GESTIÓN DE IDENTIFICADORES DE SUSCRIPCIÓN UNIFICADA EN SISTEMAS DE COMUNICACIÓN

Campo

El campo se relaciona generalmente con sistemas de comunicación y, más particularmente, pero no exclusivamente, con la gestión de identificadores de suscripción de usuarios dentro de dichos sistemas.

Antecedentes

Esta sección presenta aspectos que pueden ser útiles para facilitar una mejor comprensión de las invenciones. Por consiguiente, las declaraciones de esta sección deben leerse de esta manera y no deben entenderse como admisiones sobre lo que está en la técnica anterior o lo que no está en la técnica anterior.

La tecnología de telecomunicaciones móviles inalámbricas de cuarta generación (4G), también conocida como tecnología de evolución a largo plazo (LTE, por sus siglas en inglés), fue diseñada para proporcionar multimedia móvil de alta capacidad con altas velocidades de datos, particularmente para la interacción humana. La tecnología de próxima generación o quinta generación (5G) está destinada a ser utilizada no solo para la interacción humana, sino también para las comunicaciones de tipo máquina en las llamadas redes de Internet de las cosas (IoT).

Si bien las redes 5G están destinadas a habilitar servicios de IoT masivos (por ejemplo, un gran número de dispositivos de capacidad limitada) y servicios de IoT de misión crítica (por ejemplo, que requieren alta confiabilidad), las mejoras sobre los servicios de comunicación móvil heredados son compatibles en forma de servicios de banda ancha móvil mejorada (eMBB, por sus siglas en inglés) que proporcionan un mejor acceso inalámbrico a Internet para dispositivos móviles.

En un sistema de comunicación de ejemplo, el equipo de usuario (UE 5G en una red 5G o, más ampliamente, un UE), tal como un terminal móvil (suscriptor) se comunica a través de una interfaz aérea con una estación base o punto de acceso denominado gNB en una red 5G. El punto de acceso (por ejemplo, gNB) es, de modo ilustrativo, parte de una red de acceso del sistema de comunicación. Por ejemplo, en una red 5G, la red de acceso se denomina Sistema 5G y se describe en la especificación técnica (TS, por sus siglas en inglés) 3GPP 23.501, V15.0.0, titulada “Technical Specification Group Services and System Aspects; System Architecture for the 5G System”, cuya descripción se incorpora a la presente mediante esta referencia en su totalidad. En general, el punto de acceso (por ejemplo, gNB) proporciona acceso para el UE a una red central (CN, por sus siglas en inglés), que luego proporciona acceso para el UE a otros UE y/o una red de datos como una red de paquetes de datos (por ejemplo, Internet). Además, los procedimientos de acceso a redes 5G se

describen en la especificación técnica (TS) 3GPP 23.502, V15.1.0, titulada “Technical Specification Group Services and System Aspects; Procedures for the 5G System”, cuya descripción se incorpora a la presente mediante esta referencia en su totalidad. Adicionalmente, la especificación técnica (TS) 3GPP 33.501, V0.7.0, titulada “Technical Specification Group Services and System Aspects; Security Architecture and Procedures for the 5G System”, descripción se incorpora a la presente mediante esta referencia en su totalidad, describe adicionalmente los detalles de gestión de seguridad asociados con una red 5G.

En las redes 5G, un UE compatible con 5G puede incluir un Identificador de Suscripción Oculto (SUCI, por sus siglas en inglés) como se describe en la TS 3GPP 33.501 durante el procedimiento de Solicitud de Registro descrito en la TS 3GPP 23.502. SUCI es la forma oculta (encriptada) del Identificador Permanente del Suscriptor (SUPI). En las redes 4G (LTE) heredadas, el identificador de suscripción utilizado es un Identificador de estación móvil internacional (IMSI, por sus siglas en inglés) de acuerdo con se define en la Especificación técnica (TS) 3GPP 23.003, V15.3.0, titulada "Technical Specification Group Core Network and Terminals; Numbering, Addressing and Identification”, cuya descripción se incorpora a la presente mediante esta referencia en su totalidad. La gestión de estos identificadores de suscripción puede presentar desafíos importantes.

La especificación técnica 3GPP; *Group Core Network and Terminals; Non-Access-Stratum (NAS) protocol for 5G Systems (5GS); Stage 3 (Release 15)* describe un método para que un equipo de usuario solicite y obtenga un tipo particular de identidad móvil entre los tipos de identidad existentes.

WO 2014/053197 A1 describe un método de control de políticas y describe, además, aparatos mejorados que permiten la compatibilidad con perfiles comunitarios de usuario que se aplican a una pluralidad de suscriptores. Además, se describe la generación y aplicación de la política comunitaria y las normas de cobro derivadas de los perfiles comunitarios de usuario y preferentemente instaladas al establecer una sesión para un primer usuario. Las sesiones que se establezcan para usuarios posteriores de la pluralidad de usuarios pueden hacerse cumplir con dicha política comunitaria y las normas de cobro pueden habilitarse sin necesidad de tratarlas de forma individual.

3GPP; 23.501: *SUPI terminology correction; 3GPP draft* describe un "Identificador permanente de suscriptor" para que se pueda asignar a cada suscriptor del sistema 5G un identificador permanente de suscriptor (SUPI) 5G único global.

3GPP; SA WG3; LS on Security aspects of ECIES for concealing IMSI or SUPI describe la próxima generación de redes móviles (llamada 5G). Se describe un nuevo término general llamado SUPI (identificador permanente de suscriptor) que se propone utilizar para designar el identificador permanente de suscripción 5G único global. D4 propone, además, ocultar el IMSI o SUPI inalámbrico en 5G por el ECIES (sigla en inglés de esquema de cifrado integrado de curva elíptica).

Compendio

Las modalidades ilustrativas proporcionan técnicas mejoradas para gestionar identificadores de suscripción en sistemas de comunicación.

Por ejemplo, en una modalidad ilustrativa, un método comprende la siguiente etapa. En un equipo de usuario dado en un sistema de comunicación inalámbrica, se construye una estructura de datos de identificación de suscripción unificada. Se almacena la estructura de identificador de suscripción unificada. La estructura de datos de identificador de suscripción unificada comprende una pluralidad de campos que especifican uno seleccionado de dos o más campos de identificador de suscripción asociados con un tipo de identificador de suscripción seleccionado. El campo seleccionado de dos o más campos de identificador de suscripción (en la estructura de datos unificada del identificador de suscripción se usa para acceder a una o más redes asociadas con el sistema de comunicación inalámbrico basándose en un caso de autenticación correspondiente al tipo de identificador de suscripción seleccionado.

Se proporcionan modalidades ilustrativas adicionales en forma de un medio de almacenamiento legible por computadora no transitorio que incorpora un código de programa ejecutable que cuando es ejecutado por un procesador hace que el procesador realice las etapas anteriores. Aún otras modalidades ilustrativas comprenden un aparato con un procesador y una memoria configurada para realizar las etapas anteriores.

Ventajosamente, durante diferentes escenarios de autenticación, el equipo de usuario dado utiliza la estructura de datos unificada del identificador de suscripción para proporcionar el identificador de suscripción apropiado (por ejemplo, SUPI, SUCI o IMSI) y los parámetros asociados para el escenario de autenticación dado.

Estas y otras características y ventajas de las modalidades descritas en la presente serán más evidentes a partir de las figuras adjuntas y la siguiente descripción detallada.

Breve descripción de las Figuras

La FIG. 1 ilustra un sistema de comunicación con el que se pueden implementar una o más modalidades ilustrativas.

La FIG. 2 ilustra el equipo de usuario y un elemento/función de red para proporcionar gestión de identificadores de suscriptor durante los procedimientos de autenticación con los que se pueden implementar una o más modalidades ilustrativas.

La FIG. 3A ilustra un formato IMSI con el que se implementan una o más modalidades ilustrativas.

La FIG. 3B ilustra un formato SUPI con el que se implementan una o más modalidades ilustrativas.

La FIG. 3C ilustra un formato SUCI con el que se implementan una o más modalidades ilustrativas.

La FIG. 4 ilustra un formato de identificador de suscripción unificado, de acuerdo con una modalidad

ilustrativa.

La FIG. 5 ilustra longitudes de campo ilustrativas de un formato de identificador de suscripción unificado, de acuerdo con una modalidad ilustrativa.

La FIG. 6 ilustra un formato de identificador de suscripción unificado, de acuerdo con otra modalidad ilustrativa.

La FIG. 7 ilustra una metodología de equipo de usuario para utilizar un formato de identificador de suscripción unificado, de acuerdo con una modalidad ilustrativa.

La FIG. 8 ilustra una metodología de entidad de red para utilizar un formato de identificador de suscripción unificado, de acuerdo con una modalidad ilustrativa.

Descripción detallada

Las modalidades se ilustrarán en la presente junto con sistemas de comunicación ilustrativos y técnicas asociadas para proporcionar gestión de identificador de suscripción durante la autenticación y otros procedimientos en sistemas de comunicación. Debe entenderse, sin embargo, que el alcance de las reivindicaciones no se limita a los tipos particulares de sistemas de comunicación y/o los procesos descritos. Las modalidades se pueden implementar en una amplia variedad de otros tipos de sistemas de comunicación, mediante el uso de procesos y operaciones alternativas. Por ejemplo, aunque se ilustra en el contexto de los sistemas celulares inalámbricos que utilizan elementos del sistema 3GPP tales como un sistema 3GPP de próxima generación (5G), las modalidades descritas se pueden adaptar de manera sencilla a una variedad de otros tipos de sistemas de comunicación.

De acuerdo con modalidades ilustrativas implementadas en un entorno de sistema de comunicación 5G, una o más especificaciones técnicas (TS) e informes técnicos (TR, por sus siglas en inglés) de 3GPP proporcionan una explicación más detallada de los elementos/funciones de red y/u operaciones que pueden interactuar con partes de las soluciones inventivas, por ejemplo, las TS 3GPP 23.003 23.501, 23.502 y 33.501 mencionadas anteriormente. Otros documentos de TS/TR de 3GPP pueden proporcionar otros detalles convencionales que un experto en la técnica comprenderá. Sin embargo, si bien las modalidades son adecuadas para los estándares de 3GPP relacionados con 5G mencionados anteriormente, no se pretende que las modalidades estén limitadas a ningún estándar particular.

Las modalidades ilustrativas están relacionadas con la gestión de identificadores de suscripción asociada con redes 5G. Antes de describir tales modalidades ilustrativas, a continuación, se realizará una descripción general de los componentes principales de una red 5G en el contexto de las FIG. 1 y 2.

La FIG. 1 muestra un sistema de comunicación 100 con el que se implementan modalidades

ilustrativas. Debe entenderse que los elementos mostrados en el sistema de comunicación 100 están destinados a representar las funciones principales proporcionadas dentro del sistema, por ejemplo, funciones de acceso del UE, funciones de gestión de movilidad, funciones de autenticación, funciones de puerta de enlace de servicio, etc. En sí, los bloques mostrados en la FIG. 1 hacen referencia a elementos específicos en redes 5G que proporcionan estas funciones principales. Sin embargo, se pueden usar otros elementos de red en otras modalidades para implementar algunas o todas las funciones principales representadas. Además, debe entenderse que no todas las funciones de una red 5G se representan en la FIG. 1. Más bien, se representan funciones que facilitan una explicación de modalidades ilustrativas. Las figuras posteriores pueden representar algunos elementos/funciones adicionales.

En consecuencia, como se muestra, el sistema de comunicación 100 comprende un equipo de usuario (UE, por sus siglas en inglés) 102 que se comunica a través de una interfaz aérea 103 con un punto de acceso (gNB) 104. El UE 102 puede ser una estación móvil y dicha estación móvil puede comprender, a modo de ejemplo, un teléfono móvil, una computadora o cualquier otro tipo de dispositivo de comunicación. Por lo tanto, la expresión "equipo de usuario", tal como se usa en la presente, se debe interpretar de manera amplia, para abarcar una variedad de diferentes tipos de estaciones móviles, estaciones de suscriptor o, de manera más general, dispositivos de comunicación, lo que incluye ejemplos tales como una combinación de una tarjeta de datos insertada en una computadora portátil u otro equipo, tal como un teléfono inteligente. Dichos dispositivos de comunicación también están destinados a abarcar dispositivos comúnmente denominados terminales de acceso.

En una modalidad, el UE 102 se compone de una parte de una tarjeta universal de circuito integrado (UICC, por sus siglas en inglés) y una parte de equipo móvil (ME, por sus siglas en inglés). La UICC es la parte del UE que depende del usuario y contiene al menos un módulo de identidad del suscriptor universal (USIM, por sus siglas en inglés) y el software de aplicación apropiado. El USIM almacena de forma segura el identificador de suscripción permanente y su clave relacionada, que se utilizan para identificar y autenticar a los suscriptores para acceder a las redes. El ME es la parte del UE independiente del usuario y contiene funciones de equipo terminal (TE) y varias funciones de terminación móvil (MT).

El punto de acceso 104 es, de modo ilustrativo, parte de una red de acceso del sistema de comunicación 100. Dicha red de acceso puede comprender, por ejemplo, un sistema 5G que tiene una pluralidad de estaciones base y una o más funciones de control de red de radio asociadas. Las estaciones base y las funciones de control de la red de radio pueden ser entidades lógicamente separadas, pero en una modalidad dada pueden implementarse en el mismo elemento de red física, tal como, por ejemplo, un enrutador de estación base o un punto de acceso celular.

El punto de acceso 104 en esta modalidad ilustrativa está acoplado operativamente a las funciones de gestión de movilidad 106. En una red 5G, la función de gestión de movilidad se implementa mediante una función de gestión de acceso y movilidad (AMF, por sus siglas en inglés). Una función de anclaje de seguridad (SEAF, por sus siglas en inglés) también se puede implementar con la AMF que permite que un UE se conecte de manera segura con la función de gestión de movilidad. Una función de gestión de movilidad, como se usa en la presente, es el elemento o función (es decir, entidad) en la parte de la red central (CN) del sistema de comunicación que gestiona o participa de otra manera en, entre otras operaciones de red, operaciones de acceso y movilidad (lo que incluye autenticación/autorización) con el UE (a través del punto de acceso 104). La AMF también puede denominarse en la presente, más generalmente, como una entidad de gestión de acceso y movilidad.

La AMF 106 en esta modalidad ilustrativa está acoplada operativamente a las funciones de suscriptor doméstico 108, es decir, una o más funciones que residen en la red doméstica del suscriptor. Como se muestra, algunas de estas funciones incluyen la función de gestión de datos unificada (UDM, por sus siglas en inglés), así como una función de servidor de autenticación (AUSF, por sus siglas en inglés). La AUSF y la UDM (por separado o colectivamente junto con un servidor de suscriptor doméstico o HSS, por sus siglas en inglés, 4G) también se pueden denominar en la presente, más generalmente, como una entidad de autenticación. Además, las funciones de suscriptor doméstico incluyen, entre otras, la función de selección de división de red (NSSF, por sus siglas en inglés), la función de exposición de red (NEF, por sus siglas en inglés), la función de depósito de red (NRF, por sus siglas en inglés), la función de control de políticas (PCF, por sus siglas en inglés) y la función de aplicación (AF, por sus siglas en inglés).

El punto de acceso 104 también está operativamente acoplado a una función de puerta de enlace de servicio, es decir, la función de gestión de sesión (SMF, por sus siglas en inglés) 110, que está operativamente acoplada a una función de plano de usuario (UPF, por sus siglas en inglés) 112. La UPF 112 está operativamente acoplada a una red de paquetes de datos, por ejemplo, Internet 114. Otras operaciones y funciones típicas de tales elementos de red no se describen en la presente cuando no son el foco de las modalidades ilustrativas y se pueden encontrar en la documentación de 5G de 3GPP apropiada.

Debe apreciarse que esta disposición particular de los elementos del sistema es solo un ejemplo y se pueden usar otros tipos y disposiciones de elementos adicionales o alternativos para implementar un sistema de comunicación en otras modalidades. Por ejemplo, en otras modalidades, el sistema 100 puede comprender otros elementos/funciones que no se muestran expresamente en la presente.

Por consiguiente, la FIG. 1 es solamente una configuración ilustrativa de un sistema celular

inalámbrico, y pueden usarse numerosas configuraciones alternativas de elementos del sistema. Por ejemplo, aunque se muestran solamente elementos/funciones individuales en la modalidad de la FIG. 1, esto es solamente por simplicidad y claridad de descripción. Una modalidad alternativa dada puede incluir, por supuesto, un mayor número de tales elementos del sistema, así como elementos adicionales o alternativos de un tipo comúnmente asociado con implementaciones de sistemas convencionales.

También debe notarse que mientras que la FIG. 1 ilustra los elementos del sistema como bloques funcionales individuales, las diversas subredes que conforman la red 5G se dividen en los denominados segmentos de red. Los segmentos de red (particiones de red) comprenden una serie de conjuntos de funciones de red (NF) (es decir, cadenas de funciones) para cada tipo de servicio correspondiente utilizando la virtualización de funciones de red (NFV, por sus siglas en inglés) en una infraestructura física común. Los segmentos de red se instancian de acuerdo con sea necesario para un servicio dado, por ejemplo, servicio eMBB, servicio IoT masivo y servicio IoT de misión crítica. Un segmento o función de red se instancia así cuando se crea una instancia de ese segmento o función de red. En algunas modalidades, esto implica instalar o ejecutar de otro modo el segmento o la función de red en uno o más dispositivos anfitriones de la infraestructura física subyacente. El UE 102 está configurado para acceder a uno o más de estos servicios a través del gNB 104.

La FIG. 2 es un diagrama de bloques de una parte de un sistema de comunicación 200 que comprende un equipo de usuario 202 y un elemento/función de red 204 para proporcionar gestión de identificador de suscripción como parte de un procedimiento de autenticación en una modalidad ilustrativa. En una modalidad, el elemento/función de red 204 puede ser un UDM (como se describió anteriormente). Sin embargo, debe apreciarse que el elemento/función de red 204 puede representar cualquier elemento/función de red que se pueda+ configurar para proporcionar gestión de identificadores de suscripción y otras técnicas de autenticación descritas en la presente.

El equipo de usuario 202 comprende un procesador 212 acoplado a una memoria 216 y un circuito de interfaz 210. El procesador 212 del equipo de usuario 202 incluye un módulo de procesamiento de autenticación 214 que puede implementarse al menos en parte en forma de software ejecutado por el procesador. El módulo de procesamiento 214 realiza la gestión del identificador de suscripción y otras técnicas relacionadas descritas junto con las figuras siguientes y de otro modo en la presente. La memoria 216 del equipo de usuario 202 incluye un módulo de almacenamiento de datos de gestión de identificadores de suscripción 218 que almacena datos generados o usados de otro modo durante la gestión de identificadores de suscripción y otras operaciones.

El elemento/función de red 204 comprende un procesador 222 acoplado a una memoria 226 y un circuito de interfaz 220. El procesador 222 del elemento/función de red 204 incluye un módulo de

procesamiento de autenticación 224 que puede implementarse al menos en parte en forma de software ejecutado por el procesador 222. El módulo de procesamiento 224 realiza técnicas de autenticación mediante el uso de un identificador de suscripción proporcionado por el UE 202 y otras técnicas descritas junto con las figuras siguientes y de otro modo en la presente. La memoria 226 del elemento/función de red 204 incluye un módulo 228 de almacenamiento de datos de procesamiento de autenticación que almacena datos generados o usados de otro modo durante la autenticación y otras operaciones.

Los procesadores 212 y 222 del equipo de usuario 202 y el elemento/función de red 204 respectivo pueden comprender, por ejemplo, microprocesadores, circuitos integrados de aplicación específica (ASIC, por sus siglas en inglés), matriz de puertas lógicas programable en campo (FPGA, por sus siglas en inglés), procesadores de señales digitales (DSP, por sus siglas en inglés) u otros tipos de dispositivos de procesamiento o circuitos integrados, así como partes o combinaciones de tales elementos. Dichos dispositivos de circuito integrado, así como partes o combinaciones de estos, son ejemplos de "circuitos", tal como se usa ese término en la presente. Se puede usar una amplia variedad de otras disposiciones de hardware y software o firmware asociado para implementar las modalidades ilustrativas.

Las memorias 216 y 226 del equipo de usuario 202 respectivo y el elemento/función de red 204 se pueden usar para almacenar uno o más programas de software que son ejecutados por los procesadores 212 y 222 respectivos para implementar al menos una parte de la funcionalidad descrita en el presente documento. Por ejemplo, las operaciones de gestión de identificador de suscripción y otras funcionalidades de autenticación descritas junto con las figuras posteriores y en otras partes de la presente pueden implementarse de manera sencilla mediante el uso de código de software ejecutado por los procesadores 212 y 222.

Por lo tanto, una de las memorias 216 o 226 dada puede verse como un ejemplo de lo que se denomina aquí más generalmente como un producto de programa informático o aún más generalmente como un medio de almacenamiento legible por procesador que tiene código de programa ejecutable incorporado en este. Otros ejemplos de medios de almacenamiento legibles por procesador pueden incluir discos u otros tipos de medios magnéticos u ópticos, en cualquier combinación. Las modalidades ilustrativas pueden incluir artículos de fabricación que comprenden dichos productos de programas informáticos u otros medios de almacenamiento legibles por procesador.

La memoria 216 o 226 puede comprender más particularmente, por ejemplo, una memoria de acceso aleatorio (RAM, por sus siglas en inglés) electrónica, tal como RAM estática (SRAM, por sus siglas en inglés), RAM dinámica (DRAM, por sus siglas en inglés) u otros tipos de memoria electrónica volátil o no volátil. Estas últimos pueden incluir, por ejemplo, memorias no volátiles como

memoria flash, RAM magnética (MRAM, por sus siglas en inglés), RAM de cambio de fase (PC-RAM, por sus siglas en inglés) o RAM ferroeléctrica (FRAM, por sus siglas en inglés). El término "memoria", tal como se usa en la presente, se pretende que se interprete de manera amplia, y puede incluir adicional o alternativamente, por ejemplo, una memoria de solo lectura (ROM, por sus siglas en inglés), una memoria basada en disco u otro tipo de dispositivo de almacenamiento, así como partes o combinaciones de tales dispositivos.

Los circuitos de interfaz 210 y 220 del equipo de usuario 202 respectivo y el elemento/función de red 204 de modo ilustrativo comprenden transceptores u otro hardware o firmware de comunicación que permite que los elementos del sistema asociados se comuniquen entre sí de la manera descrita en la presente.

Es evidente a partir de la Figura 2 que el equipo de usuario 202 está configurado para la comunicación con el elemento/función de red 204 y viceversa a través de sus respectivos circuitos de interfaz 210 y 220. En el caso de que el elemento/función de red 204 sea una UDM, el equipo de usuario y la UDM están acoplados operativamente y se comunican a través de gNB 104 y AMF 106 (tal como se muestra en la FIG. 1). Esta comunicación implica que el equipo de usuario 202 envíe datos al elemento/función de red 204 y el elemento/función de red 204 envíe datos al equipo de usuario 202. Sin embargo, en modalidades alternativas, más o menos elementos de red (además de, o alternativamente al gNB y AMF) pueden acoplarse operativamente entre elementos/funciones de red 202 y 204. Se pretende que el término "datos", tal como se usa en la presente, se interprete de manera amplia, para abarcar cualquier tipo de información que se pueda enviar entre los el equipo de usuario y uno o más elementos/funciones de red, lo que incluye, entre otros, mensajes, identificadores, claves, indicadores, datos de usuario, datos de control, etc.

Debe apreciarse que la disposición particular de los componentes mostrados en la Figura 2 es solo un ejemplo y se pueden usar numerosas configuraciones alternativas en otras modalidades. Por ejemplo, cualquier elemento/función de red dado puede configurarse para incorporar componentes adicionales o alternativos y para soportar otros protocolos de comunicación.

Otros elementos del sistema (tales como, entre otros, otros elementos mostrados en la FIG. 1) también pueden configurarse para que incluyan componentes tales como un procesador, memoria e interfaz de red. Estos elementos no necesitan implementarse en plataformas de procesamiento independientes separadas, sino que podrían, por ejemplo, representar diferentes partes funcionales de una única plataforma de procesamiento común.

Dados los conceptos generales descritos anteriormente, ahora se describirán modalidades ilustrativas que abordan problemas de gestión de identificadores de suscripción.

Tal como se mencionó anteriormente, en un sistema de comunicación 4G (LTE) heredado, el identificador de suscripción permanente es típicamente un identificador de estación móvil

internacional o IMSI de un UE. Como se define en la TS 3GPP 23.003 antes mencionada, el IMSI consta de un código de país móvil (MCC, por sus siglas en inglés), un código de red móvil (MNC, por sus siglas en inglés) y un número de identificación de estación móvil (MSIN, por sus siglas en inglés). Normalmente, si es necesario proteger el identificador de suscripción, solo es necesario cifrar la parte MSIN del IMSI. Las partes de MNC y MCC proporcionan información de enrutamiento, utilizada por la red de servicio para enrutar a la red doméstica correcta. En un sistema de comunicación 5G, el identificador de permanente de suscripción se denomina identificador permanente de suscriptor (SUPI, por sus siglas en inglés). Al igual que con un IMSI, el SUPI puede utilizar un MSIN para identificar de forma única al suscriptor. Cuando el MSIN de un SUPI está encriptado, se lo conoce como un identificador oculto de suscripción o SUCI, por sus siglas en inglés. Sin embargo, se comprende en la presente que, en diferentes escenarios operativos, el UE puede necesitar representar el identificador de suscripción como un SUCI, un SUPI o un IMSI. Para abordar estos y otros problemas de gestión de identificadores de suscripción, las modalidades ilustrativas proponen una estructura de representación unificada para el identificador de suscripción.

Más particularmente, las modalidades ilustrativas abordan el desafío de usar la representación de identificador de suscripción apropiada, es decir, SUPI o su forma cifrada SUCI o incluso IMSI, en el mensaje de solicitud de registro enviado por el UE a la red y el procedimiento de autenticación del UE en la red 5G (nótese que la misma estructura de datos unificada o similar puede intercambiarse entre entidades de red). Por ejemplo, un UE mientras realiza el procedimiento de autenticación y acuerdo de clave (AKA, por sus siglas en inglés) 5G (véase, por ejemplo, la TS 3GPP 33.501 mencionada anteriormente) puede necesitar presentar el identificador de suscripción en tres formatos diferentes: SUCI, SUPI o IMSI. Si el procedimiento de autenticación utiliza el procedimiento AKA del protocolo de autenticación extensible (EAP, por sus siglas en inglés) (consulte, por ejemplo, la TS 3GPP 33.501 mencionada anteriormente), entonces la representación utiliza el formato Identificador de acceso a la red (NAI, por sus siglas en inglés), es decir, “joe@example.com” de según se define en la solicitud de comentarios (RFC) 7542 del grupo de trabajo de ingeniería de Internet (IETF, por sus siglas en inglés), “The Network Access Identifier” de mayo de 2015, cuya descripción se incorpora a la presente mediante esta referencia en su totalidad.

El desafío de los diferentes formatos de identificador de suscripción no se aborda en la TS 33.501 mencionada anteriormente, ni en ninguna otra especificación de la Etapa 3. En la especificación técnica (TS) 3GPP 33.401, V15.3.0, titulada “Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); System architecture", cuya descripción se incorpora a la presente mediante esta referencia en su totalidad, solo se define el uso de IMSI.

La FIG. 3A ilustra un formato IMSI 300 con el que se implementan una o más modalidades ilustrativas. Tal como se muestra, el formato 300 incluye una longitud fija de 15 dígitos y consta de

un código de país móvil (MCC) de 3 dígitos, un código de red móvil (MNC) de 3 dígitos y un número de identificación de estación móvil (MSIN) de 9 dígitos. En algunos casos, el MNC puede tener 2 dígitos, mientras que el MSIN es de 10 dígitos. Más detalles sobre el IMSI se definen en la TS 3GPP 23.003 mencionada anteriormente.

Tal como se explicó anteriormente, si el procedimiento de autenticación utiliza un procedimiento EAP-AKA o un procedimiento EAP de seguridad de la capa de transporte (TLS, por sus siglas en inglés) (cada uno definido en laTS 3GPP 33.501 mencionada anteriormente), entonces la representación del identificador de suscripción usa el formato NAI. RFC 7542 especifica que, para 3GPP, la parte del "nombre de usuario" es un identificador único que se deriva de información específica del dispositivo y la parte de "reino" se compone de información sobre la red doméstica seguida de la cadena base "3gppnetwork.org". +Por ejemplo, el identificador de suscripción en el formato NAI se puede representar de la siguiente manera:

234150999999999@ims.mnc015.mcc234.3gppnetwork.org

Por lo tanto, para el procedimiento EAP-AKA, el UE codificará su identificador de suscripción SUPI o SUCI en el formato NAI como se especifica en RFC 7542, por ejemplo, MSIN@ mnc.mcc.3gppnetwork.org.

Las FIG. 3B y 3C ilustran respectivamente un formato SUPI 310 y un formato SUCI 320 con los que pueden implementarse una o más modalidades ilustrativas. En este ejemplo, el formato SUPI 310 incluye un campo MCC (3 dígitos) y un campo MNC (3 dígitos), un selector MSIN y UDM (8 bits). El formato SUCI 320 es una forma cifrada del formato SUPI 310 y, como se muestra, incluye un campo MCC (3 dígitos) y un campo MNC (3 dígitos), un campo selector UDM, un MSIN cifrado y parámetros para descifrar el código cifrado. MSIN.

Se ha acordado en 3GPP SA3 admitir al menos dos curvas elípticas, la curva A y la curva B del esquema de cifrado integrado de curva elíptica (ECIES, por sus siglas en inglés) B para cifrar la parte MSIN del SUPI mientras que el identificador cifrado se utiliza como SUCI. En versiones futuras, 3GPP puede especificar más o menos curvas de la familia de curvas de criptografía de curva elíptica (ECC, por sus siglas en inglés) o puede permitir el uso de curvas propietarias para cifrar el MSIN. Sin embargo, se sabe que, si bien se prefiere el uso de esquemas estandarizados, un operador de red también puede decidir usar su propio método de cifrado específico. Además, particularmente en la fase de transición, el operador de red puede configurar los dispositivos para que utilicen únicamente un esquema nulo para SUCI. El esquema nulo se implementa de manera que devuelva la misma salida que la entrada, que se aplica tanto al cifrado como al descifrado (es decir, el MSIN no está cifrado). El esquema nulo se indica mediante el identificador de esquema en el SUCI y, por lo tanto, se puede presentar mediante el formato de identificador de suscripción unificado de igual manera.

Dado que el identificador de suscripción oculto SUCI se intercambia entre el UE (102 en la figura 1) y el UDM (parte de 108 en la FIG. 1) en la red central, el UDM debe configurarse para poder entender cómo el UE ha codificado el MSIN. Por tanto, el método de codificación debería ser parte del formato intercambiado junto con la salida codificada en sí, ya que no hay otros intercambios de mensajes entre el UE y el UDM durante el proceso de autenticación. Por lo tanto, se comprende que un esquema para representar el SUCI debe admitir una representación flexible para ajustarse a múltiples campos, cada campo lo suficientemente flexible para admitir múltiples opciones.

Las modalidades ilustrativas abordan los desafíos anteriores y otros al proporcionar una estructura unificada para representar el identificador de suscripción. Por ejemplo, una estructura unificada en una modalidad ilustrativa puede representar identificadores de suscripción tales como SUCI, SUPI e IMSI, así como varias opciones asociadas con el uso de cada identificador durante la autenticación y otras operaciones.

La FIG. 4 ilustra un formato de identificador de suscripción unificado (estructura de datos) 400, de acuerdo con una modalidad ilustrativa. Además, la FIG. 5 ilustra longitudes de campo 500 ilustrativas para cada campo mostrado en el formato de identificador de suscripción unificado 400 de la FIG. 4.

Como se muestra, el formato de identificador de suscripción unificado 400 comprende los siguientes campos (con longitudes de campo ilustrativas entre paréntesis):

Campo MCC 402 (24 bits/3 dígitos);

Campo MNC 404 (24 bits/3 dígitos);

Campo de parámetro de selección de UDM 406 (8 bits);

Campo de activación/inactivación del cifrado 408 (1 bit);

Campo KDF (sigla en inglés de función de derivación de clave) 410 (3 bits);

Campo de parámetro opcional KDF 412 (n bits/dependiente del parámetro opcional);

Campo de tipo de identificador SUPI/SUCI/IMSI 414 (2 bits);

Campo de curva ECIES seleccionada para el de cifrado 416 (4 bits);

Campo de par de claves públicas efímeras 418 (256 bits);

Campo de longitud del MSIN cifrado 420 (4 bits/128, 192, 256, 512 bits/dependiente del formato MSIN);

Campo MSIN o MSIN cifrado 422 (longitud como se especifica en el campo 420);

Campo de MSIN MAC (sigla en inglés de código de autenticación de mensajes del campo MSIN calculado mediante el uso de las curvas ECIES seleccionadas) 424 (256 bits); y

Campo de identificador del algoritmo de cifrado 426 (4 bits).

Debe apreciarse que las longitudes de campo descritas en la presente son de naturaleza ilustrativa y, por tanto, no se pretende que sean limitantes. Dependiendo de los escenarios operativos en los

que funcionen el UE y la red 5G, las longitudes de campo pueden establecerse con valores diferentes. También se debe apreciar que, en modalidades alternativas, se pueden agregar uno o más campos a la estructura de datos y/o algunos de los campos anteriores se pueden eliminar y/o simplemente no se utilizan. Además, la ubicación del campo dentro del formato de estructura 400 en la FIG. 4 es de naturaleza ilustrativa y, por tanto, se contemplan disposiciones de campo alternativas en otras modalidades. Solamente a modo de ejemplo, un campo adicional que puede ser parte de la estructura de datos (o indicado en la selección de UDM u otro campo) es un campo de Información de asistencia para la selección de segmentos de red (NSSAI, por sus siglas en inglés).

Si bien algunas modalidades ilustrativas prevén que el UE envíe la estructura completa de datos del identificador de suscripción unificado (es decir, 400 en la Figura 4) a un UDM dado (o una o más de otras entidades de red), las modalidades ilustrativas alternativas evitan el transporte de muchos parámetros indicativos tales como, por ejemplo, KDF, parámetros opcionales de KDF, curva elíptica seleccionada, identificador de algoritmo de cifrado, etc., para minimizar la sobrecarga de transmisión. En sí, una estructura de datos de identificador de suscripción unificado 600 ilustrativa alternativa se representa en la FIG. 6. Como se muestra, el formato de identificador de suscripción unificado 600 comprende los siguientes campos (con longitudes de campo ilustrativas entre paréntesis):

Campo MCC 602 (24 bits/3 dígitos);

Campo MNC 604 (24 bits/3 dígitos);

Campo de parámetro de selección de UDM 606 (8 bits);

Campo de tipo de identificador SUPI/SUCI/IMSI 608 (2 bits);

Campo de longitud del MSIN cifrado 610 (4 bits/128, 192, 256, 512 bits/dependiente del formato MSIN);

Campo MSIN o MSIN cifrado 612 (longitud como se especifica en el campo 610);

Campo de MSIN MAC (sigla en inglés de código de autenticación de mensajes del campo MSIN calculado mediante el uso de las curvas ECIES seleccionadas) 614 (256 bits); y

Campo de selección de perfil 616 (4 bits).

Debe apreciarse que las longitudes de campo descritas en la presente son de naturaleza ilustrativa y, por tanto, no se pretende que sean limitantes. Dependiendo de los escenarios operativos en los que funcionen el UE y la red 5G, las longitudes de campo pueden establecerse con valores diferentes. También se debe apreciar que, en modalidades alternativas, se pueden agregar uno o más campos a la estructura de datos y/o algunos de los campos anteriores se pueden eliminar y/o simplemente no se utilizan. Además, la ubicación del campo dentro del formato de estructura 600 en la FIG. 6 es de naturaleza ilustrativa y, por tanto, se contemplan disposiciones de campo

alternativas en otras modalidades. Solamente a modo de ejemplo, un campo adicional que puede ser parte de la estructura de datos (o indicado en la selección de UDM u otro campo) es un campo de Información de asistencia para la selección de segmentos de red (NSSAI, por sus siglas en inglés).

Los campos 602 a 614 proporcionan la misma información que sus análogos con nombres idénticos en la estructura de datos 400. Sin embargo, la estructura de datos 600 comprende el campo de selección de perfil 616. Se comprende que puede ser beneficioso preestablecer ciertos perfiles estándar para ser usados en el formato de representación de identificador de suscripción unificado entre el UE y el UDM. Estos perfiles acordados pueden definirse como valores preestablecidos (solo a modo de ejemplo, la curva ECIES de 4 bits seleccionada para el campo de cifrado). En tal caso, los valores acordados de los perfiles serán utilizados por el remitente UE y el UDM, mediante lo cual se evita el intercambio real de valores para estos parámetros.

Por ejemplo, en una versión de campos reducidos basada en perfiles de la estructura de datos unificada del identificador de suscripción, el UDM se configuraría para saber que un campo de selección de perfil dado de "0011" (si es de 4 bits) corresponde a ciertas configuraciones predeterminadas para los campos del formato de la FIG. 4 que no se envían en la versión de campo reducido de la FIG. 6, mientras que un campo de selección de perfil de "1010" significaría diferentes configuraciones predeterminadas, etc. Por lo tanto, el UDM podría prealmacenar (u obtener en tiempo real) la estructura de datos para cada posible perfil que un UE podría enviar (ya que los UE están configurados para seleccionar diferentes escenarios de autenticación).

Las modalidades ilustrativas proporcionan para todos los UE (por ejemplo, 102 en la FIG. 1) y los elementos/funciones de red tales como, de modo no taxativo, gNB (104 en la FIG. 1), AMF (parte de 106 en la Figura 1), SEAF (parte de 106 en la FIG. 1), AUSF (parte de 108 en la Figura 1) y UDM (parte de 108 en la FIG. 1), para ser compatible con los formatos de identificador de suscripción unificado 400 y 600, así como variaciones alternativas.

La FIG. 7 ilustra una metodología 700 para utilizar un formato de identificador de suscripción unificado (por ejemplo, la estructura de datos 400 de la FIG. 4 o la estructura de datos 600 de la FIG. 6) desde la perspectiva del UE, de acuerdo con una modalidad ilustrativa.

En la etapa 702, el UE mantiene un identificador de suscripción permanente (SUPI) o IMSI.

En la etapa 704, el UE mantiene una clave pública del UDM así como su propio par de claves privadas/públicas.

En la etapa 706, el UE selecciona parámetros para cifrar el MSIN (algoritmo, curvas, etc.).

En la etapa 708, el UE construye la estructura de datos unificada del identificador de suscripción (por ejemplo, 400 en la FIG. 4) mediante el uso de los parámetros de tipo de identificador, algoritmo de cifrado, indicador de curva, clave pública, MSIN cifrado, MSIN MAC, MCC, MNC, selector UDM,

KDF, KDF opcional, etc.

En la etapa 710, el UE envía la estructura de datos unificada del identificador de suscripción al UDM seleccionado durante una solicitud de acceso a la red (por ejemplo, solicitud de registro). En una modalidad, la estructura de datos unificada del identificador de suscripción puede ser la estructura de datos 400 de la FIG. 4 (es decir, versión con todos los campos completados), mientras que, en una modalidad alternativa, la estructura de datos unificada del identificador de suscripción puede ser la estructura de datos 600 de la FIG. 6 (versión de campos reducidos basada en perfiles). Otras variaciones de la estructura de datos unificada del identificador de suscripción pueden enviarse en modalidades alternativas adicionales. Las entidades de red (por ejemplo, UDM) también están configuradas para construir o de otra manera obtener/mantener tales estructuras de datos de identificación de suscripción unificadas.

La FIG. 8 ilustra una metodología 800 para utilizar un formato de identificador de suscripción unificado (por ejemplo, la estructura de datos 400 de la FIG. 4 o la estructura de datos 600 de la FIG. 6) desde la perspectiva de una entidad de red (por ejemplo, uno o más de los elementos/funciones de red descritos en la presente), de acuerdo con una modalidad ilustrativa.

En la etapa 802, la entidad de red recibe una estructura de datos del identificador de suscripción unificado.

En la etapa 804, la entidad de red descifra la estructura de datos unificada del identificador de suscripción según sea necesario.

En la etapa 806, el elemento de red realiza la autenticación del UE emisor en base al escenario de autenticación correspondiente al tipo de identificador de suscripción seleccionado en la estructura de datos recibidos.

Por lo tanto, debe enfatizarse nuevamente que las diversas modalidades descritas en la presente se presentan solamente a modo de ejemplo ilustrativo y no deben interpretarse como limitantes el alcance de las reivindicaciones. Por ejemplo, modalidades alternativas pueden utilizar configuraciones de sistemas de comunicación, configuraciones de equipos de usuario, configuraciones de estaciones base, procesos de aprovisionamiento y uso de pares de claves, protocolos de mensajería y formatos de mensajes diferentes a los descritos anteriormente en el contexto de las modalidades ilustrativas. Estas y muchas otras modalidades alternativas dentro del alcance de las reivindicaciones adjuntas serán fácilmente evidentes para los expertos en la técnica.

Reivindicaciones

Se reivindica lo siguiente:

1. Un equipo de usuario (102, 202) para un sistema de comunicación inalámbrico (100, 200), que comprende un procesador (212) y una memoria (216) configurada para realizar lo siguiente:

construir, en el equipo de usuario (102, 202) en el sistema de comunicación inalámbrico (100, 200), una estructura de datos de identificación de suscripción unificada;

almacenar la estructura de datos unificada del identificador de suscripción (400, 600), donde la estructura de datos unificada del identificador de suscripción (400, 600) comprende una pluralidad de campos (402-426, 602-616) que especifican uno seleccionado de dos o más campos de identificador de suscripción (300, 310, 320) asociados con el tipo de identificador de suscripción seleccionado, y

usar el campo seleccionado de dos o más campos de identificador de suscripción (300, 310, 320) en la estructura de datos unificada del identificador de suscripción (400, 600) para acceder a una o más redes asociadas con el sistema de comunicación inalámbrico (100, 200) basándose en un caso de autenticación correspondiente a un tipo de identificador de suscripción seleccionado.

2. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426, 602-616) comprende un campo de tipo de identificador de suscripción (414, 608).

3. El equipo de usuario (102, 202) de la reivindicación 2, donde un tipo de identificador de suscripción se puede seleccionar de un grupo que comprende un identificador de suscripción oculto, SUCI, un identificador permanente de suscriptor, SUPI, y un identificador de estación móvil internacional, IMSI.

4. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426, 602-616) comprende un campo de parámetro de selección de entidad de red (406, 606).

5. El equipo de usuario (102, 202) de la reivindicación 4, donde una entidad de red (104, 204) realiza una o más de una función de gestión unificada de datos, UDM, y una función de servidor de autenticación, AUSF.

6. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426) comprende un campo de activación/inactivación del cifrado (408).

7. El equipo de usuario (102, 202) de la reivindicación 6, donde la pluralidad de campos (402-426) comprende un campo identificador de algoritmo de cifrado (426).

8. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426) comprende un campo de función de derivación de clave (410).

9. El equipo de usuario (102, 202) de la reivindicación 8, donde la pluralidad de campos (402-426) comprende un campo de parámetro de función de derivación de clave (412).

10. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426, 602-616) comprende un campo de código de país móvil (402, 602).

11. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426, 602-616) comprende un campo de código de red móvil (404, 604).

12. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426) comprende un campo que especifica una curva seleccionada de un esquema de cifrado integrado de curva elíptica (416).

13. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426) comprende un campo de par de claves públicas efímeras (418).

14. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (402-426, 602-616) comprende un campo que especifica una longitud de un campo de número de identificación de estación móvil, MSIN, cifrado (420, 610).

15. El equipo de usuario (102, 202) de la reivindicación 14, donde la pluralidad de campos (402-426, 602-616) comprende un campo de MSIN cifrado (422, 612).

16. El equipo de usuario (102, 202) de la reivindicación 14, donde la pluralidad de campos (402-426, 602-616) comprende un campo de código de autenticación de mensaje de MSIN (424, 614).

17. El equipo de usuario (102, 202) de la reivindicación 1, donde el sistema de comunicación inalámbrico (100, 200) comprende un sistema 5G.

18. El equipo de usuario (102, 202) de la reivindicación 1, que comprende, además, enviar la estructura unificada de datos del identificador de suscripción (400,600) a al menos una entidad de red (104, 204) en el sistema de comunicación inalámbrico (100, 200) para obtener acceso a la una o más redes asociadas con el sistema de comunicación inalámbrico (100, 200).

19. El equipo de usuario (102, 202) de la reivindicación 1, donde la pluralidad de campos (602-616) comprende un campo de selección de perfil (616).

20. El equipo de usuario (102, 202) de la reivindicación 19, donde el campo de selección de perfil (616) permite que el equipo de usuario (102, 202) notifique a una o más entidades de red en la una o más redes asociadas con el sistema de comunicación inalámbrico (100, 200) que usen valores preestablecidos para uno o más parámetros seleccionables asociados con el campo de identificador de suscripción (300, 310, 320) seleccionado.

21. El equipo de usuario (102, 202) de la reivindicación 20, que comprende, además, enviar la estructura unificada de datos del identificador de suscripción (600) con el campo de selección de perfil (616) y un conjunto reducido de campos a al menos una de las una o más entidades de red en el sistema de comunicación inalámbrico (100, 200) para obtener acceso a la una o más redes asociadas con el sistema de comunicación inalámbrico (100, 200).

22. Un método que comprende:

construir, en un equipo de usuario (102, 202) en un sistema de comunicación inalámbrico (100, 200), una estructura de datos de identificador de suscripción unificada (400, 600);

almacenar la estructura de datos unificada del identificador de suscripción (400, 600), donde la estructura de datos unificada del identificador de suscripción (400. 600) comprende una pluralidad de campos (402-426, 602-616) que especifican uno seleccionado de dos o más campos de identificador de suscripción (300, 310, 320) asociados con un tipo de identificador de suscripción seleccionado, y

usar el campo seleccionado de dos o más campos de identificador de suscripción (300, 310, 320) en la estructura de datos unificada del identificador de suscripción (400, 600) para acceder a una o más redes asociadas con el sistema de comunicación inalámbrico (100, 200) basándose en un caso de autenticación correspondiente a un tipo de identificador de suscripción seleccionado.

23. Un medio de almacenamiento legible por computadora no transitorio que incorpora código de programa ejecutable que, cuando se ejecuta mediante un procesador (212) hace que el procesador (212) realice las etapas de:

construir, en un equipo de usuario (102, 202) en un sistema de comunicación inalámbrico (100, 200), una estructura de datos de identificador de suscripción unificada (400, 600);

almacenar la estructura de datos unificada del identificador de suscripción (400, 600), donde la estructura de datos unificada del identificador de suscripción (400. 600) comprende una pluralidad de campos (402-426, 602-616) que especifican uno seleccionado de dos o más campos de identificador de suscripción (300, 310, 320) asociados con el tipo de identificador de suscripción seleccionado, y

usar el campo seleccionado de dos o más campos de identificador de suscripción (300, 310, 320) en la estructura de datos unificada del identificador de suscripción (400, 600) para acceder a una o más redes asociadas con el sistema de comunicación inalámbrico (100, 200) basándose en un caso de autenticación correspondiente a un tipo de identificador de suscripción seleccionado..

Resumen

En un equipo de usuario dado en un sistema de comunicación, se construye una estructura de datos de identificación de suscripción unificada. La estructura de datos unificada del identificador de suscripción incluye una pluralidad de campos que especifican información para uno seleccionado de dos o más tipos de identificador de suscripción y parámetros seleccionables asociados con el tipo de identificador de suscripción seleccionado, y donde la información en la estructura de datos unificada del identificador de suscripción es utilizable por el equipo de usuario dado para acceder a una o más redes asociadas con el sistema de comunicación en base a un escenario de autenticación correspondiente al tipo de identificador de suscripción seleccionado. Por ejemplo, durante diferentes escenarios de autenticación, el equipo de usuario dado utiliza la estructura de datos unificada del identificador de suscripción para proporcionar el identificador de suscripción apropiado (por ejemplo, SUPI, SUCI o IMSI) y los parámetros asociados para el escenario de autenticación dado.