

MÉTODO Y APARATO PARA LA REALIZACIÓN DE CONEXIONES SEGURAS A TRAVÉS DE REDES DE ACCESO HETEROGÉNEAS

CAMPO TÉCNICO

- 5 [0001] Esta solicitud se refiere, en general, a redes de acceso y, más específicamente, al establecimiento de sesiones por parte del equipo de usuario en múltiples redes de acceso heterogéneas.

DESCRIPCIÓN DE LA TÉCNICA RELACIONADA

- 10 [0002] Las afirmaciones en esta sección proporcionan una descripción de la técnica relacionada y no constituyen admisiones de la técnica previa. Los equipos de usuario (UE), tales como teléfonos inteligentes, tabletas inteligentes, computadoras portátiles, computadoras, relojes inteligentes, etc., a menudo incluyen capacidad de conectividad de red de área local inalámbrica (WLAN) (tal como conectividad WLAN compatible con IEEE
- 15 802.11x) y conectividad de red de acceso por radio (tal como tecnologías que cumplen total o parcialmente el conjunto de estándares del proyecto de asociación de 3.^a generación (3GPP), incluidos EVDO, UMTS, HSPA y LTE). Por lo tanto, los UE pueden conectarse a la red de núcleo de paquetes evolucionada (EPC) 3GPP mediante el uso de dos tipos de tecnologías de acceso compuestas por redes de acceso 3GPP y redes de acceso no 3GPP.
- 20 [0003] En general, las redes de acceso 3GPP cumplen total o parcialmente las tecnologías especificadas en el conjunto de estándares del 3GPP que incluye, por ejemplo, GPRS, UMTS, EDGE, HSPA, LTE y LTE Advanced. Las redes de acceso no 3GPP cumplen total o parcialmente tecnologías que no están especificadas en el conjunto de estándares del 3GPP. Estas incluyen tecnologías tales como cdma2000, WLAN (tal como WLAN
- 25 compatible con IEEE 802.11x) o redes fijas.
- [0004] El conjunto de estándares del 3GPP especifica tecnologías de acceso «no 3GPP» con diferentes mecanismos de seguridad: redes de acceso no confiables y redes de acceso confiables. Las redes de acceso no confiables incluyen redes de acceso que pueden representar un mayor riesgo de seguridad (por ejemplo, una WLAN pública o una red de
- 30 acceso de femtoceldas). Las redes de acceso confiables incluyen las redes de acceso que el operador de red considera que tienen un nivel de confianza desde un punto de vista de seguridad y pueden interactuar directamente con la red EPC.
- [0005] En el nuevo conjunto de estándares 5G, una de las características más importantes del sistema 5G es que ofrece una red principal convergente que es independiente del acceso.
- 35 Se pueden admitir diferentes tipos de redes de acceso, incluido el acceso 3GPP y el acceso no 3GPP, a través de una red de acceso común e interfaces de red principal. Una red de acceso no 3GPP (N3AN) se considera una red de acceso 5G y forma parte del sistema 5G

(5GS).

[0006] Para el acceso no 3GPP no confiable, un nodo de acceso N3G de N3IWF proporciona la terminación de interfaces de señalización para el plano de control y el plano de usuario, respectivamente, igual que un nodo NG-RAN. Por lo tanto, los UE con capacidad 5G pueden acceder a la red principal 5G conectándose a una red de acceso no 3GPP, como una red de acceso 5G a través de N3IWF. La N3IWF retransmite la señalización del plano de control del enlace ascendente y del enlace descendente entre el UE y la AMF, de modo que el UE tiene una conexión directa de señalización del plano de control hacia la AMF. Además, la N3IWF proporciona una conexión de plano de usuario entre el UE y la UPF para sesiones de PDU a través de una red de acceso no 3GPP.

[0007] Cuando un UE está registrado en el núcleo 5G a través de redes de acceso 3GPP y acceso no 3GPP, se pueden activar múltiples conexiones de estrato sin acceso (NAS) al mismo tiempo. El UE puede registrarse en la misma PLMN o en una PLMN diferente. Si el UE accede a una PLMN a través de un tipo de acceso (por ejemplo, acceso 3GPP) y accede a otra PLMN a través del otro tipo de acceso (por ejemplo, acceso no 3GPP), se realizan diferentes autenticaciones primarias. Después del registro, las conexiones NAS pueden ser atendidas por diferentes AMF que utilizan diferentes contextos de seguridad. Sin embargo, si el UE solicita el registro en la misma red de servicio a través de diferentes tipos de redes de acceso, se crea un contexto de seguridad NAS 5G común durante el procedimiento de registro a través del primer tipo de acceso, y todas las conexiones NAS son atendidas por la misma AMF.

[0008] Actualmente, para el acceso 3GPP, se supone que el identificador de conexión NAS es «0». Para el acceso no 3GPP, se supone que el identificador de conexión NAS es «1». Surge un problema cuando se agregan tipos de redes de acceso no 3GPP adicionales en versiones futuras, por ejemplo, acceso WLAN confiable, acceso por cable, acceso MuLteFire, etc. Estos diferentes tipos de redes de acceso no 3GPP podrían necesitar, cada uno, establecer conexiones NAS separadas. Sin embargo, actualmente solo existe un identificador de conexión NAS de «1» para las conexiones NAS a través de los diferentes tipos de redes de acceso no 3GPP.

[0009] Por lo tanto, existe la necesidad de proporcionar un sistema y un método que admita conexiones NAS a través de múltiples tipos diferentes de redes de acceso no 3GPP. También se proporcionan otras necesidades y beneficios con las modalidades descritas en la presente.

COMPENDIO

[0010] En la presente se describen modalidades que proporcionan un sistema, dispositivo, método y/o producto de programa informático para proporcionar servicios de red

a equipos de usuario no autenticados. Por ejemplo, se describen varios métodos para el establecimiento de sesiones para un UE no autenticado en una red de acceso no 3GPP confiable.

[0011] De acuerdo con una modalidad, se proporciona un equipo de usuario que

- 5 comprende: uno o más transceptores configurados para acceder a una red de servicio a través de múltiples tipos de redes de acceso; un dispositivo de memoria configurado para almacenar una tabla de mapeo; y un dispositivo de procesamiento configurado para: generar una solicitud de registro en la red de servicio a través de una primera red de acceso, en donde la solicitud incluye un primer tipo de red de acceso de la primera red de acceso; recibir una respuesta
- 10 que indique que la red de servicio acepta el establecimiento de la conexión NAS, en donde la respuesta incluye el primer tipo de red de acceso y el identificador de conexión NAS; y actualizar la tabla de mapeo para incluir el primer tipo de red de acceso y el identificador de conexión NAS. En algunas modalidades, el primer tipo de red de acceso incluye un valor que indica al menos uno de: acceso 3GPP, acceso no 3GPP no confiable, acceso no 3GPP
- 15 confiable, acceso WLAN no confiable, acceso WLAN confiable o acceso MuLteFire. En algunas modalidades, el dispositivo de procesamiento se configura, además, para: actualizar la tabla de mapeo para incluir el primer tipo de red de acceso, identificador de conexión NAS, identificador de red de acceso e identificador de red de servicio. En algunas modalidades, el dispositivo de procesamiento puede configurarse, además, para: generar una segunda
- 20 solicitud de registro en la red de servicio a través de una segunda red de acceso con un segundo tipo de red de acceso, en donde la segunda solicitud incluye el segundo tipo de red de acceso de la segunda red de acceso; recibir una respuesta que indique que la red de servicio acepta el establecimiento de la conexión, en donde la respuesta incluye el segundo tipo de red de acceso y un segundo identificador de conexión NAS; y actualizar la tabla de
- 25 mapeo para incluir el segundo tipo de red de acceso y el segundo identificador de conexión NAS. En algunas modalidades, el segundo tipo de red de acceso es diferente al primer tipo de red de acceso, y en donde el segundo tipo de red de acceso indica un segundo tipo diferente de: acceso 3GPP, acceso no 3GPP no confiable, acceso no 3GPP confiable, acceso WLAN no confiable, acceso WLAN confiable o acceso MuLteFire. En algunas modalidades,
- 30 el dispositivo de procesamiento puede configurarse, además, para: generar una tercera solicitud de registro en la red de servicio a través de una tercera red de acceso con un tercer tipo de red de acceso, en donde la tercera solicitud incluye el tercer tipo de red de acceso de la tercera red de acceso; recibir una respuesta que indique que la red de servicio acepta el establecimiento de la conexión, en donde la respuesta incluye el tercer tipo de red de acceso
- 35 y un tercer identificador de conexión NAS; y actualizar la tabla de mapeo para incluir el tercer tipo de red de acceso y el tercer identificador de conexión NAS. En algunas modalidades, el tercer tipo de red de acceso es diferente al primer y el segundo tipo de red de acceso, y en

donde el tercer tipo de red de acceso indica un tercer tipo diferente de: acceso 3GPP, acceso no 3GPP no confiable, acceso no 3GPP confiable, acceso WLAN no confiable, acceso WLAN confiable o acceso MuLteFire. En algunas modalidades, el dispositivo de procesamiento se configura, además, para: utilizar el contexto de seguridad NAS existente establecido en la primera red de acceso con la red de servicio. En algunas modalidades, el dispositivo de procesamiento se configura, además, para: recibir una solicitud para realizar la autenticación para la conexión a través de la tercera red de acceso; obtener un nuevo contexto de seguridad NAS de la red de servicio a través de la tercera red de acceso; establecer la conexión NAS mediante el uso del nuevo contexto de seguridad NAS a través de la tercera red de acceso; activar el nuevo contexto de seguridad NAS para la primera y la segunda red de acceso; y eliminar el contexto de seguridad NAS anterior.

[0012] De acuerdo con otra modalidad, se proporciona un equipo de usuario que comprende: uno o más transceptores configurados para acceder a una red de servicio a través de múltiples tipos de redes de acceso; un dispositivo de procesamiento configurado para: generar una solicitud de registro en la red de servicio a través de una red de acceso; y recibir un mensaje de rechazo de registro, en donde el mensaje de rechazo de registro indica que la red de servicio no está autorizada. En algunas modalidades, el mensaje de rechazo de registro incluye un elemento de información de causa, en donde el elemento de información de causa incluye un valor correspondiente a «Red de servicio no autorizada». En algunas modalidades, el dispositivo de procesamiento se configura, además, para: cancelar el registro en la red de servicio; almacenar una identidad de la red de servicio en una lista de redes de servicio no autorizadas [la «lista de PLMN prohibidas»]. En algunas modalidades, el dispositivo de procesamiento se configura, además, para seleccionar otra red de servicio para el registro.

[0013] De acuerdo con otra modalidad, una función del servidor de autenticación en un nodo de una red principal, que comprende: un transceptor configurado para comunicarse con uno o más nodos adicionales en la red principal; un dispositivo de procesamiento configurado para: recibir una solicitud de autenticación para un UE que solicita acceso a una red de servicio, en donde la solicitud de autenticación incluye un identificador de la red de servicio y una identidad de suscriptor; y determinar que la red de servicio no está autorizada; y generar una respuesta de autenticación, en donde la respuesta de autenticación indica que la red de servicio no está autorizada. En algunas modalidades, la respuesta de autenticación puede incluir un elemento de información de causa, en donde el elemento de información de causa incluye un valor correspondiente a «Red de servicio no autorizada».

[0014] De acuerdo con otra modalidad, puede proporcionarse un equipo de usuario que comprende: un transceptor configurado para comunicarse con uno o más tipos de redes de acceso; un dispositivo de procesamiento configurado para generar un SUCI mediante: la determinación de uno de múltiples formatos SUPI; la determinación de uno de múltiples tipos

de identidad para un identificador de suscriptor; la determinación de una salida de esquema del identificador de suscriptor mediante el uso de un esquema de protección; y la construcción del SUCI, que incluye un valor de formato SUPI, un valor del tipo de identidad y la salida del esquema. En algunas modalidades, uno de los múltiples tipos de identidad para el identificador de suscriptor incluye uno de: SUCI, 5G-GUTI, IMEI, 5G-S-TMSI, IMEISV, dirección MAC o una identidad de dispositivo. En algunas modalidades, uno de los múltiples formatos SUPI incluye al menos uno de: IMSI, NAI basado en IMSI, NAI no basado en IMSI o MF-NAI. En algunas modalidades, el dispositivo de procesamiento se configura, además, para generar el SUCI mediante la selección de uno de múltiples tipos de red y la inclusión de un indicador del tipo de red para el tipo de red seleccionado en la estructura SUCI.

[0015] De acuerdo con otra modalidad, puede proporcionarse un aparato que comprende: al menos un procesador y al menos una memoria, que incluye instrucciones de programa informático, la al menos una memoria y las instrucciones del programa informático configuradas, con el al menos un procesador, para hacer que el aparato al menos: genere una solicitud de registro en una red de servicio a través de una red de acceso; reciba un mensaje de rechazo de registro, en donde el mensaje de rechazo de registro indica que la red de servicio no está autorizada por una red doméstica del aparato; y, en respuesta a la recepción del mensaje de rechazo de registro que indica que la red de servicio no está autorizada por la red doméstica del aparato, ingrese a un estado de anulación de registro tal que el aparato se configure para solicitar el registro a otra red de servicio. En algunas modalidades, el mensaje de rechazo de registro incluye un elemento de información de causa, en donde el elemento de información de causa incluye un valor que indica que la red de servicio no está autorizada por la red doméstica del aparato. En algunas modalidades, el al menos un procesador se configura, además, para: cancelar el registro en la red de servicio; y almacenar una identidad de la red de servicio en una lista de redes de servicio no autorizadas. En algunas modalidades, el al menos un procesador se configura, además, para seleccionar dicha otra red de servicio para el registro. En algunas modalidades, el mensaje de rechazo de registro indica que la red de servicio no está autorizada por la red doméstica del aparato para el acceso del proyecto de asociación de tercera generación (3GPP) a la red de servicio. En algunas modalidades, el al menos un procesador se configura, además, para: en respuesta a la recepción del mensaje de rechazo de registro que indica que la red de servicio no está autorizada por la red doméstica del aparato, establecer un estado de actualización del sistema de quinta generación (5GS) en 5U2 NO ACTUALIZADO.

[0016] De acuerdo con otra modalidad, puede proporcionarse un aparato que comprende: al menos un procesador y al menos una memoria, que incluye instrucciones de programa informático, la al menos una memoria y las instrucciones del programa informático configuradas, con el al menos un procesador, para hacer que el aparato al menos: reciba una

solicitud de autenticación para un equipo de usuario que solicita acceso a una red de servicio, en donde la solicitud de autenticación incluye un identificador de la red de servicio y una identidad de suscriptor; determine si la red de servicio está autorizada; y, en caso de que la red de servicio no esté autorizada, genere una respuesta de autenticación, en donde la

5 respuesta de autenticación indica que la red de servicio no está autorizada por una red principal asociada con el aparato. En algunas modalidades, la respuesta de autenticación incluye un elemento de información de causa, en donde el elemento de información de causa incluye un valor que indica que la red de servicio no está autorizada por la red principal.

[0017] De acuerdo con otra modalidad, puede proporcionarse un aparato que comprende:

10 al menos un procesador y al menos una memoria, que incluye instrucciones de programa informático, la al menos una memoria y las instrucciones del programa informático configuradas, con el al menos un procesador, para hacer que el aparato al menos: se comunique con una red principal a través de un tipo de red de acceso seleccionado; y construya un identificador oculto de suscripción utilizado para identificar el aparato durante la

15 comunicación con la red principal y el tipo de red de acceso seleccionado, el identificador oculto de suscripción incluye al menos: un valor del tipo de formato de identificador permanente de suscripción correspondiente a uno de múltiples tipos de formato de identificador permanente de suscripción, el valor del tipo de formato de identificador permanente de suscripción está asociado con un identificador permanente de suscripción, un

20 identificador del esquema de protección correspondiente a uno de múltiples esquemas de protección configurados previamente para el identificador permanente de suscripción, y una salida de esquema derivada del identificador permanente de suscripción mediante el uso de uno de los esquemas de protección configurados previamente para el identificador permanente de suscripción. En algunas modalidades, el identificador permanente de

25 suscripción comprende uno de: una identidad de suscriptor móvil internacional (IMSI) o un tipo de identificador específico de red, el valor del tipo de formato de identificador permanente de suscripción correspondiente, lo que permite la identificación del tipo de formato de identificador de suscriptor entre IMSI o tipos de identificadores específicos de red. En algunas modalidades, el identificador oculto de suscripción se transmite a la red principal como un

30 parámetro de identidad móvil con un tipo de campo de identidad que indica un tipo de identidad del identificador oculto de suscripción. En algunas modalidades, el parámetro de identidad móvil comprende un parámetro de identidad móvil del sistema de quinta generación (5GS), y el tipo de identidad del identificador oculto de suscripción (SUCI) comprende un tipo de identidad SUCI. En algunas modalidades, el valor del tipo de formato de identificador

35 permanente de suscripción del identificador oculto de suscripción se codifica en un campo de formato de identificador permanente de suscripción (SUPI) del parámetro de identidad móvil 5GS.

[0018] De acuerdo con otra modalidad, puede proporcionarse un aparato que comprende: al menos un procesador y al menos una memoria, que incluye instrucciones de programa informático, la al menos una memoria y las instrucciones del programa informático configuradas, con el al menos un procesador, para hacer que el aparato al menos: reciba, desde el equipo de usuario, a través de un tipo de red de acceso seleccionado un identificador oculto de suscripción, el identificador oculto de suscripción incluye al menos: un valor del tipo de formato de identificador permanente de suscripción correspondiente a uno de múltiples tipos de formato de identificador permanente de suscripción, el valor del tipo de formato de identificador permanente de suscripción está asociado con un identificador permanente de suscripción, un identificador del esquema de protección correspondiente a uno de múltiples esquemas de protección configurados previamente para el identificador permanente de suscripción, y una salida de esquema derivada del identificador permanente de suscripción mediante el uso de uno de los esquemas de protección configurados previamente para el identificador permanente de suscripción; e identifique el equipo de usuario, durante la comunicación con el equipo de usuario a través del tipo de red de acceso seleccionado, al menos en base al identificador oculto de suscripción. En algunas modalidades, el identificador permanente de suscripción comprende uno de: una identidad de suscriptor móvil internacional (IMSI) o un tipo de identificador específico de red, el valor del tipo de formato de identificador permanente de suscripción correspondiente, lo que permite la identificación del tipo de formato de identificador de suscriptor entre IMSI o tipos de identificadores específicos de red. En algunas modalidades, la al menos una memoria y las instrucciones del programa informático se configuran, con el al menos un procesador, para hacer que el aparato al menos: identifique, al menos en base al valor de tipo de formato de identificador permanente de suscripción correspondiente, el tipo de formato de identificador de suscriptor entre IMSI o tipos de identificadores específicos de red. En algunas modalidades, el identificador oculto de suscripción es recibido por el aparato como un parámetro de identidad móvil con un tipo de campo de identidad que indica un tipo de identidad del identificador oculto de suscripción. En algunas modalidades, el parámetro de identidad móvil comprende un parámetro de identidad móvil del sistema de quinta generación (5GS), y la identidad del identificador oculto de suscripción (SUCI) comprende un tipo de identidad SUCI. En algunas modalidades, el valor del tipo de formato de identificador permanente de suscripción del identificador oculto de suscripción se codifica en un campo de formato de identificador permanente de suscripción (SUPI) del parámetro de identidad móvil 5GS.

BREVE DESCRIPCIÓN DE LAS FIGURAS

[0019] La FIGURA 1 ilustra un diagrama de bloques esquemático de una modalidad de tipos de redes de acceso para un núcleo de paquetes evolucionado que cumple total o

parcialmente el conjunto de estándares del proyecto de asociación de 3.^a generación (3GPP) u otro tipo de estándares de red principal de paquetes de datos de protocolo de Internet (IP), de acuerdo con algunas modalidades descritas en la presente;

[0020] la FIGURA 2 ilustra un diagrama de bloques esquemático de una modalidad de una arquitectura de sistema 5G para acceso no 3GPP, de acuerdo con algunas modalidades descritas en la presente;

[0021] la FIGURA 3 ilustra un diagrama de bloques esquemático de una modalidad de un UE que accede al sistema 5G a través de múltiples redes de acceso heterogéneas, de acuerdo con algunas modalidades descritas en la presente;

[0022] la FIGURA 4 ilustra un diagrama de flujo lógico de una modalidad de un método para el flujo de mensajes de autenticación y de acuerdo de claves entre el UE y las funciones de la red principal, cuando el UE inicia el registro inicial a través del Tipo de red de acceso A, de acuerdo con algunas modalidades descritas en la presente;

[0023] la FIGURA 5 ilustra un diagrama de bloques esquemático de una modalidad de la tabla de mapeo de la red de servicio y el tipo de acceso a las conexiones NAS, de acuerdo con algunas modalidades descritas en la presente;

[0024] la FIGURA 6 ilustra un diagrama de bloques esquemático de una modalidad del contenido de un mensaje de solicitud de registro, de acuerdo con algunas modalidades descritas en la presente;

[0025] la FIGURA 7 ilustra un diagrama de bloques esquemático de una modalidad de elemento de información del tipo de acceso en un mensaje de solicitud de registro, de acuerdo con algunas modalidades descritas en la presente;

[0026] la FIGURA 8 ilustra un diagrama de bloques esquemático de una modalidad de los valores del tipo de acceso para el elemento de información del tipo de acceso en un mensaje de solicitud de registro, de acuerdo con algunas modalidades descritas en la presente;

[0027] la FIGURA 9 ilustra un diagrama de flujo lógico de una modalidad de un método para el registro por parte de un UE a través de un Tipo de red de acceso C cuando se reutiliza el contexto de seguridad NAS existente, de acuerdo con algunas modalidades descritas en la presente;

[0028] la FIGURA 10 ilustra un diagrama de bloques esquemático de una modalidad de la tabla de mapeo de la red de servicio y el tipo de acceso a las conexiones NAS después del registro con un tipo de acceso A, un tipo de acceso B y un tipo de acceso C, de acuerdo con algunas modalidades descritas en la presente;

[0029] la FIGURA 11 es un diagrama de flujo lógico de una modalidad de un método para el registro por parte del UE a través de un tipo de red de acceso C cuando se inicia una nueva autenticación, de acuerdo con algunas modalidades descritas en la presente;

[0030] la FIGURA 12 ilustra un diagrama de bloques esquemático de una modalidad de

la tabla de mapeo de la red de servicio y el tipo de acceso a las conexiones NAS después del registro con un tipo de acceso A, un tipo de acceso B y un tipo de acceso C, de acuerdo con algunas modalidades descritas en la presente;

[0031] la FIGURA 13 ilustra un diagrama de flujo lógico de una modalidad de un método para el registro por parte de un UE a través de un Tipo de red de acceso A cuando se ha producido un error de autorización de la red de servicio, de acuerdo con algunas modalidades descritas en la presente;

[0032] la FIGURA 14 ilustra un diagrama de bloques esquemático de una modalidad del elemento de información de causa 5GMM, de acuerdo con algunas modalidades descritas en la presente;

[0033] la FIGURA 15 ilustra un diagrama de bloques esquemático de una modalidad de los valores de causa para el elemento de información de causa 5GMM, de acuerdo con algunas modalidades descritas en la presente;

[0034] la FIGURA 16 ilustra un diagrama de bloques esquemático de una modalidad de un nuevo campo de información para un Identificador oculto de suscripción (SUCI) para habilitar diferentes estructuras de SUCI, de acuerdo con algunas modalidades descritas en la presente;

[0035] la FIGURA 17 ilustra un diagrama de bloques esquemático de una modalidad de los tipos de identidad admitidos por el nuevo campo de información para el Identificador oculto de suscripción (SUCI), de acuerdo con algunas modalidades descritas en la presente;

[0036] la FIGURA 18 ilustra un diagrama de bloques esquemático de una modalidad de un formato genérico de identidad de suscriptor de SUCI, de acuerdo con algunas modalidades descritas en la presente;

[0037] la FIGURA 19 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI cuando el formato SUPI es IMSI o NAI basado en IMSI, de acuerdo con algunas modalidades descritas en la presente;

[0038] la FIGURA 20 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI cuando el formato SUPI es NAI no basado en IMSI y el tipo de identidad es «SUCI», de acuerdo con algunas modalidades descritas en la presente;

[0039] la FIGURA 21 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI cuando el formato SUPI es «NAI no basado en IMSI» y al NTI se le asigna un ID de PLMN global reservado, de acuerdo con algunas modalidades descritas en la presente;

[0040] la FIGURA 22 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI cuando el tipo de identidad es «SUCI» y el formato SUPI es «MF-NAI»; de acuerdo con algunas modalidades descritas en la presente;

[0041] la FIGURA 23 ilustra un diagrama de bloques esquemático de una modalidad del tipo de identidad de SUCI, de acuerdo con algunas modalidades descritas en la presente;

[0042] la FIGURA 24 ilustra un diagrama de bloques esquemático de una modalidad de un equipo de usuario ilustrativo, de acuerdo con algunas modalidades descritas en la presente;

[0043] la FIGURA 25 ilustra un diagrama de bloques esquemático de una modalidad de un nodo de AMF ilustrativo, de acuerdo con algunas modalidades descritas en la presente;

[0044] la FIGURA 26 ilustra un diagrama de bloques esquemático de una modalidad de una N3IWF ilustrativa, de acuerdo con algunas modalidades descritas en la presente;

DESCRIPCIÓN DETALLADA

[0045] La descripción y los dibujos simplemente ilustran los principios de varias modalidades. Por lo tanto, se apreciará que los expertos en la técnica podrán idear diversas disposiciones que, aunque no se describen o se muestran explícitamente en la presente, incorporan los principios de la presente y en las reivindicaciones, y se incluyen dentro del espíritu y el alcance de la descripción. Además, se pretende que todos los ejemplos enumerados en la presente tengan, principalmente y expresamente, fines pedagógicos para ayudar al lector a comprender los principios de la descripción y los conceptos aportados por el inventor para promover la técnica, y se interpretarán como no taxativos con respecto a los ejemplos y las condiciones que se enumeran específicamente. Además, se pretende que todas las afirmaciones en la presente que enumeran principios, aspectos y modalidades, así como ejemplos específicos de estos, comprendan sus equivalentes.

[0046] A continuación, se amplían algunas de las abreviaturas que se describen en la presente por motivos de conveniencia:

5G	Núcleo 5G
5GS	Sistema 5G
5G-AN	Red de acceso 5G
5G-GUTI	Identificador temporal único global 5G
5G-S-TMSI	Identificador temporal de suscripción móvil-S 5G
5QI	Identificador de QoS 5G
AKA	Autenticación y acuerdo de claves
AMF	Función de gestión de acceso y movilidad
AUSF	Función del servidor de autenticación
EAP	Protocolo de autenticación extensible
HPLMN	Red móvil terrestre pública doméstica
IKEv2	Intercambio de claves de internet v2
IMSI	Identidad de suscriptor móvil internacional

	IMEI	Identidad de equipo móvil internacional
	IPsec	Seguridad del protocolo de internet
	MCC	Código de móvil de país
	MCM	Modo de conexión múltiple
5	MNC	Código de móvil de red
	N3IWF	Función de interfuncionamiento no 3GPP
	NAI	Identificador de acceso a la red
	NAS	Estrato sin acceso
	ngKSI	Identificador de conjunto de claves en el sistema 5G
10	NHN-ID	ID de red de host neutral
	PDN	Red de paquetes de datos
	PLMN	Red móvil terrestre pública
	QoS	Calidad del servicio
	SA	Asociación de seguridad
15	SCM	Modo de conexión simple
	SMC	Comando del modo de seguridad
	SUCI	Identificador oculto de suscripción
	SUPI	Identificador permanente de suscripción
	UDM	Gestión de datos unificada
20	UE	Equipo de usuario
	UICC	Tarjeta de circuito integrado universal
	USIM	Identidad de suscriptor móvil en UMTS

[0047] En la presente se describen una o más modalidades que proporcionan un sistema y un método para proporcionar servicios de red a equipos de usuario no autenticados. Por ejemplo, se describen varios métodos para el establecimiento de sesiones para un UE no autenticado en una red de acceso no 3GPP confiable.

[0048] La FIGURA 1 ilustra un diagrama de bloques esquemático de una modalidad de tipos de redes de acceso para un núcleo de paquetes evolucionado que cumple total o parcialmente el conjunto de estándares del proyecto de asociación de 3.^a generación (3GPP) u otro tipo de estándares de red principal de paquetes de datos de protocolo de Internet (IP). Esta arquitectura se describe con mayor detalle en el estándar técnico 3GPP TS 23.402 V14.2.0 (diciembre de 2016) con el título «3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses», que se incorpora a la presente mediante referencia.

[0049] En la arquitectura 3GPP, la red EPC 100 se acopla de forma comunicativa a una o más redes de acceso 102. En una modalidad, las redes de acceso 102 pueden incluir una o más redes de acceso 3GPP 104 o una o más redes de acceso no 3GPP 106. Las redes de

acceso 3GPP 104 cumplen total o parcialmente las tecnologías especificadas en el conjunto de estándares del 3GPP e incluyen, por ejemplo, GPRS, UMTS, EDGE, HSPA, LTE y LTE Advanced. Las redes de acceso no 3GPP 106 cumplen total o parcialmente tecnologías que no están especificadas en el conjunto de estándares del 3GPP. Las redes de acceso no 3GPP 106 pueden especificarse como tales en el conjunto de estándares del 3GPP. Las redes de acceso no 3GPP 106 pueden incluir una o más redes de acceso confiables no 3GPP 108 o una o más redes de acceso no confiables no 3GPP 110.

[0050] Las redes de acceso no 3GPP confiables 108 son redes de área local inalámbrica (WLAN) creadas por el operador o admitidas por el operador, tal como una red WLAN compatible con IEEE 802.11x, con cifrado y un método de autenticación seguro. En una modalidad, la red de acceso no 3GPP confiable 108 admite los siguientes ejemplos de funciones: autenticación basada en 802.1x que, a su vez, también requiere cifrado de la red de acceso por radio (RAN), acceso a la red basado en 3GPP mediante el uso del método del EAP para la autenticación, y protocolos IPv4 y/o IPv6. Sin embargo, un operador puede determinar que otros tipos de redes de acceso no 3GPP con diferentes tipos de seguridad deben considerarse confiables. Las redes de acceso no 3GPP no confiables 110 incluyen redes de acceso no 3GPP desconocidas para un operador o que no incluyen estándares de autenticación admitidos. Por ejemplo, una red de acceso no 3GPP no confiable puede incluir una WLAN doméstica o pública, tal como una red WLAN compatible con IEEE 802.11x que esté abierta al público, WLAN doméstica, u otra que no sea creada y administrada por un operador.

[0051] Otro conjunto de protocolos para la tecnología inalámbrica de quinta generación, o 5G, es la última versión de tecnología celular, diseñada para aumentar en gran medida la velocidad y la capacidad de respuesta de las redes inalámbricas. El término 5G fue definido inicialmente por el estándar ITU IMT-2020, que requería una capacidad máxima de descarga teórica de 20 gigabits. Más recientemente, el grupo de estándares de la industria 3GPP está definiendo la arquitectura y los protocolos 5G. Por ejemplo, la Especificación técnica (TS) 23.501 define la arquitectura del sistema de la etapa 2 para el sistema 5G, que incluye la segmentación de red. La Especificación técnica (TS) 23.502 define los procedimientos para el Sistema 5G. La Especificación técnica (TS) 23.503 define las políticas y el marco de control de carga para el sistema 5G.

[0052] En los sistemas 5G, la red de acceso 5G puede incluir, por ejemplo, una red de acceso por radio de última generación (NG) (NG-RAN), tal como se describe en 3GPP TS 38.300. Además, una red de acceso 5G puede incluir una red de acceso no 3GPP no confiable en la que el UE puede conectarse a la red principal 5G, por ejemplo, a través de un túnel IPSec/IKE seguro que termina en una función de interfuncionamiento no 3GPP (N3IWF). La red de acceso no 3GPP (N3AN) se considera una red de acceso 5G y forma parte del sistema

5G (5GS).

[0053] Para el acceso a no 3GPP no confiables, el nodo de acceso que incluye la N3IWF proporciona la terminación de las interfaces de señalización N2 y N3 para el plano de control y el plano de usuario, respectivamente. Los UE con capacidad 5G acceden a la red principal 5G conectándose a la red de acceso no 3GPP (como una red de acceso 5G) a través de la N3IWF. La N3IWF retransmite la señalización NAS (N1) del plano de control de enlace ascendente y enlace descendente entre el UE y la red principal 5G, lo hace posible que el UE tenga una conexión de señalización NAS directa hacia la red principal. Además, la N3IWF proporciona una conexión de plano de usuario entre el UE y la red principal para sesiones de PDU a través de la red de acceso no 3GPP.

[0054] La FIGURA 2 ilustra un diagrama de bloques esquemático de una modalidad de una arquitectura de sistema 5G para acceso no 3GPP. Esta arquitectura se describe con mayor detalle en el estándar técnico TS del 3GPP 23.501, versión 15 (diciembre de 2017), con el título «System Architecture for the 5G System», que se incorpora a la presente mediante referencia.

[0055] Las redes de acceso no 3GPP se conectan a la red principal 5G a través de una función de interfuncionamiento no 3GPP (N3IWF). La N3IWF interconecta las funciones en el plano de control (CP) y el plano de usuario (UP) de la red principal 5G a través de las interfaces N2 y N3, respectivamente. Un UE establece un túnel IPSec con la N3IWF para conectarse a la red principal 5G a través de la red de acceso no 3GPP no confiable. La UE se autentica y se conecta a la red principal 5G durante el procedimiento de establecimiento de túnel IPSec. Se describen más detalles sobre la conexión del UE a la red principal 5G a través de un acceso no 3GPP no confiable en 3GPP TS 23.502, versión 15 (diciembre de 2017) con el título «Procedures for the 5G System», que se incorpora a la presente mediante referencia.

[0056] El sistema 5G incluye una red móvil terrestre pública doméstica o PLMN doméstica equivalente (HPLMN-5G) que incluye una función de gestión de acceso y movilidad (AMF). La AMF proporciona la terminación de la interfaz de plano de control RAN (N2) y la terminación del conjunto de protocolos NAS (N1), así como la protección de la integridad y el cifrado de NAS. La AMF también proporciona gestión de registro y conexión. La AMF puede incluir varias funcionalidades para admitir redes de acceso no 3GPP. Por ejemplo, la AMF puede proporcionar soporte de protocolos de control de interfaz N2 con la N3IWF, así como soporte de la señalización de NAS con un UE a través de la N3IWF. Además, la AMF puede proporcionar soporte para la autenticación de UE conectados a través de la N3IWF y gestión de la movilidad, autenticación y uno o más estados de contexto de seguridad separados de un UE conectado a través del acceso no 3GPP o conectado a través de accesos 3GPP y no 3GPP simultáneamente.

[0057] La función de gestión de sesiones (SMF) incluye la funcionalidad de gestión de

sesiones, por ejemplo, establecimiento, modificación y liberación de sesiones, lo que incluye el mantenimiento del túnel entre la UPF y el nodo de la AN. La SMF también proporciona la asignación y gestión de direcciones IP del UE (incluida la autorización opcional) y las funciones de DHCPv4 (servidor y cliente) y DHCPv6 (servidor y cliente).

5 [0058] La función del plano de usuario (UPF) proporciona un punto de sesión de PDU externo de interconexión a la red de datos y al enrutamiento y reenvío de paquetes. La UPF también admite la parte del plano de usuario del cumplimiento de las normas y políticas, por ejemplo, activación, redirección, direccionamiento del tráfico, etc.

[0059] La función de control de políticas (PCF) admite un marco de políticas unificado
10 para regir el comportamiento de la red. La gestión de datos unificada (UDM) incluye soporte para la generación de credenciales de autenticación AKA del 3GPP, autorización de acceso basada en datos de suscripción (por ejemplo, restricciones de itinerancia) y gestión de registro de NF del servicio del UE (por ejemplo, almacenamiento con servicio de AMF para el UE, almacenamiento con servicio de SMF para la sesión de PDU del UE). También proporciona
15 gestión de suscripciones y SMS. Para proporcionar esta funcionalidad, la UDM utiliza datos de suscripción (que incluyen datos de autenticación) que pueden almacenarse en el UDR. La AUSF proporciona la función de servidor de autenticación (AUSF).

[0060] La funcionalidad de la N3IWF en caso de que el acceso no 3GPP no confiable incluya el soporte del establecimiento de un túnel IPsec con el UE. La N3IWF termina los
20 protocolos de IKEv2/IPsec con el UE a través de una interfaz NWu y retransmite, a través de una interfaz N2, la información necesaria para autenticar el UE y autorizar su acceso a la red principal 5G. La N3IWF proporciona la terminación de las interfaces N2 y N3 hacia la red principal 5G para el plano de control y el plano de usuario, respectivamente. La N3IWF retransmite la señalización del plano de control de enlace ascendente y enlace descendente
25 NAS (N1) entre el UE y la AMF. El N3IWF proporciona el manejo de la señalización de N2 desde SMF (retransmitida por la AMF) relacionada con sesiones de PDU y QoS. La N3IWF proporciona, además, el establecimiento de una asociación de seguridad IPsec (SA IPsec) para brindarle soporte al tráfico de la sesión de PDU. La N3IWF también proporciona la retransmisión de paquetes en el plano de usuario de enlace ascendente y enlace descendente
30 entre el UE y la UPF.

[0061] La FIGURA 3 ilustra un diagrama de bloques esquemático de una modalidad de un UE que accede al sistema 5G a través de múltiples redes de acceso heterogéneas. Las múltiples redes de acceso heterogéneas incluyen, por ejemplo, acceso 3GPP, acceso WLAN no confiable y acceso no 3GPP. Cuando el UE está registrado en el núcleo 5G a través de
35 redes de acceso 3GPP y acceso no 3GPP, múltiples conexiones de señalización del plano de control NAS se encuentran activas entre el UE y la AMF al mismo tiempo.

[0062] Cuando el UE establece una conexión segura, envía un mensaje de «Solicitud de

registro» a la AMF/SEAF. El mensaje de solicitud de registro incluye el IE de identidad móvil de 5GS que contiene SUCI, 5G-GUTI o IMEI. Después de recibir el mensaje de solicitud de registro del UE, la AMF/SEAF prepara un mensaje de «Solicitud de inicio de autenticación» (5G-AIR) para la AUSF. El SEAF también incluye el nombre de la red de servicio en el mensaje 5G-AIR. Después de recibir el mensaje 5G-AIR de la SEAF, la AUSF prepara el mensaje «Auth-Info-Req» y lo envía a la UDM/ARPF. La UDM/ARPF genera primero un vector de autenticación con el bit de separación del campo de gestión de autenticación (AMF) = 1. La UDM/ARPF luego calcula CK' e IK'. Después de eso, la ARPF envía (RAND, AUTN, XRES, CK', IK') a la AUSF mediante el uso del mensaje Auth-Info-Rsp. La AUSF responde a la SEAF enviando un mensaje 5G-AIA que, a su vez, incluye el mensaje de Solicitud de EAP/Desafío AKA'. La SEAF reenvía de forma transparente el mensaje de Solicitud de EAP/Desafío AKA al UE en un mensaje de Auth-Req del mensaje de NAS.

[0063] Después de recibir una respuesta del UE para el mensaje Auth-Req, la SEAF reenvía la Respuesta de EAP a la AUSF, y la AUSF valida la misma con la información almacenada. En caso de verificación exitosa, la AUSF envía EAP-EXITOSO y la Clave de origen a la SEAF y luego SEAF responde al UE con EAP-EXITOSO. Si la AUSF recibió SUCI de SEAF cuando se inició la autenticación, entonces la AUSF también incluye SUPI mientras envía el mensaje EAP-EXITOSO.

[0064] Si el UE accede a una PLMN a través de un tipo de acceso (por ejemplo, acceso 3GPP) y accede a otra PLMN a través de otro tipo de acceso (por ejemplo, acceso no 3GPP), se realizan diferentes autenticaciones primarias. Después del registro, las conexiones NAS son atendidas por diferentes AMF que utilizan diferentes contextos de seguridad. Sin embargo, tal como se muestra en la FIGURA 3, el UE puede solicitar el registro en la misma red de servicio (por ejemplo, la misma HPLMN-5G) a través de diferentes tipos de acceso. Todas las conexiones NAS para el UE son atendidas luego por la misma AMF.

[0065] Actualmente, cuando el UE está registrado en una red de servicio a través de diferentes tipos de acceso, la asignación de identificadores de conexión NAS está codificada. Por ejemplo, la Reunión Plenaria del 3GPP TSG #80 aprobó la finalización de la Versión 15 independiente (SA) de las especificaciones de 5G, con fecha del 15 de julio de 2018 (REL-15), y se incorpora a la presente mediante referencia. En REL-15, se supone que el identificador de conexión NAS es «0» para el acceso 3GPP. Para el acceso no 3GPP, se supone que el identificador de conexión NAS es «1». Esta asignación de identificadores de conexión codificados no presentó un problema en Rel-15 ya que solo se admitía un tipo de acceso no 3GPP, por ejemplo, acceso WLAN no confiable. Sin embargo, se prevé que se agregarán tipos de redes de acceso no 3GPP adicionales en versiones futuras, por ejemplo, acceso WLAN confiable, acceso por cable, acceso MuLteFire, etc. Los diferentes tipos de redes de acceso no 3GPP necesitan, cada uno, establecer conexiones NAS separadas.

Dependiendo de la configuración de la red y la suscripción al servicio del UE, el UE puede estar conectado simultáneamente a múltiples redes de acceso, por ejemplo, a redes de acceso 3GPP y múltiples redes de acceso no 3GPP, tal como se muestra en la FIGURA 2. En esta situación, no funcionaría el uso del mismo identificador de conexión NAS para conexiones a través de diferentes redes de acceso que no 3GPP.

[0066] Además, se pueden activar diferentes tipos de acceso en diferentes secuencias. Por ejemplo, es posible que el UE reciba primero autenticación a través de una de las redes de acceso no 3GPP y establezca un contexto de seguridad NAS antes de que el UE se registre a través de una red de acceso 3GPP. En otra posibilidad, el UE se registra a través de múltiples redes de acceso no 3GPP, pero no a través de una red de acceso 3GPP. Como tal, se desea una unión más flexible entre la red de servicio y el par de tipos de acceso y la conexión NAS.

[0067] Para que el UE verifique que está conectado a una red de servicio que está autorizada para proporcionar servicios al UE, es necesario que la red de servicio sea verificada por la red doméstica durante los procedimientos de autenticación (AKA). La verificación es implícita, ya que se supone que, si se ha completado con éxito la autenticación primaria y el procedimiento de acuerdo de claves, la red de servicio está autorizada. Sin embargo, el caso de error no debe estar implícito y debe definirse explícitamente.

[0068] Finalmente, en un sistema 5G, un identificador de suscriptor se denomina Identificador permanente de suscripción (SUPI). El SUPI se puede definir en formato IMSI o NAI. Para garantizar la privacidad del suscriptor, el SUPI no debe transferirse en texto claro a través de una RAN 5G y se oculta de forma inalámbrica mediante el uso del Identificador oculto de suscripción (SUCI). El SUCI se genera mediante el uso de un esquema de protección con la clave pública sin procesar que se suministró de forma segura en el control de la red doméstica. Solo se oculta la parte del identificador de suscripción del SUPI, mientras que la parte del identificador de la red doméstica del SUPI debe permanecer clara con fines de enrutamiento.

[0069] La información de enrutamiento puede ser diferente para diferentes tipos de redes de acceso. Para una red de acceso 3GPP, el código de móvil de país (MCC) y el código de móvil de red (MNC) pueden ser parte de la información de enrutamiento. Sin embargo, para una red de acceso no 3GPP, se puede usar información de enrutamiento e identificador de red diferentes. Por ejemplo, para la red de acceso tipo MuLteFire, la información de enrutamiento e identificador de red se basan en una ID de red de host neutral (NHN-ID), una ID de proveedor de servicios participante (PSP-ID) y un indicador de modo de acceso de host neutral (NHAMI). El NHAMI es un valor global reservado que es igual para todas las redes MuLteFire que habilitan el modo de acceso de NHN. Existe la necesidad de definir la codificación del elemento de información SUCI de manera genérica para que SUCI admita

otros tipos de redes y formatos de identificador de suscriptor para ser utilizados como una identidad móvil durante el procedimiento de autenticación.

[0070] También dado que los formatos IMSI y NAI se pueden usar para SUPI, para la salida del esquema SUCI, MSIN corresponde a la representación en caso de que el identificador de suscripción esté en formato IMSI, y el nombre de usuario corresponde a la representación en caso de que el identificador de suscripción esté en formato NAI. Para NAI basado en IMSI, la parte del identificador de suscriptor de NAI también está compuesta por dígitos, por lo que se necesitan reglas de codificación adicionales para distinguir el formato IMSI, el formato NAI y, potencialmente, otros tipos de formatos de identificador de suscriptor dentro de la definición del elemento de información SUCI.

[0071] Una o más modalidades descritas en la presente proporcionan sistemas y métodos para permitir conexiones seguras simultáneas a través múltiples redes de acceso heterogéneas. Se describen nuevos métodos y mejoras de protocolo para permitir que el UE incluya un tipo de acceso durante el registro y para rastrear el mapeo de conexiones NAS simultáneas a través de redes de acceso heterogéneas. También se describen nuevos sistemas y métodos para el manejo de los errores de verificación de la red de servicio. Se describen, además, nuevos sistemas y métodos y mejoras de protocolo para admitir el uso de NAI como un tipo de identificador de suscripción, así como la futura extensibilidad del identificador de suscripción para admitir redes de acceso MuLteFire y redes privadas.

1. Modalidad - El UE incluye el tipo de acceso durante el registro y la capacidad para rastrear el mapeo de conexiones NAS simultáneas a través de redes de acceso heterogéneas

a) El UE inicia el registro inicial a través del Tipo de acceso A

[0072] La FIGURA 4 ilustra un diagrama de flujo lógico de una modalidad de un método para el flujo de mensajes de autenticación y de acuerdo de claves entre el UE y las funciones de la red principal, cuando el UE inicia el registro inicial a través del Tipo de red de acceso A. Los mensajes NAS que se muestran entre el UE y la AMF pueden ser canalizados a través de un túnel IPsec en caso de que el Tipo de red de acceso A sea un acceso que no 3GPP no confiable. Por ejemplo, el UE puede establecer una asociación de seguridad IPsec (SA) con la N3IWF seleccionada mediante el inicio de un intercambio inicial del protocolo de intercambio de claves de internet (IKE), por ejemplo, tal como se describe en IETF RFC 7296, «Internet Key Exchange Protocol Version 2 (IKEv2)» (octubre 2014). En este ejemplo, el Tipo de red de acceso A es un primer tipo de múltiples tipos de redes, que incluyen el acceso 3GPP, el acceso no 3GPP confiable, el acceso no 3GPP no confiable, el acceso WLAN no confiable, el acceso WLAN confiable, el acceso MuLteFire, etc.

[0073] Cuando el UE inicia el registro a través del Tipo de red de acceso A, el UE incluye

el Tipo de acceso en el mensaje de solicitud de registro. El UE envía el mensaje de solicitud de registro a la AMF. La AMF está ubicada con la función de anclaje de seguridad (SEAF), que sirve como anclaje para la seguridad en los sistemas 5G. Al recibir el mensaje de solicitud de registro, la AMF/SEAF invoca el servicio Nausf_UEAuthentication enviando un mensaje de solicitud Nausf_UEAuthentication_Authenticate a la AUSF para iniciar una autenticación. La SEAF incluye el Id. de suscripción, el nombre de la red de servicio y el tipo de acceso en la solicitud Nausf_UEAuthentication_Authenticate.

[0074] Después de recibir el mensaje de solicitud Nausf_UEAuthentication_Authenticate, la AUSF compara el nombre de la red de servicio recibido con el nombre de la red de servicio esperado. Si la SEAF solicitante en la red de servicio está autorizada a utilizar el nombre de la red de servicio, la AUSF envía la solicitud Nudm_UEAuthentication_Get a la UDM, incluido el Id. de suscripción, el nombre de la red de servicio y el tipo de acceso.

[0075] Después de recibir la solicitud Nudm_UEAuthentication_Get, la UDM/ARPF elige el método de autenticación, según los datos de suscripción. Por ejemplo, un protocolo de tipo de autenticación mutua EAP-AKA', tal como se modifica en la presente, puede ejecutarse entre el UE y AUSF (tal como EAP-AKA' descrito en IETF RFC 5448, «Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')», 5 de marzo de 2018, y se incorpora a la presente mediante referencia).

[0076] La UDM/ARPF genera un vector de autenticación y envía este vector de autenticación AV' (RAND, AUTN, XRES, CK', IK') a la AUSF desde la cual recibió la solicitud Nudm_UEAuthentication_Get. La UDM/ARPF también transmite una indicación de que el vector de autenticación AV' se utilizará para EAP-AKA' mediante el uso de un mensaje de respuesta Nudm_UEAuthentication_Get.

[0077] La AUSF y el UE luego proceden con el intercambio de Solicitud de EAP/Desafío AKA'. La AUSF deriva las claves KAUSF y KSEAF, e incluye un mensaje de EAP Exitoso y el KSEAF dentro del mensaje de respuesta Nausf_UEAuthentication_Authenticate y lo envía a la AMF/SEAF.

[0078] Después de recibir el mensaje de respuesta Nausf_UEAuthentication_Authenticate, la AMF/SEAF deriva la clave KAMF. A continuación, la AMF inicia el procedimiento de comando del modo de seguridad para enviar el contexto de seguridad y la información del algoritmo de seguridad al UE. El UE recibe el comando del modo de seguridad y deriva los contextos de seguridad de NAS y envía un mensaje completo del comando del modo de seguridad a la AMF.

[0079] Al finalizar el procedimiento, se actualiza la tabla de mapeo de la red de servicio y el tipo de acceso a conexiones NAS para incluir información de conexión para el Tipo de red de acceso A, tal como se muestra en la FIGURA 5 más adelante.

[0080] La FIGURA 5 ilustra un diagrama de bloques esquemático de una modalidad de la

tabla de mapeo de la red de servicio y el tipo de acceso a las conexiones NAS. En este ejemplo, la tabla de mapeo se actualiza para incluir información de conexión para un primer tipo de red de acceso, por ejemplo, el Tipo de red de acceso A. La tabla de mapeo se actualiza después del registro por parte de un UE a través de una red de acceso. La tabla incluye el tipo de red de acceso, el identificador de red y el identificador de red de acceso. La tabla de mapeo también incluye el identificador de conexión NAS para la conexión NAS entre el Tipo de red de acceso A y el UE. Por lo tanto, la tabla de mapeo almacena, para cada conexión NAS, el identificador de conexión NAS, el tipo de red de acceso, el identificador de red y el identificador de red de acceso.

[0081] La FIGURA 6 ilustra un diagrama de bloques esquemático de una modalidad del contenido de un mensaje de solicitud de registro. El UE transmite el mensaje de solicitud de registro a la AMF a través de una red de acceso para comenzar un registro inicial. El mensaje de solicitud de registro incluye un elemento de información del «Tipo de acceso» de la red de acceso. El objetivo del elemento de información del tipo de acceso es indicar el tipo de acceso a través del cual se enviará la señalización de enlace descendente o los datos de usuario al UE.

[0082] La FIGURA 7 ilustra un diagrama de bloques esquemático de una modalidad de elemento de información del tipo de acceso en un mensaje de solicitud de registro. El tipo de acceso es un elemento de información de tipo 1.

[0083] La FIGURA 8 ilustra un diagrama de bloques esquemático de una modalidad de los valores del tipo de acceso para el elemento de información del tipo de acceso en un mensaje de solicitud de registro. En una modalidad, los tipos de acceso incluyen acceso 3GPP, acceso no 3GPP no confiable, acceso no 3GPP confiable, acceso WLAN no confiable, acceso WLAN confiable y acceso MuLteFire. Pueden incluirse tipos de acceso alternativos o adicionales en el elemento de información del tipo de acceso en el mensaje de registro.

b1) El UE inicia el registro posterior a través del tipo de acceso C y se reutiliza el contexto de seguridad NAS existente

[0084] Cuando el UE inicia el registro posterior a través de otro tipo de red de acceso, por ejemplo, el tipo de acceso C, y el UE ya está autenticado por la red y es atendido por la misma AMF en la misma red de servicio, la AMF puede decidir no ejecutar una nueva autenticación, si tiene un contexto de seguridad disponible para usar.

[0085] La FIGURA 9 ilustra un diagrama de flujo lógico de una modalidad de un método para el registro por parte de un UE a través de un Tipo de red de acceso C cuando se reutiliza el contexto de seguridad NAS existente. En este ejemplo, se supone que el UE ha establecido una conexión NAS con el Tipo de red de acceso A y el Tipo de red de acceso B. Debe tenerse en cuenta que los mensajes NAS que se muestran entre el UE y la AMF se canalizan a través

del túnel IPsec en caso de que el Tipo de red de acceso C sea un acceso no 3GPP no confiable.

[0086] Cuando el UE inicia el registro posterior a través de otra red de acceso con el Tipo de red de acceso C, este incluye el Tipo de acceso en el mensaje de solicitud de registro. La AMF puede decidir reutilizar el contexto de seguridad existente. Se crea una nueva conexión NAS mediante el uso del contexto de seguridad NAS 5G común disponible. El contexto de seguridad NAS se actualiza con parámetros específicos para la nueva conexión NAS. Al finalizar el procedimiento, se actualiza la tabla de mapeo de la red de servicio y el tipo de acceso a conexiones NAS para incluir información de conexión para la Red de acceso C, tal como se muestra en la FIGURA 10.

[0087] La FIGURA 10 ilustra un diagrama de bloques esquemático de una modalidad de una tabla de mapeo de la red de servicio y el tipo de acceso a conexiones NAS después del registro con un tipo de acceso A, tipo de acceso B y tipo de acceso C. En este ejemplo, la tabla de mapeo se actualiza para incluir la información de conexión para el tipo de acceso C. La tabla de mapeo se actualiza después del registro por parte del UE a través de una red de acceso. La tabla incluye el tipo de red de acceso, el identificador de red y el identificador de red de acceso. La tabla de mapeo también incluye el identificador de conexión NAS para la conexión NAS entre el Tipo de red de acceso C y el UE. El identificador de conexión NAS es «2». La tabla de mapeo puede almacenarse en el UE y AMF y/o en otras funciones o nodos, tal como la AUSF.

b2) El UE inicia el registro posterior a través de la Tipo de red de acceso C y se inicia una nueva autenticación

[0088] Cuando el UE inicia el registro posterior a través del tipo de acceso C, si el UE ya está autenticado por la red para la misma red de servicio, la AMF puede decidir ejecutar el procedimiento de autenticación y acuerdo de claves nuevamente ya sea porque el UE es atendido por una AMF diferente, o debido a que el algoritmo de seguridad ha cambiado.

[0089] La FIGURA 11 es un diagrama de flujo lógico de una modalidad de un método para el registro por parte del UE a través de un tipo de red de acceso C cuando se inicia una nueva autenticación. En este ejemplo, se supone que el UE ha establecido una conexión NAS con el Tipo de red de acceso A y el Tipo de red de acceso B. Debe tenerse en cuenta que los mensajes NAS que se muestran entre el UE y la AMF se canalizan a través del túnel IPsec si el Tipo de red de acceso C es un acceso no 3GPP no confiable.

[0090] Cuando el UE inicia el registro posterior a través del Tipo de red de acceso C, este incluye el Tipo de acceso en el mensaje de solicitud de registro. La AMF decide volver a ejecutar el procedimiento de autenticación y acuerdo de claves. La AMF puede decidir volver a ejecutar el procedimiento de autenticación y acuerdo de claves, ya sea porque el UE es

atendido por una AMF diferente o debido a que el algoritmo de seguridad ha cambiado. Cuando se completa el procedimiento de autenticación y acuerdo de claves, la AMF inicia un nuevo comando de modo de seguridad NAS hacia el UE para activar el nuevo contexto de seguridad NAS 5G derivado en el Tipo de acceso C.

5 [0091] Se crea una nueva conexión NAS mediante el uso del contexto de seguridad NAS 5G derivado recientemente. El contexto de seguridad NAS se actualiza con parámetros específicos para la nueva conexión NAS. A continuación, la AMF activa procedimientos adicionales de SMC de NAS para todos los demás tipos de acceso con el fin de activar el nuevo contexto de seguridad NAS 5G para cada tipo de acceso existente. Después de
10 procedimientos exitosos de SMC de NAS a través de los otros tipos de accesos, tanto el UE como la AMF eliminan el contexto de seguridad NAS anterior. Al finalizar el procedimiento, se actualiza la tabla de mapeo de la red de servicio y el tipo de acceso a conexiones NAS para incluir información de conexión para el Tipo de red de acceso C, tal como se muestra en la FIGURA 12.

15 [0092] La FIGURA 12 ilustra un diagrama de bloques esquemático de una modalidad de una tabla de mapeo de la red de servicio y el tipo de acceso a conexiones NAS después del registro con un tipo de acceso A, tipo de acceso B y tipo de acceso C. En este ejemplo, la tabla de mapeo se actualiza para incluir la información de conexión para el tipo de acceso C. La tabla de mapeo se actualiza después del registro por parte del UE a través de una red de
20 acceso. La tabla incluye el tipo de red de acceso, el identificador de red y el identificador de red de acceso. La tabla de mapeo también incluye el identificador de conexión NAS para la conexión NAS entre el Tipo de red de acceso C y el UE. El identificador de conexión NAS es «2». La tabla de mapeo puede almacenarse en el UE y AMF y/o en otras funciones o nodos, tal como la AUSF.

25

2. Modalidad - Error de autorización de la red de servicio

[0093] Para que el UE verifique que está conectado a una red de servicio que está autorizada para proporcionar servicios al UE, es necesario que la red de servicio sea verificada por la red doméstica durante los procedimientos de AKA. Si la red de servicio está autorizada,
30 el procedimiento AKA continuará, y si la autenticación primaria y el procedimiento de acuerdo de claves se han completado con éxito, significaría que la red de servicio está autorizada.

[0094] Sin embargo, si la red de servicio no está autorizada, el procedimiento de autenticación se detendrá, y la AUSF enviará una respuesta de autenticación a la AMF para indicar un error de autenticación debido a que la red de servicio no está autorizada.

35 [0095] La FIGURA 13 ilustra un diagrama de flujo lógico de una modalidad de un método para el registro por parte de un UE a través de un Tipo de red de acceso A cuando se ha producido un error de autorización de la red de servicio. Cabe destacar que los mensajes de

NAS entre el UE y la AMF se canalizan a través del túnel IPsec en caso de que el Tipo de red de acceso A sea un acceso no 3GPP no confiable.

[0096] Al de recibir el mensaje de solicitud Nausf_UEAuthentication_Authenticate, la AUSF compara el nombre de la red de servicio recibido con el nombre de la red de servicio esperado. Si la SEAF solicitante en la red de servicio no está autorizada a utilizar el nombre de la red de servicio, la AUSF responde con «red de servicio no autorizada» en la respuesta Nausf_UEAuthentication_Authenticate.

[0097] El error de autorización de la red de servicio es diferente a otros errores relacionados con PLMN. No es un error debido a la suscripción del UE o la restricción de acceso, por ejemplo, debido a la restricción del operador, sino que se debe al error de la verificación/autorización de seguridad de la red de servicio. Actualmente no existe un código de causa para tal caso de error.

[0098] Un código de error relacionado con el error de PLMN es «PLMN no permitida», pero es para iniciar un rechazo al UE debido a la suscripción o debido a una restricción determinada por el operador. Este código de error es: Causa #11 – PLMN no permitida. Esta causa de 5GMM se envía al UE si solicita servicio, o si la red inicia una solicitud de anulación del registro, en una PLMN donde el UE, por suscripción o debido a una restricción determinada por el operador, no está autorizado a operar.

[0099] Cuando el UE recibe un rechazo debido a «PLMN no permitida», el UE necesita establecer el estado de actualización de 5GS en 5U3 ITINERANCIA NO PERMITIDA, restablecer el contador de intentos de registro, eliminar su contexto de seguridad, cualquier 5G-GUTI, último TAI registrado visitado, lista TAI, ngKSI, la lista de PLMN equivalentes, y también almacenar la identidad de la PLMN en la «lista de PLMN prohibidas».

[00100] Sin embargo, cuando se produce el error de autorización de la red de servicio, dado que el error no es un error relacionado con la suscripción del UE o una restricción de acceso, el UE no necesita restablecer su estado de actualización a 5U3 ITINERANCIA NO PERMITIDA, y podría intentar seleccionar inmediatamente otra PLMN. Por lo tanto, es más apropiado definir un nuevo código de causa para esta situación diferente, ya que el UE puede tomar acciones diferentes.

[00101] Por ejemplo, cuando se produce un error en la autorización de la red de servicio, el UE puede cancelar el procedimiento de registro inicial con la PLMN, almacenar la identidad de la PLMN en la «lista de PLMN prohibidas», establecer el estado de actualización de 5GS en 5U2 NO ACTUALIZADO, e ingresar el estado 5GMM-DEREGISTERED.PLMN-SEARCH para realizar una selección de PLMN. Como tal, se necesita una nueva causa de rechazo de 5GMM para indicar «Red de servicio no autorizada».

[00102] La FIGURA 14 ilustra un diagrama de bloques esquemático de una modalidad del elemento de información de la causa de 5GMM. El elemento de información de la causa

de 5GMM indica un motivo para el rechazo por parte de la red de una solicitud de 5GMM del UE. En este elemento de información se incluye una nueva causa de rechazo de 5GMM para indicar «Red de servicio no autorizada». Por ejemplo, el nuevo rechazo puede incluirse como un nuevo código de causa #73 para señalar un error de autorización de la red de servicio al UE. El nuevo código de causa se utiliza si el proceso de autenticación no puede continuar porque la red de servicio no está autorizada.

[00103] La FIGURA 15 ilustra un diagrama de bloques esquemático de una modalidad de valores de causa para el elemento de información de la causa de 5GMM. Los valores de causa se actualizan para incluir la nueva Causa #73 - Red de servicio no autorizada. Esta causa de 5GMM se envía al UE si el UE inicia el registro hacia una red de servicio y falló la autorización de la red de servicio.

[00104] Después del error de autenticación de la red de servicio, el UE recibe un rechazo de registro con la causa de 5GMM «Red de servicio no autorizada» para el acceso 3GPP. El UE cancela el procedimiento de registro inicial, almacena la identidad de la PLMN en la «lista de PLMN prohibidas», establece el estado de actualización de 5GS en 5U2 NO ACTUALIZADO, e ingresa el estado 5GMM-DEREGISTERED.PLMN-SEARCH para realizar una selección de PLMN. Por lo tanto, el UE puede seleccionar otra PLMN.

3. Modalidad - Métodos y mejoras de protocolo para admitir el uso de NAI como un tipo de identificador de suscripción, y futura extensibilidad del identificador de suscripción para admitir redes privadas y MuLteFire

a) Se define un nuevo campo «Formato SUPI» para permitir que se utilicen diferentes tipos/formatos de identidad de suscriptor como Identificador de suscriptor.

[00105] Se asigna un Identificador permanente de suscripción 5G (SUPI) único global a cada suscriptor en el Sistema 5G y se suministra a la UDM/UDR. El SUPI se usa solo dentro del sistema 3GPP, y su privacidad se especifica en 3GPP TS 33.501, «Security architecture and procedures for 5G System», versión 15 con fecha del 26 de marzo de 2018, y se incorpora a la presente mediante referencia. Se han identificado los siguientes tipos de SUPI válidos: IMSI y NAI.

[00106] El SUCI es un SUPI parcialmente cifrado que se utiliza durante los procedimientos asociados con el Sistema 5G cuando al dispositivo no se le ha asignado una 5G-GUTI (Identidad temporal única global 5G). El SUCI generalmente se crea mediante el cifrado del componente MSIN (Número de identificación de suscriptor móvil) del IMSI del suscriptor.

[00107] El UE genera un SUCI mediante el uso de la clave pública sin procesar que se suministró de forma segura en el control de la red doméstica. El esquema de protección utiliza la clave pública sin procesar de la red doméstica. El UE construye una entrada de esquema a partir de la parte del identificador de suscripción del SUPI, según lo especificado por el

esquema de protección (por ejemplo, aplicando algún esquema de relleno). A continuación, el UE ejecuta el esquema de protección con la entrada de esquema construida como entrada y toma la salida como salida del esquema. El UE no oculta el identificador de la red doméstica, por ejemplo, el código de móvil de país (MCC) o el código de móvil de red (MNC). Luego, el

5 UE genera el SUCI que incluye el identificador de la red doméstica, el identificador de la clave pública de la red doméstica y la salida del esquema.

[00108] Sin embargo, dado que los formatos IMSI y NAI se pueden usar para SUPI, para la salida del esquema SUCI, MSIN corresponde a la representación en caso de que el identificador de suscripción esté en formato IMSI, y el nombre de usuario corresponde a la

10 representación en caso de que el identificador de suscripción esté en formato NAI. Para NAI basado en IMSI, la parte del identificador de suscriptor de NAI también está compuesta por dígitos, por lo que se necesitan reglas de codificación adicionales para distinguir el formato IMSI, el formato NAI y, potencialmente, otros tipos de formatos de identificador de suscriptor dentro de la definición del elemento de información SUCI.

[00109] La FIGURA 16 ilustra un diagrama de bloques esquemático de una modalidad de un nuevo campo de información para un Identificador oculto de suscripción (SUCI) para habilitar diferentes estructuras de SUCI. Mediante el uso de un nuevo campo de información, el formato de identidad móvil para el SUPI y SUCI puede adaptarse según el tipo/formato de identidad SUPI usada. Por ejemplo, para IMSI, el identificador de red se basa en MNC/MCC.

20 Para NAI basado en IMSI, el identificador de red también se basa en MNC/MCC. Para NAI no basado en IMSI, el identificador de red se basa en un indicador de tipo de red genérico y un identificador de red específico del operador o la empresa, donde el indicador de tipo de red puede basarse en un valor de MCC/MNC global reservado/codificado especial. Para NAI MuLteFire (MF-NAI), el identificador de red se basa en MCC/MNC global especial

25 reservado/codificado, ID de red de host neutral (NHN-ID) e ID del proveedor de servicios participante (PSP-ID).

[00110] La FIGURA 17 ilustra un diagrama de bloques esquemático de una modalidad de los tipos de identidad admitidos por el nuevo campo de información para el Identificador oculto de suscripción (SUCI). El nuevo campo de información de SUCI habilita diferentes tipos

30 de identidad para el identificador de suscriptor. Los tipos de identidad pueden incluir SUCI, 5G-GUTI, IMEI, 5G-S-TMSI, IMEISV, dirección MAC o una identidad de dispositivo. La identidad del dispositivo puede incluir, por ejemplo, UDI, ODIN, ID de Bluetooth, número de serie, etc. También se pueden definir tipos de identidad alternativos o adicionales.

[00111] La FIGURA 18 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI genérico. La estructura de identidad del suscriptor de SUCI incluye un indicador del tipo de red (NTI). Un identificador de la red doméstica y el identificador de enrutamiento pueden ser diferentes para diferentes tipos de

redes de acceso. El campo de salida del esquema contiene el identificador de suscriptor oculto generado mediante el uso de un esquema de protección.

[00112] La FIGURA 19 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI cuando el formato SUPI es IMSI o NAI basado en IMSI. Esto ilustra el formato del elemento de información de identidad móvil 5GS cuando el tipo de identidad es «SUCI» y el formato SUPI es «IMSI» o «NAI basado en IMSI». Para la red de acceso 3GPP, el identificador de la red doméstica contiene el ID de PLMN (MCC y MNC). El código de móvil de país (MCC) y el código de móvil de red (MNC) pueden ser parte de la información de enrutamiento.

[00113] La FIGURA 20 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI cuando el formato SUPI es NAI no basado en IMSI y el tipo de identidad es «SUCI». Esto ilustra un ejemplo del formato del elemento de información de identidad móvil 5GS cuando el tipo de identidad es «SUCI» y el formato SUPI es «IMSI» o «NAI no basado en IMSI». El identificador de red y la información de enrutamiento son específicos de la red. Los valores del campo Indicador del tipo de red (NTI) se utilizan para indicar el tipo de red.

[00114] La FIGURA 21 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI cuando el formato SUPI es «NAI no basado en IMSI» y al NTI se le asigna un ID de PLMN global reservado. Cuando el formato SUPI es «NAI no basado en IMSI», el Indicador del tipo de red puede ser un valor global reservado en el ID de PLMN (MCC/MNC).

[00115] La FIGURA 22 ilustra un diagrama de bloques esquemático de una modalidad de un formato de identidad de suscriptor de SUCI cuando el tipo de identidad es «SUCI» y el formato SUPI es «MF-NAI». Para las redes MuLteFire, la información de enrutamiento e identificador de red se basan en una ID de red de host neutral (NHN-ID), una ID de proveedor de servicios participante (PSP-ID) y un indicador de modo de acceso de host neutral (NHAMI). El NHAMI es un valor global reservado que es igual para todas las redes MuLteFire que habilitan el modo de acceso de NHN.

[00116] La FIGURA 23 ilustra un diagrama de bloques esquemático de una modalidad del tipo de identidad SUCI. La tabla ilustra varios ejemplos de codificación adicional para el tipo de identidad SUCI.

[00117] La FIGURA 24 ilustra un diagrama de bloques esquemático de una modalidad de un ejemplo de equipo de usuario 220. El equipo de usuario (UE) 220 puede incluir un teléfono inteligente, una tableta inteligente, una computadora portátil, un reloj inteligente, una PC, TV u otro dispositivo. Pueden incluirse componentes y funciones adicionales o alternativos dentro del UE 220. Además, es posible que una o más de las funciones y los componentes que se muestran en la presente no estén presentes o se combinen con otros componentes o

funciones.

[00118] El UE 220 incluye un dispositivo de procesamiento 2600 y un dispositivo de memoria 2602 que se configuran para realizar una o más de las funciones descritas en la presente con respecto al UE 220. El dispositivo de memoria 2602 puede incluir un objeto gestionado 2604 que almacena aplicaciones e instrucciones operativas que controlan el dispositivo de procesamiento 2600 para realizar varias funciones descritas en la presente. El dispositivo de memoria 2602 también puede almacenar la red de servicio y el tipo de acceso en la tabla de mapeo de conexiones NAS 2650. El UE 220 también puede incluir una UICC 2606 que incluye una USIM 2608 para el almacenamiento de IMSI.

[00119] El UE 220 puede incluir, además, un transceptor de Bluetooth 2610, un transceptor de WLAN (compatible con IEEE 802.11x) 2612, un transceptor de RF móvil (3G/4G/5G) 2614 y GPS 2616. El transceptor de WLAN 2612 puede funcionar como una interfaz de acceso no 3GPP a una red WLAN. El UE 220 puede incluir, además, interfaces de usuario 2618, un adaptador de CA 2620, un módulo de batería 2622, un transceptor USB 2624 y un puerto de Ethernet 2628.

[00120] El UE 220 puede incluir, además, una cámara digital 2630, un controlador de pantalla táctil 2632, un altavoz 2634 y un micrófono 2636. El UE 220 también puede incluir una unidad de gestión de energía 2638. Uno o más buses de comunicación interna (no se muestran) pueden acoplar de forma comunicativa uno o más de los componentes del UE 220.

[00121] La FIGURA 25 ilustra un diagrama de bloques esquemático de una modalidad de un ejemplo de nodo de AMF. El nodo de AMF puede integrarse con otros nodos en la red principal 5G. Pueden incluirse componentes y funciones adicionales o alternativos dentro del nodo de AMF. Además, es posible que una o más de las funciones y los componentes que se muestran en la presente no estén presentes o se combinen con otros componentes, funciones o nodos. El nodo de AMF incluye un dispositivo de procesamiento 2700 y un dispositivo de memoria 2702 que se configuran para realizar una o más de las funciones descritas en la presente. El nodo de AMF puede incluir una interfaz de red 2704 que incluye puertos para interactuar con otros nodos de red en la red 5GC.

[00122] La FIGURA 26 ilustra un diagrama de bloques esquemático de una modalidad de un ejemplo de N3IWF. La N3IWF puede ser un punto de acceso en una red de área local inalámbrica, una puerta de enlace en una red de área local, etc. La N3IWF puede integrarse con otros nodos en una red de acceso. Pueden incluirse componentes y funciones adicionales o alternativos dentro de la N3IWF. Además, es posible que una o más de las funciones y los componentes que se muestran en la presente no estén presentes o se combinen con otros componentes o funciones. La N3IWF incluye un dispositivo de procesamiento 2800 y un dispositivo de memoria 2802 que se configuran para realizar una o más de las funciones descritas en la presente. La N3IWF puede incluir una primera interfaz de red 2804 (por

ejemplo, puertos de Ethernet, puertos IP) para interactuar con otros nodos de red en la red 5GC. La N3IWF también puede incluir uno o más de otros tipos de interfaces para comunicarse con el UE, tal como un transceptor de WLAN 2806 (por ejemplo, redes de tipo WLAN compatibles con IEEE 802.1x). La N3IWF también puede incluir un transceptor de RF móvil 2808 compatible con una interfaz aérea celular. El UE 220 puede comunicarse con la N3IWF mediante el uso de uno o más del transceptor de WLAN 2806 o el transceptor de RF móvil 2808.

[00123] Un dispositivo de procesamiento, tal como se describe en la presente, incluye al menos un dispositivo de procesamiento, tal como un microprocesador, un microcontrolador, un procesador de señales digitales, una microcomputadora, una unidad central de procesamiento, una matriz de puertas programables en campo, un dispositivo lógico programable, una máquina de estado, circuitos lógicos, circuitos analógicos, circuitos digitales y/o cualquier dispositivo que manipule señales (analógicas y/o digitales) en base a la codificación rígida de los circuitos y/o a instrucciones operativas. Un dispositivo de memoria es un dispositivo de memoria no transitorio y puede ser una memoria interna o una memoria externa, y la memoria puede ser un solo dispositivo de memoria o múltiples dispositivos de memoria. El dispositivo de memoria puede ser una memoria de solo lectura, memoria de acceso aleatorio, memoria volátil, memoria no volátil, memoria estática, memoria dinámica, memoria flash, memoria caché y/o cualquier dispositivo de memoria no transitorio que almacene información digital. El término «módulo» se usa en la descripción de una o más de las modalidades de los elementos de la presente. Un módulo incluye uno o más dispositivos de procesamiento y/o uno o más dispositivos de memoria no transitorios que se pueden utilizar para realizar una o más funciones, tal como se describe en la presente. Un módulo puede funcionar de forma independiente y/o junto con otros módulos y puede utilizar el dispositivo de procesamiento y/o la memoria de otros módulos y/o las instrucciones operativas de otros módulos. Como también se usa en la presente, un módulo puede contener uno o más submódulos, cada uno de los cuales puede ser uno o más módulos.

[00124] Como pueden usarse en la presente, los términos «que funciona para» o «que se configura para» indican que un elemento incluye uno o más de los circuitos, las instrucciones, los módulos, los datos, las entradas, las salidas, etc., para realizar una o más de las funciones correspondientes descritas o necesarias, y pueden incluir, además, el acoplamiento inferido a uno o más elementos adicionales para realizar las funciones correspondientes descritas o necesarias. Como también pueden usarse en la presente, los términos «acoplado/a», «acoplado/a a», «conectado/a a» y/o «que se conecta» o «que se interconecta» incluyen una conexión o un enlace directo entre nodos/dispositivos y/o una conexión indirecta entre nodos/dispositivos a través de un elemento intermedio (por ejemplo, un elemento incluye, de modo no taxativo, un componente, elemento, circuito, módulo, nodo, dispositivo, elemento de

red, etc.). Como pueden usarse, además, en la presente, las conexiones inferidas (es decir, cuando un elemento se conecta a otro elemento mediante inferencia) incluyen una conexión directa e indirecta entre dos elementos de la misma manera que «conectado/a a».

[00125] Cabe destacar que los aspectos de la presente descripción pueden describirse en

5 la presente como un proceso que se representa como un esquema, un esquema de flujo, un diagrama de flujo, un diagrama de estructura o un diagrama de bloques. Si bien un diagrama de flujo puede describir las operaciones como un proceso secuencial, muchas de las operaciones se pueden realizar en paralelo o al mismo tiempo. Además, el orden de las operaciones puede reorganizarse. Un proceso finaliza cuando se completan sus operaciones.
10 Un proceso puede corresponder a un método, una función, un procedimiento, una subrutina, un subprograma, etc. Cuando un proceso corresponde a una función, su terminación corresponde a un retorno de la función a la función de llamada o la función principal.

[00126] Las diversas características de la descripción que se describe en la presente pueden implementarse en diferentes sistemas y dispositivos sin apartarse de la descripción.

15 Cabe señalar que los aspectos anteriores de la descripción son meramente ejemplos y no deben interpretarse como limitantes de la descripción. Se pretende que la descripción de los aspectos de la presente descripción sea ilustrativa y no limite el alcance de las reivindicaciones. De esta forma, lo que se indica en la presente puede aplicarse fácilmente a otros tipos de aparatos, y muchas alternativas, modificaciones y variaciones resultarán
20 evidentes para los expertos en la técnica.

[00127] En la memoria descriptiva anterior, se han descrito ciertos aspectos representativos de la invención con respecto a ejemplos específicos. Sin embargo, pueden realizarse diversas modificaciones y cambios sin apartarse del alcance de la presente invención como se establece en las reivindicaciones. La memoria descriptiva y las figuras son
25 ilustrativas, en lugar de restrictivas, y se pretende que el alcance de la presente invención incluya sus modificaciones. Por consiguiente, el alcance de la invención debería estar determinado por las reivindicaciones y sus equivalentes legales, en lugar de simplemente por los ejemplos descritos. Por ejemplo, los componentes y/o elementos enumerados en cualquier reivindicación de un aparato pueden ensamblarse o configurarse operativamente de otro
30 modo en una variedad de permutaciones y, por consiguiente, no están limitados a la configuración específica mencionada en las reivindicaciones.

[00128] Además, se han descrito anteriormente ciertos beneficios, otras ventajas y soluciones a problemas con respecto a modalidades particulares; sin embargo, cualquier beneficio, ventaja, solución a un problema o cualquier elemento que produzca cualquier
35 beneficio, ventaja o solución particulares, o que los vuelva más pronunciados, no deben interpretarse como características o componentes cruciales, necesarios o esenciales de cualquiera o todas las reivindicaciones.

[00129] Tal como se usan en la presente, se pretende que los términos «comprenden», «comprende», «que comprende», «que tiene», «que incluye», «incluye», o cualquier variación de estos, hagan referencia a una inclusión no exclusiva, de modo que un proceso, método, artículo, composición o aparato que comprenda una lista de elementos no incluya únicamente los elementos enumerados, sino que pueda incluir también otros elementos que no se enumeren de forma expresa o que sean inherentes a dicho proceso, método, artículo, composición o aparato. Otras combinaciones y/o modificaciones de las estructuras, disposiciones, aplicaciones, proporciones, elementos, materiales o componentes que se describieron anteriormente, que se utilizan en la práctica de la presente invención, además de los que no se mencionan específicamente, pueden variar o adaptarse particularmente de otro modo a entornos, especificaciones de fabricación, parámetros de diseño u otros requisitos operativos específicos, sin apartarse de sus principios generales.

[00130] Además, no se pretende que la referencia a un elemento en singular signifique «uno/a solo/a», a menos que se indique específicamente, sino «uno/a o más». A menos que se indique específicamente lo contrario, el término «alguno/as» se refiere a uno/a o más. Todos los equivalentes estructurales y funcionales de los elementos de los diversos aspectos que se describen a lo largo de la presente descripción, que los expertos en la técnica conocen actualmente, o conozcan en el futuro, se incorporan expresamente a la presente mediante referencia, y se pretenden que queden comprendidos en las reivindicaciones. Además, no se pretende que nada de lo descrito en la presente esté dirigido al público, independientemente de que dicha divulgación esté explícitamente mencionada en las reivindicaciones. No se pretende que ningún elemento en las reivindicaciones se interprete según las disposiciones de 35 USC §112 (f) como un elemento del tipo de «medio más función», a menos que el elemento se mencione expresamente mediante el uso de la expresión «medio para» o, en el caso de una reivindicación de método, que el elemento se mencione mediante el uso de la expresión «etapa para».

REIVINDICACIONES

1. Equipo de usuario (UE), que comprende:
uno o más transceptores configurados para acceder a una red de servicio a través de múltiples
5 tipos de redes de acceso;
un dispositivo de memoria configurado para almacenar una tabla de mapeo; y
un dispositivo de procesamiento configurado para:
generar una solicitud de registro en la red de servicio a través de una primera red de acceso,
en donde la solicitud incluye un primer tipo de red de acceso de la primera red de acceso;
10 recibir una respuesta que indique que la red de servicio acepta el establecimiento de la
conexión NAS, en donde la respuesta incluye el primer tipo de red de acceso y el identificador
de conexión NAS; y
actualizar la tabla de mapeo para incluir el primer tipo de red de acceso y el identificador de
conexión NAS.
- 15 2. El UE de la reivindicación 1, en donde el primer tipo de red de acceso incluye un valor
que indica al menos uno de: acceso 3GPP, acceso no 3GPP no confiable, acceso no 3GPP
confiable, acceso WLAN no confiable, acceso WLAN confiable o acceso MuLteFire.
3. El UE de la reivindicación 2, en donde el dispositivo de procesamiento se configura,
además, para:
20 actualizar la tabla de mapeo para incluir el primer tipo de red de acceso, identificador de
conexión NAS, identificador de red de acceso e identificador de red de servicio.
4. El UE de la reivindicación 3, en donde el dispositivo de procesamiento se configura,
además, para:
generar una segunda solicitud de registro en la red de servicio a través de una segunda red
25 de acceso con un segundo tipo de red de acceso, en donde la segunda solicitud incluye el
segundo tipo de red de acceso de la segunda red de acceso;
recibir una respuesta que indique que la red de servicio acepta el establecimiento de la
conexión, en donde la respuesta incluye el segundo tipo de red de acceso y un segundo
identificador de conexión NAS; y
30 actualizar la tabla de mapeo para incluir el segundo tipo de red de acceso y el segundo
identificador de conexión NAS.
5. El UE de la reivindicación 4, en donde el segundo tipo de red de acceso es diferente
al primer tipo de red de acceso, y en donde el segundo tipo de red de acceso indica un
segundo: acceso 3GPP, acceso no 3GPP no confiable, acceso no 3GPP confiable, acceso
35 WLAN no confiable, acceso WLAN confiable o acceso MuLteFire diferente.
6. El UE de la reivindicación 5, en donde el dispositivo de procesamiento se configura,
además, para:

generar una tercera solicitud de registro en la red de servicio a través de una tercera red de acceso con un tercer tipo de red de acceso, en donde la tercera solicitud incluye el tercer tipo de red de acceso de la tercera red de acceso;

recibir una respuesta que indique que la red de servicio acepta el establecimiento de la conexión, en donde la respuesta incluye el tercer tipo de red de acceso y un tercer identificador de conexión NAS; y

actualizar la tabla de mapeo para incluir el tercer tipo de red de acceso y el tercer identificador de conexión NAS.

7. El UE de la reivindicación 6, en donde el tercer tipo de red de acceso es diferente al primer y el segundo tipo de red de acceso, y en donde el tercer tipo de red de acceso indica un tercer: acceso 3GPP, acceso no 3GPP no confiable, acceso no 3GPP confiable, acceso WLAN no confiable, acceso WLAN confiable o acceso MuLteFire diferente.

8. El UE de la reivindicación 7, en donde el dispositivo de procesamiento se configura, además, para:

utilizar el contexto de seguridad NAS existente establecido en la primera red de acceso con la red de servicio.

9. El UE de la reivindicación 7, en donde el dispositivo de procesamiento se configura, además, para:

recibir una solicitud para realizar la autenticación para la conexión a través de la tercera red de acceso;

obtener un nuevo contexto de seguridad NAS de la red de servicio a través de la tercera red de acceso;

establecer la conexión NAS mediante el uso del nuevo contexto de seguridad NAS a través de la tercera red de acceso;

activar el nuevo contexto de seguridad NAS para la primera y la segunda red de acceso; y eliminar el contexto de seguridad NAS anterior.

10. Equipo de usuario (UE), que comprende:

uno o más transceptores configurados para acceder a una red de servicio a través de múltiples tipos de redes de acceso;

un dispositivo de procesamiento configurado para:

generar una solicitud de registro en la red de servicio a través de una red de acceso; y

recibir un mensaje de rechazo de registro, en donde el mensaje de rechazo de registro indica que la red de servicio no está autorizada.

11. El UE de la reivindicación 10, en donde el mensaje de rechazo de registro incluye un elemento de información de causa, en donde el elemento de información de causa incluye un valor correspondiente a «Red de servicio no autorizada».

12. El UE de la reivindicación 10, en donde el dispositivo de procesamiento se configura,

además, para:

cancelar el registro con la red de servicio;

almacenar una identidad de la red de servicio en una lista de redes de servicio no autorizadas [la «lista de PLMN prohibidas»].

5 13. El UE de la reivindicación 12, en donde el dispositivo de procesamiento se configura, además, para seleccionar otra red de servicio para el registro.

14. Una función del servidor de autenticación en un nodo de una red principal, que comprende:

10 un transceptor configurado para comunicarse con uno o más nodos adicionales en la red principal;

un dispositivo de procesamiento configurado para:

recibir una solicitud de autenticación para un UE que solicita acceso a una red de servicio, en donde la solicitud de autenticación incluye un identificador de la red de servicio y una identidad de suscriptor; y

15 determinar que la red de servicio no está autorizada; y

generar una respuesta de autenticación, en donde la respuesta de autenticación indica que la red de servicio no está autorizada.

15. La función del servidor de autenticación en el nodo de la red principal de la reivindicación 14, en donde la respuesta de autenticación incluye un elemento de información de causa, en donde el elemento de información de causa incluye un valor correspondiente a «Red de servicio no autorizada».

16. Un UE, que comprende:

un transceptor configurado para comunicarse con uno o más tipos de redes de acceso;

un dispositivo de procesamiento configurado para generar un SUCI mediante:

25 la determinación de uno de múltiples formatos SUPI;

la determinación de uno de múltiples tipos de identidad para un identificador de suscriptor;

la determinación de una salida de esquema del identificador de suscriptor mediante el uso de un esquema de protección; y

30 la construcción del SUCI, que incluye un valor de formato SUPI, un valor del tipo de identidad y la salida del esquema.

17. El UE de la reivindicación 16, en donde uno de los múltiples tipos de identidad para el identificador de suscriptor incluye uno de: SUCI, 5G-GUTI, IMEI, 5G-S-TMSI, IMEISV, dirección MAC o una identidad de dispositivo.

18. El UE de la reivindicación 16, en donde uno de los múltiples formatos SUPI incluye al menos uno de: IMSI, NAI basado en IMSI, NAI no basado en IMSI o MF-NAI.

19. El UE de la reivindicación 16, en donde el dispositivo de procesamiento se configura, además, para generar el SUCI mediante la selección de uno de múltiples tipos de red y la

inclusión de un indicador del tipo de red para el tipo de red seleccionado en la estructura SUCI.

RESUMEN

Esta solicitud se refiere al establecimiento de sesiones por parte del equipo de usuario en múltiples redes de acceso heterogéneas. En un aspecto, las redes de acceso heterogéneas pueden incluir redes de acceso 3GPP y no 3GPP (106). Las redes de acceso no 3GPP (106) 5 pueden incluir una o más redes de acceso confiables no 3GPP (108) o una o más redes de acceso no confiables no 3GPP (110).