(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 471 876**

(51) Int. CI.:

G07B 15/00 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **28.01.2011 E 11705142 (5)**

(97) Fecha y número de publicación de la concesión europea: **02.04.2014 EP 2529359**

(54) Título: **Procedimiento para autenticar aparatos de vehículo**

(30) Prioridad:

29.01.2010 EP 10450009

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.06.2014

(73) Titular/es:

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

(72) Inventor/es:

SCHRÖDL, SÖREN y
NAGY, OLIVER

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Procedimiento para autenticar aparatos de vehículo

La presente invención se refiere a un procedimiento para autenticar aparatos de vehículo que pueden llevar a cabo comunicaciones DSRC con balizas de un sistema de peaje viario, disponiendo las balizas de una clave aplicable a todo el sistema y disponiendo los aparatos de vehículo sólo de claves individuales que están formadas respectivamente a partir de la clave aplicable a todo el sistema por medio de un identificador de derivación específico del aparato de vehículo, transmitiendo el aparato de vehículo el identificador de derivación a la baliza en caso de una comunicación a fin de que la baliza sea capaz de reproducir la clave individual para la codificación o descodificación de la comunicación con el aparato de vehículo y/o de acceder a datos almacenados en el aparato de vehículo.

Un procedimiento para la comunicación DSRC entre balizas y aparatos de vehículo de este tipo, en el que los aparatos de vehículo transmiten identificadores de derivación variables en comunicaciones con balizas consecutivas, se conoce por la solicitud de patente europea anterior n° 10 450 009.5, cuya prioridad se reivindica en este caso.

Los sistemas de peaje viario DSRC (*Dedicated Short Range Communication Toll Systems*, sistemas de peaje viario basado en la comunicación dedicada de corto alcance) están normalizados, por ejemplo, en las normas ISO 14906 y EN 15509; la comunicación DSRC en la interfaz de radio se puede llevar a cabo aquí, por ejemplo, según la norma IEEE 1609.11 para WAVE (conexión inalámbrica en entornos vehiculares). En este tipo de sistemas de peaje viario DSRC no se almacenan por razones de seguridad claves aplicables a todo el sistema (master keys) en los aparatos de vehículo (Onboard Units, OBUs, unidades de a bordo), sino que estos reciben sólo claves individuales derivadas de las mismas (derived keys). Por medio de la interfaz de radio DSRC se comunican o se usan sólo estas claves individuales.

El identificador de derivación requerido para esto, que se denomina „key diversifier“ en las normas ISO 14906 o EN 15509, representa un identificador individual para cada aparato de vehículo de la regla usada respectivamente para derivar la clave individual (derived key) a partir de la clave aplicable a todo el sistema (master key). Según el estado de la técnica, el aparato de vehículo notifica el identificador de derivación (key diversifier) a la baliza en cada comunicación entre un aparato de vehículo y una baliza con el fin de que también ésta pueda derivar “on the fly” (sobre la marcha) la clave individual respectiva del aparato de vehículo a partir de la clave aplicable a todo el sistema para la comunicación con el aparato de vehículo o para el acceso al aparato de vehículo.

La invención descrita en la solicitud anterior n° 10 450 009.5 se basaba en el conocimiento de que esta constelación implica un problema relativo a la protección de datos: Dado que el identificador de derivación específico del aparato de vehículo en cada comunicación de radio DSRC es transmitido primero por el aparato de vehículo a través de la interfaz de radio, sería posible identificarlo mediante la intercepción de la interfaz de radio o mediante una lectura fraudulenta dirigida de un aparato de vehículo que pasa, se podría identificar respectivamente este último y, por tanto, sería posible seguir el recorrido del mismo. De este modo se puede crear un perfil de movimiento de un aparato de vehículo determinado o de su usuario en un sistema de peaje viario.

La invención dada a conocer en la solicitud anterior n° 10 450 009.5 solucionó este problema relativo a la protección de datos al transmitir los aparatos de vehículo identificadores de derivación variables en caso de comunicaciones con balizas consecutivas, al almacenarse en un aparato de vehículo una reserva de pares de claves individuales e identificadores de derivación correspondientes y al seleccionar un aparato de vehículo en el marco de una comunicación con una baliza un par de esta reserva y lo utiliza para la comunicación. De este modo ya no resulta posible el seguimiento de aparatos de vehículo durante un periodo de tiempo mayor o después de varias secciones de baliza sobre la base de los identificadores de derivación transmitidos por estos en las comunicaciones DSRC.

La presente invención se basa en el conocimiento de que la funcionalidad anteriormente mencionada se puede emplear de manera ventajosa también para verificar la autenticidad, es decir, para autenticar un aparato de vehículo. Para este fin se prevé según la presente invención
que en el aparato de vehículo se almacene una reserva de pares de claves individuales e identificadores de derivación correspondientes y que el aparato de vehículo seleccione respectivamente un par diferente de la reserva en comunicaciones consecutivas y lo utilice para la respectiva comunicación, y
que, para la autenticación, un aparato de interrogación induce al aparato de vehículo a realizar al menos la parte de una comunicación de radio en la que transmite el identificador de derivación seleccionado, y para que éste se reciba en el aparato de interrogación y se compare con identificadores de derivación de la reserva almacenados en el aparato de interrogación, autenticando un caso de igualdad el aparato de vehículo.

De este modo se puede verificar de manera sencilla la autenticidad de un aparato de vehículo sin que sea necesario para ello una conexión con una centralita del sistema de peaje: la reserva de identificadores de derivación almacenada en el aparato de vehículo sólo se hace público respectivamente de forma individual durante un periodo de tiempo muy grande y en puntos geográficamente distribuidos, concretamente en las diferentes balizas, en la operación de radio "normal" con las balizas. El riesgo de intentos de fraude mediante una intercepción de la interfaz

aérea entre el aparato de vehículo y las balizas para descubrir esta reserva "secreta" y así, por ejemplo, dotar a aparatos de vehículo falsificados de identificadores de derivación "auténticos", es por tanto extremadamente bajo. Con el procedimiento según la invención se realiza una interrogación de la reserva de identificadores de derivación contenida de forma secreta en el aparato de vehículo y así se puede usar la misma para validar la autenticidad del aparato de vehículo.

Para el procedimiento de autenticación según la invención tampoco es necesaria ninguna modificación del protocolo de comunicación entre los aparatos de vehículo y las balizas, ya que el aparato de interrogación emula la parte de la comunicación con una baliza en la que el aparato de vehículo emite los identificadores de derivación. El aparato de interrogación se puede configurar para ello de cualquier manera, por ejemplo, como aparato transportable o móvil, en particular como aparato manual para verificar la autenticidad de un aparato de vehículo, por ejemplo directamente in situ.

Es especialmente ventajoso cuando el aparato de interrogación induzca al aparato de vehículo a realizar comunicaciones consecutivas para recibir varios identificadores de derivación diferentes y compararlos con identificadores de derivación de la reserva almacenados en el aparato de interrogación, autenticándose el aparato de vehículo sólo cuando todas las comparaciones dan como resultado el caso de igualdad. De este modo se puede conseguir una seguridad aún mayor de la autenticación (validación) del aparato de vehículo.

Preferiblemente, el par mencionado en el aparato de vehículo se selecciona de manera aleatoria o al menos seudoaleatoria de la reserva.

Como forma de realización adicional, una cantidad parcial de la reserva de identificadores de derivación almacenada en el aparato de vehículo sólo se puede usar para dichos fines de control. De este modo, además, estos identificadores de derivación no se transmiten nunca a balizas y quedan secretos y protegidos frente a intentos de intercepción hasta el momento de control.

La invención es especialmente adecuada para comunicaciones según las normas DSRC ISO 14906, EN 15509, IEEE 1609.11 o normas que se basan en las mismas, siendo el identificador de derivación el key diversifier de esta norma.

La invención se explica a continuación más detalladamente mediante ejemplos de realización representados en los dibujos adjuntos. En los dibujos muestran
las figuras 1 y 2 un diagrama de bloques y un diagrama de secuencia de un procedimiento de comunicación entre un aparato de vehículo y una baliza según la solicitud anterior n° 10 450 009.5;
las figuras 3 y 4 un diagrama de bloques y un diagrama de secuencia de una primera forma de realización del procedimiento de autenticación de la invención; y

la figura 5 un diagrama de secuencia de una segunda forma de realización del procedimiento de autenticación de la invención.

Haciendo referencia a las figuras 1 y 2 se describe primero un procedimiento de comunicación según la solicitud anterior n° 10 450 009.5 que constituye la base del presente procedimiento de autenticación.

Las figuras 1 y 2 muestran un aparato de vehículo (*Onboard Unit*, unidad de a bordo) OBU a modo de ejemplo y una baliza (*Roadside Equipment*, equipo del lado de la carretera) RSE a modo de ejemplo de un sistema de peaje viario que por regla general tiene un gran número de aparatos de vehículo OBU y balizas RSE. Los aparatos de vehículo OBU y las balizas RSE se comunican entre sí respectivamente a través de una interfaz de radio 1 de corto alcance según la norma DSRC (*Dedicated Short Range Communication*, comunicación dedicada de corto alcance), en particular según la norma ISO 14906 o EN 15509 o normas que se basan en ésta o que son compatibles con ésta.

Las balizas RSE disponen respectivamente de una o varias claves aplicables a todo el sistema MK (*Master Keys*). Por ejemplo, éstas se encuentran conectadas con una central (no representada) que administra la clave o las claves aplicables a todo el sistema MK para las balizas RSE o las distribuye a las balizas.

Por razones de seguridad, una clave aplicable a todo el sistema MK no se almacena en los aparatos de vehículo OBU, sino que estos mantienen sólo claves DK (*Derived Keys*) derivadas individualmente de ellas. Las claves individuales DK se pueden usar para codificar la comunicación en la interfaz de radio 1 (como "encryption keys") y/o como autorización de acceso ("*Access Credential Keys*") para acceder a datos almacenados en el aparato de vehículo OBU, como sabe el experto en la técnica.

Las claves individuales DK se derivan según una regla de derivación predefinida de la clave aplicable a todo el sistema MK, identificando un identificador de derivación Div ("*Key Diversifier*") la regla de derivación específica del aparato de vehículo, que se ha usado respectivamente, o siendo éste un parámetro de esta regla de derivación, es decir,

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

La clave individual DK se puede formar a partir de una clave aplicable a todo el sistema MK sólo si se conoce el identificador de derivación Div.

El aparato de vehículo OBU contiene una reserva (*pool*) 8 de pares de distintos identificadores de derivación Div_i y claves individuales DK_i correspondientes. La reserva 8 se puede calcular previamente a partir del identificador aplicable a todo el sistema MK, por ejemplo, durante la inicialización o entrega de un aparato de vehículo OBU en una estación de programación (*OBU Programming Station*, OPS, estación de programación OBU) y se puede almacenar en el aparato de vehículo OBU.

En el marco de una comunicación entre el aparato de vehículo y la baliza, la baliza RSE transmite en una primera etapa 2 su tabla de servicio (*Beacon Service Table*, BST, tabla de servicio de baliza) a un aparato de vehículo OBU que pasa. Después de la solicitud BST por parte de la baliza RSE, el aparato de vehículo OBU selecciona ahora de manera aleatoria ("randomize i") (o seudoaleatoria) un par (Div_i, DK_i) de su reserva 8 en una etapa 9 y transmite el identificador de derivación Div_i del par seleccionado en la respuesta VST a la baliza RSE (etapa 10). El par (Div_i, DK_i) se podría seleccionar alternativamente también de la lista de pares en la reserva 8 según determinadas reglas, por ejemplo, en primer lugar el par más viejo respectivamente o el par usado más tempranamente.

La baliza RSE puede derivar ahora la clave individual Dk_i del respectivo aparato de vehículo OBU a partir de la clave aplicable a todo el sistema MK basándose en el identificador de derivación Div_i (etapa 4) y usarla para la comunicación ulterior, por ejemplo como encription key o access credential key (etapa 5).

Las figuras 3 y 4 muestran un procedimiento de autenticación que se basa en el procedimiento de comunicación de las figuras 1 y 2 para verificar la autenticidad de un aparato de vehículo OBU. Para ello se emplea un aparato de interrogación CHK que implementa o emula al menos algunas (o también todas las) funcionalidades de la baliza RSE de las figuras 1 y 2, y concretamente en cualquier caso la parte de la comunicación de radio en la interfaz de radio 1 que induce al aparato de vehículo OBU a emitir uno de sus identificadores de derivación Div_i, aunque esta vez no a la baliza RSE, sino al aparato de interrogación CHK. Por consiguiente, en las figuras 3 y 4, los mismos números de referencia designan componentes idénticos como en las figuras 1 y 2 y para ello se hace referencia a su descripción.

En el aparato de interrogación CHK se almacena la misma reserva 8 de pares $\{Div_i, DK_i\}$ que en el aparato de vehículo OBU, siendo también suficiente en el caso más sencillo almacenar sólo los identificadores de derivación Div_i de la reserva 8 en el aparato de interrogación CHK.

Una vez que ahora el aparato de vehículo OBU haya emitido un identificador de derivación Div_i aleatorio de su reserva 8 después de una solicitud correspondiente por parte del aparato de interrogación CHK en la etapa 2, tal como se describió anteriormente mediante las figuras 1 y 2, (etapas 9, 10), en una etapa 4' se puede comparar ahora el identificador de derivación Div_i recibido con los identificadores de derivación Div_i de la reserva almacenada en el aparato de interrogación CHK, es decir, se comprueba si el identificador de derivación Div_i recibido está contenido en esta reserva:

$$Div_i \in \{Div_i\} \ ?.$$

Si es así (caso de igualdad "y"), entonces con ello el aparato de vehículo OBU está validado o autenticado, es decir, está verificado con respecto a su autenticidad. Si no es así (caso de desigualdad "n"), entonces el aparato de vehículo OBU no está autenticado (inválido), y, por ejemplo, se puede emitir un alarma y protocolizar una notificación correspondiente.

La figura 5 muestra una forma de realización perfeccionada del procedimiento de las figuras 3 y 4, en la que el aparato de interrogación CHK realiza varias veces de manera consecutiva las etapas de comunicación mencionadas 2, 10 con el aparato de vehículo OBU, de modo que se induce a éste de manera consecutiva a enviar varios identificadores de derivación variables Div_{i1}, Div_{i2}, Div_{i3}, etc. En la etapa de comparación 4" se comparan todos los identificadores de derivación recibidos Div_{i1}, Div_{i2}, Div_{i3}, etc. con la reserva de identificadores de derivación $\{Div_i\}$ almacenados en el aparato de interrogación CHK, y, sólo cuando todos estos identificadores de derivación recibidos estén contenidos en la reserva ("y") el aparato de vehículo OBU se declara válido o se autentica.

Una opción que se puede usar en cada uno de los procedimientos descritos consiste en usar sólo una cantidad parcial de la reserva 8 en el aparato de vehículo OBU para comunicaciones con aparatos de control CHK, es decir, seleccionar de la reserva 8 (un) identificador(es) de derivación especial(es) Div_i o Div_{i1}, Div_{i2}, Div_{i3}, etc. sólo para los

fines de autenticación mencionados. Los identificadores de derivación de esta cantidad parcial entonces tampoco se usan para las comunicaciones de los aparatos de vehículo OBU con las balizas RSE, de modo que no llegan al exterior y no pueden ser interceptados en la operación "normal" (de baliza) de los aparatos de vehículo OBU.

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

REIVINDICACIONES

1. Procedimiento para autenticar aparatos de vehículo (OBU) que pueden realizar comunicaciones DSRC con balizas (RSE) de un sistema de peaje viario, disponiendo las balizas (RSE) de una clave aplicable a todo el sistema (MK) y disponiendo los aparatos de vehículo (OBU) con respecto a las claves sólo de claves individuales (DK_i) que están formadas respectivamente a partir de la clave aplicable a todo el sistema (MK) por medio de un identificador de derivación (Div_i) específico del aparato de vehículo, transmitiendo el aparato de vehículo (OBU) el identificador de derivación (Div_i) a la baliza (RSE) en caso de una comunicación a fin de que la baliza (RSE) sea capaz de reproducir la clave individual (DK_i) para codificar o descodificar la comunicación con el aparato de vehículo (OBU) y/o de acceder a datos almacenados en el vehículo de aparato (OBU), **caracterizado por que** en el aparato de vehículo (OBU) se almacena una reserva (8) de pares de claves individuales (DK_i) e identificadores de derivación (Div_i) correspondientes y el aparato de vehículo (OBU) en comunicaciones consecutivas selecciona en cada caso un par diferente de la reserva (8) y lo usa para la respectiva comunicación, y **por que** para realizar la autenticación, un aparato de interrogación (CHK) induce al aparato de vehículo (OBU) a realizar al menos la parte (10) de una comunicación de radio en la que transmite el identificador de derivación (Div_i) elegido, y ésta se recibe en el aparato de interrogación (CHK) y se compara con identificadores de derivación (Div_i) de la reserva (8) almacenados en el aparato de interrogación (CHK), autenticando un caso de igualdad el aparato de vehículo (OBU).

2. Procedimiento según la reivindicación 1, **caracterizado por que** el aparato de interrogación (CHK) induce al aparato de vehículo (OBU) a realizar comunicaciones consecutivas (10) para recibir varios identificadores de derivación diferentes (Div_{i1}, Div_{i2}, Div_{i3}) y compararlos con identificadores de derivación (Div_i) de la reserva (8) almacenados en el aparato de interrogación (CHK), autenticándose el aparato de vehículo (OBU) sólo cuando todas las comparaciones dan como resultado el caso de igualdad.

3. Procedimiento según las reivindicaciones 1 o 2, **caracterizado por que** el par (Div_i, DK_i) en el aparato de vehículo (OBU) se selecciona de la reserva (8) de manera aleatoria o al menos seudoaleatoria.

4. Procedimiento según una de las reivindicaciones 1 a 3, **caracterizado por que** el par (Div_i, DK_i) en el aparato de vehículo (OBU) se selecciona a partir de una cantidad parcial de la reserva (8) que sólo se utiliza en comunicaciones con aparatos de control (CHK) y no en comunicaciones con balizas (RSE).

5. Procedimiento según una de las reivindicaciones 1 a 4, **caracterizado por que** la comunicación se lleva a cabo según las normas DSRC ISO 14906, EN 15509, IEEE 1609.11 o normas compatibles con las mismas y el identificador de derivación (Div_i) es el identificador de derivación de estas normas.

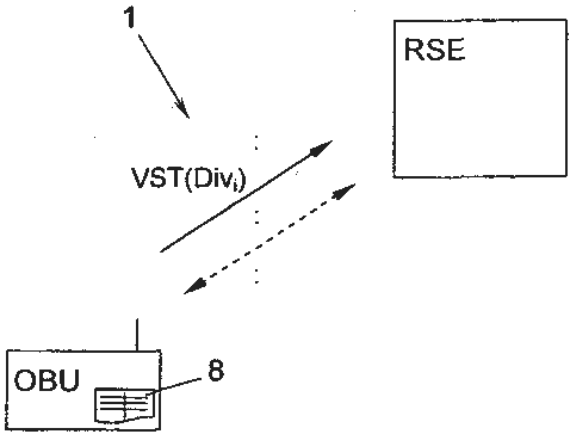
1
RSE
VST(Div$_i$)
OBU
8

Fig. 1

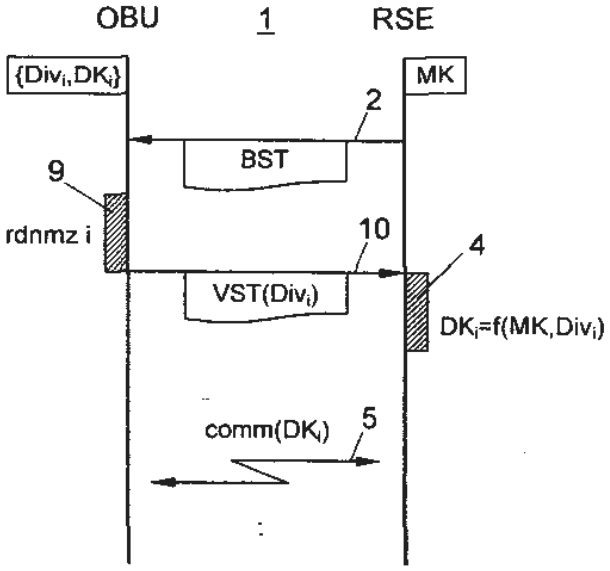
OBU
1
RSE
{Div$_i$,DK$_i$}
MK
2
BST
9
rdnmz i
10
4
VST(Div$_i$)
DK$_i$=f(MK,Div$_i$)
comm(DK$_i$)
5

Fig. 2

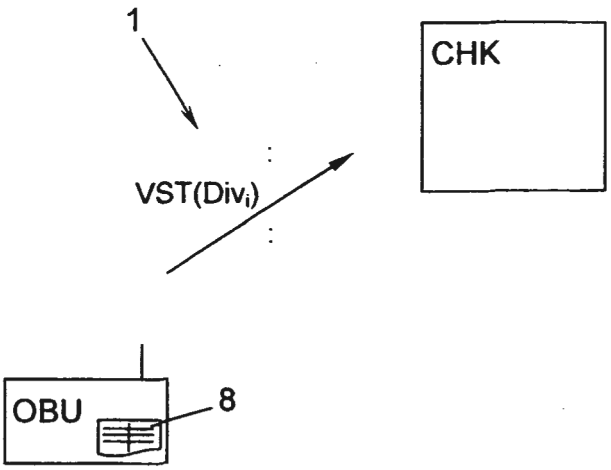
1
CHK
VST(Div$_i$)
OBU
8

Fig. 3

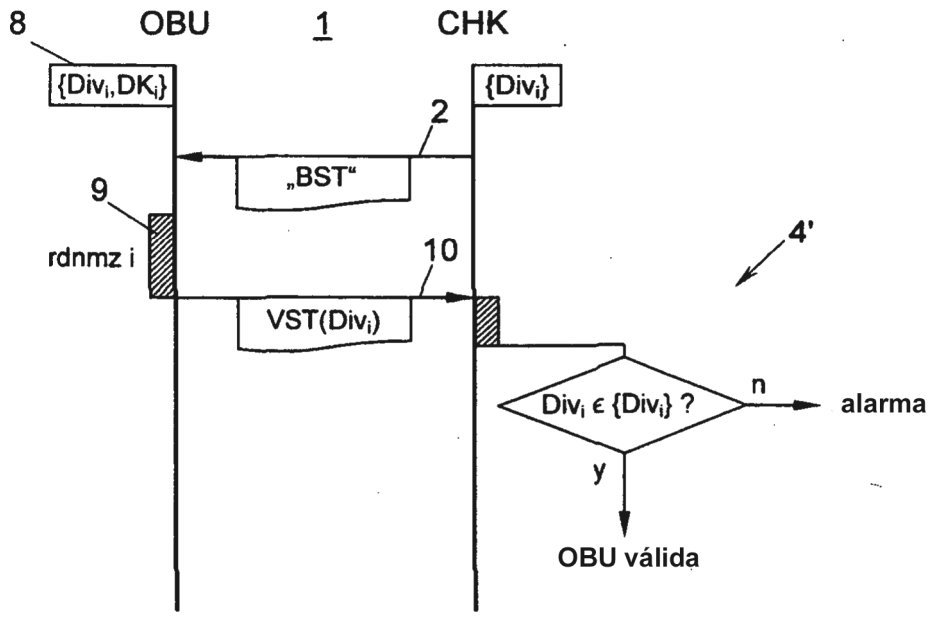
8
OBU
1
CHK
{Div$_i$,DK$_i$}
{Div$_i$}
2
„BST“
9
rdnmz i
10
4'
VST(Div$_i$)
Div$_i$ ϵ {Div$_i$} ?
n
alarma
y
OBU válida

Fig. 4

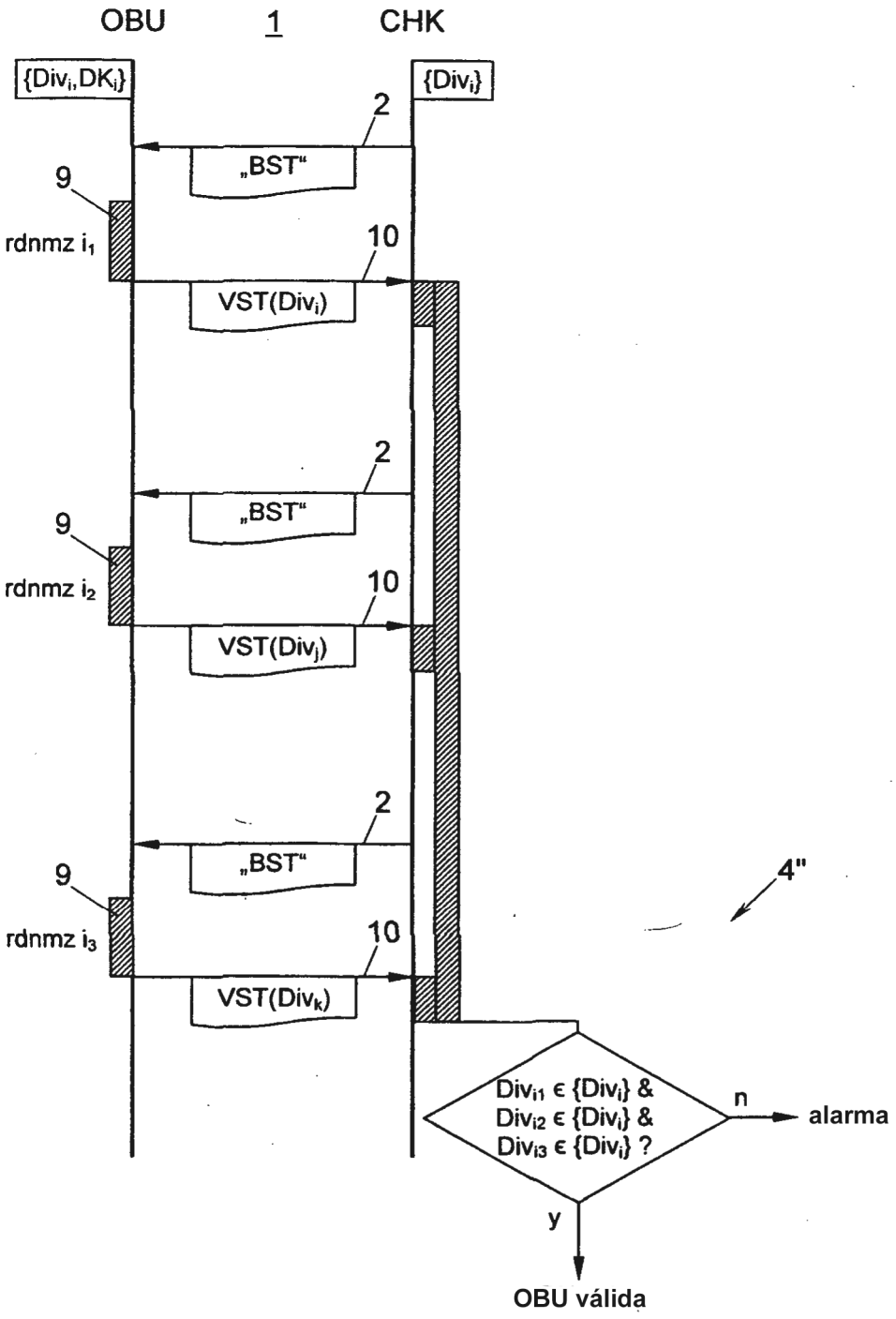
OBU
1
CHK
{Div_i, DK_i}
{Div_i}
2
„BST"
9
rdnmz i_1
10
VST(Div_i)
2
„BST"
9
rdnmz i_2
10
VST(Div_j)
2
„BST"
9
rdnmz i_3
10
VST(Div_k)
4"
Div_i1 ∈ {Div_i} &
Div_i2 ∈ {Div_i} &
Div_i3 ∈ {Div_i} ?
n
alarma
y
OBU válida

Fig. 5