(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 833 292**

(51) Int. CI.:

H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.08.2014 PCT/JP2014/004393**

(87) Fecha y número de publicación internacional: **07.05.2015 WO15063991**

(96) Fecha de presentación y número de la solicitud europea: **27.08.2014 E 14772449 (6)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2020 EP 3063970**

(54) Título: **Aparato, sistema y método de comunicación directa segura en servicios basados en proximidad**

(30) Prioridad:

30.10.2013 JP 2013225200
31.10.2013 JP 2013226681

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.06.2021

(73) Titular/es:

NEC CORPORATION (100.0%)
7-1, Shiba 5-chome Minato-ku
Tokyo 108-8001, JP

(72) Inventor/es:

ZHANG, XIAOWEI y
PRASAD, ANAND RAGHAWA

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Aparato, sistema y método de comunicación directa segura en servicios basados en proximidad

Campo técnico

La presente invención se refiere a un aparato, un sistema y un método para ProSe (Servicios basados en Proximidad). En particular, esta invención se refiere a la seguridad para la comunicación directa en ProSe y considera la comunicación directa autorizada por la red. Además, esta invención se refiere a la comunicación directa de proximidad utilizando PKI (Infraestructura de Clave Pública) y considera no solamente la comunicación directa uno a uno, sino también la comunicación directa uno a muchos.

Antecedentes de la técnica

La comunicación directa ha sido estudiada por 3GPP (Proyecto de asociación de 3ª generación) (véase NPL 1 y 2).

La cuestión clave para la comunicación directa es asegurar una interfaz PC5. Cómo asegurar la interfaz PC5 y cómo establecer el contexto de seguridad (incluyendo, por ejemplo, derivación, asignación, actualización de claves) desde una fuente de confianza, con una señalización mínima, son cuestiones importantes.

Obsérvese que la interfaz PC5 es un punto de referencia entre los UE (más de un artículo de Equipo de Usuario) de tal manera que los UE pueden tener comunicación directa a través de ellos. La interfaz PC5 se utiliza para control y plano de usuario para descubrimiento ProSe, comunicación directa y retransmisión UE. La comunicación directa del UE se puede realizar directamente o mediante LTE-Uu.

Lista de citas

Literatura que no es de patentes

NPL 1: 3GPP TR 33.cde, “Study on security issues to support Proximite Services (Release 12)” (“Estudio de cuestiones de seguridad para soportar servicios de proximidad (Lanzamiento 12)”), V0.2.0, 2013-07, Cláusulas 5.4, 5.5 y 6.3, páginas 11, 12 y 13-20.

NPL 2: 3 GPP TR 23.703, “Study on architecture enhancements to support Proximity Services (ProSe) (Release 12)” (“Estudio de mejoras en la arquitectura para soportar Servicios de Proximidad (ProSe) (Lanzamiento 12)”), V’.4.1, 2013-06, Cláusulas 5.4, 5.12 y 6.2, páginas 13, 17, 18 y 62-82.

El documento US 2006/150241 A1 describe un método y sistema para la autenticación de un dispositivo de red doméstica en una red doméstica. Según el método de autenticación de dispositivo, se mantiene una lista de claves públicas que incluye una ID e información de clave pública correspondiente al ID de los dispositivos de red doméstica. Cuando se recibe un acceso de un dispositivo de unión, se solicita al dispositivo de unión un ID e información relacionada con una clave pública del dispositivo de unión. El ID y la información de clave pública son recibidos del dispositivo de unión, y la lista de claves públicas se actualiza añadiendo el ID y la información de clave pública recibidos. La lista de claves públicas antes de actualizarse se transmite al dispositivo de unión. El ID y la información de clave pública del dispositivo de unión se transmiten a los dispositivos de la red doméstica. El dispositivo de unión es un nuevo dispositivo que se una a una red doméstica.

El documento WO 2013/118096 A1 describe un método para asegurar el descubrimiento dispositivo a dispositivo. El método puede incluir la recepción, en un terminal, de una señal de descubrimiento de dispositivo a dispositivo (D2D). La señal de descubrimiento D2D puede incluir información de descubrimiento D2D y una indicación de un nivel de seguridad aplicado a la información de descubrimiento D2D incluida en la señal de descubrimiento D2D. El método puede incluir la determinación, basándose al menos en parte, en la indicación, del nivel de seguridad aplicado a la información de descubrimiento D2D.

El documento US 2010/329465 A1 describe que una aplicación de estación de maya para un acceso a una red incluye una lista de estaciones de pares en mensajes de un protocolo de establecimiento de clave autenticada. UN distribuidor de clave de malla deriva una clave de entrega de claves y genera una clave de nivel superior, y a continuación entrega la clave de nivel superior a una estación de malla. Siguiendo el protocolo de establecimiento de clave, el distribuidor de clave de malla también crea claves por pares para utilizar entre la estación de malla y las estaciones de pares listadas en su lista de pares. La lista de pares permite que el identificador para el par se vincule a la clave derivada, lo que da como resultado una clave que se utiliza entre cada par de pares. Una vez que el distribuidor de clave de malla finaliza la creación de una clave para una de las estaciones en la lista de pares, el distribuidor de clave de malla envía un mensaje el par para iniciar una pulsación de clave.

Compendio de la Invención

Problema técnico

Sin embargo, los inventores de esta aplicación han descubierto que la solución actual en 3GPP SA3 (Grupo de

trabajo de seguridad) tiene los siguientes inconvenientes.

1) Impacto en MME (Entidad de Gestión de Movilidad): necesita que la MME se involucre en el procedimiento de comunicación directa, incluyendo la asignación de materiales clave.
2) El procedimiento de asignación de claves ocurre cada vez que el UE quiere tener comunicación directa con otro UE, lo que no solamente crea señalización sino también cuando ocurre una comunicación uno a uno concurrente. Por tanto, la solución no es eficaz.

Solución al problema

La presente invención proporciona un sistema, un UE, Funciones de Servicios de Proximidad, y métodos correspondientes, como se define en las reivindicaciones independientes adjuntas. Las características opcionales del sistema y el método se exponen en las reivindicaciones dependientes adjuntas.

En un ejemplo un UE incluye: medios de adquisición para adquirir claves de raíz de un nodo al registrar con éxito el UE con el nodo, soportando el nodo la comunicación directa entre el UE y uno o más UE diferentes que se encuentran en las proximidades del UE y se les permite comunicarse con el UE; y medios de derivación para derivar, mediante el uso de una de las claves de raíz, un par de claves de sesión para realizar de forma segura la comunicación directa con uno de los diferentes UE.

Además, un nodo según un ejemplo soporta la comunicación directa entre los UE que están en proximidad entre sí y se les permite comunicarse entre sí. Este nodo incluye: medios de adquisición para adquirir claves de raíz de un servidor al registrar con éxito uno de los UE con el nodo, utilizándose las claves de raíz para que dicho UE derive un par de claves de sesión para realizar de forma segura la comunicación directa con al menos otro de los UE, gestionando el servidor las claves de raíz; y medios de distribución para distribuir las claves de raíz a dicho uno de los UE.

Además, un servidor según un ejemplo incluye: medios de almacenamiento para almacenar claves de raíz para cada uno de los UE para derivar un par de claves de sesión para realizar una comunicación directa de forma segura con al menos otro de los UE, estando los UE en proximidad entre sí y se les permite comunicarse entre sí; y medios de respuesta para responder a una solicitud de un nodo enviando las claves de raíz al nodo, soportando el nodo la comunicación directa entre los UE.

Además, un sistema de comunicaciones según un ejemplo incluye: una pluralidad de UE que están en proximidad entre sí y se les permite realizar una comunicación directa entre sí; un nodo que soporta la comunicación directa; y un servidor que gestiona claves de raíz para cada uno de los UE para derivar un par de claves de sesión para realizar de forma segura la comunicación directa con al menos otro de los UE. El nodo adquiere las claves de raíz del servidor al registrar con éxito cada uno de los UE con el nodo, y distribuye las claves de raíz adquiridas a cada uno de los UE. Cada uno de los UE deriva las claves de sesión utilizando una de las claves de raíz distribuidas.

Además, un método según un ejemplo proporciona un método para controlar operaciones en un UE. Este método incluye: adquirir claves de raíz de un nodo al registrar con éxito el UE con el nodo, soportando el nodo la comunicación directa entre el UE y uno o más UE diferentes que están en la proximidad del UE y se les permite comunicarse con el UE; y derivar, mediante el uso de una de las claves de raíz, un par de claves de sesión para realizar de forma segura la comunicación directa con uno de los diferentes UE.

Además, un método según un ejemplo proporciona un método para controlar operaciones en un nodo que soporta la comunicación directa entre UE que están en proximidad entre sí y se les permite comunicarse entre sí. Este método incluye: adquirir claves de raíz de un servidor al registrar con éxito uno de los UE con el nodo, utilizándose las claves de raíz para que dicho UE derive un par de claves de sesión para realizar de forma segura la comunicación directa con al menos otro de los UE, gestionando el servidor las claves de raíz; y distribuir las claves de raíz a dicho uno de los UE.

Además, un método según un ejemplo proporciona un método para controlar operaciones en un servidor. Este método incluye: almacenar claves de raíz para cada uno de los UE para derivar un par de claves de sesión para realizar de forma segura la comunicación directa con al menos otro de los UE, estando los UE en proximidad entre sí y se les permite comunicarse entre sí; y responder a una solicitud de un nodo enviando las claves de raíz al nodo, soportando el nodo la comunicación directa entre los UE.

Además, un UE según un ejemplo incluye: primeros medios para registrar una clave pública del UE al registrar con éxito el UE con un nodo, y para recuperar claves públicas de uno o más UE diferentes, permitiéndose a los diferentes UE realizar una comunicación directa con el UE cuando los diferentes UE están en proximidad al UE, soportando el nodo la comunicación directa; y segundos medio para verificar, utilizando una clave pública de un primer UE entre los diferentes UE, una solicitud del primer UE para realizar una comunicación directa con el UE, estando protegida la solicitud con una clave privada del primer UE.

Además, un UE según un ejemplo incluye: primeros medios para registrar una clave pública del UE al registrar con éxito el UE con un nodo, y para recuperar claves públicas de uno o más UE diferentes, permitiéndose a los diferentes UE realizar una comunicación directa con el UE cuando los diferentes UE están en proximidad al UE, soportando el nodo la comunicación directa; y segundos medios para verificar, utilizando una clave pública de un primer UE entre los diferentes UE, una respuesta a una primera solicitud protegida para solicitar al primer UE que realice una comunicación directa uno a uno con el UE, estando protegida la respuesta con una clave privada del primer UE.

Además, un nodo según un ejemplo soporta la comunicación directa entre los UE en proximidad entre sí y se les permite comunicarse entre sí. Este nodo incluye: medios de recepción para recibir, al registrar con éxito uno de los UE con el nodo, una clave pública de dicho uno de los UE; y medios de transmisión para transmitir, a dicho UE, claves públicas de los otros UE como respuesta al registro con éxito. Las claves públicas se utilizan para cada uno de los UE para verificar al menos una solicitud de comunicación directa.

Además, un servidor según un ejemplo incluye: medios de almacenamiento para almacenar claves públicas de UE que se le permite realizar una comunicación directa entre sí cuando los UE están en proximidad entre sí, siendo registradas las claves públicas por un nodo que soporta la comunicación directa; y medios de respuesta para responder a una solicitud del nodo enviando las claves públicas almacenadas al nodo. Las claves públicas se utilizan para cada uno de los UE para verificar al menos una solicitud de comunicación directa.

Además, un sistema de comunicaciones según un ejemplo incluye: una pluralidad de UE a los que se les permite realizar una comunicación directa entre sí cuando los UE están en proximidad entre sí; y un nodo que soporta la comunicación directa. Cada uno de los UE comparte claves públicas de los UE a través del nodo al registrar con éxito cada uno de los UE con el nodo, y verifica al menos una solicitud de comunicación directa utilizando una de las claves públicas. El nodo recibe cada una de las claves públicas de cada uno de los UE al registrar cada uno de los UE con el nodo, y transmite, a cada uno de los UE, las claves públicas de diferentes UE como respuesta al registro con éxito.

Además, un método según un ejemplo proporciona un método para controlar operaciones en un UE. Este método incluye: registrar una clave pública del UE al registrar con éxito el UE con un nodo, y recuperar claves públicas de uno o más UE diferentes, permitiéndose a los diferentes UE realizar una comunicación directa con el UE cuando los diferentes UE están en proximidad al UE, soportando el nodo la comunicación directa; y verificar, utilizando una clave pública de un primer UE entre los diferentes UE, una solicitud del primer UE para realizar una comunicación directa con el UE, estando protegida la solicitud con una clave privada del primer UE.

Además, un método según un ejemplo proporciona un método para controlar operaciones en un UE. Este método incluye: registrar una clave pública del UE al registrar con éxito el UE con un nodo, y recuperar claves públicas de uno o más UE diferentes, permitiéndose a los diferentes UE realizar una comunicación directa con el UE cuando los diferentes UE están en proximidad al UE, soportando el nodo la comunicación directa; y verificar, utilizando una clave pública de un primer UE entre los diferentes UE, una respuesta a una solicitud protegida para solicitar al primer UE que realice una comunicación directa uno a uno con el UE, estando protegida la respuesta con una clave privada del primer UE.

Además, un método según un ejemplo proporciona un método para controlar un nodo que soporta una comunicación directa entre los UE en proximidad entre sí y se les permite comunicarse entre sí. Incluyendo este método: recibir, al registrar con éxito uno de los UE con el nodo, una clave pública de dicho uno de los UE; y transmitir, a dicho uno de los UE, claves públicas de los otros UE como respuesta al registro con éxito. Las claves públicas se utilizan para cada uno de los UE para verificar al menos una solicitud de comunicación directa.

Además, un método según un ejemplo proporciona un método para controlar operaciones en un servidor. Este método incluye: almacenar claves públicas de UE a los que se les permite realizar una comunicación directa entre sí cuando los UE están en proximidad entre sí, registrándose las claves públicas por un nodo que soporta la comunicación directa; y responder a una solicitud del nodo enviando las claves públicas almacenadas al nodo. Las claves públicas se utilizan para cada uno de los UE para verificar al menos una solicitud de comunicación directa.

Efectos ventajosos de la invención

Según la presente invención, es posible resolver los problemas mencionados anteriormente y así, proporcionar una solución para asegurar eficazmente la seguridad para la comunicación directa en ProSe.

Por ejemplo, según los ejemplos de la invención, es posible lograr los siguientes efectos ventajosos.

1) Gestión central de claves de raíz, impedir problemas de sincronización.
2) Reducir asignación de raíz cuando cada vez que UE necesite un servicio de comunicación directo.

Breve descripción de los dibujos

La Figura1 es un diagrama de bloques que muestra un ejemplo de configuración de un sistema de comunicaciones según una primera realización ejemplar de la presente invención.

La Figura 2 es un diagrama de secuencia que muestra un ejemplo de operaciones para asignar claves de raíz en el sistema de comunicaciones según la primera realización ejemplar.

La Figura 3 es un diagrama de secuencia que muestra otro ejemplo de operaciones para asignar claves de raíz en el sistema de comunicaciones según la primera realización ejemplar.

La Figura 4 es un diagrama de secuencia que muestra un ejemplo de operaciones para derivar una clave de sesión en el sistema de comunicaciones según la primera realización ejemplar.

La Figura 5 es un diagrama de secuencia que muestra otro ejemplo de operaciones para derivar una clave de sesión en el sistema de comunicaciones según la primera realización ejemplar.

La Figura 6 es un diagrama de bloques que muestra un ejemplo de configuración de un UE según la primera realización ejemplar.

La Figura 7 es un diagrama de bloques que muestra un ejemplo de configuración de un nodo según la primera realización ejemplar.

La Figura 8 es un diagrama de bloques que muestra un ejemplo de configuración de un servidor según la primera realización ejemplar.

La Figura 9 es un diagrama de bloques que muestra un ejemplo de configuración de un sistema de comunicaciones según una segunda realización ejemplar de la presente invención.

La Figura 10 es un diagrama de secuencia que muestra un ejemplo de operaciones para registrar UE en el sistema de comunicaciones según la segunda realización ejemplar.

La Figura 11 es un diagrama de secuencia que muestra un ejemplo de operaciones para derivar una clave de sesión para la comunicación directa uno a uno en el sistema de comunicaciones según la segunda realización ejemplar.

La Figura 12 es un diagrama de secuencia que muestra un ejemplo de operaciones para derivar una clave de sesión para la comunicación directa uno a muchos en el sistema de comunicaciones según la segunda realización ejemplar.

La Figura 13 es un diagrama de bloques que muestra un ejemplo de configuración de un UE según la segunda realización ejemplar.

La Figura 14 es un diagrama de bloques que muestra un ejemplo de configuración de un nodo según la segunda realización ejemplar.

La Figura 15 es un diagrama de bloques que muestra un ejemplo de configuración de un servidor según la segunda realización ejemplar.

Descripción de las realizaciones

En lo sucesivo, se describirán con los dibujos adjuntos una primera y segunda realizaciones ejemplares de un UE, un nodo y un servidor según la presente invención, y un sistema de comunicaciones al que se aplican estos UE, nodo y servidor.

<Primera realización ejemplar>

La Figura 1 muestra un ejemplo de configuración de un sistema de comunicaciones para servicio de proximidad. El servicio de proximidad proporciona el descubrimiento controlado por la red del operador y las comunicaciones entre los UE que se encuentran en proximidad, tanto para uso comercial/social como para uso de seguridad pública. Se requiere que el servicio ProSe debería proporcionarse a los UE con o sin cobertura de red.

Como se muestra en la Figura1, el sistema de comunicaciones según esta realización ejemplar incluye una pluralidad de UE 10_1 a 10_m (en lo sucesivo se pueden denominar colectivamente mediante un código 10), una o más Funciones ProSe 20_1 a 20_n (en lo sucesivo se pueden denominar colectivamente mediante un código 20), una E-UTRAN (Red de Acceso por Radio Terrestre Universal Evolucionada) 30, un EPC (Núcleo de Paquetes Evolucionado) 40 y un Servidor 50 de APP (Aplicación) ProSe.

El UE 10 se conecta al EPC 40 a través del E-UTRAN 30 (es decir, a través de las interfaces LTE-Uu y S1), funcionando por ello como un UE típico. Además, el UE 10 utiliza la interfaz PC5 mencionada anteriormente, realizando por ello comunicación ProSe. Antes de la comunicación ProSe, el UE 10 se registra con la función ProSe 20. Obsérvese que los UE 10_1 a 10_m pueden estar registrados con la misma Función ProSe o funciones ProSe mutuamente diferentes. Además, algunos de los UE 10_1 a 10_m pueden registrarse con la misma Función ProSe.

La función ProSe 20 es un nodo que soporta la comunicación ProSe entre los UE 10_1 a 10_m. La función ProSe 20 puede desplegarse bien en un determinado nodo de red o bien ser un nodo independiente, y puede residir dentro o fuera del EPC 40. La función ProSe 20 se comunica con el UE 10 a través de una interfaz PC3. Además, la función ProSe 20 se comunica con el EPC 40 a través de una interfaz PC4. Además, las Funciones ProSe 20_1 a 20_n pueden comunicarse entre sí a través de una interfaz PC6.

Obsérvese que la interfaz PC3 es un punto de referencia entre el UE 10 y la función ProSe 20. La interfaz PC3 se utiliza para definir la interacción entre el UE 10 y la función ProSe 20. Un ejemplo puede ser utilizar para la

configuración del descubrimiento y la comunicación de ProSe. Además, la interfaz PC4 es un punto de referencia entre el EPC 40 y la función ProSe 20. La interfaz PC4 se utiliza para definir la interacción entre el EPC 40 y la función ProSe 20. Los posibles casos de uso pueden ser cuando se configura una ruta de comunicación uno a uno entre los UE 10_1 a 10_m, o cuando se validan los servicios ProSe (autorización) para la gestión de sesiones o la gestión de movilidad en tiempo real. Además, la interfaz PC6 es un punto de referencia entre las funciones ProSe 20_1 a 20_n. La interfaz PC6 se puede utilizar para funciones tales como el descubrimiento de ProSe entre usuarios abonados a diferentes PLMN (Redes Públicas Móviles Terrestres).

La E-UTRAN 30 está formada por uno o más eNB (Nodos B evolucionados) (no mostrados). El EPC 40 incluye, como sus nodos de red, una MME (Entidad de Gestión de Movilidad) que gestiona la movilidad de los UE 10_1 a 10_m, y similares. El servidor 50 de APP ProSe puede comunicarse con el EPC 40 a través de una interfaz SGi. Además, el servidor 50 de APP ProSe puede comunicarse con el UE 10 a través de una interfaz PC1 y puede comunicarse con la Función 20 ProSe a través de una interfaz PC2. Obsérvese que la interfaz PC1 es un punto de referencia entre las APP ProSe en los UE 10_1 a 10_m y el servidor 50 de APP ProSe. La interfaz PC1 se utiliza para definir los requisitos de señalización a nivel de aplicación. Por otro lado, la interfaz PC2 es un punto de referencia entre la Función 20 ProSe y el servidor 50 de APP ProSe. La interfaz PC2 se utiliza para definir la interacción entre el servidor 50 de APP ProSe y la funcionalidad ProSe proporcionada por 3GPP EPS (Sistema de Paquetes Evolucionado) mediante la función ProSe 20. Un ejemplo puede ser para las actualizaciones de datos de aplicaciones para una base de datos ProSe en la Función 20 ProSe. Otro ejemplo pueden ser los datos para su uso por el servidor 50 de APP ProSe en la intercomunicación entre la funcionalidad 3GPP y los datos de la aplicación, por ejemplo, traducción de nombres. El servidor 50 de APP ProSe puede residir dentro o fuera del EPC 40.

Aunque se omite la ilustración, el sistema de comunicaciones también incluye un servidor operado por un tercero de confianza. En la siguiente descripción, este servidor a veces se denominará simplemente como un "tercero (3º)" y se denominará mediante un código 60. Típicamente, el 3º 60 gestiona las claves de raíz que se describirán más adelante.

A continuación, se describirán en detalle ejemplos de operación de esta realización ejemplar con referencia a las Figuras 2 a 5. Obsérvese que los ejemplos de configuración del UE 10, la función ProSe 20 y el 3º 60 se describirán más adelante con referencia a las Figuras 6 y 8.

Esta realización ejemplar propone utilizar el tercero 60 para derivar, actualizar y asignar claves de raíz. La función ProSe 20 soporta la comunicación directa y asigna todas las claves de raíz al UE 10 en su registro. La clave de sesión se deriva en el lado del UE 10 utilizando la clave de raíz. Por ejemplo, la clave de sesión es un par de claves de confidencialidad e integridad para proteger los mensajes transferidos directamente entre los UE 10_1 a 10_m.

<Operaciones para asignar la clave de raíz>
Se proponen dos opciones para la asignación de clave de raíz.

Opción 1: La clave de raíz está relacionada con un UE dado
La clave de raíz se deriva/asigna en el registro. Suponga que la función ProSe 20 tiene una lista de UE con los que se permite al UE 10_1 comunicarse, y que la función ProSe 20 puede preguntar por todas las claves de raíz para el UE 10_1 al tercero de confianza 60. El tercero 60 es responsable de la derivación y asignación de claves. Las Funciones ProSe 20_1 a 20_n pueden recuperar claves de raíz de terceros 60 para los UE 10_1 a 10_m registrados para ellos de tal manera que no se necesita sincronización entre las Funciones ProSe 20_1 a 20_n. Cada clave de raíz se identifica mediante un KSI (Identificador de Conjunto de Claves) único. Cuando ocurre la comunicación directa, la función ProSe 20 puede indicar a los UE 10_1 a 10_m qué KSI utilizar, o los UE 10_1 a 10_m pueden negociar al respecto.

Específicamente, como se muestra en la Figura 2, el UE 10_1 se registra en la función ProSe 20_1 (etapa S11).

La Función ProSe 20_1 envía Solicitar claves de raíz para el UE 10_1 al tercero 60 que gestiona la clave de raíz (etapa S12).

El tercero 60 responde a la Función ProSe 20_1 con las claves de raíz para el UE 10_1. Cada clave de raíz está relacionada con un KSI único y un UE con el que se le permite al UE 10_1 tener el servicio ProSe (etapa S13).

La Función ProSe 20_1 distribuye las claves de raíz al UE 10_1, incluyendo el ID y el KSI del UE (etapa S14).

El mismo procedimiento que en las etapas S11 a S14 se realiza entre el UE 10_2 y la Función ProSe 20_2 (etapas S15 a S18).

Opción 2: grupo de claves de raíz
De manera similar a la opción 1, los UE pueden obtener un grupo de claves, en el que cada clave tiene un KSI

único para identificarla. Cuando el UE 10_1 necesita una clave de sesión para la comunicación directa, la red (Función ProSe) puede indicar qué clave utilizar, y también dar un mismo parámetro al UE 10_1 y al UE 10_2 de tal manera que puedan derivar las mismas claves de sesión.

La diferencia en comparación con la Opción 1 es que aquí las claves de raíz no están relacionadas con ningún UE. Así, la función ProSe 20 necesita asegurar que la misma clave de raíz no se reutilice para diferentes UE.

Específicamente, como se muestra en la Figura 3, el UE 10_1 se registra en la función ProSe 20_1 (etapa S21).

La función ProSe 20_1 envía Solicitar claves de raíz para el UE 10_1 al tercero 60 que gestiona la clave de raíz (etapa S22).

El tercero 60 responde a la función ProSe 20_1 con un grupo de claves de raíz que contiene un montón de claves de raíz. Cada clave está relacionada con un KSI único (etapa S23).

La función ProSe 20_1 distribuye las claves de raíz al UE 10_1 con los KSI (etapa S24).

El mismo procedimiento que en las etapas S21 a S24 se realiza entre el UE 10_2 y la función ProSe 20_2 (etapas S25 a S28).

Según esta Opción 2, es posible reducir la cantidad de señalización al UE en comparación con la Opción 1. Esto se debe a que las claves de raíz no están relacionadas con ningún UE y así, el número de claves de raíz transmitidas al UE puede ser menor que en la Opción 1. Además, también es posible reducir recursos en el UE para almacenar las claves de raíz.

Por el contrario, según la Opción 1, es posible reducir la carga en la Función ProSe en comparación con la Opción 2. Esto se debe a que las claves de raíz se asignan a los UE de manera uno a uno y así, la función ProSe no necesita asegurar que la misma clave de raíz no se reutilizará para diferentes UE.

<Operaciones para derivar claves de sesión>
Se proponen dos opciones para la derivación y asignación de claves de sesión.

Opción 1: un UE deriva de forma autónoma la clave de sesión.
El UE 10_1, que inicia una comunicación directa, simplemente deriva una clave de sesión, la envía a la función ProSe y la función ProSe la enviará a los otros UE.

Alternativamente, como se muestra en la Figura 4, el UE 10_1 envía una solicitud de Comunicación Directa al UE 10_2 (etapa S31).

En el caso donde cada clave de raíz esté relacionada con un UE dado como se muestra en la Figura 2, los UE 10_1 y 10_2 pueden identificar la misma clave de raíz que se ha de utilizar para derivar una clave de sesión, sin recibir ninguna instrucción de la red. Por lo tanto, los UE 10_1 y 10_2 derivan la clave de sesión a partir de la clave de raíz identificada, por separado (etapa S32).

A continuación, el UE 10_1 y el UE 10_2 inician una comunicación directa con protección de seguridad utilizando la clave de sesión (etapa S33).

Opción 2: un UE deriva la clave de sesión según un KSI indicado por la función ProSe.
Esta opción es adecuada para el caso donde el grupo de claves de raíz se asigna como se muestra en la Figura3.

Como se muestra en la Figura 5, el UE 10_1 envía una solicitud de Comunicación Directa con un ID del UE 10_2 (UE con el que el UE 10_1 quiere tener un servicio de comunicación directa) a la función ProSe 20_1 (etapa S41).

La función ProSe 20_1 realiza la autorización para determinar si se le permite al UE 10_1 tener comunicación directa con el UE 10_2 (etapa S42).

Tras una autorización con éxito, la función ProSe 20_1 indica al UE 10_1 una clave de raíz KSI (etapa S43).

Además, la función ProSe 20_1 indica al UE 10_2 la clave de raíz KSI mediante la función ProSe 20_2 (etapa S44).

El UE 10_1 y el UE 10_2 derivan una clave de sesión de la clave de raíz indicada por el KSI, por separado (etapa S45).

A continuación, el UE 10_1 y el UE 10_2 inician una comunicación directa con protección de seguridad utilizando la clave de sesión (etapa S46).

A continuación, se describirán ejemplos de configuración del UE 10, la Función ProSe (nodo) 20 y el tercero (servidor) 60 según esta realización ejemplar con referencia a las Figuras 6 a 8.

Como se muestra en la Figura 6, el UE 10 incluye una unidad 11 de adquisición y una unidad 12 de derivación. La unidad 11 de adquisición adquiere las claves de raíz de la función ProSe 20, al registrar con éxito el UE 10 con la función ProSe 20. La unidad 12 de derivación acciona las claves de sesión utilizando la clave de raíz adquirida. En el caso donde cada clave de raíz está relacionada con un UE dado como se muestra en la Figura 2, la unidad 12 de derivación utiliza una clave de raíz correspondiente a un UE con la que el UE 10 desea realizar una comunicación directa, al derivar las claves de sesión. Por otro lado, en el caso donde el grupo de claves de raíz se asigne como se muestra en la Figura 3, la unidad 12 de derivación utiliza una clave de raíz que se indica mediante el KSI recibido de la función ProSe 20. Obsérvese que estas unidades 11 y 12 están conectadas mutuamente entre sí a través de un bus o similar. Estas unidades 11 y 12 pueden configurarse, por ejemplo, mediante un transceptor que realiza una comunicación directa con diferentes UE a través de la interfaz PC5, un transceptor que realiza una comunicación con la función ProSe 20 a través de la interfaz PC3, y un controlador tal como una CPU (Unidad Central de Procesamiento) que controla estos transceptores.

Como se muestra en la Figura 7, la función ProSe 20 incluye una unidad 21 de adquisición y una unidad 22 de distribución. La unidad 21 de adquisición adquiere las claves de raíz del tercero 60, al registrar con éxito el UE 10 con la función ProSe 20. La unidad 22 de distribución distribuye las claves de raíz adquiridas al UE 10. En el caso donde el conjunto de claves de raíz se asigne como se muestra en la Figura 3, la función ProSe 20 incluye además una unidad 23 de indicación. La unidad 23 de indicación indica al UE 10 el KSI de la clave de raíz que se ha de utilizar por el UE 10. Obsérvese que estas unidades 21 a 23 están conectadas mutuamente entre sí a través de un bus o similar. Estas unidades 21 a 23 pueden configurarse, por ejemplo, mediante un transceptor que realiza una comunicación con el UE 10 a través de la interfaz PC3, y un controlador tal como una CPU que controla este transceptor.

Como se muestra en la Figura 8, el tercero 60 incluye una unidad 61 de almacenamiento y una unidad 62 de respuesta. La unidad 61 de almacenamiento almacena las claves de raíz. La unidad 62 de respuesta responde a la solicitud de la función ProSe 20 enviando las claves de raíz a la función ProSe 20. Obsérvese que estas unidades 61 y 62 están conectadas mutuamente entre sí a través de un bus o similar. Estas unidades 61 y 62 pueden configurarse, por ejemplo, mediante un transceptor que realiza la comunicación con la función ProSe 20, y un controlador tal como una CPU que controla este transceptor.

<Segunda realización ejemplar>

La Figura 9 muestra un ejemplo de configuración de un sistema de comunicaciones para un servicio de proximidad. El servicio de proximidad proporciona el descubrimiento controlado por la red del operador y las comunicaciones entre los UE que se encuentran en la proximidad, tanto para uso comercial/social como para uso de seguridad pública. Se requiere que el servicio ProSe debería proporcionarse a los UE con o sin cobertura de red.

Como se muestra en la Figura9, el sistema de comunicaciones según esta realización ejemplar incluye una pluralidad de UE 110_1 a 110_m (en lo sucesivo se pueden denominar colectivamente mediante un código 110), una o más Funciones ProSe 120_1 a 120_n (en lo sucesivo se pueden denominar colectivamente mediante un código 120), una E-UTRAN (Red de Acceso por Radio Terrestre Universal Evolucionada) 130, un EPC (Núcleo de Paquetes Evolucionado) 140 y un Servidor 150 de APP (Aplicación) ProSe.

El UE 110 se conecta al EPC 140 a través del E-UTRAN 130 (es decir, a través de las interfaces LTE-Uu y S1), funcionando por ello como un UE típico. Además, el UE 110 utiliza la interfaz PC5 mencionada anteriormente, llevando realizando por ello una comunicación ProSe. Antes de la comunicación ProSe, el UE 110 se registra con la Función ProSe 120. Obsérvese que los UE 110_1 a 110_m pueden registrarse con la misma Función ProSe o Funciones ProSe mutuamente diferentes. Además, algunos de los UE 110_1 a 110_m pueden registrarse con la misma Función ProSe.

La Función ProSe 120 es un nodo que soporta la comunicación ProSe entre los UE 110_1 a 110_m. La Función ProSe 120 se puede desplegar bien en un determinado nodo de red o bien ser un nodo independiente, y puede residir dentro o fuera del EPC 140. La Función ProSe 120 se comunica con el UE 110 a través de una interfaz PC3. Además, la Función ProSe 120 se comunica con el EPC 140 a través de una interfaz PC4. Además, las Funciones ProSe 120_1 a 120_n pueden comunicarse entre sí a través de una interfaz PC6.

Obsérvese que la interfaz PC3 es un punto de referencia entre el UE 110 y la Función ProSe 120. La interfaz PC3 se utiliza para definir la interacción entre el UE 110 y la Función ProSe 120. Un ejemplo puede ser utilizar para la configuración del descubrimiento y la comunicación de ProSe. Además, la interfaz PC4 es un punto de referencia entre el EPC 140 y la Función ProSe 120. La interfaz PC4 se utiliza para definir la interacción entre el

EPC 140 y la Función ProSe 120. Los posibles casos de uso pueden ser cuando se configura un trayecto de comunicación uno a uno entre los UE 110_1 a 110_m, o cuando se validan los servicios ProSe (autorización) para la gestión de sesiones o la gestión de movilidad en tiempo real. Además, la interfaz PC6 es un punto de referencia entre las Funciones ProSe 120_1 a 120_n. La interfaz PC6 se puede utilizar para funciones como el descubrimiento de ProSe entre usuarios abonados a diferentes PLMN (Redes Públicas Móviles Terrestres).

El E-UTRAN 130 está formado por uno o más eNB (no mostrados). El EPC 140 incluye, como sus nodos de red, una MME (Entidad de Gestión de Movilidad) que gestiona la movilidad de los UE 110_1 a 110_m, y similares. El Servidor 150 de APP ProSe puede comunicarse con el EPC 140 a través de una interfaz SGi. Además, el servidor 150 de APP ProSe puede comunicarse con el UE 110 a través de una interfaz PC1, y puede comunicarse con la Función ProSe 120 a través de una interfaz PC2. Obsérvese que la interfaz PC1 es un punto de referencia entre las APP de ProSe en los UE 110_1 a 110_m y el servidor 150 de APP ProSe. La interfaz PC1 se utiliza para definir los requisitos de señalización a nivel de aplicación. Por otro lado, la interfaz PC2 es un punto de referencia entre la Función ProSe 120 y el servidor 150 de APP ProSe. La interfaz PC2 se utiliza para definir la interacción entre el servidor 150 de APP ProSe y la funcionalidad ProSe proporcionada por 3GPP EPS (Sistema de Paquetes Evolucionado) mediante la Función ProSe 120. Un ejemplo puede ser para las actualizaciones de datos de aplicaciones para una base de datos ProSe en la Función ProSe 120. Otro ejemplo pueden ser los datos para su uso por el servidor 150 de APP ProSe en la intercomunicación entre la funcionalidad 3GPP y los datos de aplicación, por ejemplo, traducción de nombres. El servidor 150 de APP ProSe puede residir dentro o fuera del EPC 140.

Aunque se omite la ilustración, el sistema de comunicaciones también incluye un servidor operado por un tercero de confianza. En la siguiente descripción, este servidor a veces se denominará simplemente como "tercero (3º)" y se denominará mediante un código 160. Típicamente, el tercero 160 gestiona las claves públicas que se describirán más adelante.

A continuación, se describirán en detalle ejemplos de operación de esta realización ejemplar con referencia a las Figuras 10 a 12. Obsérvese que los ejemplos de configuración del UE 110, la Función ProSe 120 y el tercero 160 se describirán más adelante con referencia a las Figuras 13 a 15.

Esta realización ejemplar propone utilizar PKI para comunicación directa. Los UE 110_1 a 110_m pueden registrar sus claves públicas en un procedimiento de registro y mientras tanto obtener otras claves públicas de UE. La Función ProSe 120 asegura que solamente el UE 110 es provisto con las claves públicas de los UE con los que se permite que el UE 110 solicitado tenga comunicación directa. Los UE 110_1 a 110_m utilizan la clave pública para verificar la otra extremidad de tal manera que puedan derivar la clave de sesión para iniciar la comunicación directa. Por ejemplo, la clave de sesión es un par de claves de confidencialidad e integridad para proteger los mensajes transferidos directamente entre los UE 110_1 a 110_m.

A continuación, se ofrecen opciones para la derivación de claves.

1. Utilizar un PKI para comunicación directa uno a uno:
los UE 110_1 a 110_m proporcionan su clave pública en el registro y reciben otras claves públicas de UE en un registro con éxito. Por ejemplo, el UE 110_1 protege la Solicitud de Comunicación Directa con su clave privada. El UE 110_2, que ha recibido la Solicitud de Comunicación Directa, puede verificarla con la clave pública del UE1. El UE 110_2 puede enviar material para la derivación de la clave de sesión al UE 110_1 y pueden derivar la misma clave para la protección de su comunicación directa. El UE 110_1 puede verificar el mensaje enviado desde el UE 110_2 con la clave pública del UE2, por lo que pueden autenticarse mutuamente.

La derivación de la clave de sesión puede:

> 1) utilizar una clave de raíz que se adquiere preliminarmente de la Función ProSe como una entrada con un material clave proporcionado por uno de los UE para mantener la frescura; y
> 2) utilizar también un esquema de intercambio de claves (por ejemplo esquema de intercambio de claves Diffie-Hellman) para calcular y compartir una clave secreta.

Específicamente, como se muestra en la Figura 10, el UE 110_1 registra su clave pública durante el registro en la Función ProSe 120_1 (etapa S111).

La Función ProSe 120_1 registra la clave pública del UE 110_1 en el tercero 160 (etapa S112).

El tercero 160 envía a la Función ProSe 120_1 una lista de permitidos. La lista de permitidos contiene ID de UE con los que el UE 110_1 se les permite tener comunicación directa y las claves públicas relacionadas de esos UE (etapa S113).

La Función de ProSe 120_1 reenvía la lista de permitidos al UE 110_1 (etapa S114).

El mismo procedimiento que las etapas S111 a S114 se realiza para el UE 110_2 (etapas S115 a S118).

Cuando comienza la comunicación de dirección, como se muestra en la Figura 11, el UE 110_1 envía una Solicitud de Comunicación Directa a la Función ProSe 120_1, con el ID del UE 110_2, una clave pública KSI del UE 110_1. El mensaje se puede proteger con una clave privada del UE 110_1. El mensaje se reenvía a la Función ProSe 120_2 mediante la Función ProSe 120_1 (etapa S121).

Obsérvese que el uso de KSI es adecuado para un caso donde se asigna una pluralidad de claves públicas al UE 110_1. El UE 110_2 puede hacer referencia al KSI para identificar una de las claves públicas correspondientes a la clave privada utilizada por el UE 110_1.

La Función ProSe 120_1 realiza la autorización sobre si el UE 110_1 puede tener un servicio de comunicación directa con el UE 110_2, con soporte de Función ProSe 120_2 (etapa S122).

Tras la autorización con éxito, la Función ProSe 120_2 reenvía la Solicitud de Comunicación Directa al UE 110_2 (etapa S123).

Obsérvese que si la comunicación directa ocurre cuando el UE está fuera de cobertura, la Solicitud de Comunicación Directa va directamente desde el UE 110_1 al UE 110_2, y se omite la etapa anterior S122.

El UE 110_2 puede realizar una verificación de integridad en el mensaje con la clave pública del UE 110_1 (etapa S124).

Al tener éxito en la verificación de integridad, el UE 110_2 deriva la clave de sesión, como se ha descrito anteriormente (etapa S125).

El UE 110_2 envía una Respuesta de Comunicación Directa al UE 110_1 con materiales para la derivación de la clave de sesión. Alternativamente, el UE 110_2 incluye la clave de sesión derivada en la Respuesta de Comunicación Directa. El mensaje está protegido con una clave privada del UE 110_2 (etapa S126).

El UE 110_1 realiza una verificación de integridad del mensaje con la clave pública del UE 110_2 (etapa S127).

Al tener éxito en la verificación de integridad, el UE 110_1 deriva la clave de sesión del material (etapa S128). Esta etapa S128 se omite si el UE 110_1 ha recibido la clave de sesión del UE 110_2 en la etapa S126. Alternativamente, el UE 110_1 extrae la clave de sesión de la Respuesta de Comunicación Directa utilizando la clave pública del UE 110_2.

Después de eso, la comunicación Directa comienza con la protección de seguridad mediante la clave de sesión que comparten el UE 110_1 y el UE 110_2 (etapa S129).

2. Utilizar un PKI para la comunicación directa uno a muchos:

El procedimiento de registro es el mismo que el que se muestra en la Figura10.

El UE 110_1 protege la Solicitud de Comunicación Directa con su clave privada. Otros UE (por ejemplo, UE 110_2, UE 110_3) pueden verificarlo con la clave pública de UE1.

Mientras tanto, en esta opción, el UE 110_1 deriva la clave de sesión para la comunicación directa uno a mucho y envía la clave de sesión a la Función ProSe 120 junto con la Solicitud de Comunicación Directa a través de la interfaz PC3 segura. La Función ProSe 120 envía la clave de sesión al UE 110_2 y al UE 110_3. Si el UE 110_2 o el UE 110_3 se ha registrado con una Función ProSe diferente, la Función ProSe del UE 110_1 reenviará la clave de sesión a la Función ProSe de servicio del UE 110_2/110_3. La derivación de la clave de sesión puede utilizar la clave privada del UE 110_1 o cualquier clave LTE (Evolución a Largo Plazo) como entrada.

Específicamente, como se muestra en la Figura 12, el UE 110_1 deriva una clave de sesión para la comunicación directa (etapa S131).

El UE 110_1 envía una Solicitud de Comunicación Directa a la Función ProSe 120_1, que puede enviarse a las funciones ProSe que sirven a los UE objetivo (por ejemplo, Función ProSe 20_2 y UE 110_2 y 110_3). El mensaje contiene ID de UE objetivo y el KSI de la clave pública del UE 110_1, que están protegidas con la clave privada del UE 110_1. El UE 110_1 también incluye la clave de sesión en el mensaje (etapa S132).

Las Funciones ProSe 120_1 y 120_2 realizan la autorización sobre si el UE 110_1 puede tener comunicación directa uno a muchos con los UE objetivo 110_2 y 110_3 (etapa S133).

La Función ProSe 120_2 reenvía la Solicitud de comunicación Directa a los UE 110_2 y 110_3 (etapa S134).

Cada uno de los UE 110_2 y 110_3 realiza una verificación de integridad en el mensaje con la clave pública del UE 110_1 (etapa S135).

Cada uno de los UE 110_2 y 110_3 envía la Respuesta de Comunicación Directa al UE 110_1, protegido con la clave de sesión que ha recibido (etapa S136). Después de eso, la comunicación directa comienza con la protección de seguridad mediante la clave de sesión que comparten los UE 110_1 a 110_3.

3. Utilizar una comunicación de dirección uno a muchos PKI sin utilizar la clave de sesión:

considerando un caso donde la comunicación uno a muchos es solamente de una forma desde el UE1 a otros, el UE 110_1 simplemente protege la Comunicación Directa con su clave privada a otros UE. Los otros UE que están autorizados a recibir el mensaje del UE 110_1 pueden obtener la clave pública del UE 110_1 y, por lo tanto, verificar que el mensaje se envía desde el UE 110_1 y leerlo. La red (por ejemplo, Función ProSe) debería asegurarse de que los UE no autorizados no obtengan la clave pública del UE 110_1 ', y la clave pública no debería enviarse a otros UE.

Así, puede impedir que los no miembros escuchen las transmisiones del Grupo de Comunicaciones ProSe (como se solicita en NPL 2, Cláusula 5.12).

4. Utilizar PKI para una clave pública de uno a muchos como entrada:

Los UE 110_1 a 110_m derivan la clave de sesión, y la entrada para la derivación de claves es: 1) clave pública del UE 110_1; 2) un material de derivación de claves recibido de la Función ProSe 120. Requiere la clave pública del UE 110_1 y el material de derivación de clave solamente se proporciona a los UE autorizados.

Cómo puede el UE 110_1 tener la misma clave de sesión:

a) el UE 110_1 mantiene la clave pública y recibe material de derivación de clave de la Función ProSe 120, de tal manera que pueda derivar la sesión en la misma clave de sesión;
b) la Función ProSe 120 puede derivar la clave ya que conoce tanto la clave pública del UE 110_1 como el material de derivación de clave;
c) la Función ProSe 120 proporciona un material de derivación de claves que el UE 110_1 puede utilizar con su clave privada para derivar la misma clave de sesión.

Esto requiere que los materiales de derivación de claves para el UE 110_1 y otros UE tengan alguna relación.

A continuación, se describirán ejemplos de configuración del UE 110, la Función ProSe (nodo) 120 y el tercero (servidor) 160 según esta realización ejemplar con referencia a las Figuras 13 a 15.

Como se muestra en la Figura 13, el UE 110 incluye una unidad 111 de registro/recuperación y una unidad 112 de verificación. La unidad 111 de registro/recuperación realiza los procesos mostrados en la Figura 10 o procesos equivalentes a los mismos. La unidad 112 de verificación realiza los procesos mostrados en las Figuras 11 y 12, o procesos equivalentes a los mismos. Obsérvese que estas unidades 111 y 112 están conectadas mutuamente entre sí a través de un bus o similar. Estas unidades 111 y 112 pueden configurarse, por ejemplo, mediante un transceptor que realiza la comunicación directa con diferentes UE a través de la interfaz PC5, un transceptor que realiza la comunicación con la Función ProSe 120 a través de la interfaz PC3, y un controlador, tal como una CPU (Unidad Central de Procesamiento) que controla estos transceptores.

Como se muestra en la Figura 14, la Función ProSe 120 incluye al menos una unidad 121 de recepción y una unidad 122 de transmisión. La unidad 121 de recepción realiza los procesos mostrados en las etapas S111 y S115 en la Figura 10, o procesos equivalentes a los mismos. La unidad 122 de transmisión realiza los procesos mostrados en las etapas S114 y S118 en la Figura 10, o procesos equivalentes a los mismos. Además, la Función ProSe 120 también puede incluir una unidad 123 de registro y una unidad 124 de adquisición. La unidad 123 de registro realiza los procesos mostrados en las etapas S112 y S116 en la Figura 10, o procesos equivalentes a los mismos. La unidad 124 de adquisición realiza los procesos mostrados en las etapas S113 y S117 en la Figura 10, o equivalentes a los mismos. Obsérvese que estas unidades 121 a 124 están conectadas mutuamente entre sí a través de un bus o similar. Estas unidades 121 a 124 pueden configurarse, por ejemplo, mediante un transceptor que realiza la comunicación con el UE 110 a través de la interfaz PC3, un transceptor que realiza la comunicación con el tercero 160 y un controlador tal como una CPU que controla estos transceptores.

Como se muestra en la Figura 15, el tercero 160 incluye una unidad 161 de almacenamiento y una unidad 162 de respuesta. La unidad 161 de almacenamiento almacena las claves de raíz registradas por la Función ProSe 120. La unidad 162 de respuesta responde a la solicitud de la Función ProSe 120 con el envío de las claves públicas almacenadas a la Función ProSe 120. Obsérvese que estas unidades 161 y 162 están conectadas

mutuamente entre sí a través de un bus o similar. Estas unidades 161 y 162 pueden configurarse, por ejemplo, mediante un transceptor que realiza una comunicación con la Función ProSe 120, y un controlador, tal como una CPU que controla este transceptor.

Obsérvese que la presente invención no se limita a las realizaciones ejemplares mencionadas anteriormente, y es obvio que los expertos en la técnica pueden realizar diversas modificaciones dentro del alcance de las reivindicaciones.

Lista de signos de referencia
10, 10_1-10_m, 110, 110_1-110_m UE
11, 21,124 UNIDAD DE ADQUISICIÓN
12 UNIDAD DE DERIVACIÓN
20, 20_1-20_n, 120, 120_1-120_n Función ProSe
22 UNIDAD DE DISTRIBUCIÓN
23 UNIDAD DE INDICACIÓN
30, 130 E-UTRAN
40, 140 EPC
50, 150 Servidor de APP ProSe
60, 160 terceros (servidor)
61, 161 UNIDAD DE ALMACENAMIENTO
62, 162 UNIDAD DE RESPUESTA
111 UNIDAD DE REGISTRO/RECUPERACIÓN
112 UNIDAD DE VERIFICACIÓN
121 UNIDAD DE RECEPCIÓN
122 UNIDAD DE TRANSMISIÓN
123 UNIDAD DE REGISTRO

REIVINDICACIONES

1. Un sistema de comunicaciones móviles que comprende:

un primer Equipo de Usuario, UE, (10_1) configurado para soportar Servicios de Proximidad, ProSe;
un segundo UE (10_2) configurado para soportar los ProSe;
una primera Función ProSe (20_1) configurada para soportar los ProSe y comunicar con el primer UE (10_1) mediante una interfaz PC3;
una segunda Función ProSe (20_2) configurada para soportar los ProSe y comunicar con el segundo UE (10_2) mediante una interfaz PC3; y
un servidor (60) configurado para comunicar con la primera Función ProSe (20_1) y con la segunda Función ProSe (20_2);
el primer UE (10_1) está configurado para registrarse con la primera Función ProSe (20_1) y para obtener una primera clave de la primera Función ProSe (20_1),
caracterizado por que,
el segundo UE (10_2) está configurado para registrarse con la segunda Función ProSe (20_2) y obtener una segunda clave de la segunda Función ProSe (20_2),
el primer UE (10_1) está configurado para enviar, al segundo UE (10_2) mediante una interfaz PC5, un mensaje protegido por una clave de sesión derivada de la primera clave, y
el segundo UE (10_2) está configurado para recibir el mensaje protegido utilizando la clave de sesión derivada de la segunda clave.

2. El sistema de comunicaciones móviles según la reivindicación 1, en donde el primer UE (10_1) y el segundo UE (10_2) están configurados para realizar una comunicación directa uno a uno.

3. Las Funciones de los Servicios de Proximidad, ProSe (20_1, 20_2) en un sistema de comunicaciones móviles que incluyen un primer Equipo de Usuario, UE, (10_1) configurado para soportar los ProSe, un segundo UE (10_2) y un servidor (60) configurado para comunicar con las Funciones ProSe (20_1, 20_2), comprendiendo las Funciones ProSe (20_1, 20_2):

una primera Función ProSe (20_1) configurada para soportar los ProSe, y enviar una primera clave al primer UE (10_1) basándose en un registro del primer UE (10_1); y
caracterizado por que
una segunda Función ProSe (20_2) configurada para soportar los ProSe, y enviar una segunda clave al segundo UE (10_2) basándose en el registro del segundo UE (10_2),
en donde el primer UE (10_1) está configurado para enviar, al segundo UE (10_2) mediante una interfaz PC5, un mensaje protegido por una clave de sesión derivada de la primera clave, y el segundo UE (10_2) está configurado para recibir el mensaje protegido utilizando la clave de sesión derivada de la segunda clave.

4. Las Funciones ProSe (20_1, 20_2) según la reivindicación 3, en donde el primer UE (10_1) y el segundo UE (10_2) están configurados para realizar una comunicación directa uno a uno.

5. Un Equipo de Usuario (10_1), UE, en un sistema de comunicaciones móviles que incluye una primera Función de Servicios de Proximidad, ProSe, (20_1) configurada para soportar los ProSe y comunicar con el UE (10_1) mediante una interfaz PC3, una segunda Función ProSe (20_2) configurada para soportar los ProSe y comunicar con otro UE (10_2) mediante una interfaz PC3, un servidor (60) configurado para comunicar con la Función ProSe (20_1) y la segunda Función ProSe (20_2), comprendiendo el UE (10_1):

un receptor configurado para recibir una primera clave de la primera Función ProSe (20_1) basándose en un registro en la primera Función ProSe (20_1); caracterizado por que el UE comprende además un transmisor configurado para enviar, a otro UE (10_2) mediante una interfaz PC5, un mensaje protegido por una clave de sesión derivada de la primera clave y estando configurado el otro UE (10_2) para recibir el mensaje protegido utilizando la clave de sesión derivada de una segunda clave que se obtiene de la segunda Función ProSe (20_2).

6. Un método de un sistema de comunicaciones móviles que incluye un primer Equipo de Usuario, UE, (10_1) que soporta Servicios de Proximidad, ProSe, un segundo UE (10_2) que soporta los ProSe, una primera Función ProSe (20_1) que soporta los ProSe y comunica con el primer UE (10_1) mediante una interfaz PC3, una segunda Función ProSe (20_2) que soporta los ProSe y comunica con el segundo UE (10_2) mediante una interfaz PC3, y un servidor (60) que comunica con la primera Función ProSe (20_1) y con la segunda Función ProSe (20_2), comprendiendo el método:

el registro, mediante el primer UE (10_1), con la primera Función ProSe (20_1) y la obtención de una primera clave de la primera Función ProSe (20_1);
caracterizado por

el registro, mediante el segundo UE (10_2), con la segunda Función ProSe (20_2) y la obtención de una segunda clave de la segunda Función ProSe (20_2);
el envío, mediante el primer UE (10_1) al segundo UE (10_2) mediante una interfaz PC5, de un mensaje protegido por una clave de sesión derivada de la primera clave, y
la recepción, mediante el segundo UE (10_2), del mensaje protegido utilizando la clave de sesión derivada de la segunda clave.

7. El método según la reivindicación 6, en donde el primer UE (10_1) y el segundo UE (10_2) realizan una comunicación directa uno a uno.

8. Un método de Funciones de Servicios de Proximidad, ProSe, (20_1, 20_2) en un sistema de comunicaciones móviles que incluye un primer Equipo de Usuario, UE, (10_1) que soporta los ProSe, un segundo UE (10_2) que soporta los ProSe, y un servidor (60) que comunica con las Funciones ProSe (20_1, 20_2), comprendiendo el método:

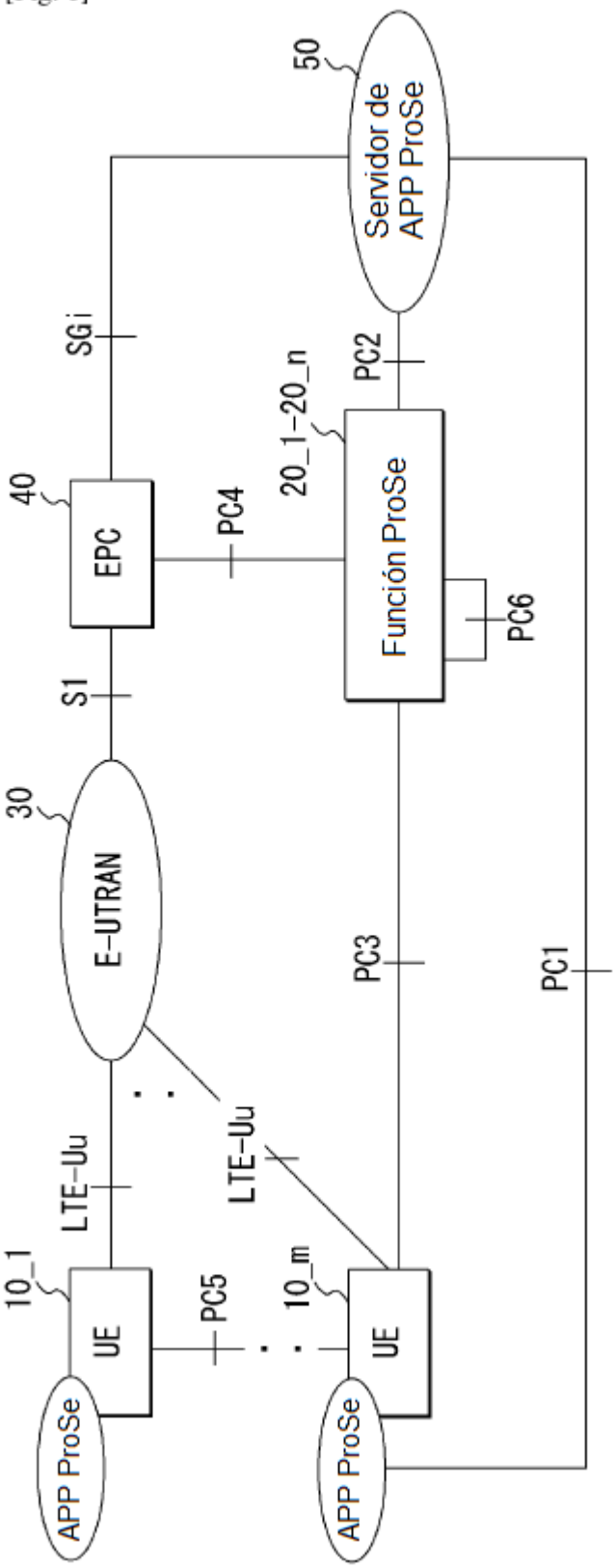
el soporte, mediante una primera Función ProSe (20_1), de los ProSe;
el envío, mediante la primera Función ProSe (20_1), de una primera clave al primer UE (10_1) basándose en un registro del primer UE (10_1);
el soporte, mediante una segunda Función ProSe (20_2), de los ProSe; y
caracterizado por
el envío, mediante la segunda Función ProSe (20_2), de una segunda clave al segundo UE (10_2) basándose en el registro del segundo UE (10_2),
en donde el primer UE (10_1), envía al segundo UE (10_2) mediante una interfaz PC5, un mensaje protegido por una clave de sesión derivada de la primera clave, y
el segundo UE (10_2) está configurado para recibir el mensaje protegido utilizando la clave de sesión derivada de la segunda clave.

9. El método según la reivindicación 8, en donde el primer UE (10_1) y el segundo UE (10_2) realizan una comunicación directa uno a uno.

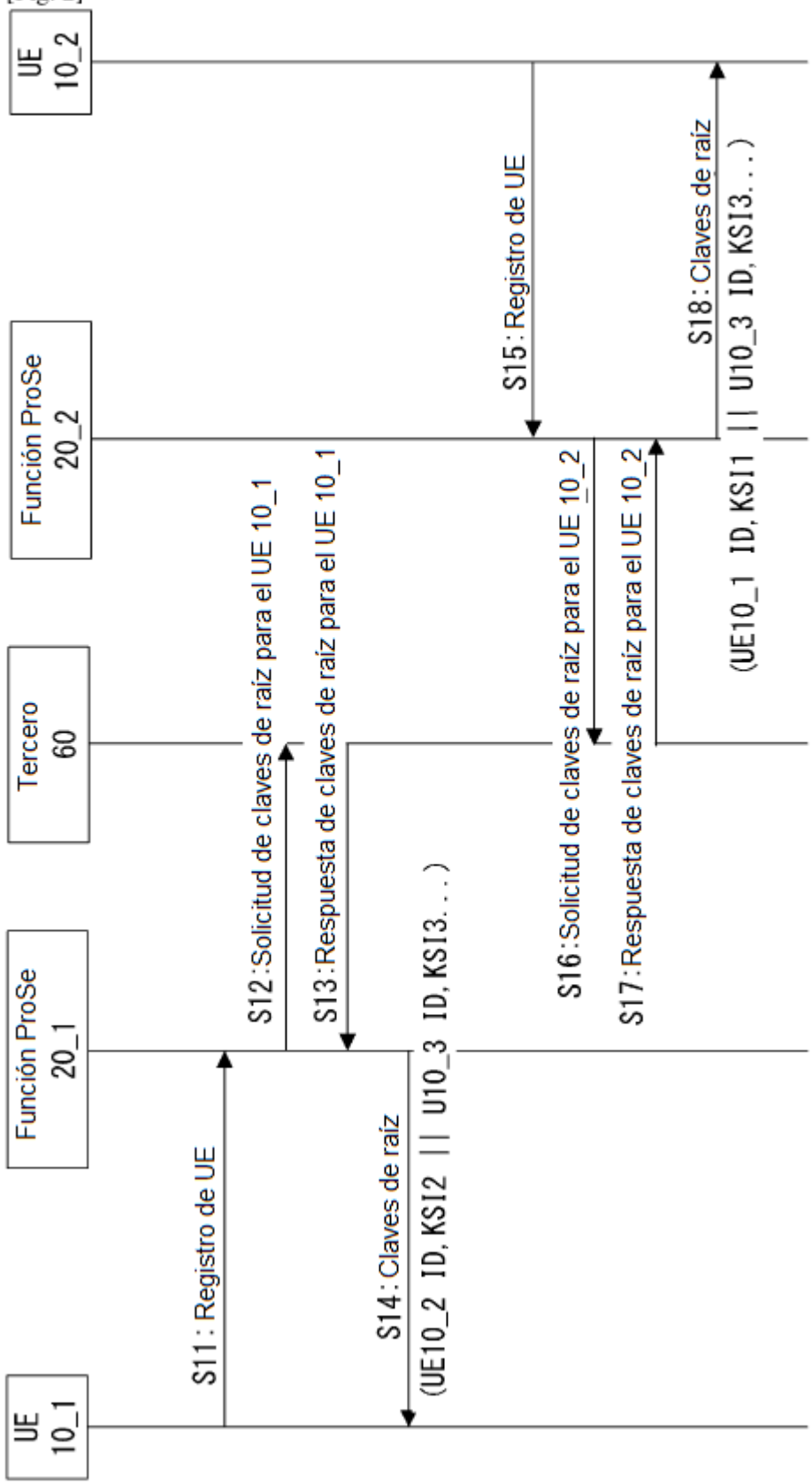
10. Un método de un Equipo de Usuario, UE, (10_1) en un sistema de comunicaciones móviles que incluye una primera Función de Servicios de Proximidad, ProSe, (20_1) que soporta los ProSe y comunica con el UE (10_1) mediante una interfaz PC3, una segunda Función ProSe (20_2) que soporta los ProSe y comunica con otro UE (10_2) mediante una interfaz PC3, y un servidor (60) que comunica con la primera Función ProSe (20_1) y con la segunda Función ProSe (20_2), comprendiendo el método:

la recepción de una primera clave de la primera Función ProSe (20_1) basándose en un registro a la primera Función ProSe (20_1); **caracterizado por que** el método comprende además el envío, a otro UE (10_2) mediante una interfaz PC5, de un mensaje protegido por una clave de sesión derivada de la primera clave, y el otro UE (10_2) que recibe el mensaje protegido utilizando la clave de sesión derivada de una segunda clave que se recibe desde la segunda Función ProSe (20_2).

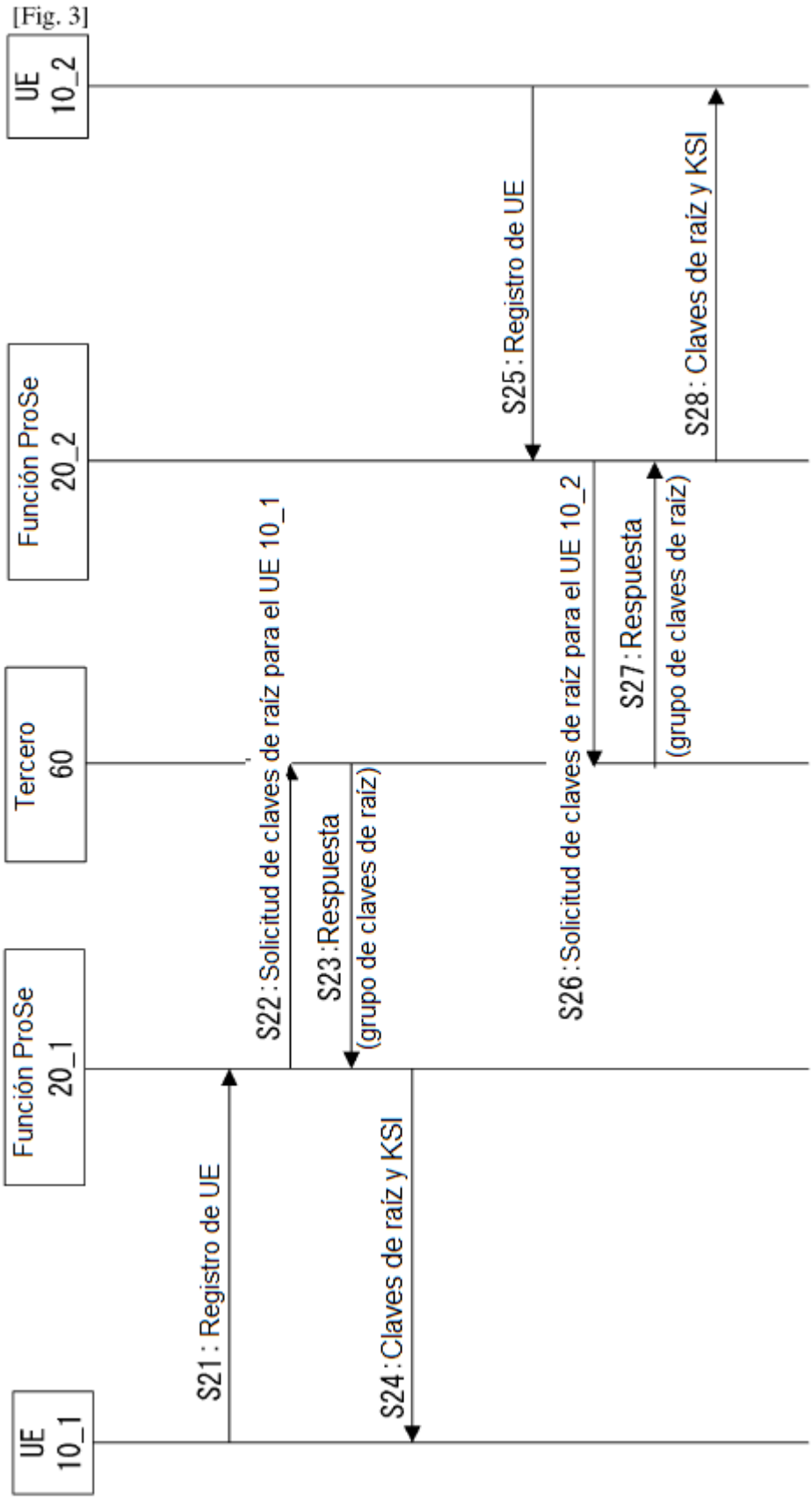
[Fig. 1]


50
Servidor de APP ProSe
SGi
PC2
20_1-20_n
Función ProSe
40
EPC
PC4
PC6
S1
30
E-UTRAN
PC3
PC1
LTE-Uu
LTE-Uu
10_1
UE
PC5
10_m
UE
APP ProSe
APP ProSe

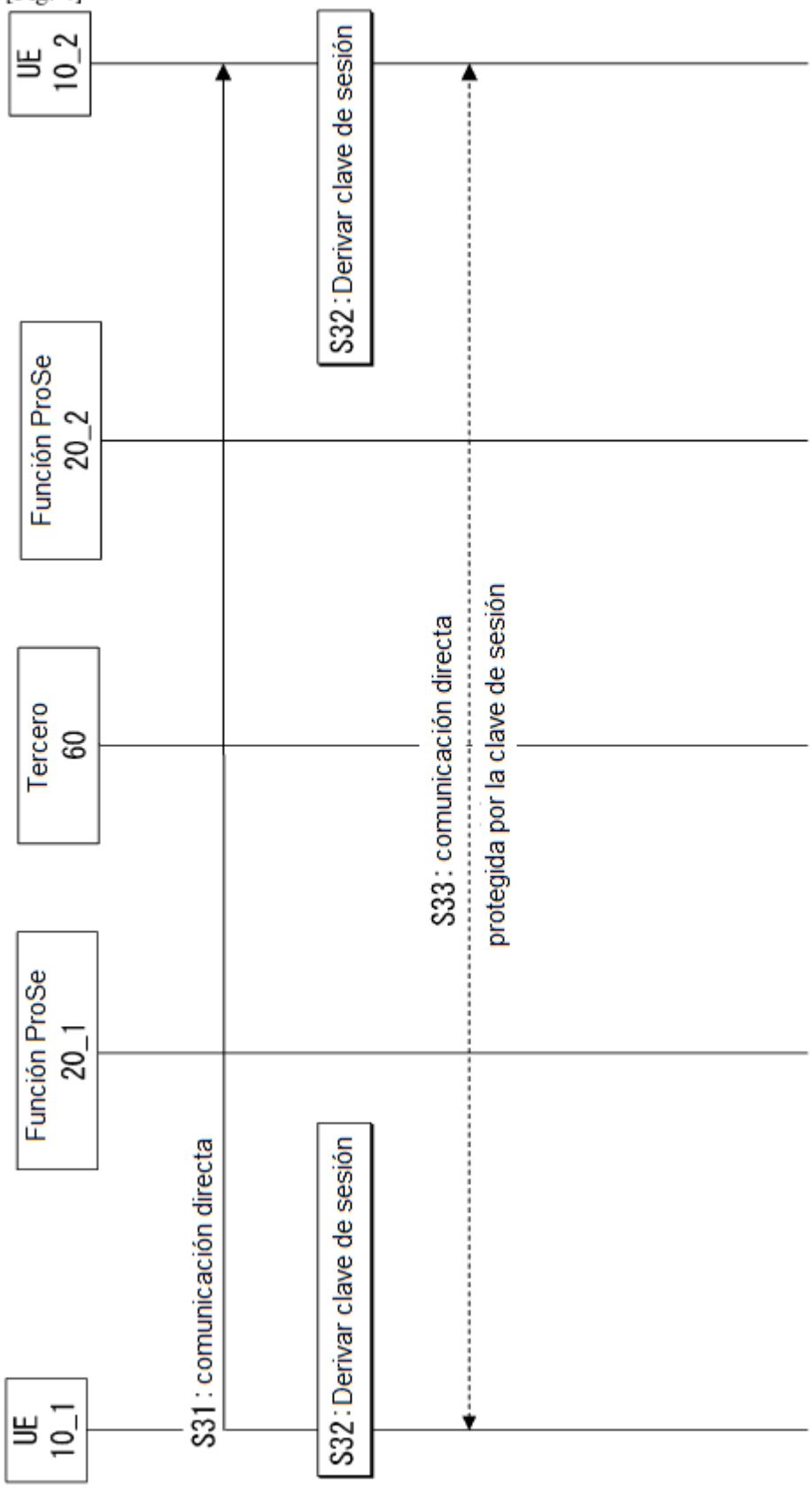
[Fig. 2]


UE 10_1
Función ProSe 20_1
Tercero 60
Función ProSe 20_2
UE 10_2
S11 : Registro de UE
S12 : Solicitud de claves de raíz para el UE 10_1
S13 : Respuesta de claves de raíz para el UE 10_1
S14 : Claves de raíz
(UE10_2 ID, KSI2 || U10_3 ID, KSI3. . .)
S15 : Registro de UE
S16 : Solicitud de claves de raíz para el UE 10_2
S17 : Respuesta de claves de raíz para el UE 10_2
S18 : Claves de raíz
(UE10_1 ID, KSI1 || U10_3 ID, KSI3. . .)

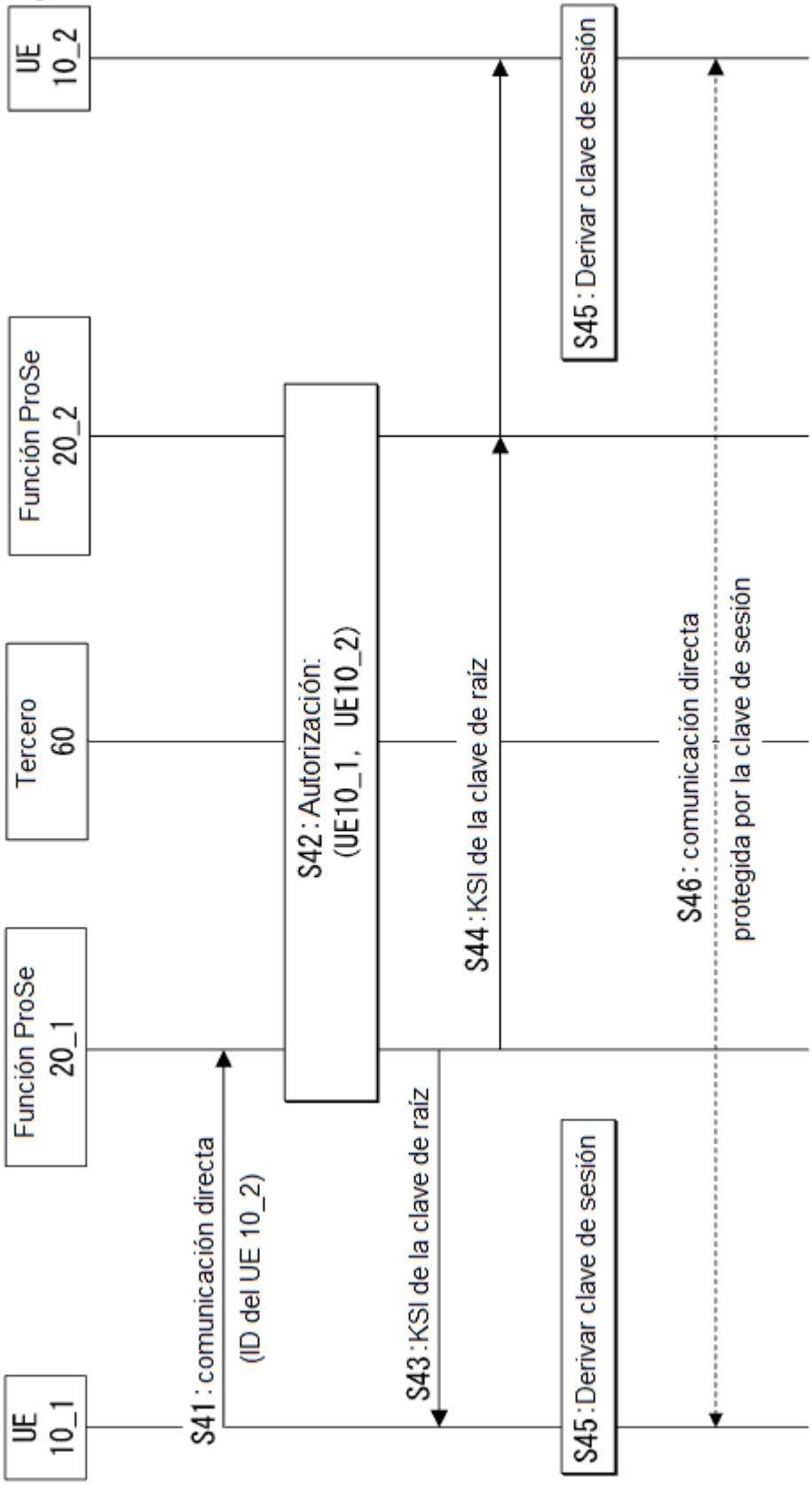
[Fig. 3]


UE 10_1
Función ProSe 20_1
Tercero 60
Función ProSe 20_2
UE 10_2
S21 : Registro de UE
S22 : Solicitud de claves de raíz para el UE 10_1
S23 : Respuesta (grupo de claves de raíz)
S24 : Claves de raíz y KSI
S25 : Registro de UE
S26 : Solicitud de claves de raíz para el UE 10_2
S27 : Respuesta (grupo de claves de raíz)
S28 : Claves de raíz y KSI

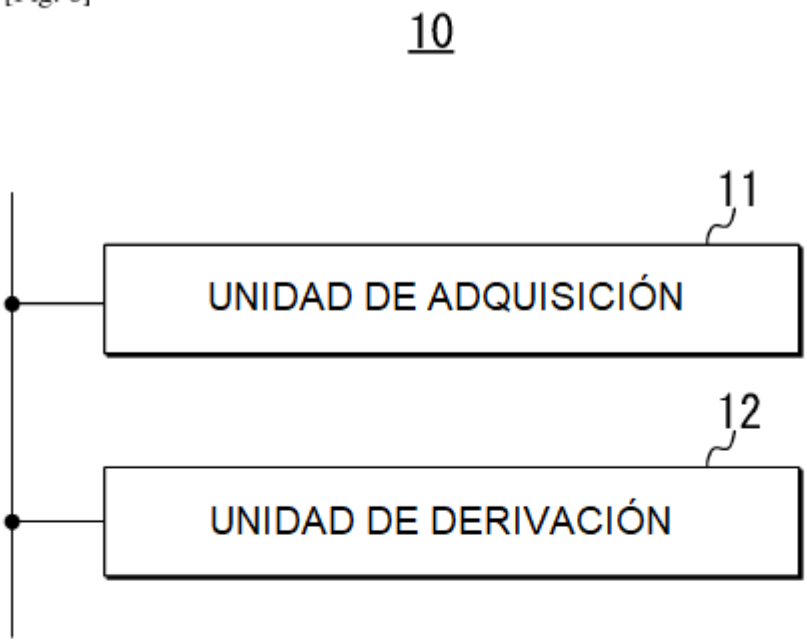
[Fig. 4]


UE 10_1
Función ProSe 20_1
Tercero 60
Función ProSe 20_2
UE 10_2
S31 : comunicación directa
S32 : Derivar clave de sesión
S33 : comunicación directa protegida por la clave de sesión
S32 : Derivar clave de sesión

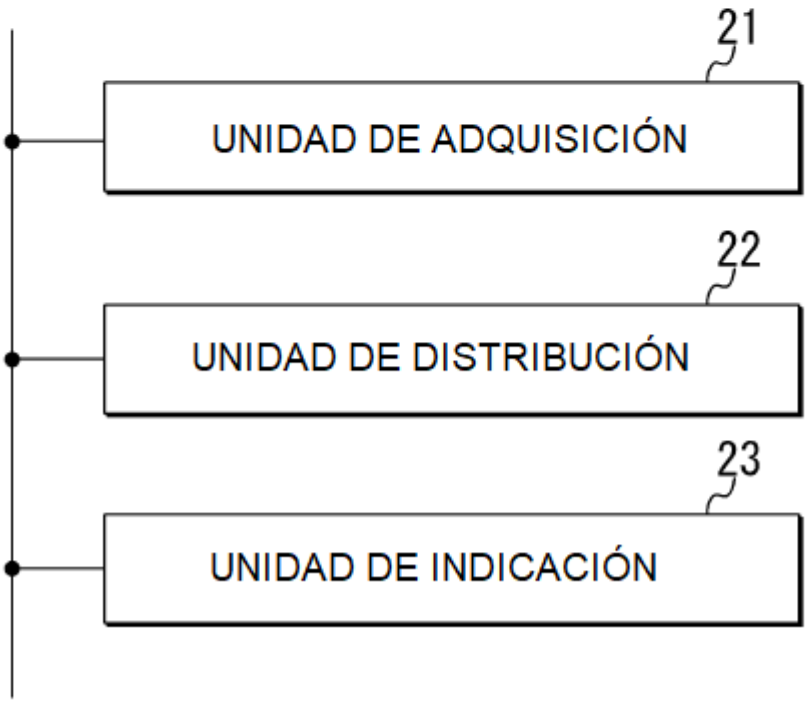
[Fig. 5]


UE 10_1
Función ProSe 20_1
Tercero 60
Función ProSe 20_2
UE 10_2
S41 : comunicación directa
(ID del UE 10_2)
S42 : Autorización:
(UE10_1, UE10_2)
S43 : KSI de la clave de raíz
S44 : KSI de la clave de raíz
S45 : Derivar clave de sesión
S45 : Derivar clave de sesión
S46 : comunicación directa
protegida por la clave de sesión

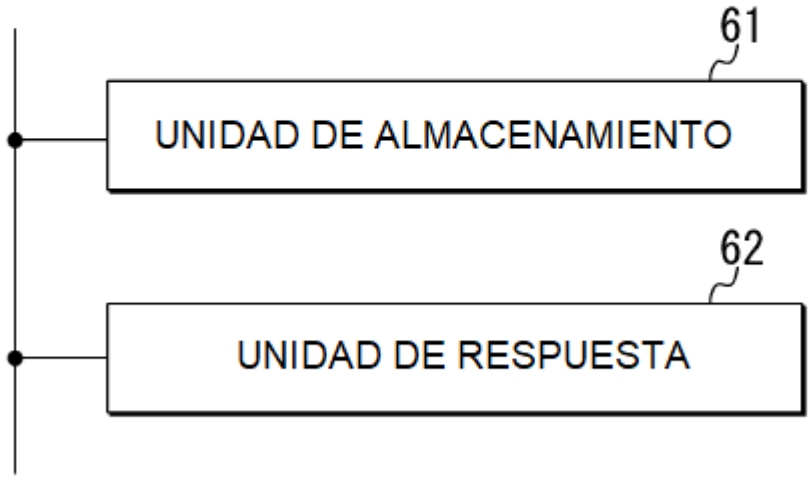
[Fig. 6]


10
11
UNIDAD DE ADQUISICIÓN
12
UNIDAD DE DERIVACIÓN

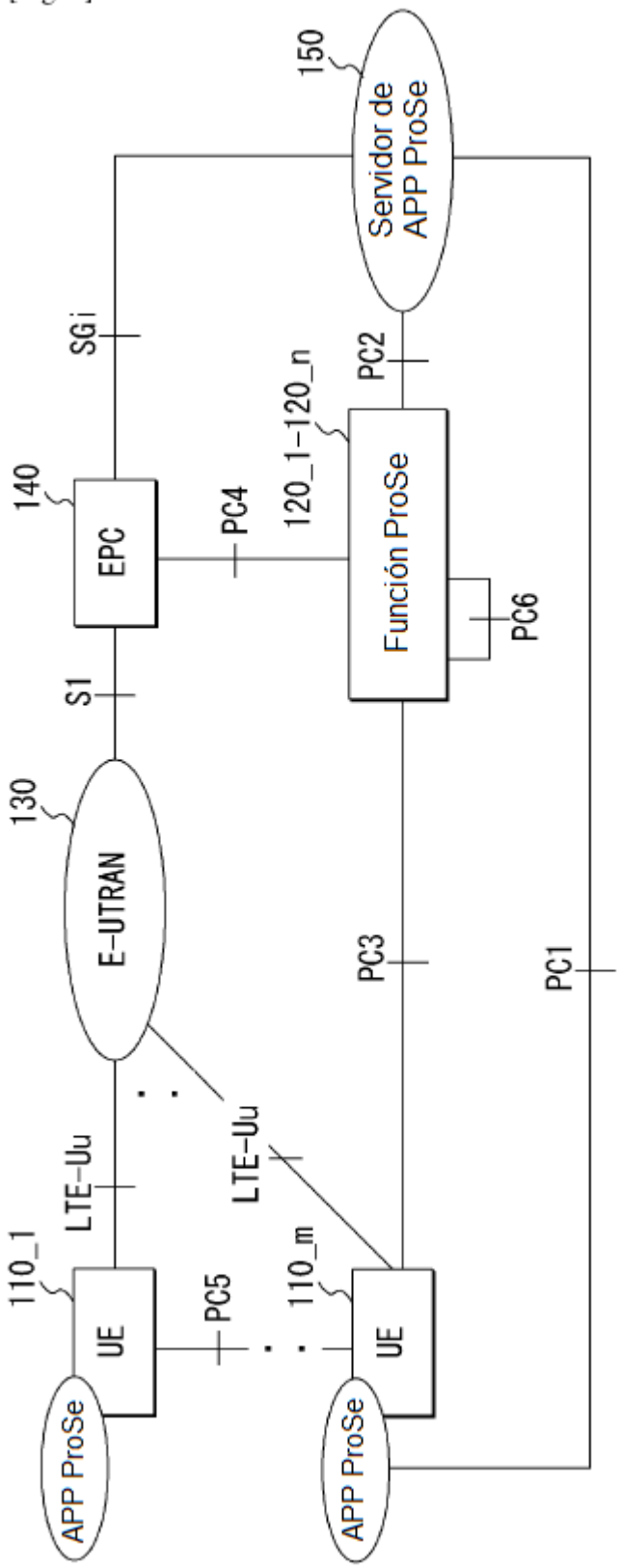
[Fig. 7]


20
21
UNIDAD DE ADQUISICIÓN
22
UNIDAD DE DISTRIBUCIÓN
23
UNIDAD DE INDICACIÓN

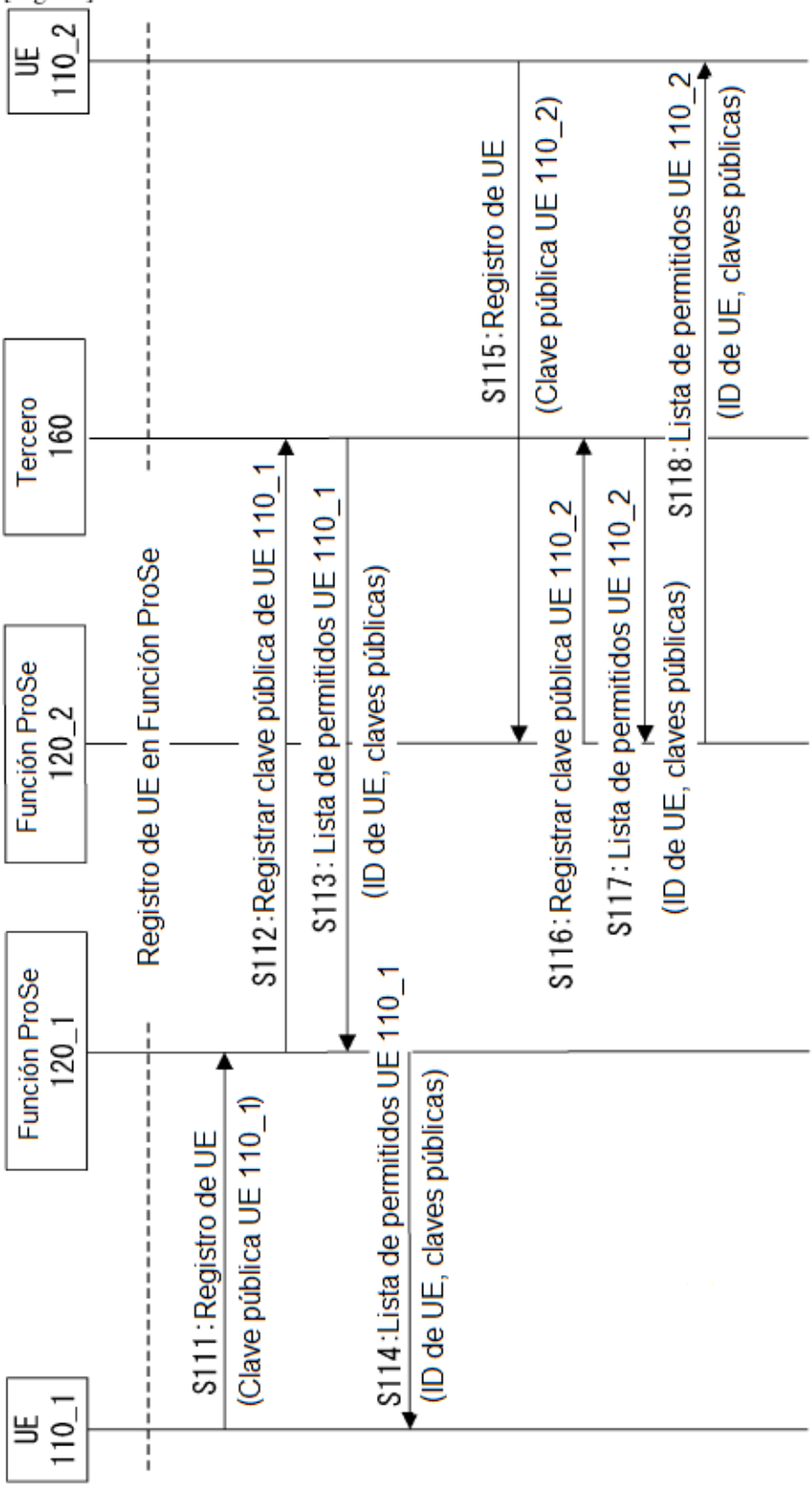
[Fig. 8]



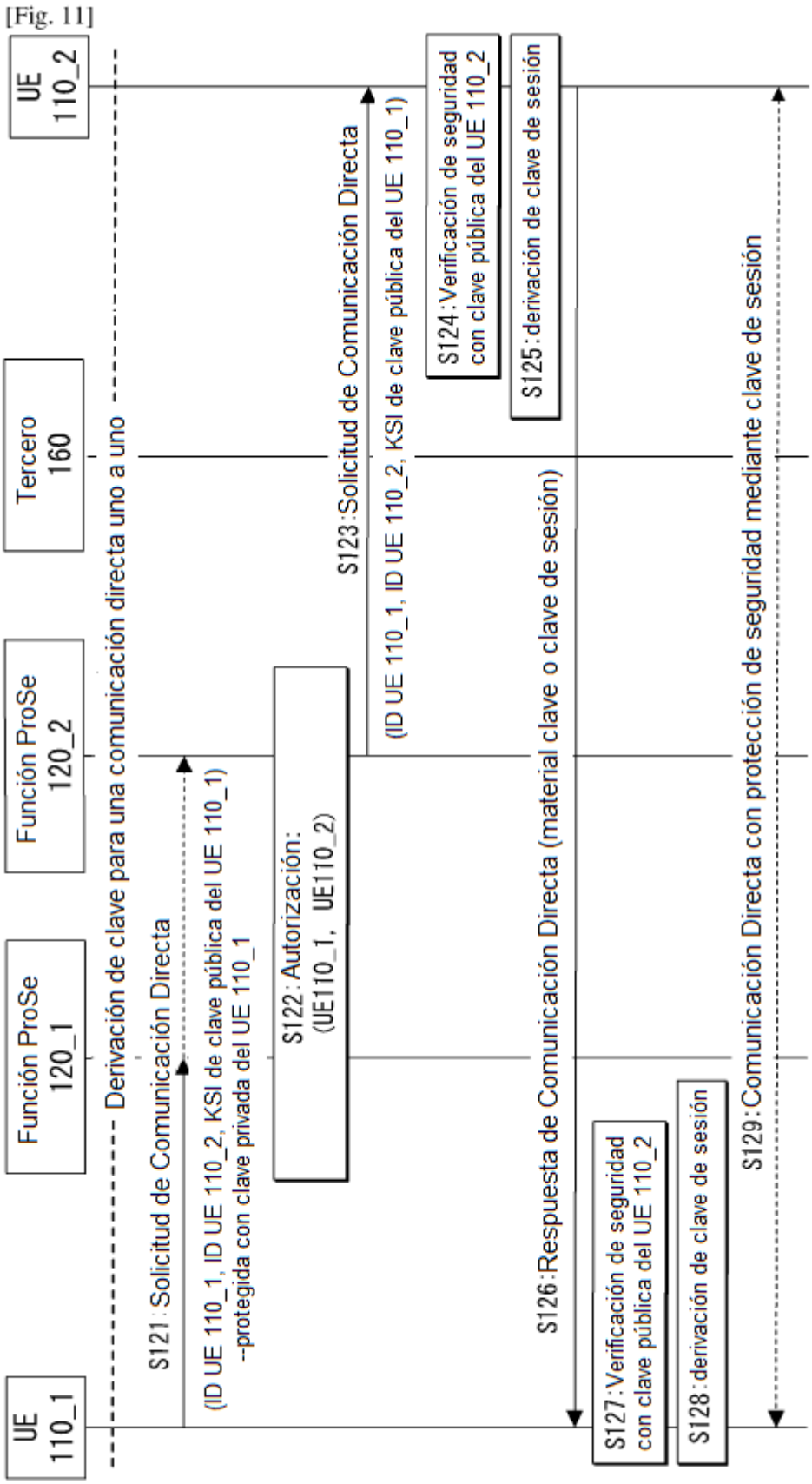
[Fig. 9]


150
Servidor de APP ProSe
SGi
PC2
120_1-120_n
140
EPC
PC4
Función ProSe
PC6
S1
130
E-UTRAN
PC3
PC1
LTE-Uu
LTE-Uu
110_1
110_m
PC5
UE
UE
APP ProSe
APP ProSe

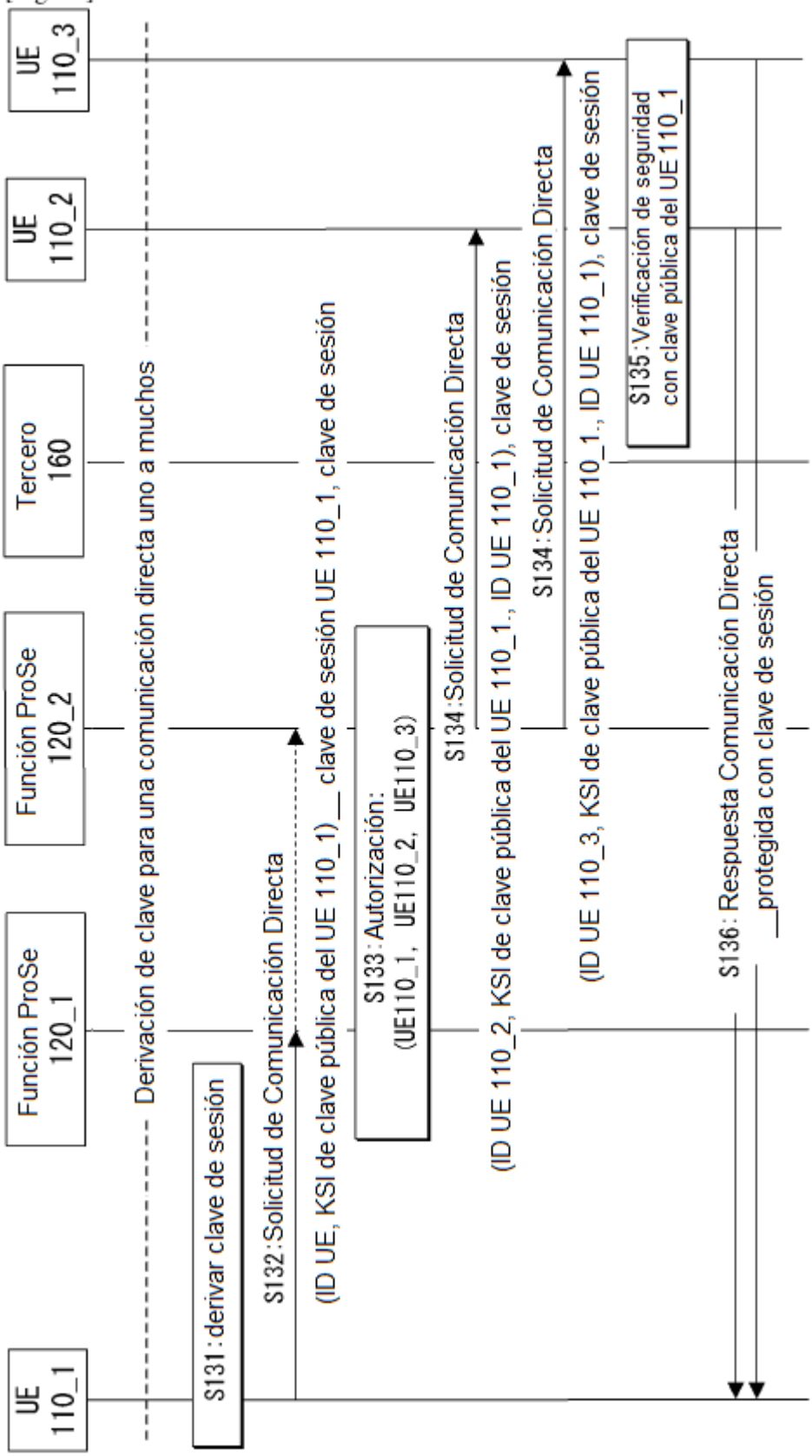
[Fig. 10]


UE 110_1
Función ProSe 120_1
Función ProSe 120_2
Tercero 160
UE 110_2
Registro de UE en Función ProSe
S111: Registro de UE
(Clave pública UE 110_1)
S112: Registrar clave pública de UE 110_1
S113: Lista de permitidos UE 110_1
(ID de UE, claves públicas)
S114: Lista de permitidos UE 110_1
(ID de UE, claves públicas)
S115: Registro de UE
(Clave pública UE 110_2)
S116: Registrar clave pública UE 110_2
S117: Lista de permitidos UE 110_2
(ID de UE, claves públicas)
S118: Lista de permitidos UE 110_2
(ID de UE, claves públicas)

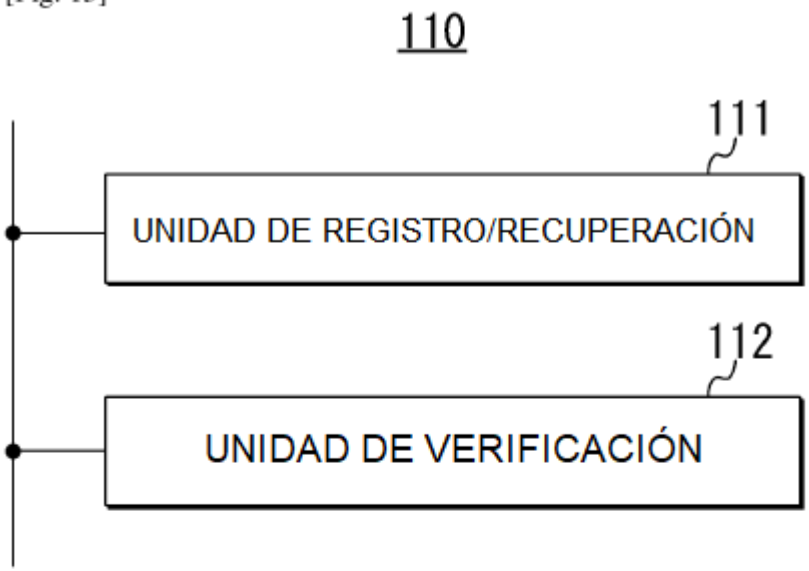
[Fig. 11]


UE 110_1
Función ProSe 120_1
Función ProSe 120_2
Tercero 160
UE 110_2
Derivación de clave para una comunicación directa uno a uno
S121: Solicitud de Comunicación Directa
(ID UE 110_1, ID UE 110_2, KSI de clave pública del UE 110_1)
--protegida con clave privada del UE 110_1
S122: Autorización:
(UE110_1, UE110_2)
S123: Solicitud de Comunicación Directa
(ID UE 110_1, ID UE 110_2, KSI de clave pública del UE 110_1)
S124: Verificación de seguridad con clave pública del UE 110_2
S125: derivación de clave de sesión
S126: Respuesta de Comunicación Directa (material clave o clave de sesión)
S127: Verificación de seguridad con clave pública del UE 110_2
S128: derivación de clave de sesión
S129: Comunicación Directa con protección de seguridad mediante clave de sesión

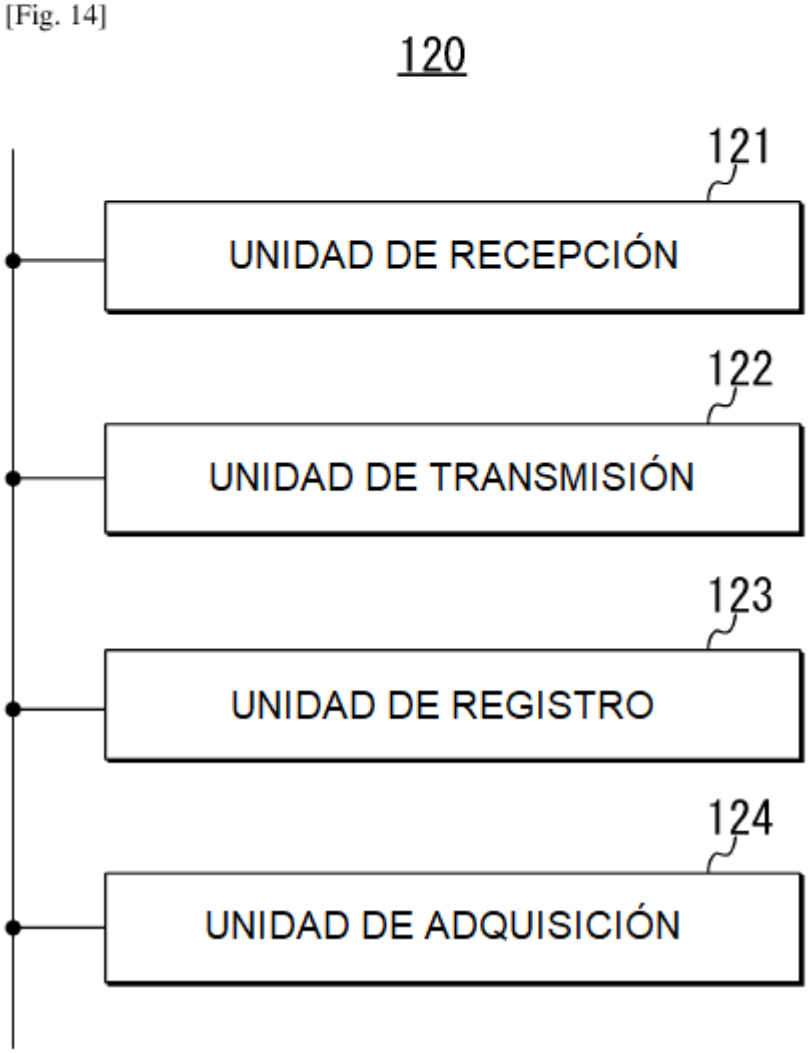
[Fig. 12]


UE 110_1
Función ProSe 120_1
Función ProSe 120_2
Tercero 160
UE 110_2
UE 110_3
Derivación de clave para una comunicación directa uno a muchos
S131: derivar clave de sesión
S132: Solicitud de Comunicación Directa
(ID UE, KSI de clave pública del UE 110_1)__ clave de sesión UE 110_1, clave de sesión
S133: Autorización:
(UE110_1, UE110_2, UE110_3)
S134: Solicitud de Comunicación Directa
(ID UE 110_2, KSI de clave pública del UE 110_1., ID UE 110_1), clave de sesión
S134: Solicitud de Comunicación Directa
(ID UE 110_3, KSI de clave pública del UE 110_1., ID UE 110_1), clave de sesión
S135: Verificación de seguridad con clave pública del UE 110_1
S136: Respuesta Comunicación Directa
__protegida con clave de sesión

[Fig. 13]


110
111
UNIDAD DE REGISTRO/RECUPERACIÓN
112
UNIDAD DE VERIFICACIÓN

[Fig. 14]


120
121
UNIDAD DE RECEPCIÓN
122
UNIDAD DE TRANSMISIÓN
123
UNIDAD DE REGISTRO
124
UNIDAD DE ADQUISICIÓN

[Fig. 15]