(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 672 591**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04W 74/08 (2009.01)
H04W 76/02 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.08.2013 E 16166959 (3)**

(97) Fecha y número de publicación de la concesión europea: **07.03.2018 EP 3079391**

(54) Título: **Establecimiento de una sesión de comunicación de dispositivo a dispositivo**

(30) Prioridad:

06.09.2012 EP 12183256

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.06.2018

(73) Titular/es:

KONINKLIJKE KPN N.V. (50.0%)
Wilhelminakade 123
3072 AP Rotterdam, NL y
NEDERLANDSE ORGANISATIE VOOR TOEGEPAST- NATUURWETENSCHAPPELIJK ONDERZOEK TNO (50.0%)

(72) Inventor/es:

NORP, ANTONIUS;
FRANSEN, FRANK y
DE KIEVIT, SANDER

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Establecimiento de una sesión de comunicación de dispositivo a dispositivo

CAMPO DE LA INVENCIÓN

La invención se refiere a un método para establecer una sesión de comunicación de dispositivo a dispositivo (D2D) entre dispositivos móviles. La invención se refiere además a un dispositivo móvil para establecer la sesión de comunicación D2D con otro dispositivo móvil. La invención se refiere además a un software de control que comprende instrucciones para su ejecución en el dispositivo móvil. La invención se refiere además a la red móvil.

Las redes de comunicación móvil, también llamadas redes celulares o redes móviles, se han desplegado ampliamente en las últimas décadas con el fin de abordar la creciente necesidad de comunicación móvil. La comunicación entre dispositivos móviles que están conectados a tal red móvil tiene lugar típicamente a través de la red móvil, es decir, a través de una o más estaciones base y nodos centrales de la red móvil.

ANTECEDENTES DE LA INVENCIÓN

Es deseable habilitar dispositivos móviles que están conectados típicamente a una red móvil para comunicarse también directamente entre sí, es decir, a través de la así denominada comunicación de dispositivo a dispositivo (D2D).

La comunicación D2D está caracterizada por una trayectoria de comunicación inalámbrica directa entre dos terminales móviles, tales como los dispositivos móviles, mientras que mantiene, al menos en algunos momentos en el tiempo, al menos una conexión de señalización con/a través de una estación base de la red de comunicación inalámbrica, es decir, de la red móvil. La trayectoria de comunicación inalámbrica directa entre terminales móviles permite descargar a la estación o estaciones base, a la red de acceso y a la red central de la red de comunicación inalámbrica la mayoría de los datos y señalizaciones intercambiados entre los terminales móviles. La conexión de señalización con (una estación base de) la red de comunicación inalámbrica permite a la red de comunicación inalámbrica controlar los recursos asignados a la trayectoria de comunicación directa entre los terminales.

Un dispositivo móvil que, en un momento dado, utiliza comunicación D2D en lugar de comunicar a través de la red móvil puede decirse que opera en Modo de Funcionamiento Directo ((DMO). El DMO ofrece ventajas tales como, por ejemplo, habilitar la comunicación móvil entre usuarios fuera de un rango de la red móvil, reduciendo la carga de las estaciones de base y/o de los nodos centrales de la red móvil, etc.

Un ejemplo de una norma de comunicación móvil que permite la comunicación móvil entre dispositivos móviles tanto a través de la red móvil así como a través de la comunicación D2D antes mencionada es la Radio Troncal Terrestre (TETRA).

Otro ejemplo de tal normal de comunicación móvil es el Sistema Global para Comunicaciones Móviles (GSM). La norma GSM incluye una así denominada llamada local, característica de conmutación local en la que la comunicación móvil entre dispositivos que están conectados a una misma estación base de la red móvil no es encaminada a través de los nodos centrales de la red móvil, sino más bien directamente desde la estación base a cada dispositivo móvil respectivo.

Aún otro ejemplo es la Evolución a Largo Plazo (LTE). Desarrollos recientes de la LTE incluyen comunicación D2D entre dispositivos móviles. Se ha observado que en el contexto de la LTE, tal comunicación D2D también es llamada LTE Directa.

La publicación WO 2011117677 A1 expone un método y un aparato para gestión de claves de dispositivo a dispositivo. Un método ejemplar incluye generar una clave de seguridad de un dispositivo local basándose en una clave secreta y un valor base. El método también puede incluir recibir un valor de combinación de la clave de seguridad, y descomponer el valor de combinación de la clave de seguridad utilizando la clave de seguridad del dispositivo local para determinar una clave de seguridad de un dispositivo asociado. La clave de seguridad del dispositivo asociado también se puede configurar para su utilización en comunicaciones de dispositivo a dispositivo.

RESUMEN DE LA INVENCIÓN

Un problema de los dispositivos móviles y de las redes móviles anteriores es que un operador de la red móvil no tiene control o tiene un control limitado sobre la comunicación D2D. Los inventores han reconocido que tal control es deseable por distintas razones. Por ejemplo, la comunicación D2D tiene lugar en un espectro de frecuencia que es autorizado al operador y así necesita ser gestionado por el operador, por ejemplo, para evitar interferencias. Otro ejemplo es que el operador puede desear conceder sólo a los usuarios específicos acceso a la comunicación D2D, por ejemplo, trabajadores de emergencias, abonados a un servicio D2D, etc.

Sería ventajoso proporcionar más control sobre la comunicación D2D entre dispositivos móviles que se pueden conectar a una red móvil.

Para abordar mejor esta cuestión, un primer aspecto de la invención proporciona un método para establecer una sesión de comunicación D2D entre dispositivos móviles que se pueden conectar mutuamente a través de un canal de

comunicación D2D y que se pueden conectar individualmente a una red móvil, que comprende:

- la carga previa de una clave de inicio en cada uno de los dispositivos móviles, estando asociada la clave de inicio con un período de validez; y

en cada uno de los dispositivos:

- verificar una validez de la clave de inicio basándose en un tiempo actual;

- si la clave de inicio es considerada válida, generar una clave de sesión que utiliza la clave de inicio utilizando la clave de inicio en la realización de un procedimiento de concordancia de clave entre los dispositivos móviles sobre el canal de comunicación D2D, dando como resultado el procedimiento de concordancia de clave la clave de sesión si la clave de inicio utilizada por cada uno de los dispositivos móviles coincide; y

- establecer la sesión de comunicación D2D sobre el canal de comunicación D2D basándose en la clave de sesión.

Otro aspecto de la invención proporciona un software de control que comprende instrucciones para, durante la ejecución del software de control en un dispositivo móvil, hacer que el dispositivo móvil establezca la sesión de comunicación D2D de acuerdo con el método descrito.

Otro aspecto de la invención proporciona un dispositivo móvil para establecer una sesión de comunicación D2D con otro dispositivo móvil, pudiendo conectarse mutuamente el dispositivo móvil y el otro dispositivo móvil a través de un canal de comunicación D2D y pudiendo conectarse individualmente a una red móvil, comprendiendo el dispositivo móvil:

- un área de almacenamiento para almacenar una clave de inicio que es proporcionada durante una procedimiento de carga previa, estando asociada la clave de inicio con un período de validez; y

- un subsistema informático para:

- verificar una validez de la clave de inicio basándose en un tiempo actual;

- si la clave de inicio es considerada válida, generar una clave de sesión que utiliza la clave de inicio utilizando la clave de inicio en la realización de un procedimiento de concordancia de clave con el otro dispositivo móvil sobre el canal de comunicación D2D, dando como resultado el procedimiento de concordancia de clave la clave de sesión si la clave de inicio utilizada por el dispositivo móvil y el otro dispositivo móvil coinciden; y

- un subsistema móvil para establecer la sesión de comunicación D2D sobre el canal de comunicación D2D basándose en la clave de sesión.

Otro aspecto de la invención proporciona una red móvil dispuesta para cargar previamente una clave de inicio en el dispositivo móvil descrito cuando el dispositivo móvil está conectado a la red móvil, estando asociada la clave de inicio con un período de validez.

Las medidas antes mencionadas establecen, o proporcionan los medios para establecer una sesión de comunicación D2D entre dispositivos móviles que pueden conectarse mutuamente a través de un canal de comunicación D2D y que se pueden conectar individualmente a una red móvil. Aquí, el término canal de comunicación se refiere a un conducto para un intercambio de información entre los dispositivos móviles, y el término sesión de comunicación se refiere al intercambio de información, teniendo típicamente el intercambio de información un comienzo y un final definidos.

Los dispositivos móviles pueden conectarse a la red móvil porque, cuando los dispositivos móviles están conectados a la red móvil, la comunicación móvil entre los dispositivos móviles puede tener lugar a través de la red móvil, por ejemplo, a través de las estaciones base y de los nodos centrales de la red móvil. Los dispositivos móviles también están dispuestos para establecer una canal de comunicación D2D entre los dispositivos móviles de modo que habiliten la comunicación directa. La comunicación D2D puede ser establecida entre dos dispositivos móviles. Sin embargo, la comunicación D2D puede implicar igualmente una pluralidad de más de dos dispositivos móviles.

La sesión de comunicación D2D es establecida, es decir, configurada, de la siguiente manera. En primer lugar, una clave de inicio es cargada previamente en cada uno de los dispositivos móviles. Aquí, el término cargar previamente se refiere a una carga de la clave de inicio en un dispositivo móvil antes de establecer la sesión de comunicación D2D. Por ejemplo, la clave de inicio puede ser cargada en el dispositivo móvil ya antes de recibir una solicitud para establecer la sesión de comunicación D2D. La clave de inicio es utilizada en cada uno de los dispositivos móviles en el establecimiento de la sesión de comunicación D2D. De ahí que, cuando se recibe una solicitud para establecer la sesión de comunicación D2D, por ejemplo, desde el usuario o desde otro dispositivo móvil, ya no es necesario obtener la clave de inicio con el fin de establecer la sesión de comunicación D2D, es decir, ya está disponible en el dispositivo móvil.

La clave de inicio se utiliza en el establecimiento de la sesión de comunicación D2D de las siguientes maneras. La clave de inicio está asociada con un período de validez. El período de validez está disponible para el dispositivo móvil, por ejemplo, siendo proporcionado junto a la clave de inicio, pudiendo derivarse de la clave de inicio, etc. El período de

validez indica un período de tiempo en el que la clave de inicio es considerada válida para utilizar en el establecimiento de la sesión de comunicación D2D. En cada uno de los dispositivos móviles que van a tomar parte en la sesión de comunicación D2D, una validez de la clave de inicio es verificada basándose en el tiempo actual. Esto puede ser en respuesta a una solicitud para establecer la sesión de comunicación D2D. El tiempo actual es así utilizado para determinar si la clave de inicio es considerada válida o no. Si la clave de inicio es considerada válida, por ejemplo, debido al tiempo actual que hay en el período de validez, la clave de inicio es utilizada en realizar un procedimiento de concordancia de clave entre los dispositivos móviles.

Aquí, el término procedimiento de concordancia de clave se refiere a un procedimiento que es realizado entre los dispositivos móviles lo que da como resultado una clave de sesión acordada, con los dispositivos móviles siendo cada uno capaz de influir en el resultado del procedimiento, es decir, la clave de sesión. El procedimiento de concordancia de clave es realizado a través del canal de comunicación D2D, por ejemplo, intercambiando mensajes entre los dispositivos móviles, constituyendo los mensajes juntos el procedimiento de concordancia de clave. Los mensajes pueden ser intercambiados como parte de una sesión de comunicación D2D inicial que se ha establecido sobre el canal de comunicación D2D.

El procedimiento de concordancia de clave proporciona la clave de sesión basándose en si la clave de inicio, cuando es utilizada por cada dispositivo móvil respectivo en el procedimiento de concordancia de clave, coincide. Como tal, se obtiene una clave de sesión válida siempre que cada dispositivo móvil respectivo utiliza una misma clave de inicio en el procedimiento de concordancia de clave. La clave de sesión constituye una clave utilizada para proteger criptográficamente mensajes en una sesión de comunicación, tal como la protección de confidencialidad mediante el uso de cifrado o protección de integridad que utiliza códigos de autenticación de mensaje. La sesión de comunicación D2D es establecida utilizando la clave de sesión. Así, se obtiene una sesión de comunicación D2D en la que mensajes, tales como los de una transmisión de voz o de video entre los dispositivos móviles, son protegidos criptográficamente utilizando la clave de sesión. La clave de sesión es utilizada para una sesión de comunicación D2D particular. De ahí que, con el fin de establecer una nueva sesión de comunicación D2D en un momento posterior en el tiempo, típicamente se necesita obtener o generar una nueva clave de sesión.

Las medidas anteriores tienen el efecto de que se establece una sesión de comunicación D2D basada en una clave de inicio. Aquí, la clave de inicio funciona esencialmente como una credencial de autorización porque un dispositivo móvil necesita la clave de inicio para establecer la sesión de comunicación D2D. Proporcionando una clave de inicio que está asociada con un periodo de validez y verificando la validez de la clave de inicio en el dispositivo móvil basada en un tiempo actual, se ha previsto un mecanismo de control basado en el tiempo porque la clave de inicio es considerada válida sólo en un período predeterminado y considerada inválida fuera de dicho período.

Las medidas anteriores ofrecen control al operador sobre la comunicación D2D de las siguientes maneras. Requiriendo una clave de inicio válida para establecer la sesión de comunicación D2D, el operador obtiene control porque puede elegir a quien se proporciona la clave de inicio, de acuerdo con qué condiciones, etc. además, por medio del periodo de validez, el operador obtiene control basado en el tiempo, por ejemplo, de modo que impide la reutilización de claves de inicio antiguas. Utilizando la clave de inicio en un procedimiento de concordancia de clave que está basado en una coincidencia de las claves de inicio utilizadas por los dispositivos móviles, el operador obtiene control porque no cualquier clave de inicio puede ser utilizada en establecer la sesión de comunicación D2D; si no que, un éxito del procedimiento de concordancia de clave depende de si la clave de inicio, cuando es utilizada por cada uno de los dispositivos móviles en establecer la sesión de comunicación D2D, coincide.

Ventajosamente, cargando previamente la clave de inicio, se puede establecer la sesión de comunicación D2D bajo el control del operador incluso cuando uno o más de los dispositivos móviles están actualmente fuera del control directo del operador, por ejemplo, estando fuera de un rango de la red móvil. Ventajosamente, los dispositivos móviles pueden establecer de forma autónoma la sesión de comunicación D2D, es decir, sin una necesidad de contactar terceras partes.

Opcionalmente, la carga previa de la clave de inicio comprende proporcionar la clave de inicio a cada uno de los dispositivos móviles a través de la red móvil cuando cada dispositivo móvil está conectado a la red móvil. Es conveniente cargar previamente la clave de inicio a través de la red móvil cuando los dispositivos móviles son conectados frecuentemente a la red móvil y así no se necesita ningún medio adicional para cargar previamente la clave de inicio. Ventajosamente, la red móvil proporciona un canal seguro para cargar previamente la clave de inicio. Ventajosamente, la clave de inicio puede ser cargada previamente de forma automática, es decir, sin requerir acciones del usuario.

Opcionalmente, la carga previa de la clave de inicio comprende almacenar la clave de inicio en un área de almacenamiento segura de cada dispositivo móvil respectivo. La clave de inicio es así almacenada de tal manera que no puede ser leída fácilmente, por ejemplo, por el usuario o una aplicación que se ejecuta en el dispositivo móvil. Ventajosamente, se hace más difícil una falsificación de la clave de inicio.

Opcionalmente, el área de almacenamiento segura es proporcionada por un subsistema informático fiable de cada dispositivo móvil respectivo. Aquí, el dispositivo móvil comprende, bien como una parte integral o bien como una parte que se puede separar, un subsistema informático fiable. Tal subsistema informático fiable puede ser utilizado para realizar operaciones de cómputo en el dispositivo móvil que requiere un cierto nivel de seguridad, tal como autentificar el dispositivo móvil en la red móvil. Un ejemplo de un subsistema informático fiable que se puede separar es una así

denominada Tarjeta de Circuito Integrado Universal (UICC) que puede, a su vez, comprender una aplicación de Módulo de Identidad de Abonado Universal (USIM) para utilizar en autentificar el dispositivo móvil en la red móvil. El área de almacenamiento segura proporcionada por tal subsistema informático fiable, por ejemplo, la memoria de la UICC, es muy adecuada para almacenar de forma segura la clave de inicio en el dispositivo móvil.

Opcionalmente, al menos uno del grupo de: verificar la validez de la clave de inicio, y utilizar la clave de inicio en realizar el procedimiento de concordancia de clave, es realizado por el subsistema informático fiable. De ahí que, la utilización de la clave de inicio fuera del área de almacenamiento segura proporcionada por el sistema informático fiable es reducida o evitada. Ventajosamente, se hace más difícil una falsificación de la clave de inicio.

Opcionalmente, el método comprende además:

- cargar previamente un conjunto de claves de inicio en cada uno de los dispositivos móviles, estando asociado el conjunto de claves de inicio con un conjunto respectivo de períodos de validez; y

- realizar un procedimiento de sincronización de clave entre los dispositivos móviles sobre el canal de comunicación D2D para seleccionar una coincidente del conjunto de claves de inicio en cada uno de los dispositivos móviles como la clave de inicio.

Como tal, cada uno de los dispositivos móviles está provisto con múltiples claves de inicio diferentes. Para habilitar una misma clave de inicio que está siendo utilizada por cada uno de los dispositivos móviles en el establecimiento de la sesión de comunicación D2D, se realiza un procedimiento de sincronización de clave en el que se identifica que clave de inicio está disponible para todos o para la mayoría de los dispositivos móviles, siendo dicha clave de inicio seleccionada para utilizar en el establecimiento de la sesión de comunicación D2D. Ventajosamente, se puede establecer una clave de inicio adecuada. Ventajosamente, el procedimiento de sincronización de clave proporciona realimentación si un dispositivo móvil no tiene una clave de inicio adecuada antes de realizar el procedimiento de concordancia de clave.

Opcionalmente, el método comprende además:

- cargar previamente un conjunto de identificadores de clave en cada uno de los dispositivos móviles, identificando cada uno del conjunto de identificadores de clave una clave respectiva del conjunto de claves de inicio; y

- realizar el procedimiento de sincronización de clave basándose en un intercambio de uno o más del conjunto de identificadores de clave entre los dispositivos móviles.

Realizando el procedimiento de sincronización de clave basado en un intercambio de uno o más del conjunto de identificadores de clave, no es necesario implicar a las propias claves de inicio en el procedimiento de sincronización de clave, por ejemplo, intercambiando las claves de inicio sobre el canal de comunicación D2D. Ventajosamente, se hace más difícil una falsificación de las claves de inicio ya que sólo se intercambian los identificadores de clave. Sin embargo, una falsificación de los identificadores de clave, por ejemplo, de modo que simulen una coincidencia de claves de inicio, fallará aún ya que el procedimiento de concordancia de clave sólo proporciona la clave de sesión si la clave de inicio actual coincide.

Opcionalmente, el método comprende además deshabilitar o eliminar la clave de inicio del conjunto de clave de inicio después de utilizarla en el establecimiento de la sesión de comunicación D2D. Así, una clave de inicio sólo puede ser utilizada una vez en el establecimiento de una sesión de comunicación D2D. Para establecer una nueva sesión de comunicación D2D, se necesita una clave de inicio nueva. Ventajosamente, el operador obtiene control sobre un número de veces que puede establecerse una sesión de comunicación D2D, por ejemplo, para limitar dicho número de veces.

Opcionalmente, el conjunto de períodos de validez está constituido al menos en parte por períodos de validez diferentes pero solapados. Los periodos de validez diferentes pero solapados constituyen juntos un periodo de tiempo mayor. Como los periodos de validez se solapan, no hay espacios en el periodo de tiempo mayor. Los períodos de tiempo diferentes pero solapados están asociados con claves de inicio. Como resultado, en cualquier punto en el tiempo en el periodo mayor, hay disponible una clave de inicio que puede ser utilizada de forma válida en el establecimiento de la sesión de comunicación D2D.

Opcionalmente, la clave de inicio está asociada con una identidad de red virtual, y la verificación de la validez de la clave de inicio comprende además determinar una coincidencia de la identidad de red virtual en cada uno de los dispositivos móviles a través del canal de comunicación D2D. Así, la sesión de comunicación D2D sólo se puede establecer entre dispositivos móviles que tienen una misma identidad de red virtual. Ventajosamente, el operador puede configurar una red virtual de dispositivos móviles entre los que es posible la comunicación D2D, mientras que impide la comunicación D2D con dispositivos móviles fuera de dicha red virtual o entre dispositivos móviles que pertenecen a redes virtuales diferentes.

Opcionalmente, la clave de inicio está asociada con un recuento de uso para limitar un número de usos de la clave de inicio, y la verificación de la validez de la clave de inicio está además basada en el recuento de usos. Ventajosamente, el operador obtiene control sobre un número de veces que se puede establecer una sesión de comunicación D2D. Ventajosamente, dicho control puede estar provisto con una clave de inicio, por ejemplo, una clave maestra, que puede

ser utilizada para establecer múltiples sesiones de comunicación D2D. Así, no hay necesidad de proporcionar un conjunto de claves de inicio que sólo pueden ser utilizadas una vez cada una para establecer una sesión de comunicación D2D.

Opcionalmente, el método comprende además ajustar el recuento de uso después de utilizar la clave de inicio en el establecimiento de la sesión de comunicación D2D. De ahí que, una utilización de la clave de inicio en el establecimiento de una sesión de comunicación D2D queda reflejada en el recuento de uso.

Opcionalmente, el método comprende además solicitar otra clave de inicio a través de la red móvil si i) ninguna clave de inicio es considerada válida, o ii) si el procedimiento de concordancia de clave falla al proporcionar la clave de sesión.

Opcionalmente, el procedimiento de concordancia de clave comprende:

- un procedimiento de autenticación de tres pasos; o

- una utilización de la clave de inicio para cifrar un intercambio de mensajes entre los dispositivos móviles para obtener un secreto compartido, y un procedimiento Diffie-Hellman de intercambio de clave que es iniciado basándose en el secreto compartido.

Pueden llevarse a cabo modificaciones y variaciones del software de control, del dispositivo móvil y de la red móvil, que corresponden a las modificaciones y variaciones descritas del método, por expertos en la técnica basándose en la presente descripción.

La invención está definida en las reivindicaciones adjuntas. Aún de forma ventajosa realizaciones opcionales están definidas en las reivindicaciones dependientes.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Estos y otros aspectos de la invención son evidentes a partir de las realizaciones descritas de aquí en adelante y serán aclarados con referencia a las mismas. En los dibujos,

La fig. 1 muestra dispositivos móviles que se pueden conectar mutuamente a través de un canal de comunicación D2D y que se pueden conectar de forma individual a una red móvil;

La fig. 2 muestra un método para el establecimiento de una sesión de comunicación D2D entre los dispositivos móviles;

La fig. 3 muestra un dispositivo móvil que comprende un subsistema móvil y un subsistema informático, comprendiendo el subsistema informático un área de almacenamiento;

La fig. 4 muestra una determinación de una coincidencia de una identidad de red virtual en cada uno de los dispositivos móviles a través del canal de comunicación D2D;

La fig. 5 muestra una realización de un procedimiento de sincronización de clave entre los dispositivos móviles sobre el canal de comunicación D2D;

La fig. 6 muestra un procedimiento de concordancia de clave que se inicia sobre el canal de comunicación D2D utilizando una clave de inicio para cifrar un intercambio de mensajes entre los dispositivos móviles para obtener un secreto compartido;

La fig. 7 muestra un procedimiento de concordancia de clave que es realizado sobre el canal de comunicación D2D, que está basado en un procedimiento de autenticación de tres pasos; y

La fig. 8 muestra otro procedimiento de concordancia de clave que es realizado sobre el canal de comunicación D2D en el que los identificadores que identifican los dispositivos móviles están cifrados.

Debería observarse que artículos que tienen los mismos números de referencia en diferentes Figuras, tienen las mismas características estructurales y las mismas funciones, o son las mismas señales. Donde se ha explicado la función y/o la estructura de tal artículo, no hay necesidad de una explicación repetida de lo mismo en la descripción detallada.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

La fig. 1 muestra un primer dispositivo móvil MD1 y un segundo dispositivo móvil MD2, en lo sucesivo también denominados conjuntamente como dispositivos móviles MD. Los dispositivos móviles MD se pueden conectar individualmente a una red móvil MN. Esto se ha ilustrado en la fig. 1 por una canal de comunicación que existe entre cada dispositivo móvil MD y la red móvil MN, es decir, un canal de comunicación de dispositivo a red DNC. La red móvil MN se ha mostrado que comprende estaciones base BS1, BS2. En este ejemplo particular, cada uno de los dispositivos móviles MD está conectado a una diferente de las estaciones base BS1, BS2. Las estaciones base BS1, BS2 están conectadas mutuamente a través de los nodos centrales CN de la red móvil. Como tal, cuando los dispositivos móviles MD están conectados a la red móvil MN, la comunicación entre los dispositivos móviles MD puede tener lugar a través de la red móvil MN porque se puede realizar un intercambio de información a través de una primera de las estaciones

base BS1, los nodos centrales CN, y una segunda de las estaciones base BS2 de la red móvil MN, o viceversa.

Los dispositivos móviles MD también se pueden conectar mutuamente a través de un canal DDC de comunicación D2D. El canal DDC de comunicación D2D puede haber sido establecido o configurado utilizando un subsistema móvil MS1, MS2 de cada dispositivo móvil respectivo MD1, MD2. La presente invención implica el establecimiento de una sesión de comunicación D2D entre los dispositivos móviles MD sobre el canal DDC de comunicación D2D.

La sesión de comunicación D2D puede ser establecida de acuerdo con el método 100 como se ha mostrado en la fig. 2. El método 100 comprende en primer lugar la carga previa 120 de una clave de inicio en cada uno de los dispositivos móviles MD. La carga previa 120 puede ser realizada utilizando la red móvil MN. Para ese propósito, la red móvil MN puede estar dispuesta para, cuando uno de los dispositivos móviles MD está conectado a la red móvil MN, proporcionar la clave de inicio a dicho dispositivo móvil MD a través del canal de comunicación de dispositivo a red DNC. Sin embargo, la carga previa 120 puede implicar también otro canal de comunicación, y en particular un canal de comunicación segura. Por ejemplo, la clave de inicio puede ser cargada previamente utilizando Comunicación de Campo Cercano (NFC), por ejemplo, en un punto de venta físico, o utilizando Wi-Fi, por ejemplo, a través de una Red de Área Local Inalámbrica (WLAN).

Aunque no se ha mostrado en la fig. 1, cada dispositivo móvil MD puede comprender un área de almacenamiento para almacenar la clave de inicio en el dispositivo móvil MD respectivo. Por consiguiente, la operación de carga previa 120 de la clave de inicio en cada uno de los dispositivos móviles MD puede comprender almacenar la clave de inicio en el área de almacenamiento del dispositivo móvil MD respectivo.

La clave de inicio está asociada con un periodo de validez. El método 100 comprende además, en cada uno de los dispositivos móviles MD, la verificación 140 de una validez de la clave de inicio basada en el tiempo actual. Para ese propósito, cada dispositivo móvil MD1, MD2 comprende un subsistema informático CS1, CS2 que está previsto para realizar dicha operación y que puede tener conocimiento del tiempo actual o estar previsto para obtener el tiempo actual. Se ha observado que el periodo de validez puede ser expresado en cualquier cantidad basada en el tiempo adecuada, por ejemplo, un día, una hora de un día, un minuto de una hora, etc. Por consiguiente, el término tiempo actual puede referirse a, por ejemplo, un día actual y/o un momento actual del día. De ahí que, la verificación de la validez de la clave de inicio puede comprender determinar si el día actual cae dentro del periodo de validez, y si es así, si el día actual es bien un primer día o bien un último día del periodo de validez, y si es así, si el tiempo actual del día cae dentro del periodo de validez.

El método 100 comprende además, en cada uno de los dispositivos móviles MD, si la clave de inicio es considerada válida, la generación 160 de una clave de sesión que utiliza la clave de inicio utilizando la clave de inicio en la realización de un procedimiento de concordancia de clave en los dispositivos móviles MD sobre el canal DDC de comunicación D2D. El subsistema informático CS1, CS2 de cada dispositivo móvil MD está previsto para realizar dicha operación, mientras que implica que el subsistema móvil MS1, MS2 lleva a cabo un intercambio de mensajes actual sobre el canal DDC de comunicación D2D.

El procedimiento de concordancia de clave está previsto para dar como resultado la clave de sesión si la clave de inicio utilizada por cada uno de los dispositivos móviles MD coincide. Habiendo obtenido la clave de sesión, el método 100 comprende, en cada uno de los dispositivos móviles MD, el establecimiento 180 de la sesión de comunicación D2D sobre el canal DDC de comunicación D2D basado en la clave de sesión. El subsistema móvil MS1, MS2 de cada dispositivo móvil MD está previsto para realizar dicha operación utilizando la clave de sesión obtenida a partir del subsistema informático CS1, CS2.

Aunque no se ha mostrado en la fig. 2, el software de control puede ser proporcionado comprendiendo instrucciones para, durante la ejecución del software de control de un dispositivo móvil, hacer que el dispositivo móvil establezca la sesión de comunicación D2D de acuerdo con el método 100 como se ha mostrado en la fig. 2, es decir, mediante la verificación 140 de una validez de la clave de inicio basada en un tiempo actual, la generación 160 de una clave de sesión utilizando la clave de inicio, y el establecimiento 180 de la sesión de comunicación D2D sobre el canal de comunicación D2D basado en la clave de sesión.

La fig. 3 muestra el primer dispositivo móvil MD1 de forma más detallada, siendo aquí ejemplar el primer dispositivo móvil MD1 de cada uno de los dispositivos móviles MD. El primer dispositivo móvil MD1 comprende un subsistema móvil MS1 y un subsistema informático CS1 como se ha introducido anteriormente con referencia a las figs. 1 y 2. Aquí, el término subsistema móvil se refiere a un subsistema del dispositivo móvil que realiza y/o habilita la funcionalidad principal del dispositivo móvil, incluyendo el establecimiento de un canal de comunicación, el intercambio de mensajes sobre el canal de comunicación establecido, la realización de distintas funciones de cómputo, etc. Un ejemplo de un subsistema móvil es un Sistema móvil en un Chip (SoC) que comprende un procesador de aplicación, un procesador de presentación, uno o más módems, una radio LTE integrada. Otro ejemplo es dicho SoC móvil y una radio LTE externa que está conectada al SoC móvil.

La fig. 3 muestra el primer dispositivo móvil MD1 que comprende un área de almacenamiento SA1 para almacenar la clave de inicio como es proporcionada durante el procedimiento de carga previa. El área de almacenamiento SA1 puede ser un área de almacenamiento segura. En el ejemplo de la fig. 3, el área de almacenamiento SA1 es proporcionada por

el subsistema informático CS1. El subsistema informático CS1 puede ser un subsistema informático fiable, proporcionando automáticamente de este modo un área de almacenamiento segura. Tal subsistema informático CS1 fiable puede estar constituido por una UICC que comprende una aplicación USIM. La aplicación USIM puede estar prevista para establecer la sesión de comunicación D2D de acuerdo con el método 100 como se ha mostrado en la fig. 2. La interfaz hacia y desde la UICC puede estar protegida por medio del protocolo de canal seguro, por ejemplo, de acuerdo con la especificación técnica ETSI TS 102 484, de modo que haga más difícil las escuchas ilegales y la falsificación.

A continuación, se presentan dos realizaciones detalladas de la presente invención que comprenden cada una distintas medidas ventajosas aún opcionales. Se apreciará que aquellas medidas también pueden ser combinadas y/o aplicadas individualmente al concepto general de la presente invención, a menos que sea impedido por incompatibilidades técnicas.

La primera realización detallada comprende la carga previa de un conjunto de claves de inicio en cada uno de los dispositivos móviles MD, estando asociado el conjunto de claves de inicio con un conjunto respectivo de períodos de validez. Para ese propósito, la red móvil MN puede enviar uno o más mensajes al subsistema informático CS1, CS2 de cada dispositivo móvil MD1, MD2 a través de cada subsistema móvil MS1, MS2 respectivo. Los uno o más mensajes pueden comprender el conjunto de claves de inicio y el conjunto de períodos de validez. Además, los uno o más mensajes pueden comprender un tiempo de red actual y/o un conjunto de limitaciones. Además del conjunto de claves de inicio y del conjunto de períodos de validez, los uno o más mensajes pueden comprender un conjunto de identificadores de clave, identificando cada uno del conjunto de identificadores de clave una clave respectiva del conjunto de claves de inicio. Además del conjunto de claves de inicio y del conjunto de períodos de validez, los uno o más mensajes pueden comprender un conjunto de identidades de red virtual, estando asociada cada una del conjunto de identidades de red virtual con una clave respectiva del conjunto de claves de inicio.

La siguiente tabla muestra un ejemplo de la información que puede ser cargada previamente en un dispositivo móvil:

Id Red Virtual	Id Clave	Clave de Inicio	Valido desde (hh:mm dd:mm:yyyy)	Válido a Través de (hh:mm dd:mm:yyyy)
Corporación X	102	Secret123	11:00 01/01/2012	13:00 02/01/2012
Corporación X	103	Geheim123	11:00 01/01/2012	13:00 02/01/2012
Corporación X	104	gEHEIM321	11:00 01/01/2012	13:00 02/01/2012
Corporación X	105	SeCRet123	11:00 02/01/2012	13:00 03/01/2012
Corporación X	106	GeHEim123	11:00 02/01/2012	13:00 03/01/2012
Corporación X	107	sEcrET321	11:00 02/01/2012	13:00 03/01/2012
Operador Y	53	sECRET321	00:00 01/12/2011	03:00 01/01/2012
Operador Y	54	123secret	00:00 01/12/2011	03:00 01/01/2012
Operador Y	55	sECRet321	00:00 01/01/2012	03:00 01/02/2012
Operador Y	56	123seCRet	00:00 01/01/2012	03:00 01/02/2012

En general, como es el caso en el ejemplo anterior, el conjunto de períodos de validez puede estar constituido al menos en parte por períodos de validez diferentes pero solapados.

Cada subsistema informático CS1, CS2 puede almacenar el conjunto de claves de inicio, el conjunto de identificadores de clave y el tiempo de red actual en un área de almacenamiento segura SA1 del subsistema informático. Cada subsistema informático CS1, CS2 también puede disponer de cualesquiera claves de inicio ya almacenadas que han expirado de acuerdo con el tiempo de red actual. El conjunto de identidades de red virtuales puede ser almacenado en otro lugar en cada uno de los dispositivos móviles MD1, MD2, es decir, puede no necesitar ser almacenado en el subsistema informático CS1, CS2.

Como parte del establecimiento de la sesión de comunicación D2D sobre el canal DDC de comunicación D2D, se puede determinar si una identidad de red virtual en cada uno de los dispositivos móviles MD coincide. Esto permite habilitar que se establezcan sesiones de comunicación D2D entre dispositivos móviles MD que comparten una identidad de red virtual, mientras que impide que se establezcan sesiones de comunicación D2D entre dispositivos móviles MD que no comparten una identidad de red virtual. Por ejemplo, un dispositivo móvil corporativo puede comprender una identidad de red virtual de la corporación así como una identidad de red virtual de la propia red virtual del operador. Esto último puede permitir a los usuarios establecer una sesión de comunicación D2D con otros usuarios de la red móvil del operador. En general, se pueden proporcionar identidades de red virtuales para, por ejemplo, una cierta localidad, un cierto grupo de usuarios, empresas, familias, etc. También se puede proporcionar una identidad de red virtual que permite que se establezcan sesiones de comunicación D2D a través del operador, es decir, entre dispositivos móviles que normalmente pertenecen a redes móviles que son operadas por diferentes operadores.

La fig. 4 muestra un ejemplo 142 de cómo se puede determinar una coincidencia de una identidad de red virtual en cada uno de los dispositivos móviles MD a través del canal DDC de comunicación D2D. Aquí, el subsistema informático CS1 y el subsistema móvil MS1 del primer dispositivo móvil MD1 se han mostrado esquemáticamente en un lado izquierdo, y el subsistema informático CS2 y el subsistema móvil MS2 del segundo dispositivo móvil MD2 se han mostrado en un lado derecho. Además, se ha mostrado un intercambio de mensajes entre los dispositivos móviles MD1, MD2 a través del

canal DDC de comunicación D2D a lo largo del tiempo por medio de flechas que indican una fuente y destino del mensaje. Además, se han utilizado rectángulos redondeados para indicar las operaciones realizadas por cualquiera de los dispositivos móviles MD1, MD2, indicando una posición horizontal de un rectángulo en qué subsistema se realiza la operación.

Una coincidencia de la identidad de red virtual puede ser determinada como sigue. En primer lugar, el primer dispositivo móvil MD1 envía un mensaje al segundo dispositivo móvil MD2 sobre el canal de comunicación D2D, comprendiendo el mensaje muchas o todas las identidades de red virtual que son almacenadas en el primer dispositivo móvil MD1. En respuesta, en una operación titulada DET_OVERLAP_STEP, el segundo dispositivo móvil MD2 determina cuál de las identidades de red virtuales del primer dispositivo móvil MD1 se solapa con la almacenada localmente, es decir, en el segundo dispositivo móvil MD2. Además, en una operación titulada ORDER_STEP, las identidades de red virtuales que se solapan son ordenadas de acuerdo con una lista de prioridad del segundo dispositivo móvil MD2, y un resultado de las mismas es enviado por mensaje al primer dispositivo móvil MD1. Durante la recepción, en una operación titulada SELECT_STEP, las identidades de red virtuales que se solapan también son ordenadas de acuerdo con una lista de prioridad del primer dispositivo móvil MD1, y una de las identidades de red virtuales que se solapan es seleccionada que ocupa el primer lugar cuando se combinan ambas listas de prioridad. Finalmente, la identidad de red virtual seleccionada es enviada por mensaje al segundo dispositivo móvil MD2, que a su vez reconoce la identidad de red virtual seleccionada por el mensaje de retorno.

La verificación de la validez de la clave de inicio puede comprender la determinación antes mencionada de la coincidencia de la identidad de red virtual en cada uno de los dispositivos móviles a través del canal de comunicación D2D. Por consiguiente, si no puede encontrarse una coincidencia de identidad de red virtual, las claves de inicio en ambos dispositivos móviles pueden ser consideradas inválidas con el propósito de establecer una sesión de comunicación D2D entre los dispositivos móviles MD ya que dichas claves están asociadas con identidades de red virtuales no coincidentes.

Habiendo verificado la coincidencia de la identidad de red virtual, el establecimiento de la sesión de comunicación D2D puede continuar como sigue. Cada uno de los dispositivos móviles MD1, MD2 puede estar previsto para realizar un procedimiento de sincronización de clave entre los dispositivos móviles sobre el canal de comunicación D2D para seleccionar una clave coincidente del conjunto de claves de inicio en cada uno de los dispositivos móviles como la clave de inicio. La fig. 5 muestra un ejemplo 162 de tal procedimiento de sincronización de claves. Este ejemplo particular está basado en un intercambio de uno o más del conjunto de identificadores de clave entre los dispositivos móviles MD1, MD2. Aquí al solicitar del subsistema móvil MS1, el subsistema informático CS1 busca un identificador de clave que está asociado con una clave de inicio válida, significando que dicha clave de inicio es válida en el momento actual y no ha sido utilizada antes en el establecimiento de una sesión de comunicación D2D. El subsistema informático CS1 puede buscar el identificador de clave basado en distintos criterios, tales como por ejemplo, si un identificador de clave es válido en el momento actual y en un período razonable en el futuro, por ejemplo, los siguientes 15 minutos. La búsqueda puede también estar basada en un número de secuencia de clave asociado con cada uno de los identificadores de clave, seleccionando el subsistema informático CS1 uno de los identificadores de clave que está asociado con un número de secuencia de clave más bajo. En caso de que los identificadores de clave sean numéricos, el subsistema informático CS1 puede también seleccionar uno de los identificadores de clave más bajo. En caso de que los identificadores de clave estén ordenados secuencialmente, el subsistema informático CS1 puede también seleccionar un primero o un último de los identificadores de clave. Se apreciará que pueden ser combinados distintos criterios tales como los anteriores.

El subsistema informático CS1 envía el identificador de clave KeyID que se ha encontrado al subsistema móvil MS1, que a su vez lo envía al segundo dispositivo móvil MD2. Sobre el segundo dispositivo móvil MD2, el subsistema móvil MS2 reenvía el identificador de clave KeyID al subsistema informático CS2. Además, el segundo dispositivo móvil MD2 también realizada un mismo proceso, bien en paralelo o después de recibir el identificador de clave KeyID desde el primer dispositivo móvil MD1. Como resultado, los subsistemas informáticos CS1, CS2 en cada dispositivo móvil MD1, MD2 comprenden ambos identificadores de clave. Cada subsistema informático CS1, CS2 selecciona entonces, en una operación titulada MAX_KEYID_STEP, el identificador de clave que es más alto, seleccionando también por lo tanto la clave de inicio que es identificada por dicho identificador de clave.

Se ha observado que, en general, las claves de inicio pueden ser deshabilitadas o eliminadas después de su uso en el establecimiento de una sesión de comunicación D2D. En este caso, sin embargo, ciertos tipos de procedimientos de sincronización de claves, tales como el ejemplo mostrado en la fig. 5, pueden conducir a un consumo rápido de claves de inicio. Alternativamente, el primer dispositivo móvil MD1 puede enviar el identificador de clave al segundo dispositivo móvil MD2. El segundo dispositivo móvil MD2 puede solicitar a su subsistema informático CS2 que determine si comprende una clave de inicio válida asociada con este identificador de clave. Si es así, la clave de inicio puede ser seleccionada directamente. Si no es así, el subsistema informático CS2 puede buscar un identificador de clave más bajo que esté asociado con una clave de inicio válida, y devolver el identificador de clave encontrado al subsistema móvil MS2 para enviarlo al primer dispositivo móvil MD1. Al recibirlo, el primer dispositivo móvil MD1 puede solicitar a su subsistema informático CS1 que determine si comprende una clave de inicio válida asociada con este identificador de clave. Si es así, la clave de inicio puede ser seleccionada directamente. Si no es así, el subsistema informático CS1 puede buscar el identificador de clave más bajo y repetir de nuevo el proceso anterior.

Se ha observado que el procedimiento de sincronización de clave alternativo anterior puede ser repetido varias veces. Alternativamente, el procedimiento de sincronización de clave puede estar basado en un intercambio de muchos o de todos los identificadores de clave disponibles a cada dispositivo móvil respectivo así como en determinar más rápidamente un identificador de clave que identifica una coincidencia y una clave de inicio válida.

Se ha observado además que el procedimiento de intercambio de clave puede ser combinado con un procedimiento de autenticación. El procedimiento de autenticación puede ser una parte de un requisito previo de la configuración de la sesión de comunicación D2D. Como resultado, los mensajes que son intercambiados entre los dispositivos móviles pueden servir tanto para el propósito de autenticación así como para el intercambio de claves. Las figs. 7 y 8 muestran un ejemplo de esto. Por ejemplo, un mensaje puede constituir una respuesta al desafío desde un dispositivo móvil mientras al mismo tiempo es parte del procedimiento de intercambio de claves entre los dispositivos móviles.

Habiendo seleccionado una de las claves coincidentes del conjunto de claves de inicio en cada uno de los dispositivos móviles como la clave de inicio, el establecimiento de la sesión de comunicación D2D puede continuar utilizando la clave de inicio en la realización de un procedimiento de concordancia de clave entre los dispositivos móviles sobre el canal de comunicación D2D. La fig. 6 muestra un ejemplo 164 de una primera parte de tal procedimiento de concordancia de clave, que comprende utilizar la clave de inicio para cifrar un intercambio de mensajes entre los dispositivos móviles para obtener un secreto compartido. Esta primera parte del procedimiento de concordancia de clave puede ser utilizada para inicializar un procedimiento de intercambio de clave basado en el secreto compartido. Esencialmente, la primera parte del procedimiento de concordancia de clave puede ser considerada como un arranque del intercambio de claves subsiguiente. Un ejemplo de tal procedimiento de intercambio de claves es el intercambio de claves Diffie-Hellman como se conoce a partir del campo de la criptografía.

En el ejemplo de la fig. 6, cada uno de los subsistemas informáticos CS1, CS2 recupera la clave de inicio desde el área de almacenamiento. En una operación titulada ENC_SECRET1_STEP, el subsistema informático CS1 del primer dispositivo móvil MD1 crea un mensaje que comprende un secreto, es decir, secret1, cifrado con la clave de inicio. El mensaje es reenviado al subsistema móvil MS1 que a su vez envía el mensaje al segundo dispositivo móvil MD2. Aquí, el subsistema móvil MS2 reenvía el mensaje al subsistema informático CS2. En una operación titulada DEC_SECRET1_STEP, el subsistema informático CS2 cifra el mensaje con la clave de inicio. En una operación titulada ENC_SECRET2_STEP, el subsistema informático CS2 crea un mensaje con otro secreto, es decir, secret2, cifrado con la clave de inicio. Además, en una operación titulada CALC_SK_STEP, una clave de sesión SK es calculada basándose en la combinación de ambos secretos, es decir, secret1 y secret2, e incluida en el mensaje. El mensaje es enviado de nuevo por el segundo dispositivo móvil MD2 al primer dispositivo móvil MD1. Aquí, el subsistema móvil MS1 reenvía el mensaje al subsistema informático CS1. En una operación titulada DEC_SECRET2_STEP, el subsistema informático CS1 descifra el mensaje con la clave de inicio. En una operación titulada CALC_SK_STEP, la clave de sesión SK es calculada basándose en la combinación de ambos secretos. Como resultado, en cada uno de los subsistemas informáticos CS1, CS2, ambos secretos están disponibles, es decir, secret1 y secret2, permitiendo así que los subsistemas informáticos respectivos calculen una misma clave de sesión SK.

Se ha observado que en lugar del ejemplo de la fig. 6, pueden utilizarse distintos mecanismo alternativos también para obtener el secreto compartido. Por ejemplo, se puede utilizar uno de los mecanismos del establecimiento de clave punto a punto como se ha descrito en la norma ISO/IEC 11770-2. Por ejemplo, se puede utilizar el mecanismo de establecimiento de clave 5 como se ha descrito en la sección 6.5 de dicho documento.

Como un resultado del procedimiento de intercambio de claves subsiguiente, una clave de sesión es obtenida en cada uno de los dispositivos móviles MD1, MD2. Esto permite que se establezca la sesión de comunicación D2D sobre el canal de comunicación D2D basándose en la clave de sesión.

Una segunda realización detallada comprende cargar previamente una así denominada clave maestra en cada uno de los dispositivos móviles MD1, MD2. Aquí, el término clave maestra se refiere a una clave de inicio que es combinada con un recuento de uso de modo que permita establecer múltiples sesiones de comunicación D2D utilizando una clave de inicio. La clave de inicio y el recuento de uso constituyen una alternativa a la carga previa de una pluralidad de claves de inicio que pueden ser utilizadas cada una sólo una vez en el establecimiento de una sesión de comunicación D2D. Se ha observado que la clave de inicio puede constituir una clave maestra porque, cada vez que se necesita una clave de inicio para el establecimiento de una sesión de comunicación D2D particular, una clave de inicio temporal es derivada de la clave maestra para ese propósito. De ahí que, la clave de inicio puede ser utilizada múltiples veces para establecer una clave de inicio temporal para utilizar en una sesión de comunicación D2D particular. La red móvil MN puede proporcionar al subsistema informático CS1, CS2 de cada dispositivo móvil MD1, MD2 tal clave de inicio, siendo válida la clave de inicio para un período de validez particular. Además, la red móvil MN puede proporcionar o establecer el recuento de uso. El recuento de uso puede representar, por ejemplo, un número de veces que se permite al subsistema informático generar una clave de sesión utilizando la clave de inicio. La red móvil MN también puede proporcionar periódicamente el tiempo de red actual de modo que permita a cada subsistema informático CS1, CS2 disponer de cualquiera de las claves de inicio almacenadas en el subsistema informático que ya han expirado de acuerdo con el tiempo de red actual. Adicional o alternativamente, la red móvil MN puede proporcionar el tiempo de red actual cuando carga previamente una clave de inicio en el dispositivo móvil MD1, MD2.

Después de haber verificado posiblemente una coincidencia de una identidad de red virtual, la validez de la clave de

inicio es verificada basándose en un tiempo actual y en el recuento de uso, y si la clave de inicio es considerada válida, la clave de inicio es utilizada en la realización de un procedimiento de concordancia de clave entre los dispositivos móviles sobre el canal de comunicación D2D. Un ejemplo 166 de esto se ha mostrado en la fig. 7, donde se ha mostrado el procedimiento de concordancia de clave que está basado en un procedimiento de autenticación de tres pasos, como se ha especificado, por ejemplo, por la norma ISO/IEC 9798-4.

Inicialmente, cada uno de los subsistemas informáticos CS1, CS2 proporciona un identificador, es decir, ID1 e ID2, respectivamente, a cada uno de los subsistemas móviles MS1, MS2 respectivo. Cada identificador ID1, ID2, identifica el dispositivo móvil respectivo MD1, MD2. La identificación puede ser indirecta porque cada identificador ID1, ID2 puede identificar el subsistema informático CS1, CS2 respectivo, que a su vez permite que el dispositivo móvil MD1, MD2 sea identificado ya que el subsistema informático CS1, CS2 es un parte integral o que se puede separar del dispositivo móvil.

Las operaciones adicionales mostradas en la fig. 7 pueden ser explicadas como sigue. Aquí, los números corresponden a los mostrados en la fig. 7.

1. El primer dispositivo móvil MD1, que es en este ejemplo el dispositivo móvil que inicia el procedimiento de concordancia de clave, solicita al subsistema informático CS1 proporcionar un identificador de clave KeyID que identifica una clave de inicio que es válida en el tiempo actual. El subsistema informático CS1 determina, en una operación titulada SELECT_KEYID_STEP, si comprende tal clave de inicio y si es así, si el uso de la clave de inicio está aún permitido, por ejemplo, comprobando si el recuento de uso está aún por debajo de un umbral dado en el caso de que el recuento de uso corresponda a un número de usos, o si el recuento de uso está aún por encima de cero en el caso de que el recuento de uso corresponda a un número de usos restantes. Si es este el caso, la clave de inicio se considera que es válida, y el subsistema informático CS1 establece un identificador de clave KeyID que identifica la clave de inicio. Además, el subsistema informático CS1 genera un RND1 aleatorio, constituyendo el RND1 aleatorio un desafío en la autenticación del subsistema informático CS2 del segundo dispositivo móvil MD2.

2. El subsistema informático CS1 proporciona el identificador de clave KeyID y el RND1 aleatorio al subsistema móvil MS1 del primer dispositivo móvil MD1.

3. El primer dispositivo móvil MD1 envía el identificador de clave KeyID, el RND1 aleatorio y el identificador ID1 al segundo dispositivo móvil MD2 sobre el canal DDC de comunicación D2D de modo que inicie el procedimiento de concordancia de clave.

4. En respuesta, el segundo dispositivo móvil MD2 solicita a su subsistema informático CS2 que inicie el procedimiento de concordancia de clave. Para ese propósito, proporciona el identificador de clave KeyID, el RND1 aleatorio y el identificador ID1 al subsistema informático CS2. Además, el subsistema informático CS2 puede solicitar al segundo dispositivo móvil MD2 que proporcione el tiempo actual de modo que habilite al subsistema informático CS2 para verificar si la clave de inicio identificada por el identificador KeyID es válida para el tiempo actual. Esto constituye una operación de verificación adicional en el final de recepción, es decir, no inicialización, del procedimiento de concordancia de clave. Cuando la clave de inicio identificada por el identificador de clave KeyID está disponible para el subsistema informático CS2 y si el uso de la clave de inicio está aún permitido, por ejemplo, en el caso de que su recuento de uso esté aún por encima de cero, el subsistema informático CS2 genera, en una operación titulada CALC_RESP1_STEP, un RND2 aleatorio y una clave de sesión SK_A para la autenticación. El subsistema informático CS2 calcula además una respuesta al desafío del primer dispositivo móvil MD1, que está indicada como $E\_SK_A(X)$ con X = RND1 ‖ RND2 ‖ ID2. Aquí, el E_SK_A indica una función de cifrado que utiliza SK_A como la clave de sesión y X como el mensaje. Un ejemplo de tal función es un Código de Autenticación de Mensaje (MAC).

5. El subsistema informático CS2 proporciona $E\_SK_A(X)$ y el RND2 aleatorio al subsistema móvil MS2 del segundo dispositivo móvil MD2.

6. El segundo dispositivo móvil MD2 envía $E\_SK_A(X)$, el RND2 aleatorio y el identificador ID2 al primer dispositivo móvil MD1, constituyendo una respuesta a la operación 3.

7. El primer dispositivo móvil MD1 solicita a su subsistema informático CS1 que autentifique la respuesta recibida desde el segundo dispositivo móvil MD2 y que genere una respuesta al desafío proporcionado en la forma de RND2.

8. En una operación titulada CALC_RESP2_STEP, el subsistema informático CS1 genera una clave de sesión para la autenticación de SK_A, y comprueba la respuesta $E\_SK_A(X)$ desde el segundo dispositivo móvil MD2. El subsistema informático CS1 entonces calcula una respuesta al desafío desde el segundo dispositivo móvil MD2, que está indicada por $E\_SK_A(Y)$ con Y = RND2 ‖ RND1 ‖ ID1. El subsistema informático CS1 genera una clave de sesión para utilizar en la sesión SK_C de comunicación D2D, y opcionalmente una clave de sesión para protección de integridad SK_1. El subsistema informático CS1 puede entonces ajustar, por ejemplo, disminuir, el recuento de uso de la clave de inicio. Finalmente, el subsistema informático CS1 proporciona $E\_SK_A(Y)$, la clave de sesión SK_C, y opcionalmente SK_1, al subsistema móvil MS1.

9. El primer dispositivo móvil MD1 envía una respuesta al desafío desde el segundo dispositivo móvil MD2 en la forma de $E\_SK_A(Y)$ al segundo dispositivo móvil MD2.

10. En respuesta, el segundo dispositivo móvil MD2 solicita a su subsistema informático CS2 que compruebe, es decir, autentifique, $E\_SK_A(Y)$.

11. El subsistema informático CS2 entonces determina, en una operación titulada CALC_SESSIONKEY_STEP, si $E\_SK_A(Y)$ es válido, y si es así genera la clave de sesión SK_C, y opcionalmente SK_I, y proporciona ambos al subsistema móvil MS2. El subsistema informático CS2 puede entonces ajustar, por ejemplo, disminuir, el recuento de uso de la clave de inicio.

12. El subsistema móvil MS2 del segundo dispositivo móvil MD2 establece la sesión de comunicación D2D con el subsistema móvil MS1 del primer dispositivo móvil MD1 utilizando la clave de sesión SK_C. De ahí que, se obtiene una sesión de comunicación D2D segura.

La fig. 8 muestra una alternativa 168 al procedimiento de concordancia de clave 166 como se ha mostrado en la fig. 7. Una diferencia se refiere a que aquí, los identificadores ID1 e ID2 son cifrados durante el intercambio, mientras que en el procedimiento de concordancia de clave de la fig. 7, los identificadores ID1 e ID2 se intercambiaron sin ser cifrados. Cifrando los identificadores ID1 e ID2 durante el intercambio, se puede impedir que los usuarios sean seguidos y/o identificados a través de escuchas ilegales del intercambio de mensajes entre los dispositivos móviles MD1, MD2.

Las operaciones adicionales mostradas en la fig. 8 puede ser explicada como sigue. Aquí, los números corresponden a los mostrados en la fig. 8.

1. La operación 1 corresponde a la operación 1 como se ha descrito con referencia a la fig. 7, con la adición de que el subsistema informático CS1 genera un desafío, que es esencialmente un mensaje que es cifrado utilizando la clave de inicio, estando indicado el mensaje cifrado por E_MK, y comprendiendo el mensaje cifrado el RND1 aleatorio y el identificador ID1.

2. El subsistema informático CS1 proporciona el identificador de clave KeyID y el desafío al subsistema móvil MS1 del primer dispositivo móvil MD1.

3. El primer dispositivo móvil MD1 envía el identificador de clave KeyID, y el desafío al segundo dispositivo móvil MD2 sobre el canal DDC de comunicación D2D de modo que inicialice el procedimiento de concordancia de clave.

4. En respuesta, el segundo dispositivo móvil MD2 solicita a su subsistema informático CS2 que inicie el procedimiento de concordancia de clave. Para ese propósito, proporciona el identificador de clave KeyID, el desafío al subsistema informático CS2. Además, el subsistema informático CS2 puede solicitar al segundo dispositivo móvil MD2 proporcionar el tiempo actual de modo que habilite al subsistema informático CS2 para que verifique si la clave de inicio identificada por el identificador de clave KeyID es válida para el tiempo actual. Esto constituye una operación de verificación adicional en el final de recepción, es decir, no inicialización del procedimiento de concordancia de clave. Cuando la clave de inicio identificada por el identificador de clave KeyID está disponible para el subsistema informático CS2 y si el uso de la clave de inicio está aún permitido, por ejemplo, en el caso de que su recuento de uso esté aún por encima de cero, el subsistema informático CS2 genera, en una operación titulada CALC_RESP1_STEP, un RND2 aleatorio y una clave de sesión SKA para la autenticación. El subsistema informático CS2 calcula además una respuesta al desafío desde el primer dispositivo móvil MD1, estando indicada como E_SKA(X) con X = RND1 ‖ RND2 ‖ ID2. Aquí, el E_SKA indica una función de cifrado que utiliza SKA como la clave de sesión y X como el mensaje. Un ejemplo de tal función es un Código de Autenticación de Mensaje (MAC). El subsistema informático CS2 también calcula un desafío, E_MK (RND2‖ID2), para el que se utiliza el mismo E_MK que el subsistema informático CS1 del primer dispositivo móvil MD1 ha utilizado en su desafío.

5. El subsistema informático CS2 proporciona E_SKA(X) y el desafío al subsistema móvil MS2 del segundo dispositivo móvil MD2.

6. El segundo dispositivo móvil MD2 envía E_SKA(X) y el desafío al primer dispositivo móvil MD1, que constituye una respuesta a la operación 3.

7. El primer dispositivo móvil MD1 solicita a su subsistema informático CS1 que autentifique la respuesta recibida desde el segundo dispositivo móvil MD2 y que genere una respuesta al desafío proporcionado en la forma de E_MK(RND2‖ID2).

8-12. Las operaciones 8-12 corresponden a las operaciones 8-12 como se ha descrito con referencia a la fig. 7.

Se ha observado que en general, un subsistema informático de un dispositivo móvil puede solicitar una clave de inicio adicional a través de la red móvil si i) ninguna clave de inicio es considerada válida, o ii) el procedimiento de concordancia de clave falla al proporcionar la clave de sesión.

Se apreciará que la presente invención puede aplicarse ventajosamente a LTE Directo, es decir, comunicación D2D basada en LTE entre dispositivos móviles. En particular, la presente invención permite los siguientes usos ventajosos.

La corporación X ha comprado una suscripción de modo directo desde el operador Y para todos sus empleados. Como resultado, por ejemplo una vez a la semana durante la noche o durante la carga de red baja, todos los dispositivos

móviles de la corporación, tales como teléfonos móviles y adaptadores inalámbricos de red, son proporcionados con un conjunto de un centenar de claves de inicio que son válidas para todos los días de la siguiente semana. En un Lunes próximo, varios empleados tienen una reunión en la que les gustaría compartir una presentación. Sin embargo, están situados en una sala de reuniones sin cobertura de red, es decir, están fuera de un rango de la red móvil. Ellos enchufan sus adaptadores inalámbricos de red en sus ordenadores portátiles y configuran una red ad hoc basada en una LTE Directo. Como la mayoría de los adaptadores inalámbricos de red fueron provistos con un mismo conjunto de claves de inicio, los empleados son capaces de configurar una sesión de comunicación D2D basada en LTE en la sala de reuniones sin necesitar acceso a la red móvil.

Otro uso ventajoso puede ser el siguiente. De nuevo la corporación X ha comprado una suscripción de modo directo. De nuevo, por ejemplo una vez a la semana durante la noche o durante la carga de red baja, todos los dispositivos móviles de la corporación están provistos con un conjunto de un centenar de claves de inicio que son válidas para cada día de la siguiente semana. Sin embargo, un adaptador inalámbrico de red se apagó durante dicho procedimiento de carga previa. Al lunes siguiente, varios empleados tienen una reunión en la que les gustaría compartir una presentación. Están situados en una sala con cobertura de red. Enchufan sus adaptadores inalámbricos de red y configuran una red ad hoc basada en LTE Directo. Debido a que la mayoría de los adaptadores inalámbricos de red fueron provistos con un mismo conjunto de claves de inicio, los empleados son capaces de configurar una sesión de comunicación D2D basada en LTE en la sala de reuniones sin necesitar acceder a la red móvil. Sin embargo, el adaptador inalámbrico de red que se apagó durante el procedimiento de carga previa puede aún unirse a la sesión de comunicación D2D solicitando desde la red móvil el conjunto de claves de inicio, y una vez que se ha proporcionado dicho conjunto, el adaptador inalámbrico de red se une a la sesión de comunicación D2D.

Otro uso ventajoso puede ser el siguiente, que es el mismo que el uso antes mencionado, excepto en que los empleados están situados en una sala con cobertura de red. Enchufan sus adaptadores inalámbricos de red en sus portátiles y establecen una red ad hoc basándose en LTE Directo. Algunos adaptadores inalámbricos de red ya tienen claves disponibles para la sesión de comunicación D2D, pero sólo a algunos les ha expirado la clave, por ejemplo, debido a que la comunicación D2D no ha sido utilizada durante algún tiempo y por lo tanto no ha sido necesario cargar previamente o actualizar claves de inicio. Todos los adaptadores inalámbricos de red solicitan ahora desde la red móvil un conjunto de claves de inicio y una vez que se ha proporcionado dicho conjunto, cada adaptador inalámbrico de red se une a la sesión de comunicación D2D. Más tarde ese día, los empleados vuelven a encontrarse. Ahora, puede establecerse inmediatamente una sesión e comunicación D2D, es decir, sin una necesidad de contactar la red móvil, ya que los adaptadores inalámbricos de red tienen ahora un conjunto de claves de inicio válidas.

Aún otro uso ventajoso puede ser el siguiente. Para servicios de emergencia, es de suma importancia ser capaz de comunicar en todo momento. De ahí que, un dispositivo móvil que se basa en la cobertura de red para establecer una sesión de comunicación D2D puede no ser deseable. Esto se puede evitar cargando previamente claves de inicio de forma frecuente, por ejemplo, cada vez que cuando un dispositivo móvil es encendido, y/o cargando previamente claves de inicio que están asociadas con un período de validez que es relativamente largo. La carga previa también puede ocurrir cada noche, cuando todos los dispositivos móviles están en una localización central. Durante el día, los bomberos, la policía y el personal de ambulancias pueden elegir el funcionamiento en modo directo en caso de que la recepción de red sea inadecuada, permitiendo aún de este modo la comunicación entre dicho personal de servicio de emergencia.

Debería observarse que las realizaciones mencionadas anteriormente ilustran en vez de limitar la invención, y los expertos en la técnica serán capaces de diseñar muchas realizaciones alternativas.

En las reivindicaciones, cualquier signo de referencia situado entre paréntesis no debe ser interpretado como que limita la reivindicación. La utilización de verbo “comprender” y sus conjugaciones no excluye la presencia de elementos u operaciones diferentes de las indicadas en una reivindicación. El artículo “un”, "una", “uno” precediendo a un elemento no excluye la presencia de una pluralidad de tales elementos. La invención puede ser implementada por medio de un hardware que comprende varios elementos distintos, y por medio de un ordenador programado adecuadamente. En la reivindicación del dispositivo que enumera varios medios, varios de estos medios pueden ser realizados por uno y el mismo elemento de hardware. El mero hecho de que ciertas medidas son enumeradas de nuevo en reivindicaciones dependientes mutuamente diferentes no indica que una combinación de estas medidas no pueda ser utilizada de forma ventajosa.

REIVINDICACIONES

1. El método (100) para que un dispositivo móvil (MD1) establezca una sesión de comunicación [D2D] de dispositivo a dispositivo con otro dispositivo móvil (MD2), pudiendo conectarse el dispositivo móvil (MD1) a través de un canal (DDC) de comunicación D2D al otro dispositivo móvil (MD2) y pudiendo conectarse el dispositivo móvil (MD1) a la red móvil (MN), que comprende el paso en el dispositivo móvil (MD1) de:

- cargar previamente (120) una clave de inicio en el dispositivo móvil (MD1), estando asociada la clave de inicio con un período de validez;

caracterizado por que comprende los pasos en el dispositivo móvil (MD1) de:

- verificar (140) una validez de la clave de inicio basada en el período de validez;
- si la clave de inicio se considera válida, generar (160) una clave de sesión utilizando la clave de inicio en la realización (164, 166) de un procedimiento de concordancia de clave con el otro dispositivo móvil (MD2) sobre el canal (DDC) de comunicación D2D, dando como resultado el procedimiento de concordancia de clave la clave de sesión, si la clave de inicio utilizada por el dispositivo móvil (MD1) coincide con la clave de inicio utilizada por el otro dispositivo móvil (MD2); y

- establecer (180) la sesión de comunicación D2D sobre el canal (DDC) de comunicación D2D basado en la clave de sesión.

2. El método (100) según la reivindicación 1, en el que la carga previa (120) de la clave de inicio comprende proporcionar la clave de inicio al dispositivo móvil (MD1, MD2) a través de la red móvil (MN) cuando el dispositivo móvil está conectado a la red móvil.

3. El método (100) según la reivindicación 1 ó 2, en el que la carga previa (120) de la clave de inicio comprende almacenar la clave de inicio en un área de almacenamiento segura (SA1) del dispositivo móvil (MD1, MD2).

4. El método (100) según la reivindicación 3, en el que el área de almacenamiento segura (SA1) es proporcionada por un subsistema informático fiable (CS1, CS2) del dispositivo móvil (MD1, MD2), y en el que al menos una del grupo de: la verificación (140) de la validez de la clave de inicio, y la utilización de la clave de inicio en la realización del procedimiento de concordancia de clave, es realizada por el subsistema informático fiable (CS1, CS2).

5. El método (100) según cualquiera de las reivindicaciones anteriores, que comprende además:

- cargar previamente (120) un conjunto de claves de inicio en el dispositivo móvil (MD1, MD2), estando asociado el conjunto de claves de inicio con un conjunto respectivo de períodos de validez; y

- realizar (162) un procedimiento de sincronización de clave con el otro dispositivo móvil (MD2, MD1) sobre el canal (DDC) de comunicación D2D para seleccionar una clave coincidente del conjunto de claves de inicio como la clave de inicio.

6. El método (100) según la reivindicación 5, que comprende además:

- cargar previamente (120) un conjunto de identificadores de clave en el dispositivo móvil (MD1, MD2), identificando cada uno del conjunto de identificadores de clave una clave respectiva del conjunto de claves de inicio; y

- realizar (162) el procedimiento de sincronización de clave basándose en un intercambio de uno o más del conjunto de identificadores de clave con el otro dispositivo móvil.

7. El método (100) según la reivindicación 5 ó 6, que comprende además deshabilitar o eliminar la clave de inicio del conjunto de claves de inicio después de su utilización en el establecimiento de la sesión de comunicación D2D.

8. El método (100) según cualquiera de las reivindicaciones 5-7, en el que el conjunto de períodos de validez está constituido al menos en parte por períodos de validez diferentes pero solapados.

9. El método (100) según cualquiera de las reivindicaciones anteriores, en el que la clave de inicio está asociada con una identidad de red virtual, y en el que la verificación (140) de la validez de la clave de inicio comprende además determinar (142) una coincidencia de la identidad de red virtual en el dispositivo móvil (MD1, MD2) con la identidad de red virtual utilizada en el otro dispositivo móvil (MD2, MD1), a través del canal (DDC) de comunicación D2D.

10. El método (100) según cualquiera de las reivindicaciones anteriores, en el que la clave de inicio está asociada con un recuento de uso para limitar un número de usos de la clave de inicio, y en el que la verificación (140) de la validez de la clave de inicio está además basada en el recuento de uso, comprendiendo además, opcionalmente, el método ajustar el recuento de uso después de utilizar la clave de inicio en el establecimiento de la sesión de comunicación D2D.

11. El método (100) según cualquiera de las reivindicaciones anteriores, que comprende además solicitar otra clave de inicio a través de la red móvil (MN) si i) ninguna clave de inicio es considerada válida, o ii) el procedimiento de concordancia de clave falla al proporcionar la clave de sesión.

12. El método según cualquiera de las reivindicaciones anteriores, en el que el procedimiento de concordancia de clave comprende:

- un procedimiento (166) de autenticación de tres pasos; o

- una utilización (164) de la clave de inicio para cifrar un intercambio de mensajes entre el dispositivo móvil y el otro dispositivo móvil para obtener un secreto compartido, y un procedimiento Diffie-Hellman de intercambio de claves que es iniciado basándose en el secreto compartido.

13. Un software de control que comprende instrucciones para, durante la ejecución del software de control en un dispositivo móvil (MD1, MD2), hacer que el dispositivo móvil establezca la sesión de comunicación D2D de acuerdo con el método de cualquiera de las reivindicaciones anteriores.

14. El dispositivo móvil (MD1) para el establecimiento de una sesión de comunicación [D2D] de dispositivo a dispositivo con otro dispositivo móvil (MD2), pudiendo conectarse el dispositivo móvil al otro dispositivo móvil a través de un canal (DDC) de comunicación D2D y pudiendo conectarse el dispositivo móvil a una red móvil (MN), comprendiendo el dispositivo móvil:

- un área de almacenamiento (SA1) para almacenar una clave de inicio que es proporcionada durante un procedimiento de carga previa, estando asociada la clave de inicio con un período de validez;

caracterizado por que comprende:

- un subsistema informático (CS1) para:

- verificar una validez de la clave de inicio basándose en el período de validez;

- si ninguna clave de inicio es considerada válida, solicitar otra clave de inicio a través de la red móvil (MN);

- si la clave de inicio es considerada válida, generar una clave de sesión utilizando la clave de inicio en la realización de un procedimiento de concordancia de clave con el otro dispositivo móvil (MD2) sobre el canal (DDC) de comunicación D2D, dando como resultado el procedimiento de concordancia de clave la clave de sesión si la clave de inicio utilizada por el dispositivo móvil y el otro dispositivo móvil coincide; y

- un subsistema móvil (MS1) para establecer la sesión de comunicación D2D sobre el canal de comunicación D2D basándose en el clave de sesión.

15. La red móvil (MN) dispuesta parar cargar previamente una clave de inicio en un dispositivo móvil (MD1) según la reivindicación 14 cuando el dispositivo móvil está conectado a la red móvil, estando asociada la clave de inicio con un período de validez.

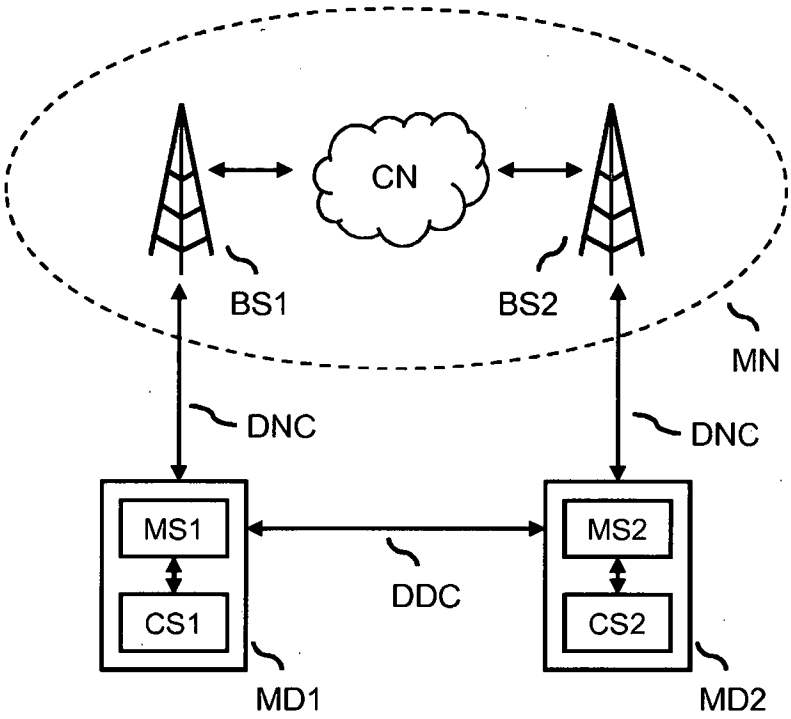

Fig. 1

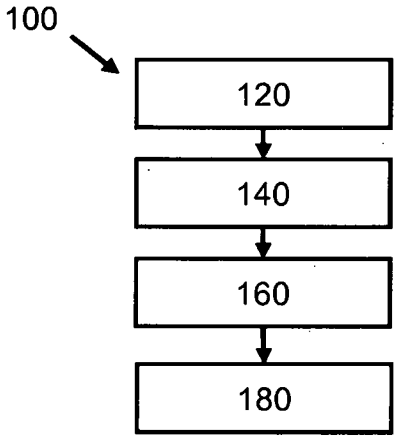

Fig. 2

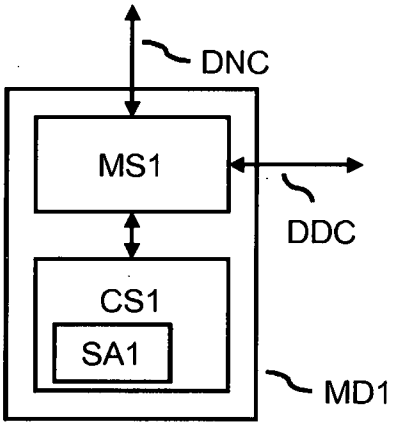

Fig. 3

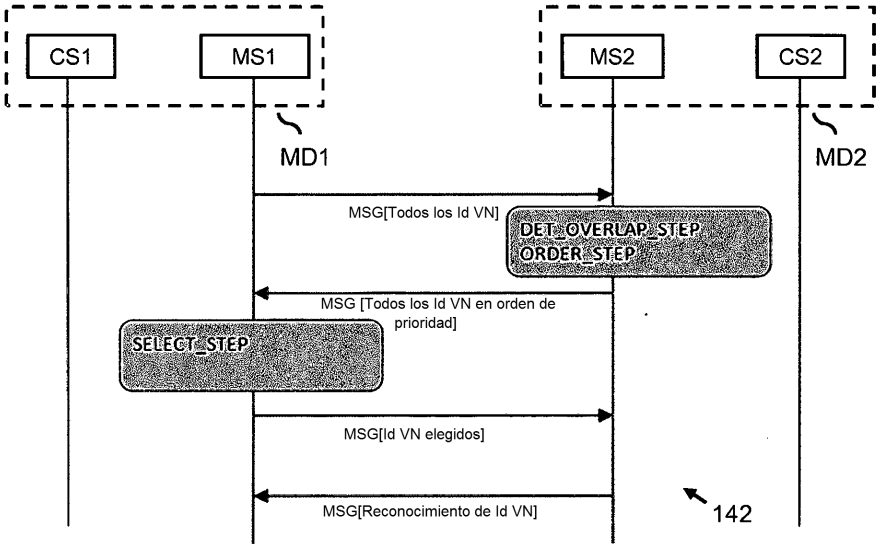
CS1
MS1
MS2
CS2
MD1
MD2
MSG[Todos los Id VN]
DET_OVERLAP_STEP
ORDER_STEP
MSG [Todos los Id VN en orden de prioridad]
SELECT_STEP
MSG[Id VN elegidos]
MSG[Reconocimiento de Id VN]
142

Fig. 4

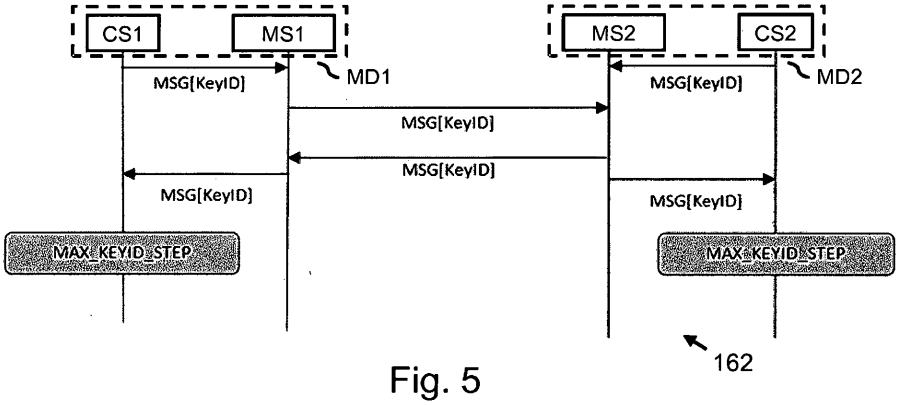
CS1
MS1
MS2
CS2
MD1
MD2
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MSG[KeyID]
MAX_KEYID_STEP
MAX_KEYID_STEP
162

Fig. 5

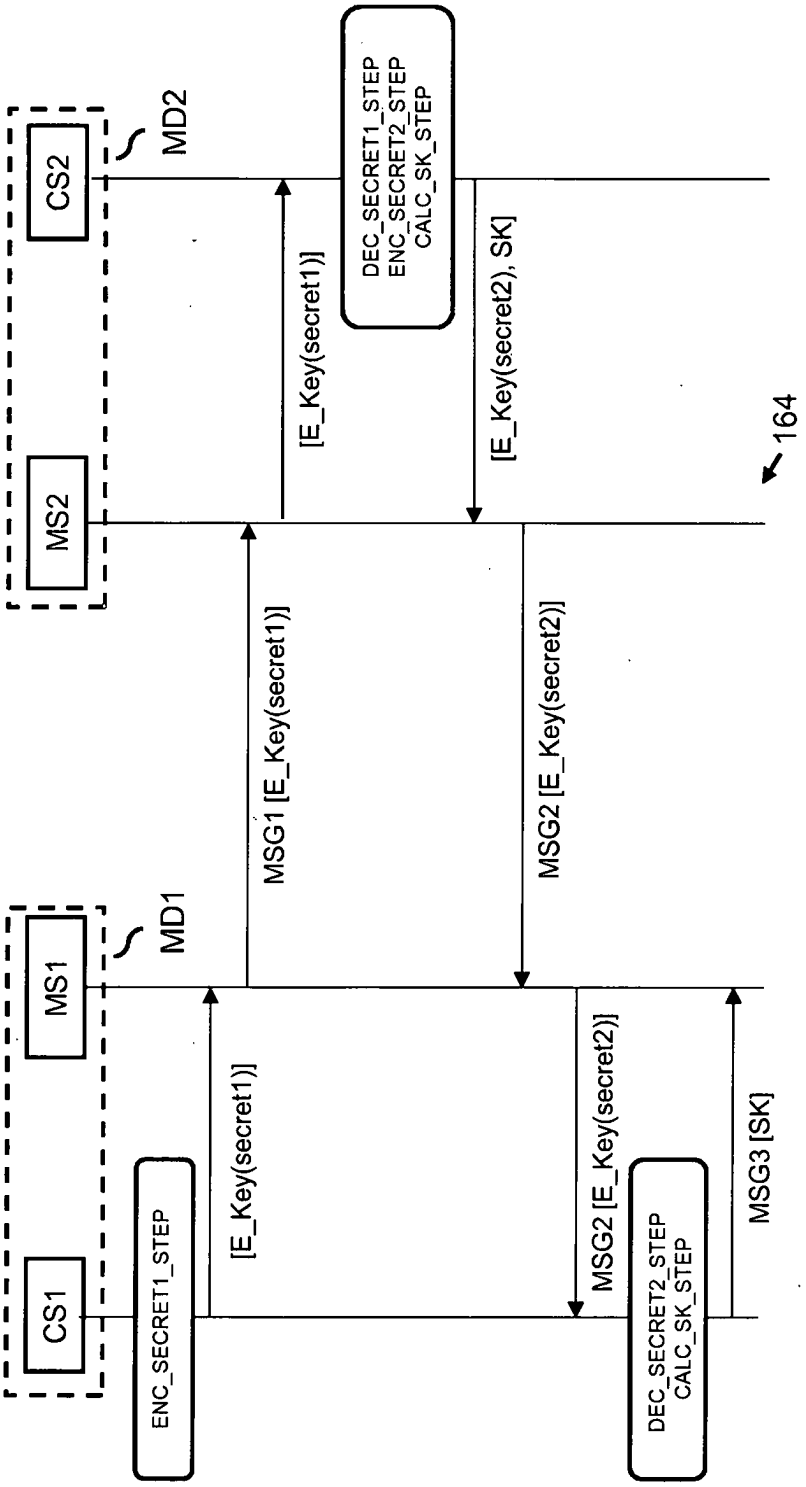
CS2
MS2
MD2
DEC_SECRET1_STEP
ENC_SECRET2_STEP
CALC_SK_STEP
[E_Key(secret1)]
[E_Key(secret2), SK]
164
MSG1 [E_Key(secret1)]
MSG2 [E_Key(secret2)]
CS1
MS1
MD1
ENC_SECRET1_STEP
[E_Key(secret1)]
MSG2 [E_Key(secret2)]
DEC_SECRET2_STEP
CALC_SK_STEP
MSG3 [SK]

Fig. 6

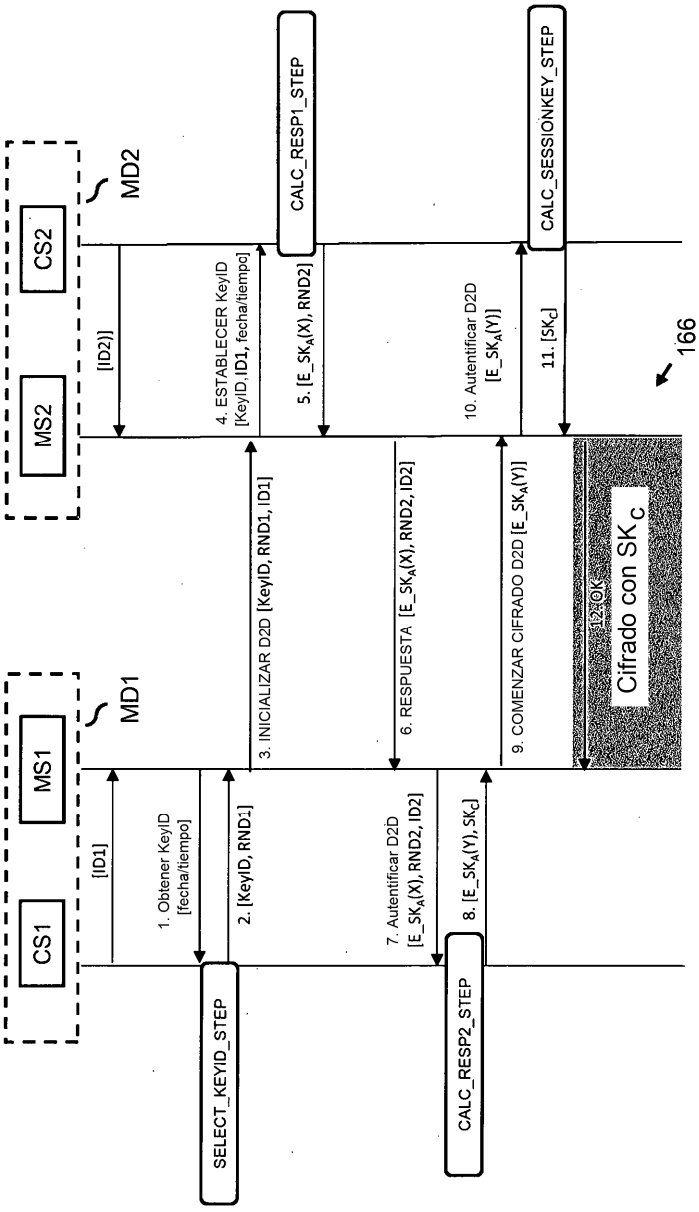
CS1
MS1
MD1
CS2
MS2
MD2
[ID1]
1. Obtener KeyID [fecha/tiempo]
2. [KeyID, RND1]
3. INICIALIZAR D2D [KeyID, RND1, ID1]
4. ESTABLECER KeyID [KeyID,ID1, fecha/tiempo]
[ID2]
SELECT_KEYID_STEP
CALC_RESP1_STEP
5. [E_SK_A(X), RND2]
6. RESPUESTA [E_SK_A(X), RND2, ID2]
7. Autentificar D2D [E_SK_A(X), RND2, ID2]
8. [E_SK_A(Y), SK_C]
CALC_RESP2_STEP
9. COMENZAR CIFRADO D2D [E_SK_A(Y)]
10. Autentificar D2D [E_SK_A(Y)]
11. [SK_C]
CALC_SESSIONKEY_STEP
Cifrado con SK_C
166

Fig. 7

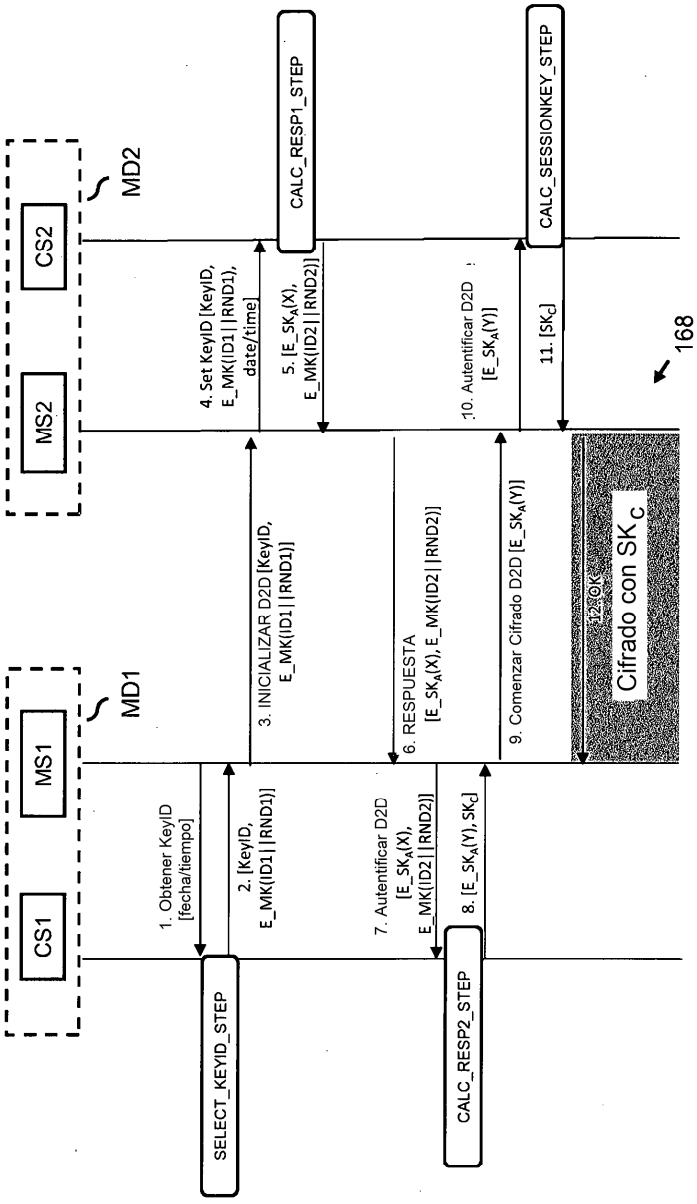
CS1
MS1
MD1
CS2
MS2
MD2
1. Obtener KeyID [fecha/tiempo]
2. [KeyID, E_MK(ID1||RND1)]
3. INICIALIZAR D2D [KeyID, E_MK(ID1||RND1)]
4. Set KeyID [KeyID, E_MK(ID1||RND1), date/time]
5. [E_SK_A(X), E_MK(ID2||RND2)]
6. RESPUESTA [E_SK_A(X), E_MK(ID2||RND2)]
7. Autentificar D2D [E_SK_A(X), E_MK(ID2||RND2)]
8. [E_SK_A(Y), SK_C]
9. Comenzar Cifrado D2D [E_SK_A(Y)]
10. Autentificar D2D [E_SK_A(Y)]
11. [SK_C]
SELECT_KEYID_STEP
CALC_RESP2_STEP
CALC_RESP1_STEP
CALC_SESSIONKEY_STEP
Cifrado con SK_C
168

Fig. 8