MANEJO DE FALLOS DE ACCESO NO 3GPP A UNA 5GCN NO PERMITIDO

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

[0001] La presente solicitud reivindica la prioridad según 35 USC §119 de la solicitud provisional estadounidense n.º 62/692.722 titulada, “Method and Apparatus For Handling Authentication Failure During Security Association Establishment” «Método y aparato para manejar fallos de autenticación durante el establecimiento de asociaciones de seguridad», presentada el 30 de junio de 2018, e incorporada expresamente a la presente mediante esta referencia.

CAMPO TÉCNICO

[0002] Esta solicitud se refiere, en general, a redes de acceso y, más específicamente, al establecimiento de sesiones por parte del equipo de usuario en una red de acceso cuando no se acepta el establecimiento de asociaciones de seguridad.

DESCRIPCIÓN DE LA TÉCNICA RELACIONADA

[0003] Las declaraciones en esta sección proporcionan una descripción de la técnica relacionada y no constituyen admisiones de técnica previa. Los equipos de usuario (UE, por sus siglas en inglés), como teléfonos inteligentes, tabletas inteligentes, computadoras portátiles, computadoras, relojes inteligentes, etc., a menudo incluyen capacidad de conectividad de red de área local inalámbrica (WLAN, por sus siglas en inglés) (como conectividad WLAN conforme al IEEE 802.11x) y conectividad de red de acceso por radio (como tecnologías total o parcialmente conforme al conjunto de estándares del proyecto de asociación de 3.ª generación (3GPP, por sus siglas en inglés), incluidos EVDO, UMTS, HSPA y LTE). Por tanto, el UE puede conectarse a la red de núcleo de paquetes evolucionado (EPC, por sus siglas en inglés) 3GPP utilizando dos tipos de tecnologías de acceso compuestas por redes de acceso 3GPP y redes de acceso no 3GPP.

[0004] En general, las redes de acceso 3GPP son total o parcialmente conformes a 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 son total o parcialmente conforme a tecnologías que no están especificadas en el conjunto de estándares del 3GPP. Estas incluyen tecnologías como cdma2000, WLAN

(como WLAN conforme al IEEE 802.11x) o redes fijas.

[0005] 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 acceso de femtoceldas). Las redes de acceso confiables incluyen redes de acceso que el operador de la red considera que tienen un nivel de confianza desde el punto de vista de la seguridad y que pueden interactuar directamente con la red de EPC.

[0006] En el nuevo conjunto de estándares 5G, una red de acceso no 3GPP (N3AN, por su siglas en inglés) se trata como una red de acceso 5G y parte del sistema 5G (5GS, por sus siglas en inglés). Para el acceso de no 3GPP no confiables, una función de interfuncionamiento no 3GPP (N3IWF, por sus siglas en inglés) proporciona la terminación de las interfaces de señalización para el plano de control y el plano de usuario, respectivamente, al igual que un nodo NG-RAN. Por lo tanto, los UE con capacidad 5G pueden acceder a la red central 5G (5GCN, por sus siglas en inglés) conectándose a una red de acceso no 3GPP, como una red de acceso 5G a través de la N3IWF. La N3IWF transmite la señalización del plano de control de enlace ascendente y enlace descendente entre el UE y la 5GCN. Además, la N3IWF proporciona una conexión de plano de usuario entre el UE y la 5GCN para sesiones en redes de acceso no 3GPP.

[0007] Actualmente, los procedimientos de señalización entre el UE y la N3IWF se especifican cuando la red acepta determinado establecimiento de autenticación de seguridad. Sin embargo, no hay ningún método disponible para manejar el caso en el que la red no acepta el establecimiento de la asociación de seguridad. De manera similar, para las conexiones en el plano de usuario, es necesario especificar un método para manejar el caso en el que la red no acepta el establecimiento de la asociación de seguridad con el plano de usuario.

[0008] Por lo tanto, existe la necesidad de proporcionar un sistema y un método que admitan en el manejo de fallos durante el establecimiento de asociaciones de seguridad para el acceso a la 5GCN a través de redes de acceso no 3GPP. También se

proporcionan otras necesidades y beneficios con las modalidades descritas en el presente documento.

COMPENDIO

[0009] A continuación, se presenta un resumen de la materia descrita, para proporcionar una comprensión básica de algunos aspectos de la materia descrita. Este resumen no es una descripción general exhaustiva de la materia descrita. No se pretende identificar elementos clave o críticos de la materia descrita ni delimitar el alcance de la materia descrita. Su único fin es presentar algunos conceptos de forma simplificada, como preludio de la descripción más detallada que se menciona más adelante.

[0010] En un aspecto, un nodo de función de interfuncionamiento para manejar una conexión de red a través de una red de acceso no confiable a una red central incluye una primera interfaz de red configurada para comunicarse con el equipo de usuario (UE) a través de la red de acceso no confiable y una segunda interfaz de red configurada para comunicarse con uno o más nodos en la red central. El nodo de función de interfuncionamiento incluye un dispositivo de procesamiento configurado para procesar una solicitud de establecimiento de conexión a la red central desde el UE en la red de acceso no confiable y generar una solicitud a la red central; determinar que la red central no acepta el establecimiento de la conexión; y generar un mensaje de respuesta al UE, en el que el mensaje de respuesta incluye un error que indica que la red central no permite el establecimiento de la conexión a través de la red de acceso no confiable.

[0011] En otro aspecto, una función de gestión de acceso y movilidad (AMF, por sus siglas en inglés) para manejar una solicitud de conexión a la red del nodo de función de interfuncionamiento incluye una interfaz de red configurada para comunicarse con un nodo de función de interfuncionamiento y una función de autenticación en una red central. La AMF también incluye un dispositivo de procesamiento configurado para procesar una solicitud de autenticación y establecimiento de conexión segura para un UE a través de una red de acceso no confiable, generar una solicitud de verificación de suscripción y autenticación para una función de servidor de autenticación (AUSF, por sus siglas en inglés), determinar que una respuesta a la verificación de suscripción y

autenticación indica un fallo de autenticación, y generar un mensaje de respuesta a la autenticación y el establecimiento de conexión segura que incluya en el mensaje de respuesta un valor de causa que indique que no se permite el acceso a la red central a través de la red de acceso no confiable.

[0012] En otro aspecto, el equipo de usuario (UE) incluye una interfaz de red configurada para comunicarse con un nodo de función de interfuncionamiento través de una red de acceso no confiable. El UE incluye un dispositivo de procesamiento configurado para generar una solicitud de registro para el establecimiento de una sesión segura con una red central, procesar un mensaje de respuesta del nodo de función de interfuncionamiento, y determinar, a partir del mensaje de respuesta que la red central no permite el establecimiento de la conexión a través de la red de acceso no confiable.

[0013] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el nodo de función de interfuncionamiento está configurado para recibir una solicitud de autenticación y establecimiento de conexión segura del UE a través de la red de acceso no confiable, generar una solicitud de verificación de suscripción y autenticación y transmitir la solicitud de verificación de suscripción y autenticación a través de la segunda interfaz a la función de gestión de acceso y movilidad (AMF), recibir una respuesta a la verificación de suscripción y autenticación de la AMF, y generar un mensaje de respuesta de intercambio de claves de internet (IKE, por sus siglas en inglés) para el UE con una carga útil de NAS que incluya el error que indique que la red central no permite el establecimiento de la conexión a través de la red de acceso no confiable.

[0014] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el nodo de función de interfuncionamiento está configurado para recibir una respuesta de la función de gestión de acceso y movilidad que encapsule un mensaje de rechazo de registro que incluya un valor de causa de 5GMM que indique que no se permite el acceso no 3GPP a la 5GCN y generar un mensaje de respuesta al intercambio de claves de internet (IKE) con la carga útil que incluya un tipo de mensaje que indique que la red central no acepta el establecimiento de la conexión.

[0015] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el nodo de función de interfuncionamiento está configurado para generar el mensaje de

respuesta al intercambio de claves de internet (IKE) con una carga útil de notificación que incluya un tipo de mensaje de notificación privado que indique el motivo del fallo.

[0016] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el nodo de función de interfuncionamiento está configurado para generar el mensaje de respuesta al IKE generando el mensaje de respuesta al IKE con una carga útil de notificación que incluya un tipo de mensaje de notificación privado que indique que no se permite el acceso no 3GPP no confiable a la 5GCN.

[0017] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el nodo de función de interfuncionamiento está configurado para transmitir el mensaje de respuesta al UE, donde el mensaje de respuesta indica que la red central no acepta el establecimiento de la conexión; recibir un mensaje de detención del UE; y generar un mensaje de fallo para el UE.

[0018] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el nodo de función de interfuncionamiento está configurado para procesar el mensaje de detención del UE, en el que el mensaje de parada incluye un formato de mensaje de detención de 5G que tiene un campo de identificador de mensaje y en el que el campo de identificador de mensaje incluye un identificador de detención de 5G.

[0019] En uno o más de los aspectos anteriores, la solicitud de establecimiento de conexión del UE en la red de acceso no confiable incluye un mensaje de solicitud de IKE para iniciar una asociación de seguridad (SA, por sus siglas en inlés) IPsec con la red central.

[0020] En uno o más de los aspectos anteriores, la red central es una 5GCN y la red de acceso no confiable es una red de acceso no 3GPP.

[0021] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en la AMF está configurado para encapsular en el mensaje de respuesta un mensaje de rechazo del registro que incluya el valor de causa, en el que el valor de causa incluye un valor de causa de 5GMM que indica que no se permite el acceso no 3GPP a la 5GCN.

[0022] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en la AMF está configurado para generar una indicación de fallo del protocolo de autenticación extensible (EAP, por sus siglas en inglés) en el mensaje de respuesta.

[0023] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el equipo de usuario está configurado para generar un mensaje de detención que indique el fin de la solicitud de registro para el establecimiento de la sesión segura con la 5GCN y transmitir el mensaje de detención mediante la red de acceso no 3GPP al nodo de función de interfuncionamiento.

[0024] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el equipo de usuario está configurado para generar el mensaje de detención como un mensaje formateado de respuesta al EAP que incluya un campo de identificador de mensaje establecido como detención de 5G.

[0025] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el equipo de usuario está configurado para procesar un mensaje de fallo del EAP del nodo de función de interfuncionamiento y realizar un procedimiento de eliminación de la asociación de seguridad.

[0026] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el equipo de usuario está configurado para reintentar el registro con la 5GCN generando una segunda solicitud de registro para el establecimiento de una sesión segura con la 5GCN y determinar, a partir de un segundo mensaje de respuesta del nodo de función de interfuncionamiento, el éxito del establecimiento de la conexión a través de la red de acceso no confiable.

[0027] En uno o más de los aspectos anteriores, el dispositivo de procesamiento en el equipo de usuario está configurado para generar la segunda solicitud de registro para el establecimiento de una sesión segura con la 5GCN con parámetros actualizados.

[0028] Se expondrán aspectos adicionales, en parte, en la descripción detallada, las figuras y cualquiera de las reivindicaciones posteriores, y en parte se derivarán de la descripción detallada. Se ha de comprender que tanto la descripción general que antecede como la descripción detallada a continuación tienen únicamente fines ilustrativos y explicativos y que las reivindicaciones no se encuentran limitadas a las modalidades descritas.

BREVE DESCRIPCIÓN DE DIVERSAS VISTAS DE LOS DIBUJOS

[0029] Algunas modalidades del aparato y/o los métodos de acuerdo con modalidades de la divulgación se describen a continuación, solo a modo de ejemplo y

con respecto a los dibujos adjuntos, en los que:

[0030] La figura 1 ilustra un diagrama de bloques esquemático de una modalidad de tipos de redes de acceso.

[0031] La figura 2 ilustra un diagrama de bloques esquemático de una modalidad de una arquitectura de sistema 5G para acceso no 3GPP.

[0032] La figura 3 ilustra un diagrama de flujo lógico que ilustra una modalidad de un método para que un UE se registre en una 5GCN a través de una red de acceso no 3GPP no confiable.

[0033] La figura 4 ilustra un diagrama de flujo lógico de una modalidad de un método para manejar el caso en el que no se acepta el establecimiento de SA de IKE ni SA IPsec de señalización.

[0034] La figura 5 ilustra un diagrama de flujo lógico de una modalidad de un método de un procedimiento de sesión de EAP-5G después de un fallo de autenticación debido a errores recuperables.

[0035] un diagrama de flujo lógico que ilustra una modalidad de un procedimiento de sesión de EAP-5G después de un fallo de autenticación.

[0036] La figura 6 ilustra un diagrama de flujo lógico que ilustra una modalidad de un procedimiento de sesión de EAP-5G de un rechazo de registro debido a fallos de errores irrecuperables.

[0037] La figura 7 ilustra un diagrama de bloques esquemático de una modalidad de un mensaje de respuesta al EAP/detención de 5G.

[0038] La figura 8 ilustra un diagrama de flujo lógico de una modalidad de un método del flujo de mensajes entre funciones de red cuando no se aceptan el establecimiento de SA de IKE ni SA IPsec de señalización para el registro de UE a través de acceso no 3GPP.

[0039] La figura 9 ilustra un diagrama de flujo lógico de una modalidad de un método de flujo de mensajes entre funciones de red cuando no se aceptan la SA de IKE ni el establecimiento de SA IPsec de señalización para el registro de UE a través de acceso no 3GPP, debido a una restricción de suscripción.

[0040] La figura 10 ilustra un diagrama de flujo lógico de una modalidad de un método de flujo de mensajes entre funciones de red cuando no se acepta el

establecimiento de asociación de seguridad IPsec en el plano de usuario.

[0041] La figura 11 ilustra un diagrama de bloques esquemático de una modalidad de un elemento de información de causa de 5GMM 1100.

[0042] La figura 12 ilustra un diagrama de bloques esquemático de una modalidad de valores para el elemento de información de causa de 5GMM.

[0043] La figura 13 ilustra un diagrama de flujo lógico de una modalidad de un método de la N3IWF.

[0044] La figura 14 ilustra un diagrama de flujo lógico de una modalidad de un método de solicitud de registro en una red central a través de una red de acceso no confiable con fallo de autenticación debido a errores recuperables.

[0045] La figura 15 ilustra un diagrama de flujo lógico de una modalidad de un método de solicitud de registro en una red central a través de una red de acceso no confiable con fallo de autenticación debido a errores irrecuperables.

[0046] La figura 16 ilustra un diagrama de bloques esquemático de una modalidad de un ejemplo de equipo de usuario.

[0047] La figura 17 ilustra un diagrama de bloques esquemático de una modalidad de un nodo de AMF.

[0048] La figura 18 ilustra un diagrama de bloques esquemático de una modalidad de N3IWF.

DESCRIPCIÓN DETALLADA

[0049] La descripción y los dibujos simplemente ilustran los principios de varias modalidades. Por tanto, se observará que los expertos en la técnica podrán concebir diversas disposiciones que, aunque no se describen o muestran explícitamente en el presente documento, representan los principios del presente documento y de las reivindicaciones y se encuentran dentro del espíritu y alcance de la divulgación. Además, todos los ejemplos citados en el presente documento están previstos, principalmente, solo con fines pedagógicos, para ayudar al lector a comprender los principios de las modalidades y los conceptos aportados por el inventor para avanzar la técnica y deben no interpretarse como limitados a dichos ejemplos y condiciones mencionados de forma específica. Asimismo, se pretende que todas las declaraciones en el presente documento que mencionan principios, aspectos y modalidades, así como

ejemplos específicos de estos, abarquen sus equivalentes.

[0050] A continuación se amplían algunas de las abreviaturas que se describen en este documento por motivos de conveniencia:

5GC	núcleo de 5G
5GCN	red central de 5G
5GS	sistema 5G
5G-AN	red de acceso a 5G
5GMM	gestión de movilidad del 5GS
5G-GUTI	identificador temporal único global de 5G
5G-S-TMSI	identificador de suscripción móvil temporal S de 5G
5QI	Identificador de QoS de 5G
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 internacional de equipo móvil
IPsec	seguridad del protocolo de internet
MCM	modo de conexión múltiple
N3IWF	función de interfuncionamiento no 3GPP
NAS	estrato sin acceso
PDN	red de paquetes de datos
PLMN	red móvil terrestre pública
QoS	calidad de servicio
SA	asociación de seguridad
SCM	modo de conexión única
UDM	gestión de datos unificada
UE	equipo de usuario
UICC	tarjeta de circuito integrado universal
USIM	identidad de suscriptor móvil en el UMTS

[0051] En el presente documento se describen una o más modalidades que proporcionan un sistema y 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.

[0052] La figura 1 ilustra un diagrama de bloques esquemático de una modalidad de tipos de redes de acceso para una red central 5G (5GCN) 100 total o parcialmente conforme al conjunto de estándares del Proyecto de Asociación de 3.ª Generación (3GPP) para el sistema 5G, como la especificación técnica (TS, por sus siglas en inglés) 23.501 «Arquitectura del sistema para el sistema 5G»; la especificación técnica (TS) 23.502 define los procedimientos para el sistema 5G y la especificación técnica (TS) 23.503 define la política y el marco de control de carga para el sistema 5G.

[0053] La 5GCN 100 está acoplada comunicativamente 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 son total o parcialmente conforme a 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 son total o parcialmente conformes a 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.

[0054] Las redes de acceso no 3GPP confiables 108 son redes de área local inalámbrica (WLAN) creadas por el operador o admitidas por el operador, como una red WLAN conforme al 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 requiera cifrado de la red de acceso por radio (RAN), acceso a la red basado en el 3GPP usando el 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, como una red WLAN conforme al IEEE 802.11x que esté abierta al público, una WLAN doméstica u otra que no sea creada y administrada por un operador.

[0055] 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 más detalle en el estándar técnico TS del 3GPP 23.501, versión 15 (diciembre de 2017), titulado «Arquitectura del sistema para el sistema 5G», que se incorpora en el presente documento mediante esta referencia.

[0056] Las redes de acceso no 3GPP se conectan a la 5GCN 100 a través de una función de interfuncionamiento no 3GPP (N3IWF). La N3IWF 204 interconecta las funciones en el plano de control (CP, por sus siglas en inglés) y el plano de usuario (UP, por sus siglas en inglés) de la 5GCN 100 a través de las interfaces N2 y N3, respectivamente. Un UE 200 establece un túnel de seguridad IP (IPSec) con la N3IWF 204, para conectarse a la 5GCN 100 a través de la red de acceso no 3GPP no confiable 110. La 5GCN 100 autentica el UE 200 y se conecta a este durante el procedimiento de establecimiento del túnel IPSec. En el TS 23.502 del 3GPP, versión 15 (diciembre de 2017), titulado «Procedimientos para el sistema 5G», que se incorpora al presente documento mediante esta referencia, se describen más detalles para la conexión del UE 200 a la 5GCN 100 a través de un acceso no 3GPP no confiable 110.

[0057] La 5GCN 100 incluye una red móvil terrestre pública doméstica o PLMN doméstica (HPLMN) equivalente, que incluye una función de gestión de acceso y movilidad (AMF) 202. La AMF 202 proporciona la terminación de la interfaz en el plano de control (N2) y la terminación del conjunto de protocolos del NAS (N1), así como la protección de la integridad y el cifrado del NAS. La AMF 202 también proporciona gestión de registro y conexión. La AMF 202 puede incluir varias funcionalidades para admitir redes de acceso no 3GPP 110. Por ejemplo, la AMF 202 puede proporcionar soporte de protocolos de control de interfaz N2 con la N3IWF 204, así como soporte de la señalización de NAS con un UE 200 a través de la N3IWF 204. Además, la AMF 202

puede proporcionar soporte de la autenticación de UE 200 conectados a través de la N3IWF 204 y gestión de la movilidad, la autenticación y el o los estados de contexto de seguridad separados de un UE 200 conectado a través del acceso no 3GPP o conectado a través de accesos 3GPP y no 3GPP simultáneamente. El estrato sin acceso (NAS) es un conjunto de protocolos en los estándares 5G. El NAS (estrato sin acceso) 5G incluye procedimientos relacionados con 5GMM (gestión de movilidad del 5GS) y 5GSM (gestión de sesiones 5G) en el 5GS (sistema 5G). El NAS se utiliza para transmitir la señalización de control entre el equipo de usuario (UE) y las funciones de la 5GCN. Una versión del protocolo de NAS 5G se define en el TS 24.501 del 3GPP: «Protocolo de estrato de acceso (NAS) para el sistema 5G (5GS)», versión 1.1, del 9 de mayo de 2018, que se incorpora en el presente documento mediante esta referencia.

[0058] La función de gestión de sesiones (SMF) 206 incluye la funcionalidad de gestión de sesiones, por ejemplo, establecimiento, modificación y liberación de sesiones, incluido el mantenimiento del túnel entre la UPF 208 y el nodo de la AN. La SMF 206 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).

[0059] La función del plano de usuario (UPF, por sus siglas en inésgl) 208 proporciona un punto de sesión de PDU externo de interconexión a la red de datos y al enrutamiento y reenvío de paquetes. La UPF 208 también admite la parte del plano de usuario del cumplimiento de las normas de la política, por ejemplo, activación, redirección, dirección del tráfico, etc.

[0060] La función de control de políticas (PCF, por sus siglas en inglés) 214 admite marco de políticas unificado para regir el comportamiento de la red. La gestión de datos unificada (UDM) 212 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 gestión de suscripciones y SMS. Para proporcionar esta funcionalidad, la UDM 212 utiliza datos de suscripción (incluidos datos de autenticación) que pueden almacenarse en el UDR. Otro

módulo proporciona la función de servidor de autenticación (AUSF) 210.

[0061] La funcionalidad de la N3IWF 204 en caso de acceso no 3GPP no confiable 110 incluye el soporte del establecimiento de un túnel IPsec con el UE 200. La N3IWF 204 termina los protocolos de IKEv2/IPsec con el UE 200 a través de una interfaz NWu y transmite, a través de una interfaz N2, la información necesaria para autenticar el UE 200 y autorizar su acceso a la 5GCN 100. La N3IWF 204 proporciona la terminación de las interfaces N2 y N3 con la 5GCN 100 para el plano de control y el plano de usuario, respectivamente. La N3IWF 204 transmite la señalización del NAS del plano de control (N1) de enlace ascendente y enlace descendente entre el UE 200 y la AMF 202. La N3IWF 204 proporciona el manejo de la señalización de N2 de la SMF 206 (transmitida por la AMF 202) relacionada con sesiones de PDU y QoS. La N3IWF 204 además proporciona el establecimiento de una asociación de seguridad IPsec (SA IPsec) para brindarle soporte al tráfico de la sesión de PDU. La N3IWF 204 también proporciona la transmisión de paquetes en el plano de usuario de enlace ascendente y descendente entre el UE 200 y la UPF 208.

[0062] La figura 3 ilustra un diagrama de flujo lógico que ilustra una modalidad de un método para que un UE 200 se registre en una 5GCN 100 a través de un acceso no 3GPP no confiable 110. El método incluye un protocolo de autenticación extensible (EAP) específico del proveedor llamado «EAP-5G». El EAP se define en el RFC de IETF 3748: «Protocolo de autenticación extensible (EAP)», con fecha de junio de 2004. El EAP-5G es un EAP específico del proveedor para 5GS (EAP-5G) que se usa para encapsular mensajes de NAS entre el UE 200 y la N3IWF 204. Los paquetes de EAP-5G utilizan el tipo de EAP «expandido» y el Id. del proveedor del 3GPP existente, registrado ante la IANA en el registro del Código de empresas privadas de SMI (es decir, 10415). En una modalidad, el EAP-5G se utiliza solo para encapsular mensajes de NAS (no para autenticación).

[0063] Si se necesita auteticar el UE 200, se ejecuta una autenticación mutua de EAP-AKA' entre el UE 200 y la AUSF 210, como se describe a continuación. En los procedimientos de registro y de registro subsiguiente a través de redes de acceso no 3GPP no confiables 110, se intercambian mensajes de NAS entre el UE 200 y la AMF 202.

[0064] En el paso 1, el UE 200 se conecta a una red de acceso no 3GPP no confiable 110 con procedimientos fuera del alcance del 3GPP (tal como se especifica en los protocolos de WLAN del IEEE 802.11) y se le asigna una dirección IP. Se puede utilizar cualquier método de autenticación no 3GPP, por ejemplo, sin autenticación (en el caso de una WLAN gratuita), el protocolo de autenticación extensible (EAP) con clave, nombre de usuario/contraseña, etc. previamente compartidos. Cuando el UE 200 decide conectarse a la 5GCN 100, el UE 200 selecciona una N3IWF 204 en una PLMN 5G.

[0065] En el paso 2, el UE 200 procede con el establecimiento de una asociación de seguridad (SA) IPsec con la N3IWF 204 seleccionada iniciando un intercambio inicial de protocolo de intercambio de claves de internet (IKE), por ejemplo, como se describe en el RFC de IETF 7296, «Protocolo de intercambio de claves de internet, versión 2 (IKEv2)» (octubre de 2014). Después del paso 2, los mensajes de IKE subsiguientes se cifran y se protege la integridad mediante el uso de la SA de IKE establecida en este paso.

[0066] En el paso 3, el UE 200 iniciará un intercambio de IKE_AUT enviando un mensaje de solicitud de IKE_AUT. La carga útil AUT no se incluye en el mensaje de solicitud de IKE_AUT, que indica que el intercambio de IKE_AUT utiliza protocolos de señalización del protocolo de autenticación extensible (EAP), por ejemplo, señalización de EAP-5G (como EAP-AKA' descrito en el RFC de IETF 5448, «Método de protocolo de autenticación extensible mejorado para el acuerdo de claves y autenticación de 3.ª generación (EAP-AKA', por sus siglas en inglés) del 5 de marzo de 2018 e incorporado mediante esta referencia en este documento).

[0067] En el paso 4, la N3IWF 204 responde con un mensaje de respuesta a IKE_AUT que incluye un paquete de solicitud de EAP/inicio de 5G. El paquete de solicitud de EAP/inicio de 5G le informa al UE 200 que inicie una sesión de EAP-5G, es decir, que comience a enviar mensajes de NAS encapsulados dentro de paquetes de EAP-5G.

[0068] En el paso 5, el UE 200 genera y transmite una solicitud de registro para la 5GCN 100, por ejemplo, una solicitud de IKE_AUT que incluya un paquete de respuesta al EAP/NAS de 5G que incluya los parámetros de red de acceso (Param. AN) y un

mensaje de solicitud de registro de NAS. De esta forma, el UE reconoce el inicio de la sesión de EAP-5G enviando el paquete de respuesta al EAP/NAS de 5G que incluye, por ejemplo: a) un campo de NAS-PDU que contiene un mensaje de NAS, por ejemplo, un mensaje de SOLICITUD DE REGISTRO; y b) un campo de parámetros de AN que contiene los parámetros de la red de acceso, tales como la SUPI o el GUTI de 5G, la red seleccionada y la S-NSSAI, etc. (ver el TS del 3GPP 23.502). La N3IWF 204 utiliza los parámetros de AN para seleccionar una AMF 202 en la 5GCN 100.

[0069] En el paso 6a, la N3IWF 204 selecciona una AMF 202 en la 5GCN 100 basándose en los parámetros de AN recibidos y la política local. La N3IWF 204 reenvía entonces la solicitud de registro recibida del UE 200 a la AMF 202 seleccionada en el paso 6b. La N3IWF 204, al recibir los mensajes de NAS de la AMF 202, incluye el mensaje de NAS dentro de un mensaje de solicitud de EAP/NAS de 5G al UE 100. El mensaje de solicitud de EAP/NAS de 5G incluye un campo de NAS-PDU que contiene un mensaje de NAS. Otros mensajes de NAS entre el UE 200 y la AMF 202, a través de la N3IWF 204, se insertan en los campos de NAS-PDU de un mensaje de respuesta al EAP/NAS de 5G (del UE a la N3IWF) y mensaje de solicitud de EAP/NAS de 5G (de la N3IWF al UE).

[0070] En los pasos 7a y 7b, la AMF 202 seleccionada puede decidir solicitar la identidad permanente (SUPI) del UE enviando un mensaje de solicitud de identidad de NAS al UE 200 a través de la N3IWF 204. La N3IWF 204 envía este mensaje de NAS y todos los mensajes de NAS subsiguientes al UE 200 encapsulados dentro de los paquetes de EAP/NAS de 5G.

[0071] En el paso 8, la AMF 202 puede decidir autenticar el UE 200. En este caso, la AMF 202 seleccionará una AUSF 210 utilizando la SUPI o la SUPI cifrada del UE 200 y enviará una solicitud de clave a la AUSF 210 seleccionada en el paso 8a. La AUSF 210 puede iniciar una autenticación de EAP-AKA' en el paso 8b, como se especifica en el TS del 3GPP 33.501: «Arquitectura de seguridad y procedimientos para el sistema 5G» (versión 15, 26 de marzo de 2018), que se incorpora en el presente documento mediante esta referencia. Los paquetes de desafío de EAP-AKA' se encapsulan dentro de los mensajes de autenticación de NAS a la N3IWF en el paso 8c y los mensajes de autenticación de NAS se encapsulan dentro de los paquetes de EAP/NAS de 5G en el

paso 8d. El UE 200 genera una respuesta de autenticación al desafío de EAP-AKA en el paso 8e que la N3IWF 204 le reenvía a la AMF en el paso 8f. A continuación, la AUSF 210 recibe la respuesta de autenticación de la AMF en el paso 8g.

[0072] Después de una autenticación exitosa del UE 100, en el paso 8h, la AUSF 210 le envía la clave de anclaje (clave de SEAF) a la AMF 202, que la AMF 202 utiliza para derivar claves de seguridad de NAS y una clave de seguridad para la N3IWF 204 (clave de N3IWF). El UE 200 también deriva la clave de anclaje (clave de SEAF) y, de esa clave, deriva las claves de seguridad de NAS y la clave de seguridad para la N3IWF 204 (clave de N3IWF). El UE 200 y la N3IWF 204 utilizan la clave de N3IWF para establecer la asociación de seguridad IPsec (en el paso 11). La AUSF 210 incluye la SUPI (sin cifrar), si en el paso 8a la AMF 202 le proporcionó a la AUSF 210 una SUPI cifrada.

[0073] En los pasos 9a y 9b, la AMF 202 le envía una solicitud de comando de modo de seguridad (SMC) al UE 200 para activar la seguridad de NAS. Esta solicitud se envía primero a la N3IWF 204 (dentro de un mensaje N2), junto con la clave de N3IWF. Si se ejecutó una autenticación de EAP-AKA' con éxito en el paso 8, entonces en el paso 9a la AMF 202 encapsula el éxito del EAP recibido de la AUSF 210 dentro del mensaje de solicitud de SMC.

[0074] En el paso 10a, el UE 200 completa la autenticación de EAP-AKA' (si se inició en el paso 8) y crea un contexto de seguridad de NAS y una clave de N3IWF. Después de que se crea la clave de N3IWF en el UE 200, el UE 200 solicita la compleción de la sesión de EAP-5G enviando un paquete de respuesta al EAP/finalización de 5G. Esto hace que la N3IWF 204 le envíe un éxito de EAP al UE 200 en el paso 10b, con la suposición de que la N3IWF 204 también haya recibido la clave de N3IWF de la AMF 202. Esto completa la sesión de EAP-5G y no se pueden intercambiar más paquetes de EAP-5G. Si la N3IWF 204 no recibió la clave de N3IWF de la AMF 202, la N3IWF 204 responde con un fallo de EAP.

[0075] En el paso 11, se establece la SA IPsec entre el UE 200 y la N3IWF 204 utilizando la clave de N3IWF común que se creó en el UE 200 y que la N3IWF 204 recibió en el paso 9a. Esta SA IPsec se denomina «SA IPsec de señalización». Después del establecimiento de la SA IPsec de señalización, todos los mensajes de

NAS entre el UE 200 y la N3IWF 204 se intercambian a través de esta SA IPsec. La SA IPsec de señalización se configurará para operar en modo de transporte. El valor de SPI se utiliza para determinar si un paquete de IPsec lleva un mensaje de NAS o no.

[0076] En el paso 12, el UE 200 envía el mensaje de SMC completo a través de la SA IPsec de señalización establecida y todos los mensajes de NAS subsiguientes se intercambian entre el UE 200 y la AMF 202 a través de esta SA IPsec.

[0077] Como se describió anteriormente, el UE 200 y la N3IWF 204 tienen un método definido cuando la 5GCN 100 acepta el establecimiento de SA de IKE y SA IPsec de señalización a través de una red de acceso no 3GPP 110. Sin embargo, no existe un sistema o método disponibles para manejar el caso en el que la 5GCN 100 no acepta el establecimiento de SA de IKE y SA IPsec de señalización. Además, para el plano de usuario, es necesario especificar un sistema y un método para manejar el caso en el que la 5GCN 100 no acepta el establecimiento de SA IPsec en el plano de usuario. En general, es necesario establecer métodos y sistemas para manejar el rechazo del acceso no 3GPP a la 5GCN 100.

Modalidad: mejoras en el proceso y protocolo para manejar el caso en el que la red central 5G no acepta el registro del UE a través de una red de acceso no 3GPP

[0078] La figura 4 ilustra un diagrama de flujo lógico de una modalidad de un método 400 para manejar el caso en el que no se acepta el establecimiento de SA de IKE ni SA IPsec de señalización. En el paso 402, el UE 200 procede con una solicitud para el establecimiento de una asociación de seguridad (SA) IPsec con la N3IWF 204 seleccionada. El UE 200 inicia el establecimiento de la SA IPsec utilizando el protocolo de intercambio de claves de internet (IKE) descrito en el RFC de IETF 7296 «Protocolo de intercambio de claves de internet, versión 2 (IKEv2)» (octubre de 2014). El UE 200 envía un mensaje de solicitud IKE_AUT en el paso 404. En el paso 406, la N3IWF 204 responde con un mensaje de respuesta a IKE_AUT que incluye un paquete de solicitud de EAP/inicio de 5G. El paquete de solicitud de EAP/inicio de 5G le informa al UE 200 que inicie una sesión de EAP-5G, es decir, que comience a enviar mensajes de NAS encapsulados dentro de paquetes de EAP-5G.

[0079] En el paso 408, el UE 200 genera una solicitud de registro para la 5GCN 100,

por ejemplo, una solicitud de IKE_AUT que incluya un paquete de respuesta al EAP/NAS de 5G que incluya los parámetros de red de acceso (Param. AN) y un mensaje de solicitud de registro de NAS. Los param. AN contienen información (por ejemplo, la SUPI o el GUTI 5G, la red seleccionada y NSSAI) que utiliza la N3IWF 204 para seleccionar una AMF 202 en la 5GCN 100.

[0080] En algunos casos, se rechaza el registro del UE a través de un acceso no 3GPP, por ejemplo, debido a un fallo de autenticación como, por ejemplo, el fracaso de la autenticación de EAP-AKA'. Entonces, la 5GCN 100 no acepta el establecimiento de la SA de IKE y SA IPsec de señalización. En una modalidad, la AMF 202 genera un mensaje RECHAZO DE REGISTRO y la N3IWF 204 le envía un mensaje de respuesta al EAP/NAS de 5G al UE que incluye un campo de NAS-PDU que contiene el mensaje RECHAZO DE REGISTRO en el paso 410.

[0081] Al recibir el mensaje de rechazo de registro, el UE 200 finaliza la solicitud de registro generando y enviando un mensaje de respuesta al EAP/detención de 5G (encapsulado en una solicitud de IKE_Aut) en el paso 412. El UE 200 recibe de la N3IWF 204 una respuesta de IKE_AUT con un mensaje de fallo del EAP en el paso 414. Al recibir el mensaje de fallo del EAP de la N3IWF 204, el UE 200 realiza el procedimiento de eliminación de la SA de IKEv2. El UE 200 no reinicia los establecimientos de SA de IKE y SA IPsec de señalización con una N3IWF 204 desde la misma PLMN hasta apagarse o hasta que se elimine la UICC que contiene el USIM.

[0082] Cuando se rechaza el registro del UE 200 a través de la red de acceso no 3GPP 110, la AMF 202 le transmite un mensaje RECHAZO DE REGISTRO a la N3IWF 204. En respuesta, la N3IWF 204 le transmite un mensaje de respuesta al EAP/NAS de 5G al UE 200 que incluye un campo de NAS-PDU que incluye un mensaje RECHAZO DE REGISTRO. La respuesta subsiguiente del UE 200 puede ser diferente, dependiendo del motivo del rechazo del registro. Para errores recuperables, como errores de sintaxis o ciertos motivos de rechazo temporal, el UE 200 puede intentar iniciar el registro nuevamente con parámetros válidos. Por otros motivos de rechazo, el UE 200 detiene el procedimiento de EAP-5G y restablece los recursos relacionados con la pila de EAP y SA de IKE. Para detener el procedimiento de EAP-5G, se necesita una indicación de detención de 5G. Ambos procedimientos se describen en la presente con

más detalle.

Modalidad: compleciion del procedimiento de EAP-5G después de un fallo de registro debido a errores recuperables

[0083] La figura 5 ilustra un diagrama de flujo lógico de una modalidad de un método 500 de un procedimiento de sesión de EAP-5G después de un fallo de autenticación debido a errores recuperables. En esta modalidad, se rechaza la solicitud de registro del UE 200 a la 5GCN 100 a través de una red de acceso no 3GPP no confiable 110.

[0084] La N3IWF 204 le transmite un mensaje de solicitud de EAP/inicio de 5G al UE 200 en el paso 502. El mensaje de inicio de 5G solicita el inicio de una sesión de EAP-5G con el UE 200, es decir, el inicio del envío de mensajes de NAS encapsulados dentro de paquetes de EAP-5G. El UE 200 genera una solicitud de registro a la 5GCN 100 en un mensaje de respuesta al EAP/NAS de 5G que incluye parámetros de AN y un campo de NAS-PDU que incluye la solicitud de registro en el paso 504. En esta modalidad, la AMF 202 rechaza el registro del UE 200 en la 5GCN 100. La AMF 202 le transmite un mensaje de RECHAZO DE REGISTRO a la N3IWF 204. En respuesta, la N3IWF 204 le transmite un mensaje de solicitud de EAP/NAS de 5G al UE 200 que incluye un campo de NAS-PDU que incluye un mensaje RECHAZO DE REGISTRO DE NAS en el paso 506.

[0085] El UE 200 puede intentar iniciar el registro en la 5GCN nuevamente, aunque no es obligatorio volver a intentar el registro. Para errores recuperables, tales como errores de sintaxis o ciertos motivos de rechazo temporal, el UE 200 puede modificar el mensaje de solicitud de registro con parámetros actualizados y reintentar el registro. Alternativamente, el UE 200 puede volver a intentar el registro más tarde sin actualizar los parámetros.

[0086] El UE 200 transmite una segunda solicitud de registro formateada como un mensaje de respuesta al EAP/NAS de 5G que incluye los parámetros de AN actualizados, en caso necesario, y un campo de NAS-PDU que incluye la solicitud de registro en el paso 508. El UE 200 y la N3IWF 204 luego realizan el establecimiento de la SA de IKE y SA IPsec de señalización para crear un contexto de seguridad de NAS y una clave de N3IWF (no mostrada).

[0087] Después de crear la clave de N3IWF en el UE 200, la N3IWF 204 transmite un mensaje de solicitud de EAP/NAS de 5G que incluye una PDU de NAS con un mensaje de comando de modo de seguridad que indica el éxito del EAP en 510. El UE 200 solicita la compleción de la sesión de EAP-5G generando y transmitiendo un mensaje de respuesta al EAP/NAS de 5G con una PDU de NAS que incluye un mensaje de modo de seguridad completo en 512. Esto hace que la N3IWF 204 le envíe un éxito del EAP al UE 200, con la suposición de que la N3IWF 204 también haya recibido la clave de N3IWF de la AMF 202. Esto completa la sesión de EAP-5G y no se pueden intercambiar más paquetes de EAP-5G.

[0088] De esta forma, el UE 200 puede volver a intentar una solicitud de registro con la 5GCN 100 a través de una red de acceso no 3GPP 110 cuando se rechaza. El rechazo puede deberse a errores recuperables, como errores de sintaxis o errores en los parámetros de AN. El segundo intento de registro puede tener éxito cuando se corrigen dichos errores recuperables. En otra modalidad, el rechazo se debe a motivos de rechazo temporal. El UE 200 puede entonces volver a intentar el registro con los mismos parámetros y completar la sesión de EAP-5G.

Modalidad: finalización del procedimiento de EAP-5G después de un fallo de registro debido a errores irrecuperables

[0089] La figura 6 ilustra un diagrama de flujo lógico que ilustra una modalidad de un procedimiento de sesión de EAP-5G de un rechazo de registro debido a errores irrecuperables o fallos permanentes. En esta modalidad, se rechaza nuevamente la solicitud de registro del UE 200 a la 5GCN 100 a través de una red de acceso no 3GPP no confiable 110.

[0090] La N3IWF 204 le transmite un mensaje de solicitud de EAP/inicio de 5G al UE 200 para iniciar el registro en la 5GCN 100 a través de la red de acceso no 3GPP 110 en el paso 602. El UE 200 responde con una solicitud de registro, por ejemplo, un mensaje de respuesta al EAP/NAS de 5G que incluya parámetros de AN y un campo de NAS-PDU que incluya la solicitud de registro en el paso 604.

[0091] Si falla la autenticación debido a errores irrecuperables, tales como el fracaso de la autenticación de EAP-AKA', la N3IWF 204 recibe un mensaje de RECHAZO DE

REGISTRO de la AMF 202 (no mostrado). En respuesta a la recepción del mensaje RECHAZO DE REGISTRO de la AMF 202, la N3IWF 204 genera un mensaje de respuesta al EAP/NAS de 5G para el UE 200 en 606. El mensaje de respuesta al EAP/NAS de 5G incluye un campo de NAS-PDU que incluye un mensaje de RECHAZO DE REGISTRO DE NAS con el campo fallo del EAP.

[0092] El UE 200 finaliza el procedimiento de registro mediante la generación y transmisión de un mensaje de respuesta al EAP/detención de 5G en el paso 608. El mensaje de detención de 5G indica el fin de la sesión de EAP para el registro en la 5GCN 100 a través de la red de acceso no 3GPP 110. Después de recibir el mensaje de respuesta al EAP/detención de 5G del UE 200, la N3IWF 204 completa el procedimiento de EAP-5G enviando un mensaje de fallo del EAP al UE 200 en el paso 610. En esta modalidad, el UE 200 detiene la sesión de EAP-5G sin reintento de registro.

[0093] La figura 7 ilustra un diagrama de bloques esquemático de una modalidad de un mensaje de respuesta al EAP/detención de 5G 700. El mensaje de respuesta al EAP/detención de 5G 700 incluye varios paquetes de EAP con campos ejemplares que incluyen el código 702, el identificador 704, la longitud 706, el tipo 708, el id. del proveedor 710, el tipo de proveedor 712, el identificador de mensaje (Id. de mensaje) 714, la reserva 716 y las extensiones 718. El campo Id. de mensaje 714 del paquete de EAP incluye un identificador para indicar un mensaje de detención de 5G. Se describe un ejemplo de los valores de los campos en el paquete de EAP en la Tabla 1 a continuación.

El campo de código se establece como 1 (decimal), como se especifica en la subcláusula 4.1 del RFC de IETF 3748 [9], e indica solicitud. El campo de identificador se establece como se especifica en la subcláusula 4.1 del RFC de IETF 3748 [9]. El campo de longitud se establece como se especifica en la subcláusula 4.1

del RFC de IETF 3748 [9] e indica la longitud del mensaje de respuesta al EAP/detención de 5G en octetos. El campo de tipo se establece como 254 (decimal), como se especifica en la subcláusula 5.7 del RFC de IETF 3748 [9], e indica el tipo expandido. El campo de Id. del proveedor se establece con el Id. del proveedor del 3GPP de 10415 (decimal) registrado ante la IANA en el registro de código de empresas privadas de SMI. El campo de tipo de proveedor se establece con el identificador de método de EAP-5G de 3 (decimal), como se especifica en el TS del 3GPP 33.402 [10], anexo C. El campo de Id. de mensaje se establece como el Id. de detención de 5G de 4 (decimal). El campo de reserva consiste en bits de reserva. El campo de extensiones es un campo opcional y consiste en bits de reserva.

TABLA 1

Ejemplo de campos para un mensaje de respuesta al EAP/detención de 5G

[0094] El campo de identificador de mensaje (Id. de mensaje) 714 en el mensaje de EAP incluye un valor o identificador de detención de 5G. Los campos y valores del mensaje de respuesta al EAP/detención de 5G 700 son ejemplos y se pueden implementar otros campos/valores o paquetes de protocolo que indiquen un significado similar a una detención del registro.

Modalidad: métodos y mejoras de protocolo para el manejo cuando no se acepta

el establecimiento de SA IPsec debido a un fallo de autenticación

[0095] La figura 8 ilustra un diagrama de flujo lógico de una modalidad de un método 800 del flujo de mensajes entre funciones de red cuando no se aceptan el establecimiento de SA de IKE ni SA IPsec de señalización para el registro del UE 200 a través de una red de acceso no 3GPP 110 debido a un fallo de autenticación. Por ejemplo, se puede no aceptar el establecimiento de SA de IKE y SA IPsec de señalización debido a un fallo en un procedimiento de autenticación, como un desarío de AKA o desafío de AKA'. El método 800 incluye un nuevo tipo de mensaje de notificación de IKEv2 privado para señalarle el fallo al UE 200 y un nuevo valor de causa para indicar que no se permite el acceso a la 5GCN 100 mediante la red de acceso no 3GPP 110.

[0096] El UE 200 se conecta a una red de acceso no 3GPP (N3AN) 110 no confiable, por ejemplo, usando los protocolos 802.1x para una WLAN pública, en el paso 802. Cuando el UE 200 decide conectarse a la 5GCN 100, el UE 200 selecciona una N3IWF 204 en una PLMN 5G en el paso 804. El UE 200 procede con el establecimiento de una asociación de seguridad (SA) IPsec con la N3IWF 204 seleccionada, iniciando un intercambio inicial IKE, por ejemplo, como se describe en el RFC de IETF 7296 «Protocolo de intercambio de claves de internet, versión 2 (IKEv2)», (octubre de 2014), en el paso 806. Después del establecimiento de la SA de IKE, los mensajes de IKE subsiguientes se cifran y la integridad se protege mediante el uso de la SA de IKE establecida en este paso 806.

[0097] Luego, el UE 200 inicia un intercambio de IKE_AUT, enviando un mensaje de solicitud de IKE_AUT en el paso 808. La carga útil de AUT no se incluye en el mensaje de solicitud de IKE_AUT, que indica que el intercambio de IKE_AUT utilizará la señalización del EAP (en este caso, la señalización del EAP-5G). El UE 200 establecerá el campo de Id. del UE en este mensaje como cualquier número aleatorio. La N3IWF 204 responde con un mensaje de respuesta a IKE_AUT que incluye un paquete de solicitud del EAP/inicio de 5G en el paso 810. El paquete de solicitud de EAP/inicio de 5G le informa al UE 200 que inicie una sesión de EAP-5G, es decir, que comience a enviar mensajes de NAS encapsulados dentro de paquetes de EAP-5G.

[0098] El UE 200 también puede validar el certificado de la N3IWF y confirmar que la

identidad de la N3IWF 204 coincide con la N3IWF 204 seleccionada por el UE 200. Una ausencia de certificado de la N3IWF 204 o el fracaso de la confirmación de identidad pueden dar lugar a un fallo en la conexión. Luego, el UE 200 envía una solicitud de IKE_AUT que incluye un paquete respuesta al EAP/NAS de 5G para solicitar el registro en la 5GCN 100 en el paso 812. El mensaje de respuesta al EAP/NAS de 5G incluye parámetros de AN (por ejemplo, GUAMI, ID de PLMN seleccionado, NSSAI solicitada) y un campo de NAS-PDU que incluye la solicitud de registro.

[0099] La N3IWF 204 luego selecciona una AMF 202 usando los parámetros de AN y reenvía la solicitud de registro recibida del UE 200 a la AMF 202 en un mensaje de transporte de NAS N2 en el paso 814.

[00100] La AMF 202 puede decidir autenticar el UE 200. En este caso, la AMF 202 selecciona una AUSF 210 en el paso 816 y le envía una solicitud de clave a la AUSF 210. La AUSF 210 puede entonces iniciar un procedimiento de autenticación, tal como un desafío de AKA o un desafío de AKA' en el paso 818. Entre la AMF 202 y el UE 200, se encapsulan los paquetes de autenticación dentro de los mensajes de autenticación de NAS y los mensajes de autenticación de NAS se encapsulan dentro de los paquetes de EAP-5G/NAS de 5G. Se transmite un mensaje de solicitud de EAP/desafío de AKA' al UE 200 a través de la N3IWF 204 en un mensaje de sol. de aut. de mensaje de NAS en los pasos 820 y 822. Este mensaje puede incluir el ngKSI que será utilizado por el UE 200 y la AMF 202 para identificar el contexto de seguridad nativo parcial que se crea en caso de autenticación exitosa. El UE 200 le reenvía el RAND y la AUTN recibidos en el mensaje de solicitud de EAP/desafío de AKA' al USIM.

[00101] Al recibir el RAND y la AUTN, el USIM verifica el vector de autenticación comprobando si se puede aceptar la AUTN. Si es así, el USIM calcula una respuesta RES en el paso 823. El UE 200 envía el mensaje de respuesta al EAP/desafío de AKA' en un mensaje de resp. de aut. de mensaje de NAS en el paso 824. El mensaje de respuesta al EAP/desafío de AKA' se transmite a la AUSF 210 a través de la AMF 202 en los pasos 826 y 828. La AUSF 210 luego intentará verificar el mensaje. Si la AUSF 210 verificó satisfactoriamente este mensaje, continuará la autenticación.

[00102] En sistemas anteriores conocidos, si la AUSF 210 determina que no se permite el acceso no 3GPP a la 5GCN 100 debido a un fallo de autenticación en el paso

830, devuelve un error. En un nuevo sistema y método mejorados, la AMF 202 genera un nuevo tipo de mensaje de notificación de IKEv2 privado para señalar que no se permite el acceso no 3GPP a la red de 5GC, por ejemplo, debido al fallo de la autenticación.

[00103] En el paso 832, la AUSF 210 envía un mensaje de sesión de EAP HTTP con una carga útil de EAP de fallo del EAP y un resultado de autenticación de fallo de autenticación. La AMF 202 genera una nueva causa de gestión de movilidad 5G (5GMM) para indicar que no se permite el acceso no 3GPP a la 5GCN 100. La AMF 202 genera un mensaje de transporte de NAS N2 con un rechazo de registro y un mensaje de EAP que indica el fallo del EAP e incluye la causa de 5GMM en el paso 834. La causa de 5GMM indica un tipo de error, por ejemplo, en este caso, «No se permite el acceso no 3GPP a la 5GCN».

[00104] El UE 200 recibe de la N3IWF 204 un mensaje de respuesta a IKE_AUT con una carga útil de notificación con un tipo de mensaje de notificación privado (por ejemplo, cualquier tipo de mensaje de notificación privado en un rango predefinido, como 8192 ... 16383) en el paso 836. El mensaje de notificación de IKEv2 privado incluye una respuesta al EAP/PDU de NAS de 5G que incluye el rechazo del registro con la causa de 5GMM de «ACCESO_NO_3GPP_A_LA_5GCN_NO_PERMITIDO» y un tipo de mensaje de EAP de fallo del EAP.

[00105] El método 800 incluye, por tanto, un nuevo tipo de mensaje de notificación de IKEv2 privado y un nuevo valor de causa de 5GMM para informarle al UE el fallo de la solicitud de registro de que no se permite el acceso no 3GPP a la 5GCN 100. Si bien se implementa un nuevo mensaje de notificación de IKEv2 privado, se pueden implementar otros tipos de mensajes o formatos o campos o tipos de error para informarle al UE 200 que no se permite o se rechaza el acceso no 3GPP a la red 5GC.

[00106] Al recibir el mensaje de notificación privado con 5GMM como causa de ACCESO_NO_3GPP_A_LA_5GCN_NO_PERMITIDO, el UE 200 finaliza la sesión de EAP-5G enviando un mensaje de respuesta al EAP/detención de 5G en el paso 838. El UE 200 recibe de la N3IWF 204 un mensaje de respuesta a IKE_AUT con un mensaje de fallo del EAP en el paso 840.

[00107] Al recibir el mensaje de fallo del EAP de la N3IWF 204, el UE 200 realiza el

procedimiento de eliminación de la SA de IKEv2 y cierra la SA de IKE en el paso 842. El UE 200 no reinicia el establecimiento de SA de IKE y SA IPsec con la N3IWF 204 desde la misma PLMN hasta apagarse o hasta que se elimine la UICC que contiene el USIM. El UE 200 puede transmitir un mensaje informativo de la eliminación de la SA de IKEv2 en el paso 844. La N3IWF 204 puede entonces cerrar la SA de IKEv2 en el paso 846.

Modalidad: métodos y mejoras de protocolo para el manejo cuando no se acepta el establecimiento de una SA IPsec debido a restricciones de suscripción

[00108] La figura 9 ilustra un diagrama de flujo lógico de una modalidad de un método 900 de flujo de mensajes entre funciones de red cuando no se acepta el establecimiento de SA de IKE ni SA IPsec de señalización para el registro de UE 200 a través de acceso no 3GPP, debido a una restricción de suscripción. Por ejemplo, el establecimiento de SA de IKE y SA IPsec de señalización puede no aceptarse debido a una restricción de suscripción. El método 900 incluye un nuevo tipo de mensaje de notificación de IKEv2 privado para señalarle el fallo al UE 200 y un nuevo valor de causa para indicar que no se permite el acceso a la 5GCN 100 mediante la red de acceso no 3GPP 110.

[00109] El UE 200 se conecta a una red de acceso no 3GPP (N3AN) 110 no confiable, por ejemplo, usando los protocolos 802.1x para una WLAN pública, en el paso 902. Cuando el UE 200 decide conectarse a la 5GCN 100, el UE 200 selecciona una N3IWF 204 en una PLMN 5G en el paso 904. El UE 200 procede con el establecimiento de una asociación de seguridad (SA) IPsec con la N3IWF 204 seleccionada, iniciando un intercambio inicial IKE, por ejemplo, como se describe en el RFC de IETF 7296 «Protocolo de intercambio de claves de internet, versión 2 (IKEv2)», (octubre de 2014), en el paso 906. Después del establecimiento de la SA de IKE, los mensajes de IKE subsiguientes se cifran y la integridad se protege usando las claves establecidas en la SA de IKE.

[00110] Luego, el UE 200 inicia un intercambio de IKE_AUT, enviando un mensaje de solicitud de IKE_AUT en el paso 908. La carga útil de AUT no se incluye en el mensaje de solicitud de IKE_AUT, que indica que el intercambio de IKE_AUT utilizará la

señalización del EAP (en este caso, la señalización del EAP-5G). El UE 200 establece el campo de Id. del UE en este mensaje como cualquier número aleatorio. La N3IWF 204 responde con un mensaje de respuesta a IKE_AUT que incluye un paquete de solicitud del EAP/inicio de 5G en el paso 910. El paquete de solicitud de EAP/inicio de 5G le informa al UE 200 que inicie una sesión de EAP-5G, es decir, que comience a enviar mensajes de NAS encapsulados dentro de paquetes de EAP-5G.

[00111] El UE 200 también puede validar el certificado de la N3IWF y confirmar que la identidad de la N3IWF 204 coincide con la N3IWF 204 seleccionada por el UE. Una ausencia de certificado de la N3IWF 204 o el fracaso de la confirmación de identidad pueden dar lugar a un fallo en la conexión. Luego, el UE 200 envía una solicitud de registro en una solicitud de IKE_AUT que incluye un paquete respuesta al EAP/NAS de 5G en el paso 912. El paquete de respuesta al EAP/NAS de 5G incluye parámetros de AN, como GUAMI, ID de PLMN seleccionado, NSSAI solicitada y una PDU de NAS con la solicitud de registro. La N3IWF 204 luego selecciona una AMF 202 y reenvía la solicitud de registro en la PDU de NAS recibida del UE 200 a la AMF 202 en el paso 914.

[00112] La AMF 202 puede decidir autenticar el UE 200. En este caso, la AMF 202 selecciona una AUSF 210 en el paso 916 y le envía una solicitud de clave a la AUSF 210. La AUSF 210 puede entonces iniciar un procedimiento de autenticación, tal como un desafío de AKA o un desafío de AKA' en el paso 918. Entre la AMF 202 y el UE 200, se encapsulan los paquetes de autenticación dentro de los mensajes de autenticación de NAS y los mensajes de autenticación de NAS se encapsulan dentro de los paquetes de EAP-5G/NAS de 5G. Se transmite un mensaje de solicitud de EAP/desafío de AKA' al UE 200 en un mensaje de sol. de aut. de mensaje de NAS mediante la AMF en el paso 920 y la N3IWF lo reenvía en el paso 922. Este mensaje puede incluir el ngKSI que será utilizado por el UE 200 y la AMF 202 para identificar el contexto de seguridad nativo parcial que se crea en caso de autenticación exitosa. El UE 200 le reenvía el RAND y la AUTN recibidos en el mensaje de solicitud de EAP/desafío de AKA' a su USIM.

[00113] Al recibir el RAND y la AUTN, el USIM verifica el vector de autenticación comprobando si se puede aceptar la AUTN. Si es así, el USIM calcula una respuesta de

autenticación en el paso 923. El UE 200 envía el mensaje de respuesta al EAP/desafío de AKA' en un mensaje de resp. de aut. de mensaje de NAS en el paso 924. La N3IWFF transmite el mensaje de respuesta al EAP/desafío de AKA' a la AMF en el paso 926 y luego a la AUSF 210 en el paso 928. La AUSF 210 luego intentará verificar el mensaje. Si la AUSF 210 verificó satisfactoriamente este mensaje, continuará la autenticación. Sin embargo, la AUSF 210 puede rechazar la autenticación y no permitir el acceso no 3GPP a la 5GCN 100 en el paso 930.

[00114] En sistemas conocidos anteriores, si la AUSF 210 determina un fallo de autenticación, entonces la AUSF 210 devuelve un error. En un nuevo método mejorado, la AMF 202 genera una nueva causa para señalar que no se permite el acceso no 3GPP a la 5GCN 100. Por ejemplo, la AMF 202 puede generar un nuevo tipo de mensaje de notificación de IKEv2 privado para señalarle al UE 200 que no se permite el acceso no 3GPP a la 5GCN 100, por ejemplo, debido a una restricción de red o suscripción.

[00115] En el paso 932, la AUSF 210 envía un mensaje de sesión de EAP HTTP con una carga útil de EAP de fallo del EAP y un resultado de autenticación de fallo de autenticación con causa. La AMF 202 genera un mensaje de transporte de NAS N2 con un rechazo del registro y un mensaje de EAP de fallo del EAP que incluye la causa de 5GMM en el paso 934. La causa de 5GMM indica un tipo de error de ACCESO_NO_3GPP_A_LA_5GCN_NO_PERMITIDO.

[00116] La N3IWF 204 recibe la respuesta de la AMF 202 que encapsula un mensaje de rechazo de registro que incluye un valor de causa de 5GMM que indica que no se permite el acceso no 3GPP a la 5GCN y un mensaje de tipo de fallo del EAP. La N3IWF 204 genera un mensaje de respuesta a IKE_AUT con una carga útil de notificación con un tipo de mensaje de notificación privado (por ejemplo, cualquier tipo de mensaje de notificación privado en un rango predefinido, como 8192 ... 16383) en el paso 936. El mensaje de notificación de IKEv2 privado incluye una respuesta al EAP/PDU de NAS de 5G que incluye el rechazo del registro con la causa de 5GMM de «ACCESO_NO_3GPP_A_LA_5GCN_NO_PERMITIDO» y un tipo de mensaje de EAP de fallo del EAP.

[00117] Por tanto, se implementa un nuevo código de causa de 5GMM para señalarle

al UE 200 que no se permite el acceso no 3GPP a la 5GCN 100. La AMF 202 genera esta causa de 5GMM y se la transmite al UE 200 si este solicita servicios a través de acceso no 3GPP en una PLMN, donde el UE 200, por restricción de red o suscripción, no puede acceder a la 5GCN 100 a través de una red de acceso no 3GPP 110. De esta forma, se informa al UE 200 el rechazo del acceso a la 5GCN 100 a través de la red de acceso no 3GPP 110.

[00118] El UE 200 recibe de la N3IWF 204 el mensaje de respuesta a IKE_AUT con una carga útil de notificación con un tipo de mensaje de notificación privado y un mensaje de EAP de fallo del EAP y la causa de 5GMM de ACCESO_NO_3GPP_A_LA_5GCN_NO_PERMITIDO en el paso 936. El UE 200, en lugar de simplemente recibir un mensaje de error, recibe así una notificación de rechazo del registro con un motivo.

[00119] Luego, el UE 200 finaliza la solicitud de registro generando un mensaje de respuesta al EAP/detención de 5G para la N3IWF 204 en el paso 938. El UE 200 recibe de la N3IWF 204 un mensaje de respuesta a la IKE_AUT con un mensaje de fallo del EAP en el paso 940.

[00120] Al recibir el mensaje de fallo del EAP de la N3IWF 204, el UE 200 realiza el procedimiento de eliminación de la SA de IKEv2 y cierra la SA de IKE en el paso 942. En este ejemplo, debido al error irrecuperable de una restricción de red o suscripción, el UE 200 no reinicia el establecimiento de SA de IKE y SA IPsec con una N3IWF 204 de la misma PLMN hasta apagarse o hasta que se elimine la UICC que contiene el USIM . El UE 200 puede transmitir un mensaje informativo de la eliminación de la SA de IKEv2 en el paso 944. La N3IWF 204 puede entonces cerrar la SA de IKEv2 en el paso 946.

Modalidad: métodos y mejoras de protocolo para el manejo cuando no se acepta el establecimiento de una SA IPsec en el plano de usuario

[00121] La figura 10 ilustra un diagrama de flujo lógico de una modalidad de un método de flujo de mensajes entre funciones de nodos de red cuando no se acepta el establecimiento de una asociación de seguridad (SA) IPsec en el plano de usuario. El UE 200 se conecta a una red de acceso no 3GPP (N3AN) 110 no confiable, por ejemplo, usando los protocolos 802.1x para una WLAN pública, en el paso 1002.

Cuando el UE 200 decide conectarse a la 5GCN 100, el UE 200 selecciona una N3IWF 204 en una PLMN 5G en el paso 1004. El UE 200 procede con el establecimiento de una asociación de seguridad (SA) IPsec con la N3IWF 204 seleccionada, iniciando un intercambio inicial IKE en el paso 1006. En esta modalidad, el UE 200 establece exitosamente una SA de IKE y SA IPsec de señalización con la N3IWF 204 seleccionada en 1008. Por ejemplo, la autenticación del UE 200, por ejemplo, como un procedimiento de EAP-AKA', es exitosa, y se completa el EAP-5G, como se muestra en la figura 3.

[00122] Luego, el UE 200 le transmite un mensaje de solicitud de establecimiento de sesión de PDU a la AMF 202 para establecer una SA IPsec en el plano de usuario en 1010. Este mensaje de solicitud de establecimiento de sesión de PDU se envía a la N3IWF 204 a través de la SA IPsec de señalización y la N3IWF 204 lo reenvía de forma transparente a la AMF 202 en la 5GCN 100 en el paso 1012. La AMF 202 puede crear un contexto de gestión de sesiones (SM) con la SMF 206 en el paso 1014. La AMF 202 le envía un mensaje de solicitud de sesión de PDU de interfaz de NAS N2 a la N3IWF 204 para establecer los recursos de acceso para esta sesión de PDU, por ejemplo, en una solicitud de configuración de recursos de sesión de PDU N2, en el paso 1016. La solicitud de sesión de PDU puede incluir un Id. de sesión de PDU, aceptación del establecimiento de sesión de PDU, QFI, perfiles de QoS, etc.

[00123] Basándose en sus propias políticas y configuración y basándose en los perfiles de QoS recibidos en la solicitud de sesión de PDU N2, la N3IWF 204 determina el establecimiento de un número de SA IPsec en el plano de usuario y los perfiles de QoS asociados con cada SA IPsec en el plano de usuario. Por ejemplo, la N3IWF 204 puede decidir establecer una SA IPsec en el plano de usuario y asociar todos los perfiles de QoS con esta SA IPsec en el plano de usuario. En este ejemplo, todos los flujos de QoS de la sesión de PDU se transferirían a través de una SA IPsec en el plano de usuario. En otro ejemplo, la N3IWF 204 puede decidir establecer una pluralidad de sub-SA IPsec en el plano de usuario y asociar ciertos perfiles de QoS con diferentes perfiles de la pluralidad de sub-SA IPsec en el plano de usuario.

[00124] La N3IWF 204 envía al UE 200 una solicitud de crear_sub-SA_de_IKE para establecer la primera sub-SA IPsec en el plano de usuario para la sesión de PDU en el

paso 1018. La solicitud de crear_sub-SA_de_IKE indica una primera sub-SA IPsec en el plano de usuario con identificación de SAup1. Esta solicitud puede incluir una carga útil de notificación específica del 3GPP que incluya (a) el o los QFI asociados con la sub-SA, (b) la identidad de la sesión de PDU asociada con esta sub-SA, (c) opcionalmente, un valor de DSCP asociado con la sub-SA y (d) una DIRECCIÓN_IP_UP. La solicitud de crear_sub-SA_de_IKE también puede incluir otra información, como la carga útil de la SA, los selectores de tráfico (TS, por sus siglas en ingles) para la N3IWF 204 y el UE 200, etc.

[00125] Cuando el UE 200 acepta la nueva sub-SA IPsec, el UE 200 envía una respuesta a crear_sub-SA_de_IKE en el paso 1020. El UE 200 y la N3IWF 204 pueden intercambiar múltiples iteraciones de solicitudes y respuestas crear_sub-SA_de_IKE para establecer una pluralidad de sub-SA IPsec en el paso 1022. Se establecen las sub-SA IPsec adicionales, cada una asociada con uno o más QFI y con una DIRECCIÓN_IP_UP.

[00126] Si el UE 200 no acepta la solicitud de SA IPsec en el plano de usuario en el paso 1024, como en el paso 1026, el UE 200 le envía un mensaje de respuesta a CREAR_SUB-SA a la N3IWF 204 con una carga útil de notificación del tipo de error en el paso 1026. El tipo de mensaje de notificación puede ser «error». El tipo de mensaje de notificación «error» indica que el UE 200 no acepta la sub-SA IPsec.

[00127] Tras recibir el mensaje de respuesta a CREAR_SUB-SA con una carga útil de notificación del tipo de error, la N3IWF 204 le indica el fallo y la lista de fallos para configurar los recursos de la sesión PDU a la AMF 202 a través de un mensaje de respuesta a la configuración de recursos de sesión de PDU N2 en el paso 1032, para desencadenar el rechazo del establecimiento de la sesión de PDU a través del acceso no 3GPP. Alternativamente, si la N3IWF 204 decidió previamente crear múltiples SA IPsec en el plano de usuario para los identificadores de flujo de QoS (QFI, por sus siglas en inglés) de la sesión de PDU y una o más SA IPsec en el plano de usuario de la sesión de PDU ya están activas, la red puede optar por completar el establecimiento de la sesión de PDU mediante una correspondencia del o de los QFI de las SA IPsec en el plano de usuario fallidas con las SA IPsec en el plano de usuario ya establecidas, como se observa en los pasos 1028 y 1030.

[00128] Tras recibir el comando de liberación de recursos de sesión de PDU N2 que incluya un mensaje de rechazo del establecimiento de la sesión de PDU que indique la PDU de NAS en el paso 1034, la N3IWF 204 le reenvía de forma transparente el rechazo del establecimiento de la sesión de PDU al UE 200 en el paso 1036. Se establece una causa de gestión de sesión 5G (5GSM) específica de «fallo de la SA IPsec» para indicar el motivo del rechazo de la sesión de PDU.

Modalidad: tipos de mensaje de notificación de IKEv2 privados para el acceso no 3GPP

[00129] La Tabla 2 posterior enumera los tipos de mensaje de notificación para el acceso no 3GPP. En este ejemplo, se describen los mensajes de notificación de IKEv2 privados y los tipos de error privados; sin embargo, se pueden usar otros protocolos de mensaje, valores y tipos de error para notificarle a un UE 200 los motivos o los errores cuando no se permite el acceso no 3GPP a una 5GCN 100.

[00130] En este ejemplo, se definen tipos de mensaje de notificación de IKEv2 privados para el uso de acceso no 3GPP. El tipo de mensaje de notificación con un valor (en decimal) entre 8192 y 16383 está reservado para usos de errores privados, aunque se pueden implementar otros valores y campos. El tipo de mensaje de notificación con un valor (en decimal) entre 40960 y 65535 está reservado para usos de estados privados. En este documento solo se describen los tipos de mensaje de notificación de IKEv2 privados que se utilizan para esta memoria descriptiva. Los tipos de error de mensaje de notificación privados definidos en la Tabla 2 son notificaciones de error que indican un error al negociar el acceso no 3GPP a una 5GCN 100. Por ejemplo, los tipos de error pueden generarse en respuesta a la negociación de una SA de IKEv2 o una SA IPsec para el acceso no 3GPP a una 5GCN 100. Los campos y valores de los tipos de mensaje de notificación privados son ejemplos y se pueden implementar otros campos/valores que indiquen significados similares.

Mensaje de notificación	**Valor (en decimal)**	**Descripciones**

AUTORIZACIÓN_RECHAZADA	9003	El tipo de error se utiliza para indicar el rechazo del servicio solicitado debido a que el UE no está autorizado para utilizar este servicio
ME_ILEGAL	9006	El tipo de error se utiliza para indicar el rechazo del servicio solicitado, ya sea debido a un fallo de autenticación o a que la red no puede aceptar una identidad del UE
TIPO_RAT_NO_PERMITIDO	11001	El tipo de error se utiliza para indicar el rechazo del servicio solicitado la PLMN no permite 1el tipo de RAT utilizado
PEI_NO_ACEPTADO	11005	El tipo de error se utiliza para indicar el rechazo de la solicitud de sesión PDU de emergencia, dado que la red no acepta una solicitud de servicio de emergencia utilizando un PEI
PLMN_NO_PERMITIDA	11011	El tipo de error se utiliza para indicar el rechazo del servicio solicitado, debido a la suscripción o debido a una prohibición determinada por el operador
FALLO_RED	10500	El tipo de error se utiliza para indicar el rechazo del servicio solicitado debido a fallos de red
CONGESTIÓN	12005	El tipo de error se utiliza para

		indicar el rechazo del servicio solicitado debido a congestión de la red
SERVICIOS_5GS_NO_ PERMITIDOS	12007	El tipo de error se utiliza para indicar el rechazo del servicio solicitado debido a que no se permiten los servicios 5GS
ACCESO_NO_3GPP_A_5GC_ NO_PERMITIDO	12071	El tipo de error se utiliza para indicar el rechazo del servicio solicitado debido a que no se permite que el UE utilice un acceso no 3GPP a la 5GC

Tabla 2

Tipos de mensaje de notificación para el acceso no 3GPP

[00131] El UE 200 puede recibir un mensaje con un tipo de error que indique que no se permite el acceso no 3GPP a la 5GCN 100. De esta forma, se informa al UE 200 el rechazo del acceso a la 5GCN 100 a través de la red de acceso no 3GPP 110.

Modalidad: código de causa que señala el fallo de la autenticación debido a la falta de suscripción para el acceso no 3GPP a la red 5GC

[00132] La figura 11 ilustra un diagrama de bloques esquemático de una modalidad de un elemento de información de causa de 5GMM 1100. El elemento de información de causa de 5GMM 1100 incluye un indicador de elemento de información de causa (IEI, por sus siglas en inglés) 1104 de 5GMM y un valor de causa 1106. El valor de causa 1106 indica un motivo por el que la red rechaza una solicitud de 5GMM de acceso a la 5GCN 100 del UE 200. En esta modalidad, un nuevo código de causa corresponde a «No se permite el acceso no 3GPP a la 5GCN». Esta causa de 5GMM

se envía al UE 200 si este solicita servicios a través de un acceso no 3GPP en una PLMN, donde no se permite el acceso del UE 200 a la 5GCN 100 a través de un acceso no 3GPP, por restricción de red o suscripción u otro fallo de autenticación.

[00133] La figura 12 ilustra un diagrama de bloques esquemático de una modalidad de valores para el elemento de información de causa de 5GMM. En este ejemplo, un valor predeterminado corresponde a «No se permite el acceso no 3GPP a la 5GCN». Otros valores recibidos por el UE 200 se tratan como «error de protocolo, no especificado». Cualquier otro valor recibido por la red también se trata como «error de protocolo, no especificado». Los campos y valores del elemento de información de causa de 5GMM son ejemplos y se pueden implementar otros campos/valores que indiquen significados similares.

[00134] La figura 13 ilustra un diagrama de flujo lógico de una modalidad de un método 1300 de la N3IWF 204. La N3IWF 204 se comunica usando una primera interfaz con nodos en la 5GCN 100, usando uno o más protocolos en el paso 1302. La N3IWF 204 se comunica con un UE a través de una red de acceso no 3GPP, usando al menos una segunda interfaz, tal como un transceptor de WLAN conforme a los protocolos del IEEE de WLAN 802.1x, en el paso 1304.

[00135] La N3IWF 204 procesa una solicitud de registro para un establecimiento de conexión segura a la red central desde el UE 200 en la red de acceso no confiable en el paso 1306. Por ejemplo, la N3IWF 204 recibe un mensaje de respuesta al EAP/NAS de 5G que incluye parámetros de AN y una solicitud de registro del UE 100. La N3IWF 204 reenvía el mensaje a la 5GCN 100 para la verificación de suscripción y autenticación del UE 200. Por ejemplo, la N3IWF 204 genera una solicitud de verificación de suscripción y autenticación y transmite la solicitud de verificación de suscripción y autenticación a través de la segunda interfaz a la AMF 202.

[00136] La N3IWF 204 determina que la red central no acepta el establecimiento de la conexión en el paso 1308, por ejemplo, debido a errores irrecuperables. Por ejemplo, la AMF 202 recibe una respuesta de fallo de autenticación de la AUSF 210. La AMF 202 genera un mensaje de transporte de NAS con un rechazo de registro y un mensaje de EAP de fallo del EAP que incluye una causa de 5GMM. La causa de 5GMM indica un tipo de error de ACCESO_NO_3GPP_A_LA_5GCN_NO_PERMITIDO. La N3IWF 204

recibe la respuesta de la AMF 202 que encapsula el mensaje de rechazo de registro que incluye el valor de causa de 5GMM que indica que no se permite el acceso no 3GPP a la 5GCN.

[00137] La N3IWF 204 genera un mensaje de respuesta al UE, en el que el mensaje de respuesta incluye el valor de causa que indica que la red central no permite el establecimiento de la conexión a través del acceso de red no confiable en el paso 1310. Por ejemplo, la N3IWF 204 genera un mensaje de respuesta al intercambio de claves de internet (IKE) con la carga útil que incluye un tipo de mensaje o fallo del EAP que indica que la 5GCN 100 no acepta el establecimiento de la conexión y la causa de 5GMM. El mensaje de respuesta al EAP/NAS de 5G al UE 200 incluye un mensaje de rechazo del registro con un campo de fallo del EAP y la causa de 5GMM. La causa de 5GMM en el mensaje de rechazo del registro indica que la 5GCN 100 no permite el acceso no 3GPP.

[00138] En una modalidad, el mensaje de respuesta al IKE para el UE puede incluir un mensaje de respuesta a IKE_AUT con una carga útil de notificación con un tipo de mensaje de notificación privado (por ejemplo, cualquier tipo de mensaje de notificación privado en un rango predefinido, como 8192 ... 16383). El mensaje de notificación de IKEv2 privado incluye una respuesta al EAP/PDU de NAS de 5G que incluye el rechazo del registro con la causa de 5GMM de «ACCESO_NO_3GPP_A_LA_5GCN_NO_PERMITIDO» y un tipo de mensaje de EAP de fallo del EAP.

[00139] La N3IWF 204 procesa una respuesta del UE 200 que incluye un mensaje de detención y genera un mensaje de fallo para el UE 200 en respuesta. Por ejemplo, el UE 200 le transmite un mensaje de respuesta al EAP/detención de 5G a la N3IWF 204 para indicar el fin de la solicitud de registro para el establecimiento de una sesión segura con la 5GCN 100. El paquete de respuesta al EAP incluye un identificador de tipo de mensaje de detención 5G. Tras la recepción del mensaje de respuesta al EAP/detención de 5G del UE 200, la N3IWF 204 completa el procedimiento de EAP-5G enviándole un mensaje de fallo del EAP al UE 200. Aunque se describe que la N3IWF 204 realiza estos pasos en el método 1300, otros nodos o módulos en comunicación con el UE y la red central pueden realizar uno o más de los pasos descritos en este

documento.

[00140] La figura 14 ilustra un diagrama de flujo lógico de una modalidad de un método 1400 de solicitud de registro a una red central a través de una red de acceso no confiable con fallo de autenticación debido a errores recuperables. El UE 200 está configurado para comunicarse a través de una red de acceso no 3GPP con una función de interfuncionamiento (tal como la N3IWF 204) en una 5GCN 100 en el paso 1402. El UE 200 puede solicitar el registro en la 5GCN 100 a través de la red de acceso no 3GPP en 1404. El UE 200 procesa un mensaje de respuesta con una notificación de que no se permite el acceso no 3GPP a la 5GCN 100 en 1406. El UE 200 determina que el error o el motivo del rechazo es recuperable en el paso 1408. El UE 200 puede corregir parámetros en esta segunda solicitud de registro a partir del primer intento. Alternativamente, el UE puede decidir volver a intentar el registro más tarde con los mismos parámetros. El UE 200 luego le transmite la segunda solicitud de registro a la 5GCN 100 a través de la red de acceso no 3GPP en 1410. El UE 200 luego procesa una respuesta de éxito del establecimiento de la sesión en el paso 1412.

[00141] La figura 15 ilustra un diagrama de flujo lógico de una modalidad de un método 1500 de solicitud de registro a una red central a través de una red de acceso no confiable con fallo de autenticación debido a errores irrecuperables. El UE 200 está configurado para comunicarse a través de una red de acceso no 3GPP con una función de interfuncionamiento (tal como la N3IWF 204) en una 5GCN 100 en el paso 1502. El UE 200 puede solicitar el registro en la 5GCN 100 a través de la red de acceso no 3GPP en 1504. El UE 200 procesa un mensaje de respuesta con una notificación de que no se permite el acceso no 3GPP a la 5GCN 100 en 1506. El UE 200 determina que el error o el motivo del rechazo no es recuperable en el paso 1508. El UE 200 finaliza la sesión y genera una respuesta con un mensaje de detención en el paso 1510. El UE 200 recibe un mensaje de fallo y realiza un procedimiento de eliminación y cierra la sesión en el paso 1512.

[00142] La figura 16 ilustra un diagrama de bloques esquemático de una modalidad de un ejemplo de equipo de usuario 200. El equipo de usuario (UE) 200 puede incluir un teléfono inteligente, una tableta inteligente, una computadora portátil, un reloj inteligente, una PC, TV u otro dispositivo que se pueda utilizar para comunicarse a

través de una red de acceso no 3GPP 110. Pueden incluirse componentes y funciones adicionales o alternativos dentro del UE 200. Además, una o más de las funciones y los componentes mostrados en el presente documento pueden no estar presentes o combinarse con otros componentes o funciones.

[00143] El UE 200 incluye un dispositivo de procesamiento 1600 y un dispositivo de memoria 1602 que están configurados para realizar una o más de las funciones descritas en este documento con respecto al UE 200. El dispositivo de memoria 1602 puede incluir un objeto gestionado 1604 que almacena aplicaciones e instrucciones operativas que controlan el dispositivo de procesamiento 1600 para realizar varias funciones descritas en este documento. El UE 200 también puede incluir una UICC 1606 que incluya una USIM 1608 para el almacenamiento de la IMSI. En otras modalidades, el UE 200 no tiene capacidades de UICC, por ejemplo, el UE 200 no tiene una UICC 1606, tiene una UICC 1606 inoperable, etc.

[00144] El UE 200 puede incluir además un transceptor de Bluetooth 1610, un transceptor de WLAN (conforme al IEEE 802.11x) 1612, un transceptor de RF móvil (3G/4G) 1614 y GPS 1616. El transceptor de WLAN 1612 puede funcionar como una interfaz de acceso no 3GPP a una red WLAN. El UE 200 puede incluir además interfaces de usuario 1618, adaptador de CA 1620, módulo de batería 1622, transceptor USB 1624 y puerto de Ethernet 1628.

[00145] El UE 200 puede incluir además una cámara digital 1630, un controlador de pantalla táctil 1632, un altavoz 1634 y un micrófono 1636. El UE 200 también puede incluir una unidad de gestión de energía 1638. Uno o más buses de comunicación interna (no mostrados) pueden acoplar comunicativamente uno o más de los componentes del UE 200.

[00146] La figura 17 ilustra un diagrama de bloques esquemático de una modalidad de un ejemplo de AMF 202. La AMF 202 incluye cualquier nodo o nodos con la funcionalidad de la AMF 202. La AMF 202 puede integrarse con otros nodos en la 5GCN 100. Se pueden incluir componentes y funciones adicionales o alternativos dentro de la AMF 202. Además, una o más de las funciones y los componentes mostrados en el presente documento pueden no estar presentes o combinarse con otros componentes o funciones o nodos. La AMF 202 incluye un dispositivo de

procesamiento 1700 y un dispositivo de memoria 1702 que están configurados para realizar una o más de las funciones descritas en este documento con respecto a la AMF 202. La AMF 202 puede incluir una interfaz de red 1704 que incluya puertos para interactuar con otros nodos de red en la 5GCN 100.

[00147] La figura 18 ilustra un diagrama de bloques esquemático de una modalidad de un ejemplo de N3IWF 204. La N3IWF 204 puede ser un punto de acceso en una red de área local inalámbrica, una pasarela en una red de área local u otro tipo de nodo que incluya las funciones de interfuncionamiento descritas en este documento. La N3IWF 204 puede integrarse con otros nodos en una red de acceso o 5GCN 100. Se pueden incluir componentes y funciones adicionales o alternativos dentro de la N3IWF 204. Además, una o más de las funciones y los componentes mostrados en el presente documento pueden no estar presentes o combinarse con otros componentes o funciones.

[00148] La N3IWF 204 incluye un dispositivo de procesamiento 1800 y un dispositivo de memoria 1802 que están configurados para realizar una o más de las funciones descritas en este documento. La N3IWF 204 puede incluir una primera interfaz de red 1804 (por ejemplo, puertos de Ethernet, puertos de IP) para interactuar con otros nodos de red en la 5GCN 100. La N3IWF 204 también puede incluir uno o más tipos adicionales de interfaces para comunicarse con el UE, como un transceptor de WLAN 1806 (por ejemplo, acorde a las redes de tipo WLAN del IEEE 802.1x). La N3IWF 204 también puede incluir un transceptor de RF móvil 1808 acorde a una interfaz aérea celular. El UE 200 puede comunicarse con la N3IWF 204 usando uno o más del transceptor de WLAN 1806 o el transceptor de RF móvil 1808.

[00149] En una modalidad, el dispositivo de procesamiento está configurado para recibir la solicitud de asociación de seguridad (SA) IPsec del UE 200 a través de la red de acceso no 3GPP no confiable y realizar un protocolo de autenticación del UE 200 en la red de acceso no 3GPP no confiable, tal como el protocolo de IKE. La N3IWF 204 puede entonces obtener una respuesta a la autenticación que indique que la red central no acepta la solicitud de SA IPsec. La N3IWF 204 puede generar entonces una respuesta a la autenticación para el UE 200, donde la respuesta a la autenticación indica el rechazo del acceso del UE 200 a la red central a través de la red de acceso no

confiable.

[00150] Un dispositivo de procesamiento como se describe en este documento incluye al menos un dispositivo de procesamiento, como un microprocesador, un microcontrolador, un procesador de señales digitales, una microcomputadora, una unidad central de procesamiento, una matriz de puertas programables in situ, 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) basándose en la codificación rígida de los circuitos y/o en 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 una pluralidad de 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 transitoria que almacene información digital. El término «módulo» se usa en la descripción de una o más de las modalidades de los elementos en el presente. Un módulo incluye uno o más dispositivos de procesamiento y/o uno o más dispositivos de memoria no transitoria que se puedan utilizar para realizar una o más funciones como se describan en este documento. 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 el presente, un módulo puede contener uno o más submódulos, cada uno de los cuales puede ser uno o más módulos.

[00151] Como se pueden usar en este documento, los términos «que se puede utilizar para» o «configurable para» indican que un elemento incluye uno o más de los circuitos, las instrucciones, los módulos, los datos, las entradas, los productos, etc., para realizar una o más de las funciones correspondientes descritas o necesarias y puede incluir además el acoplamiento inferido a uno o más elementos adicionales para realizar las funciones correspondientes descritas o necesarias. Como también se pueden utilizar en este documento, 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 directos entre nodos/dispositivos y/o una conexión indirecta entre nodos/dispositivos a través de un elemento intermedio (por ejemplo, un elemento incluye, sin limitación, un componente, elemento, circuito, módulo, nodo, dispositivo, elemento de red, etc.). Como puede usarse adicionalmente en el presente documento, 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».

[00152] Nótese que los aspectos de la presente divulgación pueden describirse en el presente documento 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. 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.

[00153] Las diversas características de la divulgación descrita en este documento se pueden implementar en diferentes sistemas y dispositivos sin apartarse de la divulgación. Cabe señalar que los aspectos anteriores de la divulgación son meramente ejemplos y no deben interpretarse como limitantes de la divulgación. Se pretende que la descripción de los aspectos de la presente divulgación sea ilustrativa y no limitar el alcance de las reivindicaciones. De esta forma, las presentes enseñanzas se pueden aplicar fácilmente a otros tipos de aparatos y muchas alternativas, modificaciones y variaciones serán evidentes para los expertos en la técnica.

[00154] 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 ilustrativas, en lugar de restrictivas, y se pretende que las modificaciones se incluyan dentro del alcance de la presente invención. 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 aparato pueden ensamblarse o configurarse operativamente de otro modo en una variedad de permutaciones y, por lo tanto, no están limitados a la configuración específica mencionada en las reivindicaciones.

[00155] 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 dé lugar a cualquier beneficio, ventaja o solución particulares o que se produzca o se vuelva más pronunciado no debe interpretarse como una característica o un componentes críticos, requeridos o esenciales de ninguna ni de todas las reivindicaciones.

[00156] Como se usan en el presente, se pretende que los términos «comprenden», «comprende», «que comprende», «que tiene», «que incluye», «incluye» o cualquier otra variación de estos hagan referencia a una inclusión no exclusiva, de forma tal que un proceso, método, artículo o aparato que comprenda una lista de elementos no incluya únicamente los elementos mencionados, 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, las disposiciones, las aplicaciones, las proporciones, los elementos, los materiales o los componentes descritos anteriormente que se utilizan en la práctica de la presente invención, además de los que no se mencionan específicamente, pueden variarse o adaptarse particularmente a entornos específicos, especificaciones de fabricación, parámetros de diseño u otros requisitos operativos, sin apartarse de sus principios generales.

[00157] Además, la referencia a un elemento en singular no se pretende con el significado de «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 descritos en toda la presente descripción que los expertos en la técnica conozcan actual o posteriormente se incorporan expresamente al

presente mediante esta referencia y se pretenden que queden comprendidos en las reivindicaciones. Además, no se pretende que nada de lo descrito en el presente esté dirigido al público, independientemente de que tal divulgación esté explícitamente citada 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 usando la frase «medio para» o, en el caso de una reivindicación de método, que el elemento se recite utilizando la frase «paso para»