como por ejemplo un avión, pero también en un tren, un barco o un autobús, en una unidad de salida específica del usuario AE (por ejemplo una tablet, un smartphone, un ordenador portátil, etc.). El sistema comprende varios componentes, de modo ideal, realizados de forma centralizada. Los componentes mencionados se tratan de al menos un servidor de claves EKS, un servidor de catálogo MCS y un servidor de cifrado MES que pueden estar realizados como servidores particulares o pueden estar reunidos en un servidor común. Además, como componentes se proporcionan al menos un banco de datos de claves KDB, un banco de datos de información MDB, así como un banco de datos de inventario IDB, que igualmente pueden estar realizados como bancos de datos particulares o pueden estar reunidos en un banco de datos.

El servidor de claves EKS, así como el banco de datos de claves KDB, se utilizan para generar y almacenar pares de claves (Sg1, Sp1, Sg2, Sp2, Sg3, Sp3) que respectivamente se componen de una clave secreta (Sg1, Sg2, Sg3) y de una clave pública (Sp1, Sp2, Sp3). En el banco de datos de información MDB están almacenados contenidos de información IN actuales disponibles para usuarios del medio de transporte BF. Una oferta de contenidos de información IN disponibles puede ser solicitada mediante el servidor de catálogo MCS, desde el cual se adjudican también identificaciones únicas para los respectivos contenidos de información IN seleccionados. Contenidos de

información seleccionados son cifrados por el servidor de cifrado MES y en el banco de datos de inventario IDB son almacenadas asociaciones creadas por el método acorde a la invención, como por ejemplo la asociación de la identificación única de un contenido de información IN seleccionado con respecto a un medio de transporte BF y a un usuario del medio de transporte BF.

Además, el sistema acorde a la invención comprende un servidor a bordo OB que se encuentra instalado dentro del medio de transporte BF y desde el cual se establece una conexión hacia la unidad de salida específica del usuario AE, mediante una red de comunicaciones K2. Por ejemplo, el servidor a bordo OB puede estar realizado como dispositivo móvil, operado mediante batería, el cual está ubicado a bordo del medio de transporte BF, y se activa durante un funcionamiento del medio de transporte BF (por ejemplo en un vuelo, un viaje en tren, etc.). De manera alternativa, el servidor a bordo puede estar realizado también como módulo de software que, a modo de ejemplo, se instala en una instalación o infraestructura ya existente en el medio de transporte BF, como por ejemplo en un servidor web local o en un así llamado sistema de conectividad. De manera adicional también es posible que el servidor a bordo OB se encuentre instalado por fuera del medio de transporte BF - por ejemplo en los otros componentes del sistema - y que, mediante una red de comunicaciones general (por ejemplo una red de telefonía móvil), datos (como por ejemplo una clave Sg3, etc.) sean transmitidos inmediatamente antes de una utilización del medio de transporte BF a la unidad de salida AE específica del usuario.

En el sistema acorde a la invención se proporciona además una aplicación AW que puede instalarse en una unidad de salida AE específica del usuario o que, en el caso de una ejecución del método acorde a la invención, se instala en la unidad de salida AE específica del usuario. La aplicación AW, a modo de ejemplo, puede ser cargada por sugerencia de una compañía operadora del medio de transporte BF (por ejemplo por una aerolínea, etc.) por el usuario o pasajero antes de una utilización del medio de transporte BF, en su unidad de salida AE (por ejemplo tablet, smartphone, ordenador portátil, etc.) y puede ser instalada en la misma.

Además, el sistema acorde a la invención comprende al menos una red de comunicaciones K1, K2 en cada caso, respectivamente para una comunicación dentro y fuera del medio de transporte BF. Como red de comunicaciones K1 por fuera del medio de transporte BF puede utilizarse por ejemplo Internet o una red de telefonía móvil (por ejemplo WirelessLAN, UMTS, etc.), mediante la cual se establece una comunicación entre la unidad de salida AE y/o la aplicación AW y los componentes del sistema, como por ejemplo el servidor de catálogo MCS, el servidor de claves EKS, el servidor de cifrado MES. Una comunicación entre el servidor a bordo OB y por ejemplo el servidor de claves EKS se realiza igualmente mediante la red de comunicaciones K1, por fuera del medio de transporte BF. De este modo, por ejemplo, claves Sg1, Sg3 pueden ser transmitidas al servidor a bordo OB antes del funcionamiento del medio de transporte.

Para una comunicación dentro del medio de transporte BF - por ejemplo entre el servidor a bordo OB y las unidades de salida AE que se encuentran en el medio de transporte BF - se utiliza una red de comunicaciones K2 dentro del medio de transporte BF. Como red de comunicaciones K2 dentro del medio de transporte BF puede utilizarse por ejemplo una red de telefonía móvil, como por ejemplo WirelessLAN, GSM, UMTS o Next Generation Mobile Networks (NGMN, por sus iniciales, del inglés, redes móviles de próxima generación).

Un inicio del método acorde a la invención, el cual se realiza mediante el sistema acorde a la invención, representado de forma esquemática y a modo de ejemplo en la figura 1), tiene lugar en un primer paso del método 1, en donde mediante un primer par de claves Sg1, Sp1 que se compone de una primera clave secreta Sg1 y de una primera clave pública Sp1, el servidor a bordo OB es asociado a un medio de transporte BF (por ejemplo a un avión, etc.) de la compañía operadora del medio de transporte BF (por ejemplo aerolínea, etc.). El servidor a bordo OB se encontrará usualmente en el medio de transporte BF - como dispositivo móvil particular o como módulo de software - el cual se instala en una infraestructura que se encuentra en el medio de transporte BF. Del modo antes descrito, existe también la posibilidad de que el servidor a bordo OB se encuentre instalado o colocado por fuera del medio de transporte BF. Una información sobre a qué servidor a bordo OB corresponde qué medio de transporte BF (por ejemplo avión, etc.), puede ser almacenado por ejemplo en el banco de datos de inventario IDB. Una asociación de medios de transporte BF a determinados tramos de un recorrido (por ejemplo vuelos, rutas de recorrido de un tren, etc.) puede ser almacenada en un sistema de la compañía operadora del medio de transporte BF. En el primer paso del método 1, por tanto, un primer par de claves Sg1, Sp1 se genera para cada servidor a bordo OB de la compañía operadora. De este modo, la primera respectiva clave secreta Sg1 es enviada al respectivo servidor a bordo OB, y la respectiva clave pública Sp1 es almacenada por el servidor de claves EKS en el banco de datos de claves KDB. De esta manera, en el sistema de la compañía operadora del medio de transporte se sabe qué servidor a bordo OB pertenece a qué medio de transporte BF y a qué tramo del recorrido (por ejemplo en un vuelo, etc.).

En un segundo paso del método 2, por ejemplo por el respectivo pasajero/usuario del medio de transporte BF, por sugerencia de la compañía operadora, una aplicación AW es instalada en la unidad de salida AE específica del usuario del pasajero, antes de la utilización del medio de transporte. En un tercer paso del método 3, por la aplicación AW es solicitado un segundo par de claves Sg2, Sp2 desde el servidor de claves EKS. El segundo par de claves Sg2, Sp2 se compone igualmente de una segunda clave secreta Sg2 y de una segunda clave pública Sp2. La segunda clave secreta Sg2, en el tercer paso del método 3, mediante la red de comunicaciones K1, es transmitida a

la unidad de salida AE, así como a la aplicación AW allí instalada y es almacenada. La segunda clave pública Sp2, desde el servidor de claves EKS, igualmente es almacenada en el banco de datos de claves KDB. El segundo par de claves es asociado entonces de forma unívoca al pasajero, así como a su unidad de salida AE, donde la identidad del pasajero es conocida para la compañía operadora del medio de transporte BF.

Desde la compañía operadora del medio de transporte BF puede ser transmitido al pasajero o al usuario del medio de transporte BF un registro de datos de información, desde el cual se describe de forma unívoca la utilización del medio de transporte por el pasajero (por ejemplo vuelo, viaje en tren, etc.). Lo mencionado puede tener lugar por ejemplo mediante correo electrónico (eventualmente cifrado y/o marcado), como mensaje o por ejemplo, en el caso de un vuelo, mediante el pasaporte de abordaje. Una aceptación del registro de datos de información puede tener lugar por ejemplo de forma automática a través de la aplicación AW o desde la aplicación AW, mediante el registro de datos de información, por ejemplo en su inicio, puede verificarse si para el pasajero o usuario de la unidad de salida AE se encuentra reservada una utilización de un medio de transporte BF en la compañía operadora.

En un cuarto paso del método 4, los contenidos de información IN disponibles son visualizados por la aplicación AW. Una oferta de contenidos de información IN disponibles que están almacenados en el banco de datos de información MDB es puesta a disposición de la aplicación AW desde el servidor de catálogo MCS, mediante la red de comunicaciones K1 (por ejemplo Internet, etc.). Mediante la aplicación AW pueden ser seleccionados uno o varios contenidos de información IN que desean ser consumidos por el pasajero en una próxima utilización del medio de transporte BF. Para cada contenido de información IN seleccionado se crea y se adjudica una identificación única a través del servidor de catálogo MCS. A dicha identificación única, en el cuarto paso del método 4, se asocia el pasajero, así como su unidad de salida AE, la respectiva utilización del medio de transporte BF (por ejemplo avión, etc.) y el contenido de información IN seleccionado. En el cuarto paso del método 4, de manera conveniente, debe tener lugar el registro de datos de operaciones de liquidación (por ejemplo cuenta bancaria, datos de la tarjeta de crédito, etc.). De modo opcional, ya en el cuarto paso del método 4 puede tener lugar también el pago por los contenidos de información IN seleccionados, en caso de que la compañía operadora desee ofrecer el servicio a cambio de un pago.

En un quinto paso del método 5, desde la aplicación AW, ingresando la identificación única, desde el servidor de cifrado MES, se solicita el respectivo contenido de información IN seleccionado. De este modo, a la identificación única del respectivo contenido de información IN seleccionado se asocia un tercer par de claves Sg3, Sp3 generado por el servidor de claves EKS. El tercer par de claves Sg3, Sp3 se compone igualmente de una tercera clave secreta Sg3 y de una tercera clave pública Sp3. La tercera clave pública Sp3 se pone a disposición del servidor de cifrado MES para un cifrado del contenido de información IN seleccionado.

En un sexto paso 6, la tercera clave secreta Sg3 es cifrada primero desde el servidor de claves EKS primero con la segunda clave pública Sp2 y después con la primera clave pública Sp1 desde el banco de datos de claves KDB. A continuación, la tercera clave secreta Sg3 doblemente cifrada es asociada al servidor a bordo OB de aquel medio de transporte BF que será utilizado por el pasajero o usuario de la unidad de salida AE. Por motivos de seguridad debe omitirse un almacenamiento exacto de la tercera clave secreta Sg3. Como resultado del sexto paso del método 6 se dispone entonces de una asociación de la identificación única de un contenido de información IN seleccionado, de un servidor a bordo OB, del pasajero, así como de la unidad de salida AE del pasajero, del contenido de información seleccionado, así como del primer, del segundo o del tercer par de claves Sg1, Sp1, Sg2, Sp2, Sg3, Sp3. Ese resultado o esa asociación pueden almacenarse en el banco de datos de inventario IDB. La tercera clave secreta Sg3 se transmite poco antes del funcionamiento del medio de transporte BF (por ejemplo antes de la salida del vuelo, de un viaje en vehículo, durante la noche, etc.) con otras claves Sg3 doblemente cifradas para descifrar contenidos de información IN en el servidor a bordo OB del medio de transporte BF, para que esas claves Sg3 estén disponibles durante la utilización del medio de transporte BF.

En un séptimo paso del método 7, el contenido de información IN seleccionado, por el servidor de cifrado MES, es solicitado desde el banco de datos de información MDB y es cifrado con la tercera clave pública Sp3. De este modo, el contenido de información cifrado es transmitido a la unidad de salida AE mediante la red de comunicaciones K1, por fuera del medio de transporte BF. Asimismo, una transmisión puede tener lugar por ejemplo sin la interacción del usuario o del pasajero. Dependiendo del momento de una selección del contenido de información, la transmisión de los contenidos de información seleccionados puede realizarse por ejemplo con un ancho de banda menor y con un tiempo de carga correspondientemente más prolongado, o puede limitarse a tiempos en los cuales la unidad de salida AE no se utiliza o en donde es posible una transmisión de datos gratuita o conveniente en cuanto a los costes. También es posible que los contenidos de información IN seleccionados sean marcados de forma individual en el proceso de cifrado - por ejemplo con marcas de agua digitales (por ejemplo señal de imagen, acústica y/o de video), para detectar mejor un uso indebido.

Durante la utilización del medio de transporte BF, la unidad de salida AE en donde se encuentra instalada la aplicación AW y se encuentra almacenado el contenido de información IN seleccionado, es llevada por el pasajero a bordo del medio de transporte BF. A bordo del medio de transporte BF, en un octavo paso del método 8, desde la unidad de salida AE, mediante la red de comunicaciones K2 dentro del medio de transporte BF, se establece una

conexión hacia el servidor a bordo OB. Esa conexión puede efectuarse por ejemplo mediante WirelessLAN con Service Set Identifier (SSID - identificador de conjunto de servicios) y mediante una clave de red intercambiada previamente, donde la clave de red puede estar almacenada en la aplicación AW.

Desde la aplicación AW se ofrecen los contenidos de información IN almacenados cifrados en la unidad de salida y previamente seleccionados. Si ese contenido de información IN se selecciona para ser reproducido, entonces, en un noveno paso del método 9, desde el servidor a bordo OB se solicita la tercera clave secreta Sg3, necesaria para descifrar el contenido de información IN seleccionado. La tercera clave secreta Sg3 doblemente cifrada es descifrada por el servidor a bordo OB con la primera clave secreta Sg1 que está almacenada en el servidor a bordo OB, y después, en un décimo paso del método 10, es transmitida cifrada una vez con la segunda clave pública Sp2 a la aplicación AW en la unidad de salida AE. En un undécimo paso del método 11, la tercera clave secreta Sg3 es descifrada con la segunda clave secreta Sg2, que se encuentra disponible en la unidad de salida AE, así como para la aplicación AW. Seguidamente, el contenido de información IN seleccionado en la unidad de salida AE puede ser descifrado con la tercera clave secreta Sg3 y puede ser visualizado. En el undécimo paso del método 11, en caso de que la compañía operadora desee ofrecer los contenidos de información IN, así como su oferta, a cambio de un pago, el envío de la clave Sg3 puede ser registrado para realizar un proceso de pago para la utilización de los contenidos de información IN durante la próxima conexión posible hacia la red de comunicaciones K1.

Por motivos de seguridad, se considera conveniente que los contenidos de información IN seleccionados y almacenados en la unidad de salida AE sean borrados por la aplicación AW - independientemente de si los mismos fueron o no consumidos - después de la utilización del medio de transporte BF (por ejemplo después de finalizado un vuelo, etc.). Igualmente, todas las claves secretas Sg1, Sg2, Sg3 deben ser borradas por el servidor a bordo OB, así como por el servidor de claves EKS. Con ello, un acceso a los contenidos de información cifrados ya no es posible una vez finalizado el uso del medio de transporte. También es posible que las claves secretas Sg1, Sg3 ya sean borradas por el servidor de claves EKS después de confirmada la transmisión en el servidor a bordo OB. Eventualmente, el borrado de los contenidos de información, así como también de las claves secretas Sg1, Sg2, Sg3, puede realizarse también con un retardo temporal, por ejemplo para calcular también retrasos del medio de transporte BF.

De manera alternativa, existe la posibilidad de que el tercer par de claves Sg3, Sp3 no sea generado durante la solicitud de un contenido de información IN seleccionado y después sea asociado al servidor a bordo en el sexto paso del método 6, sino que previamente se genera una cantidad de terceros pares de claves Sg3, Sp3 como cantidad de reserva, donde dicha cantidad de reserva se asocia previamente al servidor a bordo OB y eventualmente también se transmite. Si en el quinto paso del método 5 se solicita un contenido de información IN seleccionado mediante identificación única desde la aplicación AW, entonces un tercer par de claves Sg3, Sp3 se extrae de la cantidad de reserva y se asocia a la identificación única. Lo mencionado ofrece la ventaja de que un pasajero, poco antes de iniciar la utilización del medio de transporte BF (por ejemplo antes de la salida del vuelo en el área de espera en el aeropuerto o en un sala de espera, etc.) y, eventualmente después de una transmisión de las terceras claves Sg3 al servidor a bordo OB, puede seleccionar contenidos de información IN. La tercera clave secreta Sg3 para el contenido de información IN seleccionado, cifrada una vez con la primera clave pública Sp1, en el sexto paso del método 6, es transmitida al servidor a bordo.

Durante la utilización del medio de transporte BF, en el noveno paso del método, esa tercera clave secreta Sg3 es descifrada con la primera clave secreta Sg1 desde el servidor a bordo. Una transmisión de la tercera clave secreta Sg3 a la aplicación AW puede tener lugar por ejemplo de forma no cifrada, mediante un procedimiento seguro. A modo de ejemplo, para una transmisión puede utilizarse Secure Socket Layer (SSL, capa de puertos seguros). Sin embargo, para ello puede utilizarse también la segunda clave pública Sp2 que, por ejemplo, es enviada de forma no asegurada al servidor a bordo OB. La tercera clave secreta Sg3 puede ser cifrada por ejemplo con esa clave Sp2 y ser transmitida de ese modo a la unidad de salida AE, así como a la aplicación AW que dispone de la respectiva segunda clave secreta Sg2 correspondiente.

En el sexto paso del método 6 existe también la posibilidad de descifrar contenidos de información IN seleccionados en varios segmentos con diferentes terceros pares de claves Sg3, Sp3. Para ello, en el quinto paso del método 5, a la identificación única del contenido de información IN seleccionado se asocian por ejemplo varios terceros pares de claves Sg3, Sp3 que después se emplean para el cifrado de los respectivos segmentos. De esa forma se impide que un consumo del contenido de información IN pueda continuar después de finalizada la utilización del medio de transporte BF sobre una longitud de un segmento, y en ningún momento existe la posibilidad de descifrar completamente el contenido de información IN.

Además, en el método acorde a la invención, es posible también por ejemplo que una selección automática de contenidos de información IN sea efectuada por la compañía operadora del medio de transporte BF antes de la utilización del medio de transporte BF, y que la misma sea cargada en la unidad de salida AE. Dichos contenidos pueden tratarse por ejemplo de cualquier contenido de información IN o de contenidos de información IN seleccionados con frecuencia, los cuales presentan una similitud con contenidos de información IN ya seleccionados anteriormente por el pasajero.

A través del método acorde a la invención y del sistema para ejecutar el método, a través de una separación de la transmisión de los contenidos de información IN cifrados y de la transmisión de las claves Sg1, Sg2, Sg3, Sp1, Sp2, Sp3, se ofrece una posibilidad para implementar algoritmos de cifrado potentes e intensivos en cuanto al tiempo de cálculo, los cuales no pueden utilizarse en sistemas streaming a bordo debido a las capacidades de memoria y de cálculo. El cifrado de los contenidos de información IN es realizado individualmente por usuario o pasajero, donde el usuario es conocido y, con ello, eventualmente, sería posible comprobar un robo de contenidos de información. Puesto que el servidor a bordo OB sólo pone a disposición la clave Sg3 para descifrar los contenidos de información IN, el mismo puede ser realizado de forma sencilla y conveniente en cuanto a los costes. También la inversión logística para la carga o la actualización de los contenidos de información IN es relativamente reducida. Los contenidos de información IN son actualizados en el banco de datos de información IDB y en el servidor a bordo OB, antes de cada utilización del medio de transporte BF o al menos diariamente, son cargadas las nuevas claves Sg3 para descifrar los contenidos de información IN seleccionados por los pasajeros. De este modo, de forma individual, puede ponerse a disposición de los pasajeros una gran oferta actual de contenidos de información IN que adicionalmente se encuentra protegida contra robos, con una seguridad muy elevada.

REIVINDICACIONES

1. Método para asociar contenidos de información (IN) que, en el caso de una utilización de un medio de transporte (BF), en particular de un avión, son visualizados y consumidos en una unidad de salida (AE) específica del usuario, caracterizado porque

- a cada medio de transporte (BF), mediante un primer par de claves que está compuesta por una primera clave secreta y una primera clave pública (Sg1, Sp1), se asocia un servidor a bordo (OB), y la primera clave secreta (Sg1) es almacenada en el servidor a bordo (OB) (1),

- antes de una utilización del medio de transporte (BF) se instala una aplicación (AW) en la unidad de salida (AE) específica del usuario (2),

- un segundo par de claves con una segunda clave secreta y una segunda clave pública (Sg2, Sp2) es entonces solicitado por la aplicación (AW) y la segunda clave secreta (Sg2) es transmitida a la aplicación (AW) (3),

- contenidos de información (IN) disponibles son visualizados por la aplicación (AW) y entonces para cada contenido de información (IN) seleccionado se crea una identificación única (4),

- los contenidos de información (IN) seleccionados son solicitados por la aplicación (AW) mediante la identificación única y a la identificación única se asocia un tercer par de claves con una tercera clave secreta y una tercera clave pública (Sg3, Sp3) (5),

- la tercera clave secreta (Sg3) es cifrada con la primera clave pública y la segunda clave pública (Sp1, Sp2) y es asociada al servidor a bordo (OB) del medio de transporte (6),

- y porque los contenidos de información (IN) seleccionados son transmitidos a la unidad de salida (AE) cifrados con la tercera clave pública (AE) (7).

2. Método según la reivindicación 1, caracterizado porque al ser utilizado el medio de transporte (BF) se establece una conexión desde la unidad de salida (AE) hacia el servidor a bordo (OB) (8), porque antes de una reproducción del contenido de información (IN) seleccionado por el servidor a bordo (OE), la tercera clave secreta (Sg3) es descifrada (9) con la primera clave secreta (Sg1) y entonces es transmitida (10) a la aplicación (AW) en la unidad de salida (AE), porque en la unidad de salida (AE) la tercera clave secreta (Sg3) es descifrada con la segunda clave secreta (Sg2), y porque entonces el contenido de información (IN) seleccionado es descifrado por la aplicación (AW) con la tercera clave secreta (Sg3) y es visualizado (11).

3. Método según una de las reivindicaciones a 1 a 2, caracterizado porque una asociación entre el servidor a bordo (OB), la unidad de salida (AE) específica del usuario, contenidos de información (IN) seleccionados y/o el primer, el segundo y el tercer para de claves (Sg1, Sp1, Sg2, Sp2, Sg3, Sp3), es almacenada en un banco de datos de inventario (IDB) (6).

4. Método según una de las reivindicaciones a 1 a 3, caracterizado porque después de la instalación de la aplicación (AW) y de una transmisión de la segunda clave secreta (Sg2) a la aplicación (AW), se transmite un registro de datos de información sobre una utilización del medio de transporte (BF) (3).

5. Método según una de las reivindicaciones 1 a 4, caracterizado porque los pares de claves (Sg1, Sp1, Sg2, Sp2, Sg3, Sp3) son generados por un servidor de claves (EKS).

6. Método según una de las reivindicaciones 1 a 5, caracterizado porque la primera y la segunda clave pública (Sp1, Sp2) del primer y del segundo par de claves se almacenan en un banco de datos de claves (KDB) (1, 3).

7. Método según una de las reivindicaciones 1 a 6, caracterizado porque después de abandonar el medio de transporte (BF), las claves secretas (Sg1, Sg2, Sg3), así como todos los contenidos de información (IN) seleccionados, son borrados por la unidad de salida (AW).

8. Método según una de las reivindicaciones 1 a 7, caracterizado porque la identificación única para cada contenido de información (IN) seleccionado es adjudicada por un servidor de catálogo (MCS) (4).

9. Método según una de las reivindicaciones 1 a 8, caracterizado porque el tercer par de claves (Sg3, Sp3) se genera en el momento de una selección de un contenido de información (IN) (5).

10. Método según una de las reivindicaciones 1 a 8, caracterizado porque previamente se genera una cantidad de terceros pares de claves (Sg3, Sp3) y esos terceros pares de claves (Sg3, Sp3) se transmiten al servidor a bordo (OB).

11. Método según una de las reivindicaciones 1 a 10, caracterizado porque los contenidos de información (IN) seleccionados son marcados durante un cifrado (7).

12. Sistema para ejecutar el método según las reivindicaciones 1 a 11, caracterizado porque se proporcionan:

- un servidor a bordo (OB) para establecer una conexión con una unidad de salida (AE) específica del usuario dentro de un medio de transporte (BF),

- una aplicación (AW) que puede instalarse en una unidad de salida (AE) específica del usuario,

- un servidor de claves (EKS) y un banco de datos de claves (KDB) para generar y crear pares de claves (Sg1, Sp1, Sg2, Sp2, Sg3, Sp3) que se componen cada uno de una clave secreta y de una clave pública,

- un servidor de catálogo (MCS) para solicitar una oferta de contenidos de información (IN) disponibles y para adjudicar identificaciones únicas para contenidos de información (IN) seleccionados,

- un servidor de cifrado (MES) para cifrar contenidos de información (IN) seleccionados,

- un banco de datos de inventario (IDB) para almacenar asociaciones entre el servidor a bordo (OB), la unidad de salida (AE) específica del usuario, contenidos de información (IN) seleccionados y/o respectivos pares de claves (Sg1, Sp1, Sg2, Sp2, Sg3, Sp3) correspondientes,

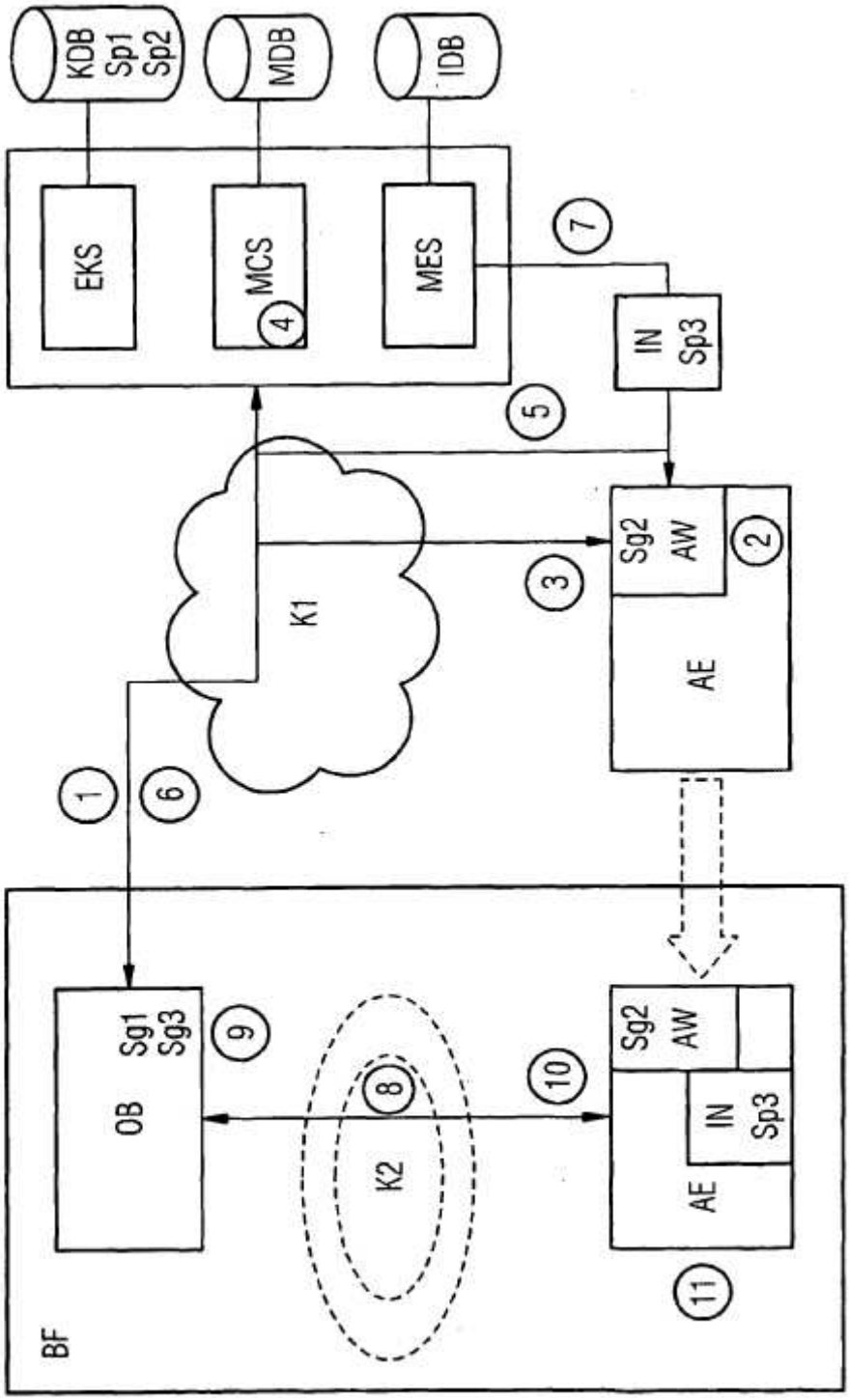
- un banco de datos de información (IDB) para almacenar contenidos de información (IN) disponibles y que pueden ser seleccionados,

- y al menos una red de comunicaciones (K1, K2) en cada caso, respectivamente para una comunicación dentro y fuera del medio de transporte (BF).

13. Sistema según la reivindicación 12, caracterizado porque el servidor de claves (EKS), el servidor de catálogo (MCS) y el servidor de cifrado (MES) en un servidor y/o en un servidor y/o en un banco de datos de claves (KDB), en un banco de datos de inventario (IDB) y en un banco de datos de información (MDB) están agrupados en un banco de datos.

14. Sistema según una de las reivindicaciones 11 a 12, caracterizado porque el servidor a bordo (OB) está realizado como unidad móvil.

15. Sistema según una de las reivindicaciones 11 a 12, caracterizado porque el servidor a bordo (OB) está realizado como un módulo de software.


KDB
Sp1
Sp2
MDB
IDB
EKS
MCS
4
MES
7
IN
Sp3
5
K1
3
Sg2
AW
2
AE
1
6
BF
OB
Sg1
Sg3
9
8
K2
10
Sg2
AW
IN
Sp3
AE
11