(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 387 756**

(51) Int. CI.:
G07B 15/00 (2011.01)
G07B 15/06 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **11005132 .3**
(96) Fecha de presentación: **29.01.2010**
(97) Número de publicación de la solicitud: **2378489**
(97) Fecha de publicación de la solicitud: **19.10.2011**

(54) Título: **Procedimiento para la comunicación DSRC**

(45) Fecha de publicación de la mención BOPI:
01.10.2012

(45) Fecha de la publicación del folleto de la patente:
01.10.2012

(73) Titular/es:
Kapsch TrafficCom AG
Am Europlatz 2
1120 Wien, AT

(72) Inventor/es:
Güner, Refi-Tugrul;
Tijink, Jasja y
Karner, Georg

(74) Agente/Representante:
Zea Checa, Bernabé

DESCRIPCIÓN

Procedimiento para la comunicación DSRC

La presente invención hace referencia a un procedimiento para la comunicación DSRC entre balizas y dispositivos de a bordo de un sistema de peaje de carretera, disponiendo las balizas de una clave común al sistema y no disponiendo los dispositivos de a bordo de la clave común al sistema, sino de claves individuales, cada una de las cuales está formada a partir de la clave común al sistema por medio de un identificador de derivación específico del identificador de derivación, en el cual, en una comunicación, el identificador de derivación se envía del dispositivo de a bordo a la baliza con objeto de hacer posible a la baliza la reproducción de la clave individual para codificación y la descodificación de la comunicación con el dispositivo de a bordo y/o para el acceso a los datos almacenados en el dispositivo de a bordo.

Por la EP 0 769 763 A2 se conoce un procedimiento de codificación para la comunicación entre balizas y dispositivos de a bordo, los cuales, al principio de una comunicación, intercambian identificadores de derivación para esta comunicación de balizas. Para ello, los dispositivos de a bordo disponen de copias locales de la clave común al sistema.

Yixin Jiang *et al., "BAT: A robust Signature Scheme for Vehicular Networks Using Binary Authentication Trees", IEEE Transactions on Wireless Communications*, volumen 6, abril de 2009, páginas 1974-1983, describe un procedimiento de codificación de clave pública/privada para comunicaciones DSRC entre balizas y dispositivos de a bordo, en el que los dispositivos de a bordo disponen asimismo de copias locales de la clave pública común al sistema, y en la codificación seleccionan la clave privada propia a partir de un conjunto de claves privadas.

Los sistemas de peaje de carretera DSRC (*Dedicated ShortRange Communication Toll Systems*, sistemas de peaje de comunicación dedicada de corto alcance) están normalizados, por ejemplo, en los estándares ISO 14906 y EN 15509; en ellos, la comunicación DSRC en la interfaz radioeléctrica puede tener lugar, por ejemplo, de acuerdo con el estándar WAVE IEEE 1609.11. Por motivos de seguridad, en los sistemas de peajes de carretera DSRC de este tipo no se guardan las claves comunes al sistema (*Master Keys*) en los dispositivos de a bordo (*Onboard Units*, OBUs), sino que estos reciben solamente claves individuales derivadas de ellas (*Derived Keys*). Por medio de la interfaz radioeléctrica DSRC solo se comunican o se utilizan estas claves individuales.

El identificador de derivación necesario para ello, denominado "*Key Diversifier*" en los estándares ISO 14906 y EN 15509, representa para cada dispositivo de a bordo un identificador individual de las reglas utilizadas en cada caso para la derivación de la clave individual (*Derived Key*) a partir de la clave común al sistema (*Master Key*). El dispositivo de a bordo comunica a la baliza el identificador de derivación (*Key Diversifier*) según el estado de la técnica en cualquier comunicación entre un dispositivo de a bordo y una baliza, para que también esta pueda derivar "sobre la macrha" ("*on the fly*") de la clave común al sistema la clave individual respectiva del dispositivo de a bordo para la comunicación o el acceso al dispositivo de a bordo.

La presente invención se basa en el reconocimiento de que esta situación comporta un problema de protección de datos: Dado que en toda radiocomunicación DSRC se emite primero el identificador de derivación - específico del dispositivo de a bordo - por el dispositivo de a bordo a través de la interfaz radioeléctrica, mediante la intercepción de la interfaz radioeléctrica o una lectura fraudulenta deliberada de un dispositivo de a bordo que pase sería posible identificar este dispositivo en todos los casos y de esta forma seguir su recorrido. De este modo se podría elaborar el perfil de movimiento de un dispositivo de a bordo determinado o de su usuario en un sistema de peaje de carretera.

La invención resuelve este problema de protección de datos reconocido aquí por primera vez, y, para resolverlo, el dispositivo de a bordo, en comunicaciones con balizas consecutivas, emite identificadores de derivación que van cambiando, para lo cual se almacena en un dispositivo de a bordo una reserva de pares de claves individuales y los identificadores de derivación asociados, y, cuando tiene lugar una comunicación con una baliza, el dispositivo de a bordo selecciona un par de esta reserva y lo utiliza para la comunicación. De este modo ya no es posible seguir dispositivos de a bordo durante un tiempo relativamente largo o a través de varias secciones de balizas mediante los identificadores de derivación emitidos por ellos en las comunicaciones DSRC. La invención representa un alivio para las balizas y no requiere ningún tipo de modificación o ampliación del protocolo de comunicaciones en la interfaz radioeléctrica, aunque sí memoria y funcionalidad adicional adecuadas en los dispositivos de a bordo. El par citado se selecciona de la reserva en el dispositivo de a bordo preferiblemente de forma aleatoria o, como mínimo, pseudoaleatoria.

Otra configuración ventajosa de la invención consiste en que, en una comunicación con un dispositivo de a bordo, la baliza envía a este como mínimo un nuevo par formado por la clave individual y el identificador de derivación asociado, que el dispositivo de a bordo almacena en su reserva para su posterior selección

De esta forma se puede conseguir una gran seguridad en la protección de datos, porque el identificador de derivación cambia frecuentemente, y, al mismo tiempo, se reduce la sobrecarga de las balizas y de las interfaces radioeléctricas.

La baliza envía el par citado preferiblemente al final de la comunicación, y también muy preferiblemente solo cuando el tráfico de comunicación es reducido ("en función del tráfico") para no alterar sus funciones de peaje con las funciones adicionales de protección de datos.

La invención es especialmente apropiada para comunicaciones de acuerdo con los estándares de DSRC ISO 14906 o EN 15509, o estándares compatibles con ellos, siendo el identificador de derivación el *Key Diversifier* de este estándar.

La invención se explica más detalladamente a continuación con ayuda de los ejemplos de ejecución representados en los dibujos que se incluyen. En los dibujos,
las fig. 1 y 2 muestran un diagrama de bloques y un diagrama de secuencia de una primera forma de ejecución del procedimiento de la invención; y
las fig. 3 y 4 muestran un diagrama de bloques y un diagrama de secuencia de una segunda forma de ejecución del procedimiento de la invención.

En las fig. de la 1 a la 4 están representados un dispositivo de a bordo (*Onboard Unit*) OBU a modo de ejemplo y una baliza (*Roadside Equipment*) RSE a modo de ejemplo de un sistema de peaje de carretera con un gran número de dispositivos de a bordo OBU y balizas RSE. Cada dispositivo de a bordo OBU se comunica con la baliza RSE correspondiente por medio de una interfaz radioeléctrica 1 de corto alcance de acuerdo con el estándar DSRC (*Dedicated Short Range Communication*), en especial de acuerdo con el estándar ISO 14906 o EN 15509, o estándares basados en ellos o compatibles con ellos. Dos formas de ejecución diferentes de un procedimiento de comunicación DSRC de acuerdo con la invención en la interfaz radioeléctrica se muestran en las fig. 1 y 2 por una parte y en las fig. 3 y 4 por otra.

En ambas variantes, cada una de las balizas RSE dispone de una o más claves comunes al sistema MK (*Master Keys*). Por ejemplo, están en comunicación con una central (no representada) que administra la clave o las claves MK comunes al sistema para las balizas RSE o las distribuye a dichas balizas.

Por motivos de seguridad, una clave común al sistema MK no se guarda en los dispositivos de a bordo OBU, sino que estos reciben solamente claves individuales derivadas de ellas DK (*Derived Keys*). Las claves individuales DK pueden utilizarse para la codificación de la comunicación en la interfaz radioeléctrica 1 (como "*Encryption Keys*") y/o como autorización de acceso ("*Access Credential Keys*") para acceder a los datos OBU guardados en el dispositivo de a bordo, como sabe el especialista.

Las claves individuales DK se derivan de la clave común al sistema MK según una regla de derivación especificada, de manera que un identificador de derivación ("*Key Diversifier*") Div identifica las reglas de derivación específicas de los respectivos dispositivos de a bordo o es un parámetro de esta regla de derivación, es decir,

$$DK = F(MK, Div) .$$

Solo conociendo el identificador de derivación Div se puede formar la clave individual DK a partir de una clave común al sistema MK.

Según la variante del procedimiento de las fig. 1 y 2, la baliza RSE envía en un primer paso 2 su tabla de servicio de la baliza (*Beacon Service Table*, BST) a un dispositivo de a bordo OBU que pase. El dispositivo de a bordo OBU responde a ello con su propia tabla de servicio del vehículo (*Vehicle Service Table*, VST), que también contiene su identificador de derivación Div actual (paso 3). La baliza RSE puede ahora, basándose en el identificador de derivación Div, derivar la clave individual DK del dispositivo de a bordo OBU a partir de la clave común al sistema MK (paso 4) y utilizarla para la comunicación ulterior, p. ej., como *Encryption Key* o *Access Credential Key* (paso 5).

Al final de la comunicación 5, la baliza RSE genera un identificador de derivación Div, p. ej., controlado aleatoriamente, y calcula la clave individual DK correspondiente (paso 6). En un paso 7, la baliza RSE envía este par (Div,DK) al dispositivo de a bordo OBU. El dispositivo de a bordo OBU guarda el par recibido (Div,DK) para utilizarlo en su recorrido para la siguiente o por lo menos una de las siguientes comunicaciones 2 - 5, ya sea con esta baliza RSE o con otra.

Las fig. 3 y 4 muestran una forma de ejecución alternativa en la que los mismos signos de referencia designan los mismos elementos. El dispositivo de a bordo OBU contiene aquí una reserva (conjunto) 8 de pares de identificadores de derivación Divi diferentes y claves individuales DKi asociadas. Por ejemplo, en la inicialización o en la salida de

un dispositivo de a bordo OBU, la reserva 8 puede calcularse previamente en una unidad de programación (OBU *Programming Station*, OPS) a partir del identificador común al sistema MK y guardarse en el dispositivo de a bordo OBU.

Después del requerimiento BST por la baliza RSE, el dispositivo de a bordo OBU selecciona ahora en un paso 9 ("*randomize i*") aleatoriamente (o pseudoaleatoriamente) un par (Divi,DKi) de su reserva 8 y envía el identificador de derivación Divi del par seleccionado en la respuesta VST a la baliza RSE (paso 10). Alternativamente, el par (Divi, DKi) también podría seleccionarse de la lista de pares de la reserva 8 según determinadas reglas, p. ej., primero el par más antiguo o par utilizado más lejano en el tiempo en cada caso. La baliza RSE puede ahora, en el paso 4, derivar a partir de la clave común al sistema MK y del identificador de derivación Divi la clave individual DKi y utilizarla para la comunicación ulterior 5.
Opcionalmente pueden combinarse entre sí las formas de ejecución de las fig.1, 2 y 3, 4. Así, por ejemplo, la baliza RSE de la forma de ejecución de las fig. 3, 4 podría generar al final de una comunicación 5 – si dispone de tiempo suficiente, es decir, si el tráfico de comunicación con este y otros dispositivos de a bordo OBU es reducido en ese momento, - análogamente al paso 6, un par (Divj,DKj) nuevo, y, análogamente al paso 7, enviarlo al dispositivo de a bordo OBU, que guarda el par (Divj,DKj) recibido en su reserva 8 – reemplazando un par ya utilizado o adicionalmente a pares ya existentes – para la utilización ulterior.

La invención no está limitada a las formas de ejecución mostradas, sino que abarca todas las variantes y modificaciones que estén contempladas en el ámbito de las reivindicaciones indicadas a continuación:

REIVINDICACIONES

1. Procedimiento para la comunicación DSRC entre balizas (RSE) y dispositivos de a bordo (OBU) de un sistema de peaje de carretera, disponiendo las balizas (RSE) de una clave común al sistema (MK) y no disponiendo los dispositivos de a bordo (OBU) de la clave común al sistema (MK), sino de claves individuales (DK), cada una de las cuales está formada a partir de la clave común al sistema (MK) por medio de un identificador de derivación (Div) específico del dispositivo de a bordo, en el cual, en una comunicación (3), el identificador de derivación se envía del dispositivo del vehículo (OBU) a la baliza (RSE) con objeto de hacer posible a la baliza (RSE) la reproducción de la clave individual (DK) para codificación y la descodificación de la comunicación (5) con el dispositivo de a bordo (OBU) y/o para el acceso a los datos almacenados en el dispositivo de a bordo OBU), **caracterizado porque,** en comunicaciones (2 - 5) con balizas (RSE) sucesivas, el vehículo de a bordo (OBU) envía identificadores de derivación (Div) que van cambiando, guardándose en un dispositivo de a bordo (OBU) una reserva (8) de pares de claves individuales (DKi) e identificadores de derivación (Divi) asociados, y porque, en una comunicación (2 – 5) con una baliza (RSE), el dispositivo de a bordo (OBU) selecciona un par de esta reserva (8) y lo utiliza para esta comunicación (2 – 5).

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado porque** el par (Divi,DKi) del dispositivo de a bordo (OBU) se selecciona de la reserva (8) de forma aleatoria o, por lo menos, pseudoaleatoria.

3. Procedimiento de acuerdo con la reivindicación 1 o 2, **caracterizado porque** en una comunicación (2 - 5) con un dispositivo de a bordo (OBU), la baliza envía a dicho dispositivo como mínimo un par nuevo de clave individual (DKj) e identificador de derivación (Divj) asociado, que el dispositivo de a bordo (OBU) guarda en su reserva (8).

4. Procedimiento de acuerdo con la reivindicación 1 o 2, **caracterizado porque** en una comunicación (2 - 5) con un dispositivo de a bordo (OBU), la baliza envía a dicho dispositivo como mínimo un par nuevo de clave individual (DKj) e identificador de derivación (Divj) asociado, que el dispositivo de a bordo (OBU) guarda en su reserva (8).

5. Procedimiento de acuerdo con la reivindicación 3 o 4, **caracterizado porque** la baliza (RSE) envía el par citado (Div,DK) solo cuando el tráfico de comunicación es reducido.

6. Procedimiento de acuerdo con una de las reivindicaciones de la 1 a la 5, **caracterizado porque** la comunicación (2 - 5) se realiza según los estándares de DSRC ISO 14906 o EN 15509 o estándares compatibles con ellos, y el identificador de derivación (Div) es el *Key Diversifier* de este estándar.

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

Esta lista de referencias citadas por el solicitante es únicamente para la comodidad del lector. No forma parte del documento de la patente europea. A pesar del cuidado tenido en la recopilación de las referencias, no se pueden excluir errores u omisiones y la EPO niega toda responsabilidad en este sentido.

Documentos de patentes citados en la descripción

- EP 0769763 A2

Literatura diferente de patentes citada en la descripción

- **Yixin Jiang *et al.*** BAT: A robust Signature Scheme for Vehicular Networks Using Binary Authentication Trees. IEEE Transactions on Wireless Communications, abril 2009, vol. 6, 1974-1983

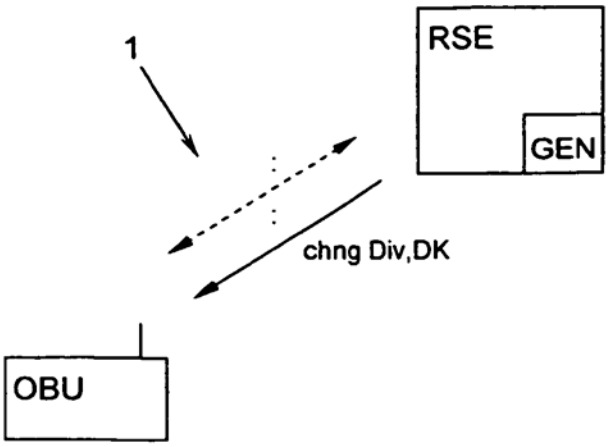
1
RSE
GEN
chng Div,DK
OBU

Fig. 1

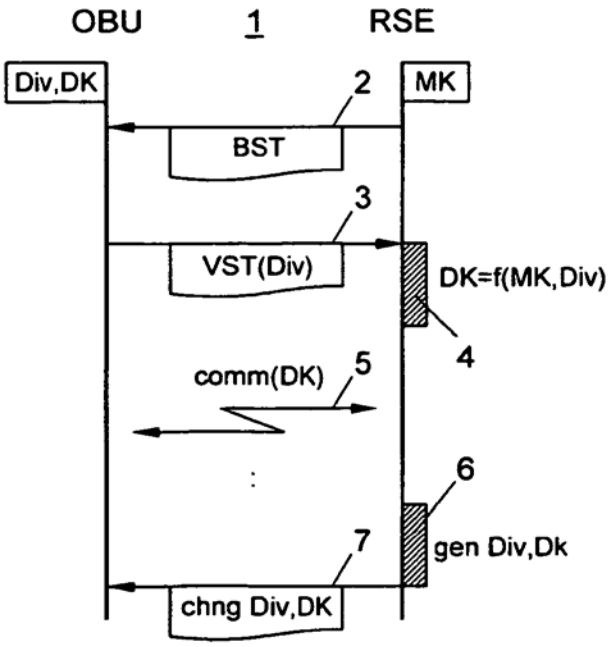
OBU
1
RSE
Div,DK
MK
2
BST
3
VST(Div)
DK=f(MK,Div)
4
comm(DK)
5
6
gen Div,Dk
7
chng Div,DK

Fig. 2

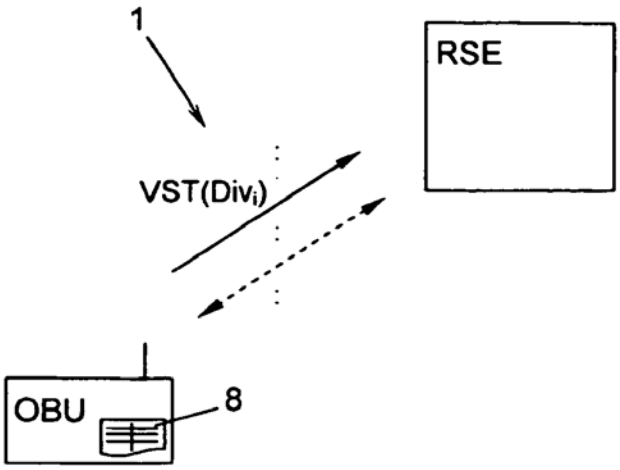
1
RSE
VST(Div$_i$)
OBU
8

Fig. 3

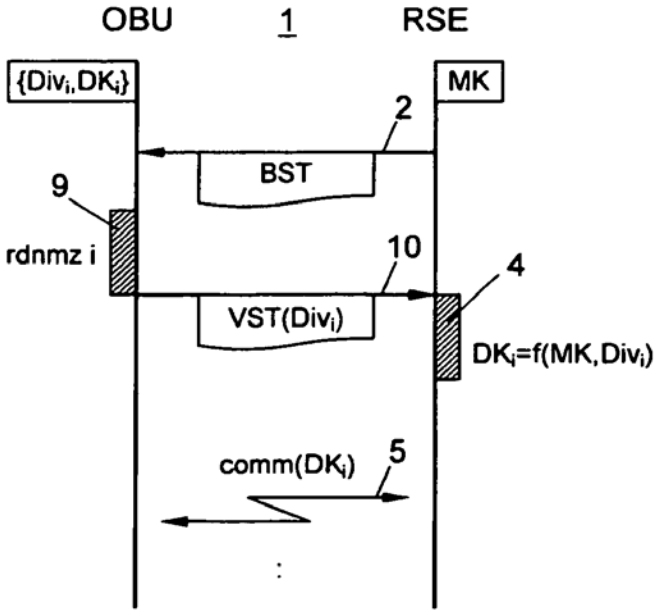
OBU
1
RSE
{Div$_i$,DK$_i$}
MK
2
BST
9
rdnmz i
10
4
VST(Div$_i$)
DK$_i$=f(MK,Div$_i$)
comm(DK$_i$)
5

Fig. 4