

SISTEMAS Y MÉTODO PARA ACTUALIZACIONES SEGURAS DE CONFIGURACIÓN DE PARÁMETROS PROVISIONADOS EN EQUIPO DE USUARIO

SOLICITUDES RELACIONADAS

5 Esta solicitud de patente no provisional reivindica la prioridad para la Solicitud de Patente Provisional de Estados Unidos No. 62/742,341 presentada el 6 de octubre de 2018, la cual se incorpora como referencia como si estuviera completamente proporcionada en la presente.

CAMPO DE LA INVENCION

10 Esta descripción está relacionada con el campo de los sistemas de comunicación y, en particular, con la actualización de dispositivos móviles.

ANTECEDENTES DE LA INVENCION

15 Los operadores o proveedores de servicios implementan redes móviles para ofrecer numerosos servicios de voz y datos a los usuarios finales de teléfonos móviles u otros dispositivos/terminales móviles, a los que generalmente se hace referencia como Equipo de Usuario (UE). Algunos ejemplos de los servicios de voz son llamadas de voz, transferencia de llamadas, llamada en espera, etc. Algunos ejemplos de los servicios de datos son acceso a
20 Internet, transmisión de audio, transmisión de video, juegos en línea, televisión de Protocolo de Internet (IP-TV), etc. Una red móvil es un tipo de red donde el último enlace al usuario final es inalámbrico. Una red móvil incluye generalmente una red central y una o más Redes de Acceso de Radio (RAN) que intercambian señalización y datos con los UE a través de una interfaz de radio.

25 Un UE está típicamente aprovisionado con la Identidad Internacional del Suscriptor Móvil (IMSI) del suscriptor, autenticación de seguridad, información de cifrado, y otros parámetros de configuración. Puede haber casos donde la red doméstica del UE necesite actualizar uno o más de los parámetros de configuración en un UE. Por ejemplo, la red doméstica del UE puede actualizar los parámetros de configuración cuando ocurre un cambio
30 de suscripción, cuando hay una nueva asignación de servicio, cuando las redes móviles migran de Evolución a Largo Plazo (LTE) a redes de próxima generación, etc. Por lo tanto, es

beneficioso identificar procedimientos mejorados para actualizar parámetros de configuración en un UE.

BREVE DESCRIPCIÓN DE LA INVENCION

5 Las modalidades descritas en la presente proporcionan actualizaciones a los parámetros de configuración de UE usando mensajes de Estrato Sin Acceso (NAS). Como resumen, las redes móviles que migran a redes de próxima generación pueden incluir una Gestión de Datos Unificada (UDM) y una Función de Gestión de Acceso y Movilidad (AMF). La UDM, que está en la red doméstica de un UE, está configurada para ensamblar una
10 actualización de parámetros de configuración de UE para un UE con protección de seguridad (por ejemplo, un paquete seguro, protección de integridad, etc.). La UDM envía la actualización de parámetros de configuración de UE, con protección de seguridad, a la AMF. La AMF, a su vez, está configurada para enviar de forma transparente la actualización de parámetros de configuración de UE al UE usando un mensaje de NAS. Nuevamente, la actualización de
15 parámetros de configuración de UE tiene protección de seguridad en el mensaje de NAS. Tras la recepción del mensaje de NAS, el UE está configurado para actualizar sus parámetros de configuración de UE con base en la actualización proporcionada en el mensaje de NAS. Un beneficio técnico de este procedimiento es que se proporciona seguridad de un extremo a otro para la actualización de parámetros de configuración de UE. Otro beneficio técnico es que se
20 pueden usar las funcionalidades del plano de control nativo para actualizar los parámetros de configuración de UE. Por lo tanto, no es necesario desplegar un elemento de red especializado para proporcionar las actualizaciones para los UE.

Una modalidad comprende un elemento de AMF de una red móvil. El elemento de AMF incluye un procesador o procesadores y una memoria que incluye un código de programa
25 informático ejecutable por el procesador. El procesador está configurado para hacer que el elemento de AMF reciba un mensaje de plano de control de un elemento de UDM que incluye una actualización de parámetros de configuración de UE para un UE. La actualización de parámetros de configuración de UE tiene protección de seguridad de acuerdo con un mecanismo de protección. El procesador está configurado además para hacer que el elemento
30 de AMF inserte la actualización de parámetros de configuración de UE que tiene protección de seguridad en un contenedor de un primer mensaje de NAS, donde el contenedor está designado

para la actualización de parámetros de configuración de UE. El procesador está configurado además para hacer que el elemento de AMF envíe el primer mensaje de NAS al UE con el contenedor que incluye la actualización de parámetros de configuración de UE que tiene protección de seguridad.

5 En otra modalidad, la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro de acuerdo con el mecanismo de protección.

En otra modalidad, la actualización de parámetros de configuración de UE tiene protección de integridad usando un contexto de seguridad de NAS del UE de acuerdo con el mecanismo de protección.

10 En otra modalidad, la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro, y el paquete seguro tiene protección de integridad usando un contexto de seguridad de NAS del UE de acuerdo con el mecanismo de protección.

En otra modalidad, el primer mensaje de NAS comprende un mensaje de aceptación de registro de NAS enviado al UE durante un procedimiento de registro de NAS. El procesador está configurado además para hacer que el elemento de AMF reciba un segundo mensaje de NAS del UE durante el procedimiento de registro de NAS con un contenedor que incluye un reconocimiento de UE de que se recibió la actualización de parámetros de configuración de UE, y envíe otro mensaje de plano de control al elemento de UDM con el reconocimiento de UE. El segundo mensaje de NAS recibido del UE puede comprender un mensaje completo de registro de NAS o un mensaje de Transporte de NAS de Enlace Ascendente.

15 En otra modalidad, el primer mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Descendente de un procedimiento de transporte de NAS realizado después de un procedimiento de registro de NAS. El procesador está configurado además para hacer que el elemento de AMF reciba un segundo mensaje de NAS del UE con un contenedor que incluye un reconocimiento de UE del UE de que se recibió la actualización de parámetros de configuración de UE, y envíe otro mensaje de plano de control al elemento de UDM con el reconocimiento de UE. El segundo mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Ascendente.

20 Otra modalidad comprende un método para realizar un procedimiento de actualización para actualizar los parámetros de configuración de UE provisionados en un UE.

25 En otra modalidad, el primer mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Descendente de un procedimiento de transporte de NAS realizado después de un procedimiento de registro de NAS. El procesador está configurado además para hacer que el elemento de AMF reciba un segundo mensaje de NAS del UE con un contenedor que incluye un reconocimiento de UE del UE de que se recibió la actualización de parámetros de configuración de UE, y envíe otro mensaje de plano de control al elemento de UDM con el reconocimiento de UE. El segundo mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Ascendente.

30 Otra modalidad comprende un método para realizar un procedimiento de actualización para actualizar los parámetros de configuración de UE provisionados en un UE.

El método comprende recibir un mensaje de plano de control en un elemento de AMF de un elemento de UDM que incluye una actualización de parámetros de configuración de UE para el UE. La actualización de parámetros de configuración de UE tiene protección de seguridad de acuerdo con un mecanismo de protección. El método comprende además insertar, en el
5 elemento de AMF, la actualización de parámetros de configuración de UE que tiene protección de seguridad en un contenedor de un primer mensaje de NAS, donde el contenedor está designado para la actualización de parámetros de configuración de UE. El método comprende además enviar el primer mensaje de NAS desde el elemento de AMF al UE con el contenedor que incluye la actualización de parámetros de configuración de UE que tiene protección de
10 seguridad.

En otra modalidad, la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro de acuerdo con el mecanismo de protección.

En otra modalidad, la actualización de parámetros de configuración de UE tiene protección de integridad usando un contexto de seguridad de NAS del UE de acuerdo con el
15 mecanismo de protección.

En otra modalidad, la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro, y el paquete seguro tiene protección de integridad usando un contexto de seguridad de NAS del UE de acuerdo con el mecanismo de protección.

En otra modalidad, el primer mensaje de NAS comprende un mensaje de
20 aceptación de registro de NAS enviado desde el elemento de AMF al UE durante un procedimiento de registro de NAS.

En otra modalidad, el método comprende además recibir un segundo mensaje de NAS en el elemento de AMF desde el UE durante el procedimiento de registro de NAS con un contenedor que incluye un reconocimiento de UE de que se recibió la actualización de
25 parámetro de configuración de UE, y enviar otro mensaje de plano de control desde el elemento de AMF al elemento de UDM con el reconocimiento de UE. El segundo mensaje de NAS puede comprender un mensaje completo de registro de NAS o un mensaje de Transporte de NAS de Enlace Ascendente.

En otra modalidad, el primer mensaje de NAS comprende un mensaje de
30 Transporte de NAS de Enlace Descendente de un procedimiento de transporte de NAS realizado después de un procedimiento de registro de NAS.

En otra modalidad, el método comprende además recibir un segundo mensaje de NAS en el elemento de AMF desde el UE con un contenedor que incluye un reconocimiento de UE del UE de que se recibió la actualización de parámetros de configuración de UE, y enviar otro mensaje de plano de control desde el elemento de AMF al elemento de UDM con el reconocimiento de UE. El segundo mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Ascendente.

En otra modalidad, el método comprende además recibir el primer mensaje de NAS en el UE desde el elemento de AMF que tiene el contenedor que incluye la actualización de parámetros de configuración de UE para el UE que tiene protección de seguridad, realizar una comprobación de seguridad en el UE para verificar la actualización de parámetros de configuración de UE y actualizar uno o más de los parámetros de configuración de UE con base en la actualización de parámetros de configuración de UE cuando se verifica la actualización de parámetros de configuración de UE.

En otra modalidad, cuando el primer mensaje de NAS incluye un indicador de nuevo registro, el método comprende además iniciar un procedimiento de registro de NAS en el UE para el nuevo registro usando los parámetros de configuración de UE actualizados.

Otra modalidad comprende un UE que incluye una Tarjeta Universal de Circuito Integrado (UICC) que aloja un Módulo Universal de Identidad del Suscriptor (USIM), un procesador, y una memoria que incluye código de programa informático ejecutable por el procesador. Uno o ambos de la UICC y la memoria almacena los parámetros de configuración de UE para el UE. El procesador está configurado para hacer que el UE reciba un primer mensaje de NAS desde un elemento de AMF que tiene un contenedor que incluye una actualización de parámetros de configuración de UE para el UE que tiene protección de seguridad de acuerdo con un mecanismo de protección. La UICC y/o el procesador están configurados para hacer que el UE realice una comprobación de seguridad para verificar la actualización de parámetros de configuración de UE, y actualizar uno o más de los parámetros de configuración de UE con base en la actualización de parámetros de configuración de UE cuando la actualización de parámetros de configuración de UE está verificada.

En otra modalidad, la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro dentro del contenedor del primer mensaje de NAS.

En otra modalidad, la actualización de parámetros de configuración de UE tiene

protección de integridad usando un contexto de seguridad de NAS del UE.

En otra modalidad, la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro dentro del contenedor del primer mensaje de NAS, y el paquete seguro tiene protección de integridad usando un contexto de seguridad de NAS del UE.

En otra modalidad, el primer mensaje de NAS comprende un mensaje de aceptación de registro de NAS enviado al UE durante un procedimiento de registro de NAS.

En otra modalidad, cuando el mensaje de aceptación de registro de NAS incluye un indicador de reconocimiento de UE, el procesador está configurado además para hacer que el UE envíe un segundo mensaje de NAS al elemento de AMF con un contenedor que incluye un reconocimiento de UE de que se recibió la actualización de parámetros de configuración de UE. El segundo mensaje de NAS puede comprender un mensaje completo de registro de NAS o un mensaje de Transporte de NAS de Enlace Ascendente.

En otra modalidad, el primer mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Descendente de un procedimiento de transporte de NAS realizado después de un procedimiento de registro de NAS.

En otra modalidad, cuando el mensaje de Transporte de NAS de Enlace Descendente incluye un indicador de reconocimiento de UE, el procesador está configurado además para hacer que el UE envíe un mensaje de Transporte de NAS de Enlace Ascendente al elemento de AMF con un contenedor que incluye un reconocimiento de UE del UE de que se recibió la actualización de parámetros de configuración de UE.

En otra modalidad, cuando el primer mensaje de NAS incluye un indicador de nuevo registro, el procesador está configurado además para hacer que el UE inicie un procedimiento de registro de NAS para el nuevo registro usando los parámetros de configuración de UE actualizados.

Otra modalidad comprende un elemento de AMF que incluye un medio para recibir un mensaje de plano de control desde un elemento de UDM que incluye una actualización de parámetros de configuración de UE para un UE. La actualización de parámetros de configuración de UE tiene protección de seguridad de acuerdo con un mecanismo de protección. El elemento de AMF además incluye un medio para insertar la actualización de parámetros de configuración de UE que tiene protección de seguridad en un contenedor de un

primer mensaje de NAS, y un medio para enviar el primer mensaje de NAS al UE con el contenedor que incluye la actualización de parámetros de configuración de UE que tiene protección de seguridad.

Otra modalidad comprende un UE que incluye un medio para almacenar parámetros de configuración de UE para el UE. El UE incluye además un medio para recibir un primer mensaje de NAS desde un elemento de AMF que tiene un contenedor que incluye una actualización de parámetros de configuración de UE para el UE que tiene protección de seguridad de acuerdo con un mecanismo de protección, un medio para realizar una comprobación de seguridad para verificar la actualización de parámetros de configuración de UE, y un medio para actualizar uno o más de los parámetros de configuración de UE con base en la actualización de parámetros de configuración de UE cuando se verifica la actualización de parámetros de configuración de UE.

La breve descripción anterior proporciona una comprensión básica de algunos aspectos de la especificación. Esta breve descripción no es una descripción general extensa de la especificación. No se pretende identificar elementos clave o críticos de la especificación ni delinear ningún alcance de las modalidades particulares de la especificación, o cualquier alcance de las reivindicaciones. Su único propósito es presentar algunos conceptos de la especificación en una forma simplificada como preludio a la descripción más detallada que se presenta más adelante.

BREVE DESCRIPCIÓN DE LAS FIGURAS

Algunas modalidades de la invención se describen ahora, sólo a modo de ejemplo, y con referencia a las figuras acompañantes. El mismo número de referencia representa el mismo elemento o el mismo tipo de elemento en todas las figuras.

La FIG. 1 ilustra una red móvil en una modalidad ilustrativa.

La FIG. 2 ilustra una red de Núcleo de Paquetes Evolucionado (EPC).

La FIG. 3 ilustra una arquitectura no itinerante de una red de próxima generación.

La FIG. 4 ilustra una arquitectura itinerante de una red de próxima generación.

La FIG. 5 ilustra una pila de protocolos de radio.

La FIG. 6 es un diagrama de bloques de un UE en una modalidad ilustrativa.

La FIG. 7 es un modelo funcional para un UE en una modalidad ilustrativa.

La FIG. 8 es un diagrama de bloques de un elemento de AMF en una modalidad ilustrativa.

La FIG. 9 es un diagrama de bloques de un elemento de UDM en una modalidad ilustrativa.

5 La FIG. 10 es un diagrama de flujo que ilustra un método para realizar un procedimiento de actualización en un elemento de UDM en una modalidad ilustrativa.

La FIG. 11 es un diagrama de flujo que ilustra un método para realizar un procedimiento de actualización en un elemento de AMF en una modalidad ilustrativa.

10 La FIG. 12 es un diagrama de flujo que ilustra un método para realizar un procedimiento de actualización en un UE en una modalidad ilustrativa.

La FIG. 13 es un diagrama de mensaje que ilustra un procedimiento de actualización durante el registro en una modalidad ilustrativa.

La FIG. 14 es un diagrama de mensaje que ilustra un procedimiento de actualización después del registro en una modalidad ilustrativa.

15 La FIG. 15 es un diagrama de mensaje que ilustra un procedimiento de actualización durante el registro en una modalidad ilustrativa.

La FIG. 16 es un diagrama de mensaje que ilustra un procedimiento de actualización después del registro en una modalidad ilustrativa.

20 La FIG. 17 es un diagrama de mensaje que ilustra un procedimiento de actualización durante el registro en una modalidad ilustrativa.

La FIG. 18 es un diagrama de mensaje que ilustra un procedimiento de actualización después del registro en una modalidad ilustrativa.

DESCRIPCIÓN DETALLADA DE LA INVENCION

25 Las figuras y la siguiente descripción ilustran modalidades ejemplares específicas. Por lo tanto, se apreciará que los expertos en la técnica podrán idear diverso arreglos que, aunque no se describen o muestran explícitamente en la presente, incorporan los principios de las modalidades y están incluidos dentro del alcance de las modalidades. Además, cualquier ejemplo descrito en la presente está destinado a ayudar a comprender los principios de las modalidades, y debe interpretarse sin limitación a los ejemplos y condiciones citados
30 específicamente. Como resultado, el(los) concepto(s) de la invención no se limita(n) a las

modalidades o ejemplos específicos que se describen a continuación, sino a las reivindicaciones y sus equivalentes.

La FIG. 1 ilustra una red móvil 100 en una modalidad ilustrativa. La red móvil 100 (también referida como una red celular) es un tipo de red donde el último enlace es inalámbrico, y proporciona servicios de voz y/o datos a una pluralidad de dispositivos. La red móvil 100 puede ser una red de Tercera Generación (3G), Cuarta Generación (4G) y/o próxima generación (por ejemplo, Quinta Generación (5G)).

La red móvil 100 se ilustra proporcionando servicios de comunicación a los UE 110 (junto con otros UE no mostrados). Los UE 110 pueden habilitarse para servicios de voz, servicios de datos, servicios de Máquina a Máquina (M2M) o Comunicaciones de Tipo de Máquina (MTC), servicios de Internet de las Cosas (IoT) y/u otros servicios. Un UE 110 puede ser un dispositivo de usuario final tal como un teléfono móvil (por ejemplo, teléfono inteligente), una tableta o PDA, una computadora con un adaptador de banda ancha móvil, etc.

La red móvil 100 incluye una o más Redes de Acceso de Radio (RAN) 120 que se comunican con los UE 110 a través de una interfaz de radio 122. La RAN 120 puede soportar el acceso a la Red de Acceso de Radio Terrestre de UMTS Evolucionado (E-UTRAN), acceso a la Red de Área Local Inalámbrica (WLAN), acceso fijo, acceso de radio por satélite, nuevas Tecnologías de Acceso de Radio (RAT), etc. Como ejemplo, la RAN 120 puede comprender una E-UTRAN o una RAN de Próxima Generación (NG-RAN) que incluye una o más estaciones base 124 que están dispersas en un área geográfica. Una estación base 124 puede comprender una entidad que usa tecnología de comunicación por radio para comunicarse con un UE en el espectro autorizado e interconectar el UE con una red central. Las estaciones base 124 en una E-UTRAN son referidas como NodosBs evolucionado (eNodeB). Las estaciones base 124 en una NG-RAN son referidas como gNodosBs (estaciones base de NR) y/o ng-eNodeB (estaciones base de LTE que soportan una Red Central 5G). Como otro ejemplo, la RAN 120 puede comprender una WLAN que incluye uno o más Puntos de Acceso Inalámbricos (WAP) 125. Una WLAN es una red en la que un UE puede conectarse a una Red de Área Local (LAN) a través de una conexión (radio) inalámbrica. Un WAP 125 es un nodo que usa tecnología de comunicación por radio para comunicarse con un UE a través del espectro no autorizado y proporciona el acceso a UE a una red central. Un ejemplo de WAP 125 es un punto de acceso WiFi que opera en las bandas de radio de 2.4 GHz o 5 GHz. El término “estación base” como

se usa en la presente puede referirse a un eNodoB, un gNodoB, un ng-eNodoB, un WAP, etc.

Los UE 110 pueden conectarse a la celda 126 de la RAN 120 para acceder a una red central 130. Por lo tanto, la RAN 120 representa la interfaz de radio entre los UE 110 y red central 130. La red central 130 es la parte central de la red móvil 100 que proporciona varios servicios a los clientes que están conectados por RAN 120. Un ejemplo de la red central 130 es la red de Núcleo de Paquetes Evolucionado (EPC) como lo sugiere el 3GPP para LTE. Otro ejemplo de red central 130 es una red central 5G como lo sugiere el 3GPP. La red central 130 incluye elementos de red 132, que pueden comprender servidores, dispositivos, aparatos o equipos (incluyendo hardware) que proporcionan servicios para los UE 110. Los elementos de red 132, en una red de EPC, pueden comprender una Entidad de Gestión de Movilidad (MME), una Puerta de Enlace de Servicio (S-GW), una Puerta de Enlace de Red de Paquetes de Datos (P-GW), etc. Los elementos de red 132, en una red 5G, pueden comprender una Función de Gestión de Acceso y Movilidad (AMF), una Función de Gestión de Sesión (SMF), una Función de Control de Políticas (PCF), una Función de Aplicación (AF), una Función de Plano de Usuario (UPF), etc.

La FIG. 2 ilustra una red de Núcleo de Paquetes Evolucionado (EPC) 200, que es la red central para LTE. La red EPC 200 incluye una Entidad de Gestión de Movilidad (MME) 214, una Puerta de Enlace de Servicio (S-GW) 215, una Puerta de Enlace de Red de Paquetes de Datos (P-GW) 216, un Servidor de Suscriptor Local (HSS) 217, y una Función de Reglas de Políticas y Cargos (PCRF) 218, pero puede incluir otros elementos no mostrados, tales como Servidores de Aplicaciones de Subsistema Multimedia IP (IMS). Dentro de la red EPC 200, los datos de usuario (también referidos como el “plano de usuario”) y la señalización (también referida como el “plano de control”) están separados. La MME 214 maneja el plano de control dentro de la red EPC 200. Por ejemplo, la MME 214 maneja la señalización relacionada con la movilidad y la seguridad para el acceso a E-UTRAN. La MME 214 es responsable de rastrear y localizar al UE 110 en modo inactivo. La S-GW 215 y P-GW 216 manejan el plano de usuario. La S-GW 215 y P-GW 216 transportan el tráfico de datos entre el UE 110 y redes de datos externas 240 (DN o Red de Paquetes de Datos (PDN)). La S-GW 215 es el punto de interconexión entre el lado de radio y la red EPC 200, y sirve al UE 110 enrutando los paquetes IP entrantes y salientes. La S-GW 215 también es el punto de anclaje para la movilidad intra-LTE (es decir, en caso de traspaso entre eNodoB), y entre LTE y otros accesos de 3GPP. La

P-GW 216 es el punto de interconexión entre la red EPC 200 y redes de datos externas 240 (es decir, el punto de entrada o salida de la red de datos 240) y enruta los paquetes hacia y desde la red de datos 240. La HSS 217 es una base de datos que almacena información relacionada con el usuario y relacionada con el suscriptor. La PCRF 218 proporciona una solución de Control de Políticas y Cargos (PCC) en la red EPC 200, y es un nodo o entidad de red EPC 200 que formula reglas de PCC para los servicios solicitados por un usuario final.

La MME 214 se conecta a la RAN 120 (es decir, eNodoB) a través de la interfaz S1-MME, y la S-GW 215 se conecta a la RAN 120 a través de la interfaz S1-U. La MME 214 se conecta a la S-GW 215 a través de la interfaz S11 y se conecta a la HSS 217 a través de la interfaz S6a. La PCRF 218 se conecta a la P-GW 216 a través de la interfaz Gx, que proporciona la transferencia de reglas de políticas y cargos de PCRF 218 a una Función de Aplicación de Políticas y Cargos (PCEF) en la P-GW 216. La PCRF 218 se conecta a la S-GW 215 a través de la interfaz Gxx y la S-GW 215 se conecta a la P-GW 216 a través de la interfaz S5.

La FIG. 3 ilustra una arquitectura no itinerante 300 de una red de próxima generación. La arquitectura en la FIG. 3 es una representación de punto de referencia, como se describe adicionalmente en 3GPP TS 23.501 (v15.3.0), que se incorpora como referencia como si estuviera completamente incluido en la presente. La arquitectura 300 está comprendida de Funciones de Red (NF) para una red central, y las funciones de red para el plano de control están separadas del plano de usuario. El plano de control de la red central incluye una Función de Servidor de Autenticación (AUSF) 310, una Gestión de Datos Unificada (UDM) 312, una Función de Selección de Segmentos de Red (NSSF) 313, una Función de Gestión de Acceso y Movilidad (AMF) 314, una Función de Gestión de Sesión (SMF) 316, una Función de Control de Políticas (PCF) 318, y una Función de Aplicación (AF) 320. El plano de usuario de la red central incluye una o más Funciones de Plano de Usuario (UPF) 324 que se comunican con la red de datos 240. El UE 110 puede acceder al plano de control y al plano de usuario de la red central a través de la (R)AN 120.

La AUSF 310 está configurada para soportar la autenticación del UE 110. La UDM 312 está configurada para almacenar datos/información de suscripción del UE 110. La UDM 312 puede almacenar tres tipos de datos de usuario: suscripción, política y contexto relacionado con la sesión (por ejemplo, ubicación del UE). La AMF 314 está configurada para proporcionar autenticación, autorización, gestión de movilidad, etc. basada en UE. La SMF 316 está

configurada para proporcionar la siguiente funcionalidad: gestión de sesiones (SM), asignación y gestión de direcciones de Protocolo de Internet (IP) de UE, selección y control de UPF(s), terminación de interfaces hacia la PCF 318, parte de control de aplicación de políticas y Calidad de Servicio (QoS), intercepción legal, terminación de partes SM de mensajes de NAS, Notificación de Datos de Enlace Descendente (DNN), funcionalidad itinerante, manejo de aplicación local para aplicar QoS para Acuerdos de Nivel de Servicio (SLA), interfaz de cargos y recopilación de datos de cargos, etc. Si el UE 110 tiene múltiples sesiones, se pueden asignar diferentes SMF a cada sesión para administrarlas de manera individual y posiblemente proporcionar diferentes funcionalidades por sesión. La PCF 318 está configurada para soportar un marco de políticas unificado para gobernar el comportamiento de la red y proporcionar reglas de políticas para controlar las funciones del plano para la aplicación de QoS, cargos, control de acceso, enrutamiento del tráfico, etc. La AF 320 proporciona información sobre un flujo de paquetes a la PCF 318. Con base en la información, la PCF 318 está configurada para determinar reglas de política sobre gestión de sesiones y movilidad para hacer que la AMF 314 y SMF 316 funcionen correctamente.

La UPF 324 soporta varias operaciones y funcionalidades del plano de usuario, tales como enrutamiento y reenvío de paquetes, manejo del tráfico (por ejemplo, aplicación de QoS), un punto de anclaje para la movilidad Intra-RAT/Inter-RAT (cuando aplique), aplicación de reglas de política e inspección de paquetes, intercepción legal (recopilación de UP), reporte y contabilidad de tráfico, etc. La red de datos 240 no es parte de la red central y proporciona acceso a Internet, servicios de operador, servicios de terceros, etc. Por ejemplo, la Unión Internacional de Telecomunicaciones (ITU) ha clasificado los servicios de redes móviles 5G en tres categorías: Banda Ancha Móvil Mejorada (eMBB), Comunicaciones Ultra Fiables y de Baja Latencia (uRLLC) y Comunicaciones de Tipo Máquina Masiva (mMTC) o Internet de las Cosas Masiva (MIoT). La eMBB se enfoca en servicios que tienen altos requisitos de ancho de banda, tales como videos HD, Realidad Virtual (VR) y Realidad Aumentada (AR). La uRLLC se enfoca en servicios sensibles a la latencia, tal como la gestión remota y conducción automatizada. Las mMTC y MIoT se enfocan en servicios que incluyen altos requisitos de densidad de conexión, tales como ciudad inteligente y agricultura inteligente. La red de datos 240 puede configurarse para proporcionar estos y otros servicios.

La arquitectura 300 incluye los siguientes puntos de referencia. El punto de

referencia N1 se implementa entre el UE 110 y AMF 314. El punto de referencia N2 se implementa entre (R)AN 120 y AMF 314. El punto de referencia N3 se implementa entre (R)AN 120 y UPF 324. El punto de referencia N4 se implementa entre la SMF 316 y UPF 324. El punto de referencia N5 se implementa entre la PCF 318 y AF 320. El punto de referencia N6 se implementa entre UPF 324 y red de datos 240. El punto de referencia N7 se implementa entre SMF 316 y PCF 318. El punto de referencia N8 se implementa entre UDM 312 y AMF 314. El punto de referencia N9 se implementa entre dos UPF 324. El punto de referencia N10 se implementa entre UDM 312 y SMF 316. El punto de referencia N11 se implementa entre AMF 314 y SMF 316. El punto de referencia N12 se implementa entre AMF 314 y AUSF 310. El punto de referencia N13 se implementa entre UDM 312 y AUSF 310. El punto de referencia N14 se implementa entre dos AMF. El punto de referencia N15 se implementa entre PCF 318 y AMF 314 en el caso de un escenario no itinerante. El punto de referencia N22 se implementa entre NSSF 313 y AMF 314.

La FIG. 4 ilustra una arquitectura itinerante 400 de una red de próxima generación. La arquitectura en la FIG. 4 es un escenario de ruptura local en representación de punto de referencia, como se describe adicionalmente en 3GPP TS 23.501 (v15.30.0). En un escenario itinerante, se muestran una Red Móvil Terrestre Pública Visitada (VPLMN) 402 y una PLMN Doméstica (HPLMN) 404. Una HPLMN 404 identifica la PLMN en la que se mantiene el perfil de un suscriptor móvil. Una VPLMN es una PLMN por la que el suscriptor móvil se ha desplazado al dejar su HPLMN. Los usuarios que se desplacen a otras redes recibirán información de suscripción de la HPLMN 404. En un escenario de ruptura local, la PCF 318 (hPCF), UDM 312 y AUSF 310 están en la HPLMN 404 para UE 110. Las otras funciones de red, incluyendo una PCF visitada (vPCF) 418, están en la VPLMN 402.

La FIG. 5 ilustra una pila de protocolos de radio 500, tal como para la interfaz de radio 122. Como se describe en la presente, el plano de usuario 512 comprende un conjunto de protocolos usados para transferir los datos de usuario reales a través de una red, y el plano de control 514 comprende protocolos usados para controlar y establecer las conexiones de usuarios y portadores dentro de la red. Para el plano de usuario 512 y el plano de control 514, la pila de protocolo de radio 500 incluye la capa física (PHY) 501, la capa de Control de Acceso al Medio (MAC) 502, la capa de Control de Enlace de Radio (RLC) 503 y la capa de Protocolo de Convergencia de Paquetes de Datos (PDCP) 504. El plano de control 514 incluye

adicionalmente la capa de Control de Recursos de Radio (RRC) 505 y la capa de Estrato Sin Acceso (NAS) 506.

La capa física 501 porta toda la información de los canales de transporte de MAC sobre la interfaz de radio. Los datos y mensajes de señalización se transportan por canales físicos entre los diferentes niveles de la capa física 501. Los canales físicos se dividen en canales de datos físicos y canales de control físicos. Los canales de datos físicos pueden incluir el Canal Físico Compartido de Enlace Descendente (PDSCH), el Canal Físico de Transmisión (PBCH), el Canal Físico de Multidifusión (PMCH), el Canal Físico Compartido de Enlace Ascendente (PUSCH) y el Canal Físico de Acceso Aleatorio (PRACH). Los canales de control físicos pueden incluir el Canal Físico Indicador de Formato de Control (PCFICH), el Canal Físico Indicador de ARQ Híbrido (PHICH), el Canal Físico de Control de Enlace Descendente (PDCCH) y el Canal Físico de Control de Enlace Ascendente (PUCCH).

La capa de MAC 502 es responsable del mapeo entre canales lógicos y canales de transporte, multiplexión de Unidades de Datos de Servicio (SDU) de MAC desde uno o diferentes canales lógicos en bloques de transporte (TB) para ser suministrados a la capa física en los canales de transporte, desmultiplexión de SDU de MAC desde uno o diferentes canales lógicos de bloques de transporte suministrados desde la capa física en los canales de transporte, programación de reportes de información, corrección de errores a través de Solicitud de Repetición Automática Híbrida (HARQ), manejo de prioridad entre los UE por medio de programación dinámica, manejo de prioridad entre canales lógicos de un UE, priorización de canal lógico. La capa de RLC 503 es responsable de la transferencia de las Unidades de Datos de Protocolo (PDU) de capa superior, corrección de errores a través de ARQ, y concatenación, segmentación y reensamblaje de SDU de RLC. La capa de RLC 503 también es responsable de la resegmentación de las PDU de datos de RLC, reordenamiento de las PDU de datos de RLC, detección de duplicados, descarte de SDU de RLC, restablecimiento de RLC y detección de errores de protocolo. La capa de PDCP 504 es responsable de la compresión y descompresión de encabezado de datos de IP, transferencia de datos (plano de usuario o plano de control), mantenimiento de Números de Secuencia (SN) de PDCP, suministro en secuencia de PDU de capa superior en el restablecimiento de capas inferiores, eliminación de duplicado de SDU de capa inferior en el restablecimiento de capas inferiores para portadoras de radio mapeadas en el Modo Reconocido (AM) de RL, cifrado y descifrado de datos del plano de

usuario y datos del plano de control, protección de integridad y verificación de integridad de los datos del plano de control, descarte basado en temporizador, descarte de duplicado, etc. La capa de RRC 505 es responsable de la difusión de Información del Sistema relacionada con el NAS, difusión de Información del Sistema relacionada con el Estrato de Acceso (AS),
5 paginación, establecimiento, mantenimiento, y liberación de una conexión de RRC entre el UE y la RAN, funciones de seguridad incluyendo la gestión de claves, establecimiento, configuración, mantenimiento, y liberación de Portadores de Radio (RB) de punto a punto. La capa de NAS 506 representa el estrato más alto del plano de control 514 entre el UE y la red central (por ejemplo, MME/AMF), y soporta la movilidad del UE y los procedimientos de gestión
10 de sesión para establecer y mantener la conectividad de IP entre el UE y la red central.

Cada UE 110 que recibe servicios de una red móvil está provisto de parámetros de configuración. La red doméstica (es decir, HPLMN) puede querer actualizar uno o más de los parámetros de configuración en un UE. En redes móviles anteriores, la actualización de parámetros de configuración se realizaba con un mecanismo Por Aire (OTA). El mecanismo de
15 OTA requirió el despliegue de un elemento de red especializado llamado una Puerta de Enlace de OTA. Cuando se realizó una actualización de parámetros de configuración, la red del sistema de servicios de fondo del operador envió solicitudes de servicio a la Puerta de Enlace de OTA. Diferentes “portadores” de OTA se especificaron para enviar la solicitud de servicio al UE, tales como Servicios de Mensajes Cortos (SMS), Datos de Servicios Suplementarios No Estructurados (USSD), Protocolo de Transferencia de Hipertexto (HTTP), etc. La Puerta de
20 Enlace de OTA mapeó las solicitudes de servicio en los “portadores” de OTA para que las solicitudes de servicio se enviaran al UE. Por ejemplo, cuando se utilizó un portador de SMS, la Puerta de Enlace de OTA encapsuló los parámetros de configuración actualizados en uno o más mensajes SMS. La Puerta de Enlace de OTA luego envió los mensajes SMS a un Centro
25 de SMS (SMSC), que transmitió los mensajes SMS al UE. Es deseable proporcionar una solución de plano de control nativa que un operador de red pueda usar para actualizar los parámetros de configuración de UE sin tener que desplegar un elemento de red especializado, tal como una Puerta de Enlace de OTA. También es deseable proporcionar una solución donde los parámetros de configuración de UE tengan protección de seguridad.

30 En las modalidades descritas en la presente, la red envía una actualización de parámetros de configuración de UE con protección de seguridad de manera transparente a un

UE vía un mensaje de NAS de plano de control. Por ejemplo, la actualización de parámetros de configuración de UE puede tener protección de seguridad usando un paquete seguro, usando una clave de protección de integridad de un contexto de seguridad de NAS, o ambos. Tras la recepción de la actualización de parámetros de configuración de UE en un mensaje de NAS, el UE puede actualizar sus parámetros de configuración de UE. La solución proporcionada en la presente se describe en relación con una red de próxima generación (por ejemplo, 5G), pero se pueden proporcionar soluciones similares en redes de generación anterior o posterior. A continuación se proporcionan detalles adicionales de las modalidades.

La FIG. 6 es un diagrama de bloques de un UE 110 en una modalidad ilustrativa.

El UE 110 incluye un componente de interfaz de radio 602, uno o más procesadores 604, una memoria 606, un componente de interfaz de usuario 608 y una batería 610. El componente de interfaz de radio 602 es un componente de hardware que representa los recursos de radio local del UE 110, tal como una unidad de RF 620 (por ejemplo, transceptor) y una o más antenas 622, usadas para comunicaciones inalámbricas con una estación base (por ejemplo, estación base 124) a través de señales de radio o “por aire”. El procesador 604 representa los circuitos internos, lógica, hardware, software, etc., que proporciona las funciones del UE 110. El procesador 604 puede configurarse para ejecutar instrucciones 640 para software que se cargan en la memoria 606. El procesador 604 puede comprender un conjunto de uno o más procesadores o puede comprender un núcleo de multiprocesadores, dependiendo de la implementación particular. El procesador 604 puede implementar una o más aplicaciones 630. Estas aplicaciones 630 pueden acceder a datos de enlace descendente (DL) a través de la RAN 120 y red central 130, y también pueden generar datos de enlace ascendente (UL) para la transferencia a un destino a través de la RAN 120 y red central 130. La memoria 606 es un medio de almacenamiento legible por computadora de los datos, instrucciones 640, aplicaciones, etc., y es accesible por el procesador 604. La memoria 606 es un dispositivo de almacenamiento de hardware capaz de almacenar información en una base temporal y/o una base permanente. La memoria 606 puede comprender una Memoria de Acceso Aleatorio (RAM), o cualquier otro dispositivo de almacenamiento volátil o no volátil. El componente de interfaz de usuario 608 es un componente de hardware para interactuar con un usuario final. Por ejemplo, el componente de interfaz de usuario 608 puede incluir un dispositivo de visualización 650, pantalla, pantalla táctil, o similares (por ejemplo, una Pantalla de Cristal

Líquido (LCD), una pantalla de Diodo Emisor de Luz (LED), etc.). El componente de interfaz de usuario 608 puede incluir teclado o bloque numérico 652, un dispositivo de seguimiento (por ejemplo, una bola de seguimiento o almohadilla de seguimiento), un altavoz, un micrófono, etc.

El UE 110 también incluye una Tarjeta Universal de Circuito Integrado (UICC) 660, que es un dispositivo de hardware que proporciona funciones de seguridad e integridad para el UE 110. Aunque no se muestra en la FIG. 6, la UICC 660 puede incluir un procesador (es decir, Unidad de Procesamiento Central (CPU)), memoria (por ejemplo, Memoria de Sólo Lectura (ROM), RAM, Memoria de Sólo Lectura Eléctricamente Borrable y Programable (EEPROM), y circuitos de entrada/salida (I/O). La UICC 660 puede alojar o almacenar un Módulo Universal de Identidad del Suscriptor (USIM) 662 que almacena información, tales como la Identidad Internacional del Suscriptor Móvil (IMSI), información de cifrado y autenticación de seguridad y otra información de configuración del operador doméstico.

La UICC 660 y/o memoria 606 pueden almacenar información del operador doméstico que se usa para configurar el UE 110, que es referida en la presente como parámetros de configuración de UE 664. Uno o más de los parámetros de configuración de UE 664 se pueden usar exclusivamente por la UICC 660, y uno o más de los parámetros de configuración de UE 664 se pueden usar por el procesador 604. Los parámetros de configuración de UE 664 pueden incluir un Indicador de Enrutamiento, un identificador de red doméstica (por ejemplo, una identidad de PLMN e información de MCC/MNC), un identificador de esquema de protección de red doméstica, un identificador de clave pública de red doméstica, certificados públicos de red doméstica, información de selección de red (por ejemplo, Selector de PLMN Controlado por Operador con lista de Tecnología de Acceso), y/u otra información. Los parámetros de configuración de UE 664 pueden representar los datos pre-provisionados por un operador de red, o los datos provisionados por la red, tal como a través de un procedimiento de actualización como se describe a continuación. El UE 110 puede incluir varios otros componentes no ilustrados específicamente en la FIG. 6.

La FIG. 7 es un modelo funcional para UE 110 en una modalidad ilustrativa. El UE 110 se puede subdividir en dominios, tales como Equipo Móvil (ME) 702 y USIM 662. Como se describió anteriormente, las funciones para USIM 662 se pueden realizar por un procesador y memoria en UICC 660. Las funciones para ME 702 se pueden realizar por el procesador 604 y memoria 606. El ME 702 realiza transmisión de radio y contiene aplicaciones. El USIM 662

contiene datos y procedimientos que se identifican de forma inequívoca y segura. Estas funciones suelen estar integradas en una tarjeta inteligente independiente, tal como la UICC 660. Como se indicó anteriormente, uno o más de los parámetros de configuración de UE 664 pueden almacenarse exclusivamente en el USIM 662 para su uso o manejo dentro de la UICC 660, y uno o más de los parámetros de configuración de UE 664 pueden almacenarse exclusivamente en el ME 702 para uso o manejo dentro del ME 702.

La FIG. 8 es un diagrama de bloques de un elemento de AMF 314 en una modalidad ilustrativa. Como se describió anteriormente, un elemento de AMF 314 está configurado para proporcionar autenticación, autorización, gestión de movilidad, etc. basada en UE. En esta modalidad, el elemento de AMF 314 incluye los siguientes subsistemas: un componente de interfaz de red 802 y un administrador de actualizaciones 804 que operan en una o más plataformas. El componente de interfaz de red 802 puede comprender circuitos, lógica, hardware, medios, etc., configurados para intercambiar mensajes del plano de control o señalización con otros elementos de red y/o UE (por ejemplo, a través de RAN 120). El componente de interfaz de red 802 puede operar usando una variedad de protocolos (incluido el protocolo de NAS) o puntos de referencia. El administrador de actualizaciones 804 puede comprender circuitos, lógica, hardware, medios, etc., configurados para manejar actualizaciones de los parámetros de configuración de UE en UE. Uno o más de los subsistemas del elemento de AMF 314 pueden implementarse en una plataforma de hardware comprendida de circuitos analógicos y/o digitales. Uno o más de los subsistemas del elemento de AMF 314 pueden implementarse en un procesador 830 que ejecuta instrucciones almacenadas en la memoria 832. El procesador 830 comprende un circuito de hardware integrado configurado para ejecutar instrucciones, y la memoria 832 es un medio de almacenamiento no transitorio legible por computadora para datos, instrucciones, aplicaciones, etc., y es accesible por el procesador 830. El elemento de AMF 314 puede incluir varios otros componentes no ilustrados específicamente en la FIG. 8.

La FIG. 9 es un diagrama de bloques de un elemento de UDM 312 en una modalidad ilustrativa. Como se describió anteriormente, un elemento de UDM 312 está configurado para almacenar datos de suscripción de acceso y movilidad de los UE. En esta modalidad, el elemento de UDM 312 incluye los siguientes subsistemas: un componente de interfaz de red 902, un depósito de datos del suscriptor 904 y un administrador de

actualizaciones 906 que opera en una o más plataformas. El componente de interfaz de red 902 puede comprender circuitos, lógica, hardware, medios, etc., configurados para intercambiar mensajes del plano de control o señalización con otros elementos de red. El componente de interfaz de red 902 puede operar usando una variedad de protocolos o puntos de referencia. El depósito de datos del suscriptor 904 puede comprender circuitos, lógica, hardware, medios, etc., configurados para almacenar datos de suscripción de acceso y movilidad. El administrador de actualizaciones 906 puede comprender circuitos, lógica, hardware, medios, etc., configurados para manejar actualizaciones de los parámetros de configuración de UE en los UE. Uno o más de los subsistemas del elemento de UDM 312 pueden implementarse en una plataforma de hardware comprendida de circuitos analógicos y/o digitales. Uno o más de los subsistemas del elemento de UDM 312 pueden implementarse en un procesador 930 que ejecuta instrucciones almacenadas en la memoria 932. El elemento de UDM 312 puede incluir varios otros componentes no ilustrados específicamente en la FIG. 9.

Se puede realizar o invocar un procedimiento de actualización cuando un UE se registra en la red, o después de que el UE se registra en la red. Las FIGS. 10-12 ilustran un procedimiento de actualización general realizado por el elemento de UDM 312, elemento de AMF 314 y UE 110. Se describen detalles adicionales de un procedimiento de actualización en los diagramas de mensajes de ejemplo a continuación. Por lo tanto, los diagramas de flujo proporcionados en la presente pueden complementarse con los procedimientos de actualización descritos en relación con los diagramas de mensajes.

La FIG. 10 es un diagrama de flujo que ilustra un método 1000 para realizar un procedimiento de actualización en un elemento de UDM 312 en una modalidad ilustrativa. Los pasos del método 1000 se describirán con referencia al elemento de UDM 312 en la FIG. 9, pero los expertos en la técnica apreciarán que el método 1000 se puede realizar en otros elementos o dispositivos de red. Además, los pasos de los diagramas de flujo descritos en la presente no todos están incluidos y pueden incluir otros pasos no mostrados, y los pasos pueden realizarse en un orden alternativo.

Se puede suponer para esta modalidad que el UE 110 se está registrando en la red a través de un procedimiento de registro de NAS, o ya está registrado en la red. El administrador de actualizaciones 906 del elemento de UDM 312 inicia un procedimiento de actualización para actualizar uno o más de los parámetros de configuración de UE 664 en el

UE 110 (paso 1002). Por ejemplo, el administrador de actualizaciones 906 puede procesar la información de configuración de UE almacenada en el depósito de datos del suscriptor 904 y determinar que se necesita o desea una actualización de parámetros de configuración de UE 664. El administrador de actualizaciones 906 ensambla una actualización de parámetros de configuración de UE para el UE 110 (paso 1004). La actualización de parámetros de configuración de UE comprende información, un comando, instrucción, etc., que se usa para realizar una actualización de parámetros de configuración de UE 664 en el UE 110. Por ejemplo, una actualización de parámetros de configuración de UE puede incluir uno o más parámetros de configuración de UE actualizados para el UE 110 como parte de los datos de suscripción de acceso y movilidad.

El administrador de actualizaciones 906 aplica protección de seguridad a la actualización de parámetros de configuración de UE (etapa 1006) de acuerdo con uno o más mecanismos de protección. En una modalidad, el mecanismo de protección puede ser un paquete seguro. Por lo tanto, el administrador de actualizaciones 906 puede configurar o encapsular la actualización de parámetros de configuración de UE en un paquete seguro para aplicar protección de seguridad (paso opcional 1008). Generalmente, un paquete seguro contiene mensajes de aplicación a los que se han aplicado ciertos mecanismos. Los mensajes de aplicación son comandos o datos intercambiados entre un elemento de red y una UICC. El remitente antepone un Encabezado de Seguridad (el Encabezado de Comando) al Mensaje de la Aplicación y luego aplica la seguridad solicitada a parte del Encabezado de Comando y a todo el Mensaje de la Aplicación. La estructura resultante es referida como el Paquete de Comandos (Seguro) que incluye los datos seguros como carga útil. El administrador de actualizaciones 906 puede acceder a una biblioteca de paquetes segura local o una biblioteca de paquetes segura remota para configurar o encapsular la actualización de parámetros de configuración de UE en un paquete seguro. En otra modalidad, el mecanismo de protección puede tener protección de integridad. Por lo tanto, el administrador de actualizaciones 906 puede emplear protección de integridad en la actualización de parámetros de configuración de UE usando un contexto de seguridad de NAS para el UE 110 (paso opcional 1010). La seguridad de NAS se usa para entregar de forma segura mensajes de señalización de NAS entre el UE 110 y el elemento de AMF 314 en el plano de control usando claves de seguridad de NAS. Un contexto de seguridad de NAS es una colección de claves y parámetros de seguridad de NAS

que se usan para proteger los mensajes de NAS. Las claves de seguridad de NAS se generan cuando el UE 110 es autenticado en la red. Por lo tanto, después de la autenticación, el administrador de actualizaciones 906 puede emplear protección de integridad en la actualización de parámetros de configuración de UE usando una clave de protección de integridad del contexto de seguridad de NAS. En todavía otra modalidad, el administrador de actualizaciones 906 puede usar tanto un paquete seguro como el contexto de seguridad de NAS para proteger la actualización de parámetros de configuración de UE (paso opcional 1012). El administrador de actualizaciones 906 entonces puede insertar o incluir de otro modo la actualización de parámetros de configuración de UE con protección de seguridad en un mensaje de plano de control (paso 1014).

El administrador de actualizaciones 906 también puede insertar o incluir de otro modo un indicador de reconocimiento de UE en el mensaje de plano de control (paso opcional 1016). Un indicador de reconocimiento de UE puede incluirse cuando la red doméstica desea un reconocimiento de UE 110 de una comprobación de seguridad exitosa de la actualización de parámetros de configuración de UE. El administrador de actualizaciones 906 también puede insertar o incluir de otro modo un indicador de nuevo registro en el mensaje de plano de control (paso opcional 1016). Un indicador de nuevo registro puede incluirse cuando la red doméstica desea que el UE 110 se registre de nuevo en la red con los parámetros de configuración de UE actualizados. El administrador de actualizaciones 906 entonces envía el mensaje de plano de control al elemento de AMF 314 que incluye la actualización de parámetros de configuración de UE con protección de seguridad (paso 1018) y el indicador de reconocimiento de UE y/o el indicador de nuevo registro (si se solicita), a través del componente de interfaz de red 902.

La FIG. 11 es un diagrama de flujo que ilustra un método 1100 para realizar un procedimiento de actualización en un elemento de AMF 314 en una modalidad ilustrativa. Los pasos del método 1100 se describirán con referencia al elemento de AMF 314 en la FIG. 8, pero los expertos en la técnica apreciarán que el método 1100 puede realizarse en otros elementos o dispositivos de red.

El administrador de actualizaciones 804 del elemento de AMF 314 recibe el mensaje de plano de control del elemento de UDM 312 que incluye la actualización de parámetros de configuración de UE con protección de seguridad (paso 1102) a través del componente de interfaz de red 802. El administrador de actualizaciones 804 inserta la

actualización de parámetros de configuración de UE con protección de seguridad en un contenedor de un mensaje de NAS (paso 1104). Una transmisión de la actualización de parámetros de configuración de UE con protección de seguridad se considera “transparente” para el elemento de AMF 314. Por lo tanto, el administrador de actualizaciones 804 está

5 programado para reenviar la actualización de parámetros de configuración de UE con protección de seguridad sin modificar o cambiar la actualización de parámetros de configuración de UE. Por lo tanto, el administrador de actualizaciones 804 puede insertar la actualización de parámetros de configuración de UE con protección de seguridad recibida en el mensaje de plano de control desde el elemento de UDM 312 en un contenedor “transparente” que está

10 designado para la actualización de parámetros de configuración de UE. Un ejemplo de un contenedor transparente tal como este se describe con más detalle a continuación.

El tipo de mensaje de NAS usado por el elemento de AMF 314 para transportar la actualización de parámetros de configuración de UE con protección de seguridad puede depender del procedimiento de NAS que se esté realizando. Por ejemplo, cuando se está

15 realizando un procedimiento de registro de NAS, el mensaje de NAS puede comprender un mensaje de aceptación de registro de NAS. Cuando se realiza un procedimiento de transporte de NAS, el mensaje de NAS puede comprender un mensaje de Transporte de NAS de DL. El administrador de actualizaciones 804 entonces envía el mensaje de NAS al UE 110 (paso 1106) a través del componente de interfaz de red 802.

20 La FIG. 12 es un diagrama de flujo que ilustra un método 1200 para realizar un procedimiento de actualización en el UE 110 en una modalidad ilustrativa. Los pasos del método 1200 se describirán con referencia al UE 110 en las FIGS. 6-7, pero los expertos en la técnica apreciarán que el método 1200 puede realizarse en otros dispositivos.

El UE 110 (por ejemplo, a través del ME 702) recibe el mensaje de NAS del

25 elemento de AMF 314 (paso 1202). El ME 702 o USIM 662 realiza una comprobación de seguridad para verificar que la actualización de parámetros de configuración de UE con protección de seguridad incluida en el contenedor del mensaje de NAS es proporcionada por la red doméstica (es decir, HPLMN) para el UE 110 (etapa 1204). Por ejemplo, el ME 702 o USIM 662 puede calcular una suma de verificación para determinar si la actualización de parámetros

30 de configuración de UE con protección de seguridad que se recibió coincide con la actualización de parámetros de configuración de UE con protección de seguridad enviada por el elemento de

UDM 312. Cuando la comprobación de seguridad no es exitosa, el ME 702 o USIM 662 descarta la actualización de parámetros de configuración de UE con protección de seguridad (etapa 1206). Cuando la comprobación de seguridad es exitosa, el ME 702 o USIM 662 actualiza uno o más parámetros de configuración de UE 664 proporcionados en el UE 110 con base en la actualización de parámetros de configuración de UE (paso 1208). Como se describió anteriormente, la actualización de parámetros de configuración de UE puede encapsularse en un paquete seguro. En este escenario, el USIM 662 está configurado para decodificar o desempaquetar la actualización de parámetros de configuración de UE del paquete seguro usando una biblioteca de paquetes seguros. El USIM 662 entonces actualiza uno o más parámetros de configuración de UE 664 locales para el USIM 662 con base en la actualización de parámetros de configuración de UE.

Cuando el mensaje de NAS incluye un indicador de reconocimiento de UE, el ME 702 o USIM 662 envía un mensaje de NAS al elemento de AMF 314 con un contenedor que incluye un reconocimiento de UE (paso opcional 1210). Una transmisión del reconocimiento de UE se considera “transparente” al elemento de AMF 314. Por lo tanto, el ME 702 o USIM 662 está programado para insertar el reconocimiento de UE en un contenedor “transparente” que está designado para el reconocimiento de UE. Un ejemplo de un contenedor transparente tal como este se describe con más detalle a continuación.

El tipo de mensaje de NAS puede depender del procedimiento de NAS que se esté realizando. Por ejemplo, cuando se está realizando un procedimiento de registro de NAS, el mensaje de NAS puede comprender un mensaje completo de registro de NAS o un mensaje de Transporte de NAS de UL. Cuando se está realizando un procedimiento de transporte de NAS, el mensaje de NAS puede comprender un mensaje de Transporte de NAS de UL.

En la FIG. 11, el administrador de actualizaciones 804 del elemento de AMF 314 recibe el mensaje de NAS del UE 110 con un contenedor que incluye el reconocimiento de UE (paso opcional 1108) a través del componente de interfaz de red 802. El administrador de actualizaciones 804 entonces envía un mensaje de plano de control al elemento de UDM 312 con el reconocimiento de UE (paso opcional 1110) a través del componente de interfaz de red 802. En la FIG. 10, el administrador de actualizaciones 906 del elemento de UDM 312 recibe el mensaje de plano de control con el reconocimiento de UE del elemento de AMF 314 (paso opcional 1020) a través del componente de interfaz de red 902. El administrador de

actualizaciones 906 entonces verifica que el reconocimiento de UE es proporcionado por el UE 110 (paso opcional 1022).

En la FIG. 12, cuando el mensaje de NAS del elemento de AMF 314 incluye un indicador de nuevo registro, el UE 110 (tal como a través del ME 702) inicia un procedimiento de registro de NAS para el nuevo registro usando los parámetros de configuración de UE actualizados (paso opcional 1212). Entonces el procedimiento de actualización puede finalizar.

A continuación se proporcionan ejemplos de cómo realizar un procedimiento de actualización en modalidades adicionales.

10 Ejemplo 1: Procedimiento de actualización durante el registro usando paquete seguro

La FIG. 13 es un diagrama de mensaje que ilustra un procedimiento de actualización durante el registro en una modalidad ilustrativa. En esta modalidad, el UE 110 está en modo inactivo (por ejemplo, RRC_IDLE). El UE 110 inicia un procedimiento de registro de NAS enviando una solicitud de registro de NAS al elemento de AMF 314 (S1). En respuesta a la solicitud de registro de NAS (de tipo “inicial”), el elemento de AMF 314 puede iniciar un procedimiento de autenticación (S2) para autenticar el UE 110. Para el procedimiento de autenticación, el elemento de AMF 314 puede interactuar con el elemento de AUSF 310 y elemento de UDM 312. Por ejemplo, el elemento de AMF 314 puede enviar una solicitud de autenticación (es decir, Solicitud Nausf_UEAuthentication_Authenticate) al elemento de AUSF 310. En respuesta a la recepción de la solicitud de autenticación, el elemento de AUSF 310 puede enviar una solicitud de autenticación (es decir, Solicitud Nudm_UEAuthentication_GET) al elemento de UDM 312. El elemento de UDM 312 aloja funciones relacionadas con la Función de Procesamiento y Depósito de Credencial de Autenticación (ARPF), que selecciona un método de autenticación y calcula los datos de autenticación y materiales de codificación (por ejemplo, tokens) para el elemento de AUSF 310 (si es necesario). El elemento de UDM 312 puede enviar una respuesta de autenticación (es decir, Respuesta Nudm_UEAuthentication_GET) al elemento de AUSF 310, que incluye el vector de autenticación (AV) y otra información. El elemento de AUSF 310 entonces puede enviar una respuesta de autenticación (es decir, Respuesta Nuasf_UEAuthentication_Authenticate) al elemento de AMF 314, que incluye el AV y otra información. El elemento de AMF 314 está configurado para realizar un procedimiento de autenticación con el UE 110 usando información

proporcionada por UDM/AUSF. Por ejemplo, el elemento de AMF 314 puede enviar una solicitud de autenticación al UE 110 junto con un token de autenticación del AV, y el UE 110 intenta validar el token de autenticación. Si es exitosa, el UE 110 calcula un token de respuesta, y envía una respuesta de autenticación con el token de respuesta, que se recibe por el elemento de AMF 314. El elemento de AMF 314 puede formatear o generar otra solicitud de autenticación (es decir, Solicitud Nausf_UEAuthentication_Authenticate) e insertar el token de respuesta del UE 110 en la solicitud de autenticación, junto con otra información. El elemento de AMF 314 entonces puede enviar la solicitud de autenticación al elemento de AUSF 310. El elemento de AUSF 310 puede verificar si el token de respuesta del UE 110 coincide con un token de respuesta esperado, y enviar una respuesta de autenticación (es decir, Respuesta Nausf_UEAuthentication_Authenticate) al elemento de AMF 314 que indica éxito/fracaso de la autenticación.

Después de la autenticación, el elemento de AMF 314 puede iniciar un procedimiento de seguridad de NAS para establecer un contexto de seguridad de NAS (S3). Como parte del procedimiento de seguridad del NAS, el elemento de AMF 314 selecciona un algoritmo de seguridad de NAS (o múltiples algoritmos) para el cifrado y protección de integridad. El elemento de AMF 314 entonces envía un mensaje de Comando de Modo de Seguridad al UE 110 que indica los algoritmos de seguridad de NAS, el ngKSI y otra información. El UE 110 usa el algoritmo de seguridad de NAS y ngKSI para derivar las claves correspondientes para proteger los mensajes de NAS posteriores. Por lo tanto, se establece un contexto de seguridad de NAS entre el UE 110 y elemento de AMF 314. El UE 110 entonces envía un Mensaje Completo de Modo de Seguridad al elemento de AMF 314.

Como parte adicional del procedimiento de registro de NAS, el elemento de AMF 314 envía una solicitud de datos de suscripción (por ejemplo, mensaje Nudm_SDM_Get) al elemento de UDM 312 de la HPLMN para obtener los datos de Suscripción de Acceso y Movilidad para el UE 110, entre otra información (S4). Cuando la información de suscripción de usuario indica iniciar una actualización de parámetros de configuración de UE (por ejemplo, actualización de ID de Enrutamiento), el elemento de UDM 312 inicia un procedimiento de actualización. El elemento de UDM 312 ensambla una actualización de parámetros de configuración de UE, que incluye uno o más parámetros de configuración de UE actualizados. El elemento de UDM 312 entonces aplica protección de seguridad a la actualización de

parámetros de configuración de UE accediendo a una biblioteca de paquetes seguros para encapsular la actualización de parámetros de configuración de UE en un paquete seguro. Un ejemplo de paquetes seguros y estructura de paquetes seguros se describe en 3GPP TS 131.115 (v.9.0.0), que se incorpora como referencia como si se incluyera completamente en la presente. El elemento de UDM 312 entonces envía una respuesta de datos de suscripción (por ejemplo, respuesta Nudm_SDM_Get) al elemento 314 (S5) de AMF, que incluye el paquete seguro. El elemento de UDM 312 también puede incluir un indicador de reconocimiento de UE y/o un indicador de nuevo registro en la respuesta de datos de suscripción.

Como parte todavía adicional del procedimiento de registro, el elemento de AMF 314 también puede enviar un mensaje de suscripción (por ejemplo, Nudm_SDM_Subscribe) al elemento de UDM 312 para suscribirse a la notificación de cambios a los parámetros de configuración de UE (no mostrado en la FIG. 13).

El elemento de AMF 314 está configurado para enviar de forma transparente el paquete seguro al UE 110 como parte del procedimiento de actualización. Por lo tanto, el elemento de AMF 314 formatea o genera un mensaje de aceptación de registro de NAS e inserta el paquete seguro en un contenedor de un mensaje de aceptación de registro de NAS. El elemento de AMF 314 también puede insertar el indicador de reconocimiento de UE y/o indicador de nuevo registro (si aplica) en el contenedor del mensaje de aceptación de registro de NAS. El elemento de AMF 314 entonces envía el mensaje de aceptación de registro de NAS al UE 110 (S6).

En esta modalidad, el contenedor del mensaje de aceptación de registro de NAS está designado para una actualización de parámetros de configuración de UE. La Tabla 1 ilustra un ejemplo del contenido de mensaje de un mensaje de aceptación de registro de NAS.

Tabla 1:

IEI	Elemento de información	Tipo/Referencia	Presencia	Formato	Longitud
	Discriminador de protocolo extendido	Discriminador de protocolo extendido	M	V	1
	Tipo de encabezado de seguridad	Tipo de encabezado de seguridad	M	V	1/ 2

	Medio octeto de repuesto	Medio octeto de repuesto	M	V	1/2
	Identidad del mensaje de aceptación del registro	Tipo de mensaje	M	V	1
	...				
xx	Contenedor de actualización de parámetros de configuración de UE	Contenedor de actualización de parámetros de configuración de UE	O	TLV-E	20-2048
	...				

En este ejemplo, el mensaje de aceptación de registro de NAS incluye un Elemento de Información (IE) de contenedor de actualización de parámetros de configuración de UE recién definido. Una descripción adicional del protocolo de NAS se puede encontrar en 3GPP TS 24.301 (v15.4.0), que se incorpora como referencia como si estuviera completamente incluido en la presente. La Tabla 2 es un ejemplo de un IE de contenedor de actualización de parámetros de configuración de UE. Este contenedor se considera transparente ya que el elemento de AMF 314 inserta el paquete seguro en el contenedor sin modificar el paquete seguro.

Tabla 2:

8	7	6	5	4	3	2	1
IEI de contenedor de actualización de parámetros de configuración de UE							octeto 1
Longitud del contenido del contenedor de actualización de parámetros de configuración de UE							octeto 2 octeto 3
Encabezado de actualización de parámetros de configuración de UE							octeto 4
Paquete seguro [actualización de parámetros de configuración							octeto 5

de UE]	2048*
--------	-------

La Tabla 3 ilustra un ejemplo de un encabezado de actualización de parámetros de configuración de UE para el IE de contenedor de actualización de parámetros de configuración de UE.

5 Tabla 3:

8	7	6	5	4	3	2	1	
0	0	0	0	0	RR	REC	tipo	octeto 4
Repuesto	Repuesto	Repuesto	Repuesto	Repuesto	R	ON. de UE	de datos	

En el encabezado, el bit RRR puede usarse como el indicador de nuevo registro. El bit RECON. de UE puede usarse como el indicador de reconocimiento de UE. El bit tipo de datos puede usarse para indicar si el contenedor se está usando en un mensaje de NAS que se envía desde la red a un UE (por ejemplo, valor = 0), o en un mensaje de NAS que se envía desde el UE a la red (por ejemplo, valor = 1).

Tras recibir el mensaje de aceptación de registro de NAS, el ME 702 puede comportarse como si se recibiera un mensaje SMS con el identificador de protocolo configurado en “descarga de datos de SIM”, esquema de codificación de datos configurado en “mensaje de clase 2” y carga útil de SMS como el paquete seguro. El ME 702 enruta o carga el paquete seguro a USIM 662 (S7). El USIM 662 realiza una comprobación de seguridad para verificar que el paquete seguro se envió por el elemento de UDM 312 de la red doméstica. Si la comprobación de seguridad no es exitosa, entonces el USIM 662 descarta la actualización de parámetros de configuración de UE y continua con el procedimiento de registro. Si la comprobación de seguridad es exitosa, entonces el USIM 662 desempaqueta la actualización de parámetros de configuración de UE del paquete seguro usando una biblioteca de paquetes seguros. Después de que se valida la protección de reproducción/integridad del paquete seguro, el USIM 662 actualiza uno o más de los parámetros de configuración de UE 664 con base en la actualización de parámetros de configuración de UE.

Si la red solicita un reconocimiento de UE 110 y la comprobación de seguridad es exitosa, entonces el USIM 662 puede enviar un reconocimiento de UE al ME 702 (S8). El ME 702 formatea o genera otro mensaje de NAS para transportar el reconocimiento de UE al elemento de AMF 314. En el ejemplo mostrado en la FIG. 13, el ME 702 formatea un mensaje completo de registro de NAS e inserta el reconocimiento de UE en un contenedor de un mensaje completo de registro de NAS. El contenedor del mensaje completo de registro NAS está designado para un reconocimiento de UE. La Tabla 4 ilustra un ejemplo del contenido de mensaje de un mensaje completo de registro de NAS.

Tabla 4:

IEI	Elemento de información	Tipo/Referencia	Presencia	Formato	Longitud
	Discriminador de protocolo extendido	Discriminador de protocolo extendido	M	V	1
	Tipo de encabezado de seguridad	Tipo de encabezado de seguridad	M	V	1/2
	Medio octeto de repuesto	Medio octeto de repuesto	M	V	1/2
	Identidad de mensaje de aceptación del registro	Tipo de mensaje	M	V	1
	...				
xx	Contenedor de reconocimiento de UE	Contenedor de reconocimiento de UE	O	TLV-E	20-2048

10

En este ejemplo, el mensaje completo de registro de NAS incluye un IE de contenedor de reconocimiento de UE recién definido. La Tabla 5 es un ejemplo de un IE de contenedor de reconocimiento de UE.

Tabla 5:

8	7	6	5	4	3	2	1
IEI de Contenedor de reconocimiento de UE							octeto 1
Longitud del contenido del contenedor de reconocimiento de UE							octeto 2 octeto 3
Encabezado de reconocimiento de UE							octeto 4
Reconocimiento de UE							Octeto 5

La Tabla 6 ilustra un ejemplo de un encabezado de reconocimiento de UE.

Tabla 6:

8	7	6	5	4	3	2	1
0	0	0	0	0	0	0	tipo de datos
Repues to	Repues to	Repues to	Repues to	Repues to	Repues to	Repues to	

octeto 4

5 En otro ejemplo, el USIM 662 puede aplicar protección de seguridad al reconocimiento de UE accediendo a una biblioteca de paquetes seguros para encapsular el reconocimiento de UE en un paquete seguro. Por lo tanto, el ME 702 puede insertar el paquete seguro en el IE de contenedor de reconocimiento de UE.

10 El ME 702 entonces envía el mensaje completo de registro de NAS al elemento de AMF 314 con el contenedor que incluye el reconocimiento de UE (S9). El elemento de AMF 314 envía un mensaje de información (por ejemplo, mensaje Nudm_SDM_Info) al elemento de UDM 312 con el reconocimiento de UE (S10). El elemento de UDM 312 entonces puede verificar que el reconocimiento de UE es proporcionado por el UE 110.

15 En una alternativa mostrada en la FIG. 13, el ME 702 puede usar otro tipo de mensaje de NAS para enviar el reconocimiento de UE al elemento de AMF 314. En esta alternativa, el ME 702 formatea un mensaje de Transporte de NAS de UL e inserta el reconocimiento de UE en un contenedor del mensaje de Transporte de NAS de UL. Un valor de tipo de contenedor de carga útil se puede designar para el reconocimiento de UE en el IE de contenedor de carga útil del mensaje de Transporte de NAS de UL. El ME 702 entonces envía
20 el mensaje de Transporte de NAS de UL al elemento de AMF 314 con el contenedor que incluye

el reconocimiento de UE (S9a). El elemento de AMF 314 a su vez envía un mensaje de información (por ejemplo, mensaje Nudm_SDM_Info) al elemento de UDM 312 con el reconocimiento de UE (S10a).

Si la red indica que se requiere el nuevo registro para el UE 110 y la comprobación de seguridad es exitosa, entonces el UE 110 se da de baja y reinicia un nuevo procedimiento de registro de NAS (S11) usando los parámetros de configuración de UE actualizados.

Ejemplo 2: Procedimiento de actualización después del registro usando paquete seguro

La FIG. 14 es un diagrama de mensaje que ilustra un procedimiento de actualización después del registro en una modalidad ilustrativa. En esta modalidad, el UE 110 ya se ha registrado en la red y está en modo conectado (es decir, CONECTADO A RRC). En algún momento después del registro, el elemento de UDM 312 puede recibir una instrucción o políticas locales de proceso para determinar que los parámetros de configuración de UE en el UE 110 necesitan actualizarse. Por lo tanto, el elemento de UDM 312 inicia un procedimiento de actualización y ensambla una actualización de parámetros de configuración de UE. El elemento de UDM 312 entonces aplica protección de seguridad a la actualización de parámetros de configuración de UE accediendo a una biblioteca de paquetes seguros para encapsular la actualización de parámetros de configuración de UE en un paquete seguro. El elemento de UDM 312 entonces envía una notificación de actualización (por ejemplo, Nudm_SDM_UpdateNotification) al elemento de AMF 314 (S1), que incluye el paquete seguro. El elemento de UDM 312 también puede incluir un indicador de reconocimiento de UE y/o un indicador de nuevo registro en la notificación de actualización.

El elemento de AMF 314 está configurado para enviar de forma transparente el paquete seguro al UE 110 como parte del procedimiento de actualización. Por lo tanto, el elemento de AMF 314 formatea o genera un mensaje de Transporte de NAS de Enlace Descendente (DL) e inserta el paquete seguro en un contenedor de un mensaje de Transporte de NAS de DL. El elemento de AMF 314 también puede insertar el indicador de reconocimiento de UE y/o el indicador de nuevo registro (si aplica) en el contenedor del mensaje de Transporte de NAS de DL. En esta modalidad, el contenedor del mensaje de Transporte de NAS de DL está designado para una actualización de parámetros de configuración de UE. El elemento de AMF 314 puede configurar el IE de tipo de contenedor de carga útil en “contenedor de

parámetros de configuración de UE” y configurar el IE de contenedor de carga útil en el paquete seguro. El elemento de AMF 314 entonces envía el mensaje de Transporte de NAS de DL al UE 110 (S2).

Tras recibir el mensaje de Transporte de NAS de DL, el ME 702 puede comportarse como si se recibiera un mensaje SMS con un identificador de protocolo configurado en “descarga de datos de SIM”, esquema de codificación de datos configurado en “mensaje de clase 2” y carga útil de SMS como un paquete seguro. El ME 702 enruta o carga el paquete seguro al USIM 662 (S3). El USIM 662 realiza una comprobación de seguridad para verificar que el paquete seguro se envió por el elemento de UDM 312 de la red doméstica. Si la comprobación de seguridad no es exitosa, entonces el USIM 662 descarta la actualización de parámetros de configuración de UE. Si la comprobación de seguridad es exitosa, entonces el USIM 662 desempaqueta la actualización de parámetros de configuración de UE del paquete seguro usando una biblioteca de paquetes seguros. Después de que se valida la protección de reproducción/integridad del paquete seguro, el USIM 662 actualiza uno o más de los parámetros de configuración de UE 664 con base en la actualización de parámetros de configuración de UE.

Si la red solicita un reconocimiento de UE 110 y la comprobación de seguridad es exitosa, entonces el USIM 662 puede enviar un reconocimiento de UE al ME 702 (S4). El ME 702 formatea o genera un mensaje de Transporte de NAS de UL e inserta el reconocimiento de UE en un contenedor del mensaje de Transporte de NAS de UL. El contenedor del mensaje de Transporte de NAS de UL está designado para un reconocimiento de UE. El ME 702 entonces envía el mensaje de Transporte de NAS de UL al elemento de AMF 314 con el contenedor que incluye el reconocimiento de UE (S5). El elemento de AMF 314 envía un mensaje de información (por ejemplo, mensaje Nudm_SDM_Info) al elemento de UDM 312 con el reconocimiento de UE (S6). El elemento de UDM 312 entonces puede verificar que el reconocimiento de UE es proporcionado por el UE 110.

Si la red indica que se requiere un nuevo registro para el UE 110 y la comprobación de seguridad es exitosa, entonces el UE 110 se da de baja y reinicia un nuevo procedimiento de registro de NAS usando los parámetros de configuración de UE actualizados (no mostrados).

Ejemplo 3: Procedimiento de actualización durante el registro usando clave de seguridad

La FIG. 15 es un diagrama de mensaje que ilustra un procedimiento de actualización durante el registro en una modalidad ilustrativa. En esta modalidad, el UE 110 inicia un Procedimiento de registro de NAS enviando una solicitud de registro de NAS al elemento de AMF 314 (S1). En respuesta a la solicitud de registro de NAS (de tipo “inicial”), el

5 elemento de AMF 314 puede iniciar un procedimiento de autenticación (S2) para autenticar el UE 110. Cuando el UE 110 se autentica en la red, el elemento de AMF 314 puede iniciar un procedimiento de seguridad de NAS para establecer un contexto de seguridad de NAS (S3). Con el UE 110 autenticado y el contexto de seguridad de NAS establecido, el elemento de AMF 314 envía una solicitud de datos de suscripción (por ejemplo, mensaje Nudm_SDM_Get) al

10 elemento de UDM 312 de la HPLMN para obtener los datos de Suscripción de Acceso y Movilidad para el UE 110, entre otra información (S4). Cuando la información de suscripción de usuario indica iniciar una actualización de parámetros de configuración de UE (por ejemplo, actualización de ID de Enrutamiento), el elemento de UDM 312 inicia un procedimiento de actualización. El elemento de UDM 312 ensambla una actualización de parámetros de

15 configuración de UE y emplea protección de integridad en la actualización de parámetros de configuración de UE usando un contexto de seguridad de NAS para el UE 110. Para hacerlo, el elemento de UDM 312 envía una solicitud de protección (por ejemplo, Nausf_ParameterProtectionRequest) al elemento de AUSF 310 con la actualización de parámetros de configuración de UE (S5). El elemento de AUSF 310 identifica el conteo de NAS

20 (construido de un número de secuencia de NAS) y calcula la información de protección de integridad con base en el contexto de seguridad de NAS para el UE 110, tal como un Código de Autenticación de Mensajes (MAC) de AUSF para la actualización de parámetros de configuración de UE y el conteo de NAS. El elemento de AUSF 310 también puede calcular un MAC esperado del UE 110 (X-UE-MAC). El elemento de AUSF 310 entonces envía una

25 respuesta de protección (por ejemplo, Nausf_ParameterProtectionResponse) con la información de protección de integridad (es decir, AUSF-MAC, conteo de NAS y X-UE-MAC) al elemento de UDM 312 (S6). El elemento de UDM 312 entonces envía una respuesta de datos de suscripción (por ejemplo, respuesta Nudm_SDM_Get) al elemento de AMF 314 (S7), que incluye la actualización de parámetros de configuración de UE y la información de protección

30 de integridad (es decir, AUSF-MAC y conteo de NAS). El elemento de UDM 312 también puede incluir un indicador de reconocimiento de UE y/o un indicador de nuevo registro en la respuesta

de datos de suscripción.

El elemento de AMF 314 está configurado para enviar de forma transparente la actualización de parámetros de configuración de UE al UE 110 como parte del procedimiento de actualización. Por lo tanto, el elemento de AMF 314 formatea o genera un mensaje de aceptación de registro de NAS e inserta la actualización de parámetros de configuración de UE en un contenedor de un mensaje de aceptación de registro de NAS junto con la información de protección de integridad (por ejemplo, AUSF-MAC y conteo de NAS). El elemento de AMF 314 también puede insertar el indicador de reconocimiento de UE y/o el indicador de nuevo registro (si aplica) en el contenedor del mensaje de aceptación de registro de NAS. El elemento de AMF 314 entonces envía el mensaje de aceptación de registro de NAS al UE 110 (S8).

En este ejemplo, el mensaje de aceptación de registro de NAS incluye un IE de contenedor de actualización de parámetros de configuración de UE recién definido. La Tabla 7 es un ejemplo de un IE de contenedor de actualización de parámetros de configuración de UE.

Tabla 7:

8	7	6	5	4	3	2	1
IEI de contenedor de actualización de parámetros de configuración de UE							octeto 1
Longitud del contenido del contenedor de actualización de parámetros de configuración de UE							octeto 2 octeto 3
Encabezado de actualización de parámetros de configuración de UE							octeto 4
AUSF-MAC							octeto 5-20
Conteo de NAS							octeto 21-22
Actualización de parámetros de configuración de UE							octeto 23*-2048*

Este contenedor se considera transparente ya que el elemento de AMF 314 inserta la actualización de parámetros de configuración de UE en el contenedor sin modificar la actualización de parámetros de configuración de UE. Como se describe en el Ejemplo 1, el bit

RECON. de UE del encabezado de actualización de parámetros de configuración de UE puede usarse para indicar que la red solicita un reconocimiento del UE, y el bit RRR puede usarse para indicar que la red solicita nuevo registro.

En respuesta a la recepción del mensaje de aceptación de registro de NAS, el ME 702 del UE 110 realiza una comprobación de seguridad para verificar que la actualización de parámetros de configuración de UE se envió por el elemento de UDM 312 de la red doméstica. Por ejemplo, el ME 702 calcula un UE-MAC para la actualización de parámetros de configuración de UE y el conteo de NAS, y compara el UE-MAC con el AUSF-MAC. Si los MAC coinciden, entonces la actualización de parámetros de configuración de UE se verifica que proviene de la red doméstica y la comprobación de seguridad es exitosa. Si la comprobación de seguridad no es exitosa, entonces el ME 702 descarta la actualización de parámetros de configuración de UE y continúa con el procedimiento de registro. Si la comprobación de seguridad es exitosa, entonces el ME 702 y/o USIM 662 actualiza uno o más de los parámetros de configuración de UE 664 con base en la actualización de parámetros de configuración de UE.

Si la red solicita un reconocimiento de UE 110 y la comprobación de seguridad es exitosa, entonces el ME 702 formatea un mensaje completo de registro de NAS e inserta el UE-MAC en un contenedor de un mensaje completo de registro de NAS. El contenedor del mensaje completo de registro de NAS está diseñado para un reconocimiento de UE. En este ejemplo, el mensaje completo de registro de NAS incluye un IE de contenedor de reconocimiento de UE recién definido. La Tabla 8 es un ejemplo de un IE de contenedor de reconocimiento de UE.

Tabla 8:

8	7	6	5	4	3	2	1
IEI de contenedor de actualización de parámetros de configuración de UE							octeto 1
Longitud del contenido del contenedor de actualización de parámetros de configuración de UE							octeto 2 octeto 3
Encabezado de actualización de parámetros de configuración de UE							octeto 4
UE-MAC							octeto 5-20

El ME 702 entonces envía el mensaje completo de registro de NAS al elemento de AMF 314 con el contenedor que incluye el UE-MAC (S9). El elemento de AMF 314 envía un mensaje de información (por ejemplo, mensaje Nudm_SDM_Info) al elemento de UDM 312 con el UE-MAC (S10). El elemento de UDM 312 entonces puede comparar el UE-MAC calculado por el UE 110 con el X-UE-MAC calculado por el elemento de AUSF 310 para verificar que el reconocimiento de UE es proporcionado por el UE 110.

Si la red indica que se requiere un nuevo registro para el UE 110 y la comprobación de seguridad es exitosa, entonces el UE 110 se da de baja y reinicia un nuevo procedimiento de registro de NAS usando los parámetros de configuración de UE actualizados (no mostrados).

Ejemplo 4: Procedimiento de actualización después del registro usando clave de seguridad

La FIG. 16 es un diagrama de mensaje que ilustra un procedimiento de actualización después del registro en una modalidad ilustrativa. En esta modalidad, el UE 110 ya se ha registrado en la red y está en modo conectado. En algún punto después del registro, el elemento de UDM 312 puede recibir una instrucción o políticas locales de proceso para determinar que los parámetros de configuración de UE en el UE 110 necesitan actualizarse. Por lo tanto, el elemento de UDM 312 inicia un procedimiento de actualización y ensambla una actualización de parámetros de configuración de UE. El elemento de UDM 312 también emplea protección de integridad en la actualización de parámetros de configuración de UE usando un contexto de seguridad de NAS para el UE 110. Para hacerlo, el elemento de UDM 312 envía una solicitud de protección (por ejemplo, Nausf_ParameterProtectionRequest) al elemento de AUSF 310 con la actualización de parámetros de configuración de UE (S1). El elemento de AUSF 310 identifica el conteo de NAS y calcula la información de protección de integridad con base en el contexto de seguridad de NAS para el UE 110, tal como el AUSF-MAC para la actualización de parámetros de configuración de UE y el conteo de NAS. El elemento de AUSF 310 también puede calcular un MAC esperado del UE 110 (X-UE-MAC). El elemento de AUSF 310 entonces envía una respuesta de protección (por ejemplo, Nausf_ParameterProtectionResponse) con la información de protección de integridad (es decir, AUSF-MAC, conteo de NAS y X-UE-MAC) al elemento de UDM 312 (S2). El elemento de UDM 312 entonces envía una notificación de actualización (por ejemplo, Nudm_SDM_

UpdateNotification) al elemento de AMF 314 (S3), que incluye la actualización de parámetros de configuración de UE y la información de protección de integridad (es decir, AUSF-MAC y conteo de NAS). El elemento de UDM 312 también puede incluir un indicador de reconocimiento de UE y/o un indicador de nuevo registro en la notificación de actualización.

5 El elemento de AMF 314 está configurado para enviar de forma transparente la actualización de parámetros de configuración de UE al UE 110 como parte del procedimiento de actualización. Por lo tanto, el elemento de AMF 314 formatea o genera un mensaje de Transporte de NAS de DL e inserta la actualización de parámetros de configuración de UE en un contenedor de un mensaje de Transporte de NAS de DL junto con la información de integridad (por ejemplo, AUSF-MAC y conteo de NAS). El elemento de AMF 314 también puede insertar el indicador de reconocimiento de UE y/o indicador de nuevo registro (si aplica) en el contenedor del mensaje de Transporte de NAS de DL. En esta modalidad, el contenedor del mensaje de Transporte de NAS de DL está designado para una actualización de parámetros de configuración de UE. El elemento de AMF 314 entonces envía el mensaje de Transporte de NAS de DL al UE 110 (S4).
15

En respuesta a la recepción del mensaje de Transporte de NAS de DL, el ME 702 del UE 110 realiza una comprobación de seguridad para verificar que la actualización de parámetros de configuración de UE se envió por el elemento de UDM 312 de la red doméstica. Si la comprobación de seguridad no es exitosa, entonces el ME 702 descarta la actualización de parámetros de configuración de UE. Si la comprobación de seguridad es exitosa, entonces el ME 702 y/o USIM 662 actualiza uno o más de los parámetros de configuración de UE 664 con base en la actualización de parámetros de configuración de UE.
20

Si la red solicita un reconocimiento de UE 110 y la comprobación de seguridad es exitosa, entonces el ME 702 formatea un mensaje de Transporte de NAS de UL e inserta el UE-MAC en un contenedor de un mensaje de Transporte de NAS de UL. El contenedor del mensaje de Transporte de NAS de UL está designado para un reconocimiento de UE. El ME 702 entonces envía el mensaje de Transporte de NAS de UL al elemento de AMF 314 con el contenedor que incluye el UE-MAC (S5). El elemento de AMF 314 envía un mensaje de información (por ejemplo, mensaje Nudm_SDM_Info) al elemento de UDM 312 con el UE-MAC (S6). El elemento de UDM 312 entonces puede comparar el UE-MAC calculado por el UE 110 con el X-UE-MAC calculado por el elemento de AUSF 310 para verificar que el reconocimiento
25
30

de UE es proporcionado por el UE 110.

Si la red indica que se requiere un nuevo registro para el UE 110 y la comprobación de seguridad es exitosa, entonces el UE 110 se da de baja y reinicia un nuevo procedimiento de registro de NAS usando los parámetros de configuración de UE actualizados (no mostrados).

5

Ejemplo 5: Procedimiento de actualización durante el registro usando paquete seguro y clave de seguridad

La FIG. 17 es un diagrama de mensaje que ilustra un procedimiento de actualización durante el registro en una modalidad ilustrativa. En esta modalidad, el UE 110 inicia un procedimiento de registro de NAS enviando una solicitud de registro de NAS al elemento de AMF 314 (S1). En respuesta a la solicitud de registro de NAS (de tipo “inicial”), el elemento de AMF 314 puede iniciar un procedimiento de autenticación (S2) para autenticar el UE 110. Después de la autenticación del UE 110, el elemento de AMF 314 puede iniciar un procedimiento de seguridad de NAS para establecer un contexto de seguridad de NAS (S3).
 10 Con el UE 110 autenticado y el contexto de seguridad de NAS establecido, el elemento de AMF 314 envía una solicitud de datos de suscripción (por ejemplo, mensaje Nudm_SDM_Get) al elemento de UDM 312 de la HPLMN para obtener los datos de Suscripción de Acceso y Movilidad del UE 110, entre otra información (S4). Cuando la información de suscripción de usuario indica iniciar una actualización de parámetros de configuración de UE (por ejemplo, actualización de ID de Enrutamiento), el elemento de UDM 312 inicia un procedimiento de actualización. El elemento de UDM 312 ensambla una actualización de parámetros de configuración de UE, que incluye uno o más parámetros de configuración de UE actualizados. El elemento de UDM 312 entonces aplica protección de seguridad a la actualización de parámetros de configuración de UE accediendo a una biblioteca de paquetes seguros para
 20 encapsular la actualización de parámetros de configuración de UE en un paquete seguro.

25

El elemento de UDM 312 también emplea protección de integridad en el paquete seguro usando un contexto de seguridad de NAS para el UE 110. Para hacerlo, el elemento de UDM 312 envía una solicitud de protección (por ejemplo, Nausf_ParameterProtectionRequest) al elemento de AUSF 310 con el paquete seguro (S5). El elemento de AUSF 310 identifica el
 30 conteo de NAS y calcula la información de protección de integridad con base en el contexto de seguridad de NAS para el UE 110, tal como un AUSF-MAC para el paquete seguro y el conteo

Un elemento de AMF 314 está configurado para enviar de forma transparente el paquete seguro al UE 110 como parte del procedimiento de actualización. Por lo tanto, el elemento de AMF 314 formatea o genera un mensaje de aceptación de registro de NAS e inserta el paquete seguro en un contenedor de un mensaje de aceptación de registro de NAS. El elemento de AMF 314 también puede insertar el indicador de reconocimiento de UE y/o la solicitud de nuevo registro (si aplica) en el contenedor del mensaje de aceptación de registro de NAS, junto con el AUSF-MAC y conteo de NAS. En este ejemplo, el mensaje de aceptación de registro de NAS incluye un IE de contenedor de actualización de parámetros de configuración de UE recién definido. La Tabla 9 es un ejemplo de un IE de contenedor de actualización de parámetros de configuración de UE.

Tabla 9:

8	7	6	5	4	3	2	1
IEI de contenedor de actualización de parámetros de configuración de UE							octeto 1
Longitud del contenido del contenedor de actualización de parámetros de configuración de UE							octeto 2 octeto 3
Encabezado de actualización de parámetros de configuración de UE							octeto 4
AUSF-MAC							octeto 5-20
Conteo de NAS							octeto 21-22
Paquete seguro [actualización de parámetros de configuración							octeto 23*-

de UE]	2048*
--------	-------

Este contenedor se considera transparente ya que el elemento de AMF 314 inserta el paquete seguro en el contenedor sin modificar el paquete seguro. El elemento de AMF 314 entonces envía el mensaje de aceptación de registro de NAS al UE 110 (S8). En respuesta a la recepción del mensaje de aceptación de registro de NAS, el ME 702 del UE 110 realiza una comprobación de seguridad para verificar que el paquete seguro se envió por el elemento de UDM 312 de la red doméstica. Si la comprobación de seguridad no es exitosa, entonces el ME 702 descarta el paquete seguro y continúa con el procedimiento de registro. Si la comprobación de seguridad es exitosa, entonces el ME 702 entura o carga el paquete seguro al USIM 662 (S9). El USIM 662 también realiza una comprobación de seguridad para verificar que el paquete seguro se envió por el elemento de UDM 312 de la red doméstica. Si la comprobación de seguridad no es exitosa, entonces el USIM 662 descarta la actualización de parámetros de configuración de UE. Si la comprobación de seguridad es exitosa, entonces el USIM 662 desempaqueta la actualización de parámetros de configuración de UE del paquete seguro usando una biblioteca de paquetes seguros. El USIM 662 entonces actualiza uno o más de los parámetros de configuración de UE 664 con base en la actualización de parámetros de configuración de UE.

Si la red solicita un reconocimiento de UE 110 y la comprobación de seguridad es exitosa, entonces el ME 702 formatea un mensaje completo de registro de NAS e inserta el UE-MAC en un contenedor de un mensaje completo de registro de NAS. El ME 702 entonces envía el mensaje completo de registro de NAS al elemento de AMF 314 (S11). El elemento de AMF 314 envía un mensaje de información (por ejemplo, mensaje Nudm_SDM_Info) al elemento de UDM 312 con el UE-MAC (S10). Elemento de UDM 312 entonces puede comparar el UE-MAC calculado por el UE 110 con el X-UE-MAC calculado por el elemento de AUSF 310 para verificar que el reconocimiento de UE es proporcionado por el UE 110.

Si la red indica que se requiere un nuevo registro para el UE 110 y la comprobación de seguridad es exitosa, entonces el UE 110 da de baja y reinicia un nuevo procedimiento de registro de NAS usando los parámetros de configuración de UE actualizados (no mostrados).

Ejemplo 6: Procedimiento de actualización después del registro usando paquete seguro y clave

de seguridad

La FIG. 18 es un diagrama de mensaje que ilustra un procedimiento de actualización después del registro en una modalidad ilustrativa. En esta modalidad, el UE 110 ya se ha registrado en la red y está en modo conectado. En algún momento después del registro, el elemento de UDM 312 puede recibir una instrucción o políticas locales de proceso para determinar que los parámetros de configuración de UE en el UE 110 necesitan actualizarse. Por lo tanto, el elemento de UDM 312 inicia un procedimiento de actualización y ensambla una actualización de parámetros de configuración de UE. El elemento de UDM 312 entonces aplica protección de seguridad a la actualización de parámetros de configuración de UE accediendo a una biblioteca de paquetes seguros para encapsular la actualización de parámetros de configuración de UE en un paquete seguro.

El elemento de UDM 312 también emplea protección de integridad en el paquete seguro usando un contexto de seguridad de NAS para el UE 110. Para hacerlo, el elemento de UDM 312 envía una solicitud de protección (por ejemplo, Nausf_ParameterProtectionRequest) al elemento de AUSF 310 con el paquete seguro (S1). El elemento de AUSF 310 identifica el conteo de NAS y calcula la información de protección de integridad con base en el contexto de seguridad de NAS para el UE 110, tal como un AUSF-MAC para el paquete seguro y conteo de NAS. El elemento de AUSF 310 también puede calcular un MAC esperado del UE 110 (X-UE-MAC). El elemento de AUSF 310 entonces envía una respuesta de protección (por ejemplo, Nausf_ParameterProtectionResponse) con la información de protección de integridad (es decir, AUSF-MAC, conteo de NAS y X-UE-MAC) al elemento de UDM 312 (S2). El elemento de UDM 312 entonces envía una notificación de actualización (por ejemplo, Nudm_SDM_UpdateNotification) al elemento de AMF 314 (S3), que incluye el paquete seguro y la información de protección de integridad (es decir, AUSF-MAC y conteo de NAS). El elemento de UDM 312 también puede incluir un indicador de reconocimiento de UE y/o una solicitud de nuevo registro en la notificación de actualización.

Un elemento de AMF 314 está configurado para enviar de forma transparente el paquete seguro al UE 110 como parte del procedimiento de actualización. Por lo tanto, el elemento de AMF 314 formatea o genera un mensaje de Transporte de NAS de DL e inserta el paquete seguro en un contenedor del mensaje de Transporte de NAS de DL. El elemento de AMF 314 también puede insertar el indicador de reconocimiento de UE y/o el indicador de nuevo

registro (si aplica) en el contenedor del mensaje de Transporte de NAS de DL, junto con AUSF-MAC y conteo de NAS. El elemento de AMF 314 entonces envía el mensaje de Transporte de NAS de DL al UE 110 (S4).

En respuesta a la recepción del mensaje de Transporte de NAS de DL, el ME 702 del UE 110 realiza una comprobación de seguridad para verificar que el paquete seguro se envió por el elemento de UDM 312 de la red doméstica. Si la comprobación de seguridad no es exitosa, entonces el ME 702 descarta el paquete seguro. Si la comprobación de seguridad es exitosa, entonces el ME 702 enruta o carga el paquete seguro al USIM 662 (S5). El USIM 662 también realiza una comprobación de seguridad para verificar que el paquete seguro se envió por el elemento de UDM 312 de la red doméstica. Si la comprobación de seguridad no es exitosa, entonces el USIM 662 descarta la actualización de parámetros de configuración de UE. Si la comprobación de seguridad es exitosa, entonces el USIM 662 desempaqueta la actualización de parámetros de configuración de UE del paquete seguro usando una biblioteca de paquetes seguros. El USIM 662 entonces actualiza uno o más de los parámetros de configuración de UE 664 con base en la actualización de parámetros de configuración de UE. El USIM 662 también envía un reconocimiento de UE al ME 702 (S6).

Si la red solicita un reconocimiento de UE 110 y la comprobación de seguridad es exitosa, entonces el ME 702 formatea un mensaje de Transporte de NAS de UL e inserta el UE-MAC en un contenedor del mensaje de Transporte de NAS de UL. El ME 702 entonces envía el mensaje de Transporte de NAS de UL al elemento de AMF 314 (S7). El elemento de AMF 314 envía un mensaje de información (por ejemplo, mensaje Nudm_SDM_Info) al elemento de UDM 312 con el UE-MAC (S8). El elemento de UDM 312 entonces puede comparar el UE-MAC calculado por el UE 110 con el X-UE-MAC calculado por el elemento de AUSF 310 para verificar que el reconocimiento de UE es proporcionado por el UE 110.

Si la red indica que se requiere un nuevo registro para el UE 110 y la comprobación de seguridad es exitosa, entonces el UE 110 se da de baja y reinicia un nuevo procedimiento de registro de NAS usando los parámetros de configuración de UE actualizados (no mostrados).

Cualquiera de los diversos elementos o módulos mostrados en las figuras o descritos en la presente pueden implementarse como hardware, software, firmware o alguna combinación de estos. Por ejemplo, un elemento puede implementarse como hardware especializado. Los elementos de hardware especializados pueden ser referidos como

“procesadores”, “controladores” o alguna terminología similar. Cuando las proporciona un procesador, las funciones pueden ser proporcionadas por un solo procesador especializado, por un solo procesador compartido, o por una pluralidad de procesadores individuales, algunos de los cuales pueden ser compartidos. Además, el uso explícito del término “ procesador” o “controlador” no debe interpretarse para referirse exclusivamente a hardware capaz de ejecutar software, y puede incluir implícitamente, sin limitación, hardware de procesador de señal digital (DSP), un procesador de red, circuito integrado de aplicación específica (ASIC) u otro circuito, matriz de puerta programable en campo (FPGA), memoria de solo lectura (ROM) para almacenar software, memoria de acceso aleatorio (RAM), almacenamiento no volátil, lógica o algún otro módulo o componente de hardware físico.

Además, un elemento puede implementarse como instrucciones ejecutables por un procesador o una computadora para realizar las funciones del elemento. Algunos ejemplos de instrucciones son software, código de programa y firmware. Las instrucciones son operativas cuando las ejecuta el procesador para dirigir al procesador a realizar las funciones del elemento. Las instrucciones pueden almacenarse en dispositivos de almacenamiento que sean legibles por el procesador. Algunos ejemplos de dispositivos de almacenamiento son memorias digitales o de estado sólido, medios de almacenamiento magnéticos tales como discos magnéticos y cintas magnéticas, discos duros o medios de almacenamiento de datos digitales legibles ópticamente.

Como se usa en esta aplicación, el término “circuito” puede referirse a uno o más de los siguientes:

- (a) implementaciones de circuitos solo de hardware (tales como implementaciones en circuitos solo analógicos y/o digitales);
- (b) combinaciones de circuitos de hardware y software, tales como (de acuerdo con corresponda):
 - (i) una combinación de circuito(s) de hardware analógico y/o digital con software/firmware; y
 - (ii) cualquier parte de los procesadores de hardware con software (incluyendo los procesadores de señales digitales), software y memoria(s) que funcionan juntos para hacer que un aparato, tal como un teléfono móvil o un servidor, realice diversas funciones); y
- (c) circuito(s) y/o procesador(es) de hardware, tal como un(unos)

microprocesador(es) o una parte de un(unos) microprocesador(es), que requiere(n) software (por ejemplo, firmware) para su funcionamiento, pero el software puede no estar presente cuando no es necesario para la operación.

5 Esta definición de circuito se aplica a todos los usos de este término en esta solicitud, incluyendo cualquier reivindicación. Como ejemplo adicional, como se usa en esta solicitud, el término circuito también cubre una implementación de meramente un circuito o procesador de hardware (o múltiples procesadores) o parte de un circuito o procesador de hardware y su (o su) software y/o firmware acompañante. El término circuito también cubre, por ejemplo y si aplica al elemento de reivindicación particular, un circuito integrado de banda base
10 o un circuito integrado de procesador para un dispositivo móvil o un circuito integrado similar en un servidor, un dispositivo de red celular u otro dispositivo informático o de red.

Aunque en la presente se describieron modalidades específicas, el alcance de la descripción no se limita a esas modalidades específicas. El alcance de la descripción está definido por las siguientes reivindicaciones y sus equivalentes.

REIVINDICACIONES

1. Un elemento de Función de Gestión de Acceso y Movilidad (AMF) de una red móvil, caracterizado porque el elemento de AMF comprende:

al menos un procesador; y

5 al menos una memoria que incluye un código de programa informático ejecutable por el procesador;

el procesador se configura para hacer que el elemento de AMF:

reciba un mensaje de plano de control de un elemento de Gestión de Datos Unificados (UDM) que incluye una actualización de parámetros de configuración de Equipo de Usuario (UE) para un UE, en donde la actualización de parámetros de configuración de UE tiene protección de seguridad de acuerdo con un mecanismo de protección;

10 inserte la actualización de parámetros de configuración de UE que tiene protección de seguridad en un contenedor de un primer mensaje de Estrato Sin Acceso (NAS), en donde el contenedor está designado para la actualización de parámetros de configuración de UE; y

15 envíe el primer mensaje de NAS al UE con el contenedor que incluye la actualización de parámetros de configuración de UE que tiene protección de seguridad.

2. El elemento de AMF de conformidad con la reivindicación 1, caracterizado porque:

20 la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro de acuerdo con el mecanismo de protección.

3. El elemento de AMF de conformidad con la reivindicación 1, caracterizado porque:

25 la actualización de parámetros de configuración de UE tiene protección de integridad usando un contexto de seguridad de NAS del UE de acuerdo con el mecanismo de protección.

4. El elemento de AMF de conformidad con la reivindicación 1, caracterizado porque:

30 la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro, y el paquete seguro tiene protección de integridad usando un contexto de seguridad de NAS del UE de acuerdo con el mecanismo de protección.

5. El elemento de AMF de conformidad con la reivindicación 1, caracterizado

porque:

el primer mensaje de NAS comprende un mensaje de aceptación de registro de NAS enviado al UE durante un procedimiento de registro de NAS.

5 6. El elemento de AMF de conformidad con la reivindicación 5, caracterizado porque el procesador está configurado además para hacer que el elemento de AMF:

reciba un segundo mensaje de NAS del UE durante el procedimiento de registro de NAS con un contenedor que incluye un reconocimiento de UE de que se recibió la actualización de parámetros de configuración de UE; y

10 envíe otro mensaje de plano de control al elemento de UDM con el reconocimiento de UE;

en donde el segundo mensaje de NAS recibido del UE comprende un mensaje completo de registro de NAS o un mensaje de Transporte de NAS de Enlace Ascendente.

7. El elemento de AMF de conformidad con la reivindicación 1, caracterizado porque:

15 el primer mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Descendente de un procedimiento de transporte de NAS realizado después de un procedimiento de registro de NAS.

8. El elemento de AMF de conformidad con la reivindicación 7, caracterizado porque el procesador está configurado además para hacer que el elemento de AMF:

20 reciba un segundo mensaje de NAS del UE con un contenedor que incluye un reconocimiento de UE del UE de que se recibió la actualización de parámetros de configuración de UE; y

envíe otro mensaje de plano de control al elemento de UDM con el reconocimiento de UE;

25 en donde el segundo mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Ascendente.

9. Un método para realizar un procedimiento de actualización para actualizar los parámetros de configuración de equipo de usuario (UE) aprovisionados en un UE, caracterizado porque el método comprende:

30 recibir un mensaje de plano de control en un elemento de Función de Gestión de Acceso y Movilidad (AMF) de un elemento de Gestión de Datos Unificados (UDM) que incluye

una actualización de parámetros de configuración de UE para el UE, en donde la actualización de parámetros de configuración de UE tiene protección de seguridad de acuerdo con un mecanismo de protección;

insertar, en el elemento de AMF, la actualización de parámetros de configuración de UE que tiene protección de seguridad en un contenedor de un primer Mensaje de Estrato Sin Acceso (NAS), en donde el contenedor está designado para la actualización de parámetros de configuración de UE; y

enviar el primer mensaje de NAS desde el elemento de AMF al UE con el contenedor que incluye la actualización de parámetros de configuración de UE que tiene protección de seguridad.

10. El método de conformidad con la reivindicación 9, caracterizado porque:

la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro de acuerdo con el mecanismo de protección.

11. El método de conformidad con la reivindicación 9, caracterizado porque:

la actualización de parámetros de configuración de UE tiene protección de integridad usando un contexto de seguridad de NAS del UE de acuerdo con el mecanismo de protección.

12. El método de conformidad con la reivindicación 9, caracterizado porque:

la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro, y el paquete seguro tiene protección de integridad usando un contexto de seguridad de NAS del UE de acuerdo con el mecanismo de protección.

13. El método de conformidad con la reivindicación 9, caracterizado porque:

el primer mensaje de NAS comprende un mensaje de aceptación de registro de NAS enviado desde el elemento de AMF al UE durante un procedimiento de registro de NAS.

14. El método de conformidad con la reivindicación 13, caracterizado porque comprende, además:

recibir un segundo mensaje de NAS en el elemento de AMF desde el UE durante el procedimiento de registro de NAS con un contenedor que incluye un reconocimiento de UE de que se recibió la actualización de parámetros de configuración de UE; y

enviar otro mensaje de plano de control desde el elemento de AMF al elemento de UDM con el reconocimiento de UE;

en donde el segundo mensaje de NAS comprende un mensaje completo de registro de NAS o un mensaje de Transporte de NAS de Enlace Ascendente.

15. El método de conformidad con la reivindicación 9, caracterizado porque:

5 el primer mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Descendente de un procedimiento de transporte de NAS realizado después de un procedimiento de registro de NAS.

16. El método de conformidad con la reivindicación 15, caracterizado porque comprende, además:

10 recibir un segundo mensaje de NAS en el elemento de AMF desde el UE con un contenedor que incluye un reconocimiento de UE del UE de que se recibió la actualización de parámetros de configuración de UE; y

enviar otro mensaje de plano de control desde el elemento de AMF al elemento de UDM con el reconocimiento de UE;

15 en donde el segundo mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Ascendente.

17. El método de conformidad con la reivindicación 9, caracterizado porque comprende, además:

20 recibir el primer mensaje de NAS en el UE desde el elemento de AMF que tiene el contenedor que incluye la actualización de parámetros de configuración de UE para el UE que tiene protección de seguridad;

realizar una comprobación de seguridad en el UE para verificar la actualización de parámetros de configuración de UE; y

25 actualizar, en el UE, uno o más de los parámetros de configuración de UE con base en la fecha de actualización de parámetros de configuración de UE cuando se verifica la actualización de parámetros de configuración de UE.

18. El método de conformidad con la reivindicación 17, caracterizado porque comprende, además:

30 cuando el primer mensaje de NAS incluye un indicador de nuevo registro, iniciar un procedimiento de registro de NAS en el UE para el nuevo registro usando los parámetros de configuración de UE actualizados.

19. Equipo de usuario (UE), caracterizado porque comprende:

una Tarjeta Universal de Circuito Integrado (UICC) que aloja un Módulo Universal de Identidad del Suscriptor (USIM);

al menos un procesador; y

al menos una memoria que incluye un código de programa informático ejecutable por el procesador;

en donde al menos uno de la UICC y la memoria almacena los parámetros de configuración de UE para el UE;

el procesador está configurado para hacer que el UE:

reciba un primer mensaje de Estrato Sin Acceso (NAS) de un elemento de Función de Gestión de Acceso y Movilidad (AMF) que tiene un contenedor que incluye una actualización de parámetros de configuración de UE para el UE que tiene protección de seguridad de acuerdo con un mecanismo de protección, en donde el contenedor está designado para la actualización de parámetros de configuración de UE;

al menos una de la UICC y el procesador está configurado para hacer que el UE:

realice una comprobación de seguridad para verificar la actualización de parámetros de configuración de UE; y

actualice uno o más de los parámetros de configuración de UE con base en la actualización de parámetros de configuración de UE cuando se verifica la actualización de parámetros de configuración de UE.

20. El UE de conformidad con la reivindicación 19, caracterizado porque:

la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro dentro del contenedor del primer mensaje de NAS.

21. El UE de conformidad con la reivindicación 19, caracterizado porque:

la actualización de parámetros de configuración de UE tiene protección de integridad usando un contexto de seguridad de NAS del UE.

22. El UE de conformidad con la reivindicación 19, caracterizado porque:

la actualización de parámetros de configuración de UE está encapsulada en un paquete seguro dentro del contenedor del primer mensaje de NAS, y el paquete seguro tiene protección de integridad usando un contexto de seguridad de NAS del UE.

23. El UE de conformidad con la reivindicación 19, caracterizado porque:

el primer mensaje de NAS comprende un mensaje de aceptación de registro de

NAS enviado al UE durante un procedimiento de registro de NAS.

24. El UE de conformidad con la reivindicación 23, caracterizado porque:

cuando el mensaje de aceptación de registro de NAS incluye un indicador de reconocimiento de UE, el procesador está configurado además para hacer que el UE envíe un
5 segundo mensaje de NAS al elemento de AMF con un contenedor que incluye un reconocimiento de UE del UE de que se recibió la actualización de parámetros de configuración de UE;

en donde el segundo mensaje de NAS comprende un mensaje completo de registro de NAS o un mensaje de Transporte de NAS de Enlace Ascendente.

10

25. El UE de conformidad con la reivindicación 19, caracterizado porque:

el primer mensaje de NAS comprende un mensaje de Transporte de NAS de Enlace Descendente de un procedimiento de transporte de NAS realizado después de un procedimiento de registro de NAS.

26. El UE de conformidad con la reivindicación 25, caracterizado porque:

15

cuando el mensaje de Transporte de NAS de Enlace Descendente incluye un indicador de reconocimiento de UE, el procesador está configurado además para hacer que el UE envíe un mensaje de Transporte de NAS de Enlace Ascendente al elemento de AMF con un contenedor que incluye un reconocimiento de UE del UE de que se recibió la actualización de parámetros de configuración de UE.

20

27. El UE de conformidad con la reivindicación 19, fue recibido:

cuando el primer mensaje de NAS incluye un indicador de nuevo registro, el procesador está configurado además para hacer que el UE inicie un procedimiento de registro de NAS para el nuevo registro usando los parámetros de configuración de UE actualizados.

RESUMEN DE LA INVENCION

La presente invención se refiere a sistemas y métodos que actualizan los parámetros de configuración en un UE usando funcionalidades de plano de control. En una modalidad, un elemento de AMF de una red móvil recibe un mensaje de plano de control de un elemento de UDM que incluye una actualización de parámetros de configuración de UE para el UE. La actualización de parámetros de configuración de UE tiene protección de seguridad a través de un paquete seguro, protección de integridad, etc. El elemento de AMF está configurado para enviar de forma transparente la actualización de parámetros de configuración de UE al UE. Por lo tanto, el elemento de AMF inserta la actualización de parámetros de configuración de UE (que tiene protección de seguridad) en un contenedor de un mensaje de Estrato Sin Acceso (NAS), y envía el mensaje de NAS al UE. El UE entonces puede actualizar sus parámetros de configuración con base en la actualización cuando se completan las comprobaciones de seguridad.