(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 972 798**

(51) Int. Cl.:

H04W 12/06 (2011.01)
H04W 8/18 (2009.01)
H04W 4/10 (2009.01)
H04L 65/1016 (2012.01)
H04L 65/1073 (2012.01)
H04L 65/4061 (2012.01)
H04W 8/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.07.2018 PCT/US2018/043905**

(87) Fecha y número de publicación internacional: **07.02.2019 WO19027803**

(96) Fecha de presentación y número de la solicitud europea: **26.07.2018 E 18759441 (1)**

(97) Fecha y número de publicación de la concesión europea: **07.02.2024 EP 3646629**

(54) Título: **Procedimiento y sistema para el acceso y uso de múltiples credenciales ISIM o ISIM**

(30) Prioridad:

04.08.2017 US 201715669656

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.06.2024

(73) Titular/es:

MALIKIE INNOVATIONS LIMITED (100.0%)
The Glasshouses GH2, 92 Georges Street Lower
Dun Laoghaire, Dublin A96 VR66, IE

(72) Inventor/es:

RUSSELL, NICHOLAS JAMES y
BUCKLEY, ADRIAN

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento y sistema para el acceso y uso de múltiples credenciales ISIM o ISIM

Reivindicación de prioridad

Esta solicitud reivindica la prioridad de la solicitud de patente estadounidense n.º 15/669.656 presentada el 4 de agosto de 2017.

Campo de la divulgación

La presente divulgación se refiere a los servicios del subsistema de multimedios (IMS) sobre protocolo de Internet (IP) y, en particular, al uso de un módulo de identidad de abonado IMS (ISIM) para acceder a los servicios IMS.

Estado de la técnica

El subsistema de multimedios IP es un marco utilizado para ofrecer servicios de multimedios IP a dispositivos. Utiliza redes de conmutación de paquetes en lugar de redes de conmutación de circuitos.

El ISIM es una aplicación que típicamente reside en una tarjeta de circuito integrado universal asociada a un dispositivo. El ISIM proporciona solo un único conjunto de información de credenciales IMS, lo que se traduce en que un equipo de usuario (UE) sea capaz de utilizar el ISIM para conexiones a un solo IMS.

Previamente, el Proyecto de asociación de tercera generación (3GPP) suponía que un UE solo necesitaría conectar un único IMS, donde ese único IMS era proporcionado por la red móvil terrestre pública de origen (HPLMN) del UE y los diferentes servicios en el IMS se proporcionarían por medio de servidores de aplicaciones ubicados dentro de la red central IMS o ubicados externamente al IMS y conectados por medio de una interfaz o punto de referencia.

Sin embargo, es posible que un UE necesite conectarse a múltiples servicios IMS mediante el uso de determinados datos que solo están disponibles en un ISIM (p. ej., credenciales de seguridad, identidades, etc.) para obtener diferentes servicios basados en IMS. Por ejemplo, es posible que se necesite un IMS para el acceso de voz sobre evolución a largo plazo (LTE) (VoLTE), es posible que se necesite otro IMS para la función de pulsar para hablar (MCPTT) de misión crítica y es posible que se necesite otro IMS para los servicios de comunicación enriquecidos (RCS).

En algunos casos, p. ej., un escenario de itinerancia en el que el UE está conectado a una PLMN visitada (VPLMN), el IMS de la VPLMN puede proporcionar algo de acceso para que el UE se conecte de nuevo al IMS de la HPLMN del UE. Sin embargo, el acceso al IMS de la VPLMN se basa en la autenticación y autorización por parte del IMS de la HPLMN, que utiliza el ISIM que pertenece a la HPLMN en el UE.

La divulgación EP 2 469 898 A1 enseña el uso de reglas de selección para seleccionar un USIM entre una pluralidad de USIM.

La divulgación WO 2009/141919 A1 enseña que una entidad móvil IMS utiliza el ISIM de otro dispositivo remoto para permitir el acceso ISIM remoto de modo que se permite que un UE IMS sin UICC utilice el ISIM del dispositivo remoto.

La divulgación WO 2012/054030 A1 divulga un conjunto de herramientas de aplicación de tarjeta compatible con un sistema de multimedios IP.

El documento WO 2016/167553 A1 divulga un procedimiento para realizar la autenticación y el registro de la función pulsar para hablar de misión crítica.

Breve descripción de los dibujos

La presente divulgación se entenderá mejor con referencia a los dibujos, en los que:

la figura 1 es un diagrama de bloques que muestra una arquitectura IMS funcional básica;

la figura 2 es un diagrama de flujo de datos que muestra un procedimiento de registro IMS básico;

la figura 3 es un diagrama de flujo de datos que muestra una o más autenticaciones y autorizaciones de servicios de misión crítica (MCX);

la figura 4 es un diagrama de bloques que muestra un modelo funcional para la gestión de identidad MCX;

la figura 5 es un diagrama de flujo de datos que muestra la autenticación de usuario de MCX mediante el uso de equipo de MCX;

la figura 6 es un diagrama de flujo de datos que muestra un flujo de OpenID Connect para prestar soporte a la autenticación de usuario de MCX;

la figura 7 es un diagrama de flujo de datos que muestra la autenticación y acuerdo de claves IMS;

la figura 8 es un diagrama de bloques que muestra una conexión de PDN;

la figura 9 es un diagrama de bloques que muestra el establecimiento de sesión de PDU solicitada por un equipo de usuario en una red 5G;

la figura 10 es un diagrama de flujo de datos que muestra el registro de un ME para múltiples funciones IMS mediante el uso de una pluralidad de ISIM;

la figura 11 es un diagrama de bloques que muestra una estructura de datos de ejemplo para un ISIM;

la figura 12 es un diagrama de flujo de datos que muestra un flujo de OpenID Connect para prestar soporte a la autenticación de usuario de MCX y que incluye además una indicación ISIM;

la figura 13 es un diagrama de flujo de datos que muestra la autenticación y el registro del usuario de MC desde un equipo de usuario;

Compendio

La presente invención se refiere a un procedimiento, un dispositivo y un medio legible por ordenador según las reivindicaciones.

La figura 14 es un diagrama de flujo de datos que muestra el registro de un ME para múltiples funciones IMS mediante el uso de un único ISIM que tiene múltiples credenciales;

la figura 15 es un diagrama de bloques que muestra un dispositivo informático simplificado que puede utilizarse con las realizaciones de la presente divulgación; y

la figura 16 es un diagrama de bloques que muestra una entidad móvil de ejemplo.

Descripción detallada de las figuras

La presente divulgación proporciona un procedimiento en una entidad móvil que permite el uso de múltiples servicios de multimedios (IMS) sobre protocolo de Internet (IP), comprendiendo el procedimiento: leer datos de una pluralidad de módulos de identidad de abonado IMS (ISIM) asociados con la entidad móvil; almacenar los datos en la entidad móvil; y enlazar una función en la entidad móvil a uno de la pluralidad de ISIM.

La presente divulgación proporciona además una entidad móvil que permite el uso de múltiples servicios de multimedios (IMS) sobre protocolo de Internet (IP), comprendiendo la entidad móvil: un procesador; y un subsistema de comunicaciones, en el que la entidad móvil está configurada para: leer datos de una pluralidad de módulos de identidad de abonado IMS (ISIM) asociados con la entidad móvil; almacenar los datos en la entidad móvil; y enlazar una función en la entidad móvil a uno de la pluralidad de ISIM.

La presente divulgación proporciona además un medio legible por ordenador para almacenar código de instrucción que permite el uso de múltiples servicios de multimedios (IMS) sobre protocolo de Internet (IP), que, cuando se ejecutan por un procesador de una entidad móvil, hacen que la entidad móvil: lea datos de un pluralidad de módulos de identidad de abonado IMS (ISIM) asociados con la entidad móvil; almacene los datos en la entidad móvil; y enlace una función en la entidad móvil a uno de la pluralidad de ISIM.

Es posible que un UE necesite conectarse a múltiples servicios IMS mediante el uso de determinados datos que solo están disponibles en un ISIM (p. ej., credenciales de seguridad, identidades, etc.) para obtener diferentes servicios basados en IMS. Los servicios e iniciativas basados en IMS muestran que se implementan IMS que no pertenecen a la HPLMN de un UE. Por ejemplo, en los servicios de misión crítica (MC), tal como MCPTT, vídeo MC o datos MC, el IMS que proporciona servicios MC (a veces también denominado(s) servicio(s) MCX) podría alojarse en un proveedor de servicios de misión crítica en lugar de la HPLMN de la UE.

Además, en RCS, muchos operadores PLMN en la industria subcontratan su alojamiento RCS a una entidad externa o proveedor externo, que incluye un IMS no proporcionado por la HPLMN de la UE.

En VoLTE existe la misma posibilidad de subcontratación que en RCS. Sin embargo, los operadores PLMN pueden alojar ellos mismos el IMS para VoLTE, por ejemplo, gracias al uso de una infraestructura común para llamadas VoLTE y CS.

Otros servicios IMS también podrían utilizar un IMS que no pertenezca a la HPLMN de un UE. Así, los ejemplos anteriores por sí solos no deben verse como una lista exhaustiva de servicios de la industria basados en IMS. Otras combinaciones o derivados de lo anterior, así como otros servicios basados en IMS actuales y futuros, pueden requerir que un UE se conecte a IMS separados para diferentes servicios.

Por lo tanto, según una realización de la presente divulgación, al UE se le proporciona acceso a múltiples instancias de un ISIM (que puede, pero no necesariamente, residir en una UICC) y elige qué ISIM usar para autenticarse en diferentes IMS basándose en una indicación de con qué servicio(s) o aplicación(es) está asociado el ISIM.

Según otras realizaciones de la presente divulgación, un único ISIM puede tener múltiples credenciales para la autenticación en múltiples IMS.

En las figuras siguientes, se muestran los flujos de comunicación entre funciones.

Sin embargo, los expertos en la materia apreciarán que los flujos de comunicación pueden, en algunos casos, proceder a través de entidades intermedias o funciones lógicas que no se muestran.

En la presente divulgación, los siguientes términos tienen por lo menos el significado proporcionado en la Tabla 1 a continuación.

Término	Definición
Asociación GSM (GSMA)	Un foro de la industria para empresas de comunicaciones móviles.
Información de credenciales IMS	Un conjunto de datos que permite que un agente de usuario (UA) del protocolo de inicio de sesión (SIP) (p. ej., un equipo de usuario) pueda conectarse y autenticarse en un IMS.
Operaciones aisladas (IOPS)	Donde un nodo B evolucionado (eNB) pierde conectividad con el resto de la red central y el eNB luego cambia sus características para convertirse en una red completamente aislada.
Testigo web de notación de objetos JavaScript (JSON)	El testigo web JSON (JWT) es un medio compacto y seguro del localizador uniforme de recursos (URL) para representar notificaciones que se transferirán entre dos partes.
Open Mobile Alliance (OMA)	Una organización de desarrollo de estándares.
Documento de referencia permanente (PRD)	Un tipo de documento elaborado por la GSMA.
Servicios de comunicación enriquecidos (RCS)	Un conjunto de servicios definidos por la GSMA, p. ej., en GSMA PRD RCC.07 (más otros documentos).
Equipo de usuario (UE)	Un dispositivo que consiste en por lo menos una entidad móvil (ME) y opcionalmente también una tarjeta de circuito integrado universal (UICC), donde la UICC contiene por lo menos un ISIM y opcionalmente también uno de un módulo de identidad de abonado (SIM) o módulo de identidad de abonado universal (USIM). Podría utilizar accesos de comunicaciones inalámbricos y/o fijos.
Tarjeta de circuito integrado universal (UICC)	Una entidad física que puede ser extraíble o no extraíble (también conocida como "UICC integrada") que aloja aplicaciones seguras tales como el ISIM, el USIM, el SIM, etc. A veces esto se denomina "tarjeta SIM".
Vídeo sobre evolución a largo plazo (LTE) (ViLTE)	Implica vídeo sobre IP (p. ej., mediante el uso de IMS) sobre una red radioeléctrica 4G/LTE y en general se refiere al perfil definido y mantenido por la asociación GSM en GSMA PRD IR.94. En general se requiere compatibilidad con VoLTE cuando ViLTE es compatible con cualquier dispositivo y/o implementación de red.
Voz sobre acceso de paquetes a alta velocidad (HSPA) (VoHSPA)	Implica voz sobre IP (p. ej., mediante el uso de IMS) sobre la red de acceso de paquetes de alta velocidad del sistema universal de telecomunicaciones móviles (UMTS) y en general se refiere al perfil definido y mantenido por la

Término	Definición
	asociación GSM en GSMA PRD IR.58.
Voz sobre LTE (VoLTE)	Implica voz sobre IP (p. ej., mediante el uso de IMS) sobre una red radioeléctrica 4G/LTE y en general se refiere al perfil definido y mantenido por la asociación GSM en GSMA PRD IR.92. El uso de este término también puede implicar, aunque no necesariamente, compatibilidad con ViLTE, VoWiFi, VoHSPA y/o USSI.
Voz sobre WiFi (VoWiFi)	Implica voz y, opcionalmente, vídeo sobre IP (p. ej., mediante el uso de IMS) sobre una red de área local inalámbrica (WLAN) (p. ej., utilizando un túnel hasta el EPC de un operador, utilizando acceso directo al EPC de un operador por medio de una WLAN de acceso de confianza), y en general se refiere a uno o ambos perfiles definidos y mantenidos por la asociación GSM en GSMA PRD IR.51 y GSMA PRD NG.106.
Servicio de simulación de datos de servicios suplementarios no estructurados (USSD) en IMS (USSI)	Implica mensajería USSD sobre IP (p. ej., mediante el uso de IMS) sobre una red de conmutación de paquetes, p. ej., LTE, HSPA, 5G, etc. Puede, pero no es necesario, hacer referencia al perfil definido y mantenido por la asociación GSM en GSMA PRD NG.101.
Identidad	Podría ser una identidad de usuario pública o una identidad de usuario privada. Podría ser una identidad del dispositivo o una combinación de todos. La identidad podría ser un comodín.
Red	1 o muchos nodos de red, p. ej., nodo de red 1, nodo de red 2, etc.
ID de usuario pública / IMPU (ID de usuario pública de multimedios IP)	Podría ser, entre otros: un MSISDN, dirección de correo electrónico, URI de SIP, URI de Tel, ID de servicio de misión crítica (MC). La propiedad de esta identidad es que es conocida por el público y se puede utilizar como medio de direccionamiento para llamadas/sesiones.
ID de usuario privada / IMPI (ID de usuario privada de multimedios IP)	IMSI, SIP URI La propiedad de esta identidad es que no se puede utilizar como medio de direccionamiento para llamadas/sesiones y, por lo general, solo la conocen la red y el dispositivo.
Identidad de usuario	Puede ser una ID de usuario pública o una ID de usuario privada o ambos. La identidad podría ser un comodín

TABLA 1: Definiciones de términos

IMS

A continuación, se hace referencia a la figura 1, que muestra una descripción general de un sistema de multimedios IP (red central). Una red IMS puede, aunque no es necesario, estar conectada a una red de cuarta generación (4G), una red de quinta generación (5G) o una WLAN, y puede consistir en varios elementos funcionales, un subconjunto de los cuales se describe con respecto a la figura 1.

En particular, el UE 110 puede comunicarse con una función de control de sesión de llamada al proxy (P-CSCF) 120. La P-CSCF 120 es el primer punto de entrada a la red IMS. La P-CSCF 120 puede incluir una pasarela de nivel de aplicación IMS (IMS-ALG) 122.

Las comunicaciones entre el UE 110 y la P-CSCF 120 se realizan mediante el uso de una interfaz Gm, que se utiliza para intercambiar mensajes entre los UE SIP o pasarelas de voz sobre protocolo de Internet (VOIP) y la P-CSCF 120. Los mensajes se intercambian mediante SIP.

Una función de control de sesión de servicio de llamadas (S-CSCF) 130 maneja sesiones en la red y encamina mensajes SIP a servidores de aplicaciones (AS) IMS y P-CSCF apropiados. La S-CSCF 130 se comunica con la P-CSCF mediante el uso de una interfaz Mw, que se utiliza para intercambiar mensajes entre las CSCF. Los mensajes se intercambian mediante SIP.

Se utiliza una función de control de sesión de llamada de interrogación (I-CSCF) 140 como punto de entrada para encontrar un abonado en la red y ayudar a asignar una S-CSCF 130 cuando un abonado se registra en la red. La I-CSCF 140 se comunica tanto con la P-CSCF 120 como con la S-CSCF 130 mediante el uso de una interfaz Mw y SIP.

El AS 150 típicamente proporciona una funcionalidad específica del servicio. Un ejemplo de un AS puede incluir un servidor de aplicaciones de telefonía, que típicamente se utiliza para proporcionar lógica de servicio y control para servicios de telefonía tales como voz/audio o vídeo. Otro ejemplo de un AS puede ser un AS de continuidad y centralización de servicios, que típicamente se utiliza para proporcionar lógica y control de servicios para centralizar servicios entre circuitos conmutados (CS) e IMS en el IMS y transferir sesiones SIP y sus medios asociados entre los UE y/o a través de diferentes redes IP.

En una realización, el AS 150 puede ser el servidor de aplicaciones IMS. Dicho servidor de aplicaciones IMS tiene la lógica y el software que ejecuta servicios para un abonado IMS. Puede haber de 0 a muchos servidores de aplicaciones de este tipo en una red. El AS 150 se comunica con el UE 110 mediante el uso de una interfaz Ut sobre un protocolo de acceso de configuración (XCAP) del lenguaje de marcaje extensible (XML). El AS 150 se comunica además con la I-CSCF 140 a través de una interfaz Ma mediante el uso de SIP. El AS 150 se comunica además con la S-CSCF 130 mediante el uso de la interfaz ISC y SIP.

El servidor del abonado de origen (HSS) 160 proporciona una primera base de datos que contiene el perfil del abonado, incluidas las identidades y a qué servicios se ha abonado, y proporciona funcionalidad de ubicación, así como una base de datos de autenticación/autorización (segunda base de datos). El HSS 160 se comunica con la I-CSCF 140 mediante el uso de una interfaz Cx y el protocolo Diámetro. De forma parecida, el HSS 160 se comunica con la S-CSCF 130 mediante el uso de la interfaz Cx y el protocolo Diámetro. Obsérvese que, desde una perspectiva de implementación, estas dos bases de datos pueden ser una o dos entidades físicas.

El HSS 160 se comunica además con el AS 150 mediante el uso de la interfaz Sh y el protocolo Diámetro.

Se puede encontrar una descripción más completa de la funcionalidad de los elementos anteriores en la especificación técnica (TS) 23.002 del 3GPP, "*Network Architecture*", como se establece, por ejemplo, en la versión 14.1.0 de marzo de 2017, y TS 23.228, "*IP Multimedia Subsystem (IMS); Stage 2*", como se proporciona, por ejemplo, en la versión 14.4.0 de junio de 2017.

Se necesita un registro IMS para que un abonado y su UE puedan utilizar los servicios basados en IMS. Un procedimiento de registro IMS se describe, por ejemplo, en 3GPP TS 23.228. Específicamente, la subcláusula 5.2.2.3 prevé el registro IMS y se describe a continuación con respecto a la figura 2.

Como se observa en la figura 2, el UE 210 está en una red 220 visitada. El UE 210 se comunica con la P-CSCF 212 de la red 220 visitada.

Además, una red 222 originaria incluye la I-CSCF 214 así como el HSS 216 y la S-CSCF 218.

El procedimiento de registro incluye que el UE 210 envíe un mensaje 230 de registro a la P-CSCF 212. A continuación, el mensaje de registro se reenvía en el mensaje 232 a la I-CSCF 214.

En base al mensaje recibido 232, la I-CSCF 214 envía un mensaje 240 de consulta-de-CX/extraer-selección-CX al HSS 216 y recibe, en respuesta, un mensaje 242 de respuesta (resp.) de consulta-de-CX/resp. de extraer-selección-CX.

Basándose en el mensaje 242, la I-CSCF 214 puede enviar un mensaje 250 de registro a la S-CSCF 218.

La S-CSCF 218, en respuesta al mensaje 250, envía un mensaje 252 de poner-CX/extraer-CX al HSS 216 y recibe, en respuesta al mensaje 252, un mensaje 254 de resp. de poner-CX/resp. de extraer-CX.

La S-CSCF 218 puede entonces realizar el control del servicio (p. ej., ponerse en contacto con los servidores de aplicaciones), como se muestra en el bloque 260, y proporcionar un mensaje 262 "200 OK" de regreso a la I-CSCF 214.

La I-CSCF 214 luego reenvía el mensaje 200 OK a la P-CSCF 212 como el mensaje 264. La P-CSCF 212 luego reenvía el mensaje 200 OK como el mensaje 266 de regreso al UE 210. El mensaje 200 OK 266 indica al UE 210 que se ha registrado satisfactoriamente para los servicios IMS.

Una vez que el UE 210 se ha registrado en la red, puede recibir y enviar más peticiones/mensajes SIP.

Si bien el ejemplo de la figura 2 muestra el UE 210 y la P-CSCF 212 en una red 220 visitada, en otras realizaciones el UE 210 podría estar en la VPLMN mientras que la P-CSCF 212 está en la HPLMN. En aún otras realizaciones, tanto el UE 210 como la P-CSCF 212 podrían estar en la HPLMN. Por lo tanto, la realización de la figura 2 es meramente una configuración de ejemplo.

Servicios basados en IMS

Los servicios basados en IMS pueden incluir una variedad de servicios. Los ejemplos incluyen VoLTE/ViLTE/VoWiFi y servicios de comunicación enriquecidos (RCS). Cada uno se describe a continuación.

En VoLTE/ViLTE/VoWiFi, estos son todos los servicios proporcionados por un operador u portadora de telefonía móvil o celular a sus abonados. VoLTE puede incluir voz y SMS sobre LTE. ViLTE incluye vídeo a través de LTE y VoWiFi incluye voz, SMS y vídeo a través de wifi.

En algunos escenarios, estos servicios se despliegan para suplementar, complementar o reemplazar servicios equivalentes a través del acceso con conmutación de circuitos. Por ejemplo, dado que no existen servicios de conmutación de circuitos en el acceso LTE/red de acceso radioeléctrico terrestre universal evolucionado (E-UTRAN)/de cuarta generación (4G), se puede implementar VoLTE como una solución para proporcionar servicios de voz en este acceso.

La GSMA ha elaborado perfiles de los estándares del Proyecto de asociación de tercera generación (3GPP) para los servicios mencionados anteriormente en diversos documentos.

Todos VoLTE, ViLTE y VoWiFi utilizan un IMS, con la excepción de los SMS que pueden utilizar un IMS o señalización de estrato sin acceso (NAS). Típicamente, pero no en todas las circunstancias, las portadoras de telefonía móvil ofrecen dichos servicios utilizando su propio IMS. Sin embargo, en algunos casos se podrá utilizar un IMS de otra empresa o empresa subcontratada.

Con respecto a los servicios de comunicación enriquecidos, RCS es un conjunto de servicios proporcionados por un operador u portadora de telefonía móvil a sus abonados que incluye servicios tales como voz sobre IP, chat/mensajería instantánea, transferencia de archivos, uso compartido de vídeos, entre otros servicios de esfuerzo razonable. El RCS ha pasado por muchas iteraciones, una iteración reciente conocida como perfil universal de RCS. Por ejemplo, en la Tabla 2 a continuación se proporciona un extracto de la GSMA que describe el perfil universal.

El perfil universal (UF) es un conjunto común de características y habilitadores técnicos acordados por la industria de comunicaciones avanzadas. El perfil universal se ha desarrollado para ofrecer una experiencia de usos comunes más enriquecida a nivel mundial y simplificar tanto el desarrollo de productos como la implementación de mensajería avanzada por parte de los operadores. Esto proporcionará la escala necesaria para desarrollar la mensajería como plataforma. Versión 1 (disponible ahora): incluye funciones básicas tales como la detección de capacidades que serán interoperativas entre regiones, chat, chat grupal, transferencia de archivos, mensajería de audio, uso compartido de vídeos, multidispositivo, llamadas enriquecidas, uso compartido de ubicación y esbozos en tiempo real.

Tabla 2: Extracto de GSMA sobre el perfil universal

RCS utiliza un IMS. Las portadoras de telefonía móvil ofrecen estos servicios utilizando su propio IMS o un IMS que pertenece a otra empresa. Si la portadora de telefonía móvil ofrece los servicios utilizando su propio IMS, el IMS puede ser el mismo IMS que se utiliza para VoLTE/ViLTE/VoWiFi.

Servicios de misión crítica

En 3GPP, se definen múltiples servicios de misión crítica (MC) 3GPP. Estos incluyen, entre otros. función de pulsar para hablar de misión crítica (MCPTT), vídeo de misión crítica (MCVideo), datos de misión crítica (MCData), entre otras opciones. Tal como se usa en la presente memoria, el término MCX se utiliza para indicar uno o una pluralidad de servicios genéricos de misión crítica. Además, tal como se usan en la presente memoria, los términos siguientes pueden usarse de forma intercambiable:

- UE de MCX / UE de MC / UE de servicio MC
- Cliente de MCX / cliente de MC / cliente de servicio MC
- Usuario de MCX / usuario de MC / usuario de servicio MC
- Dominio MCX / dominio MC
- Servicio MCX / servicio MC

- Sistema MCX / sistema MC

Los servicios MC son una iniciativa global 3GPP para prestar soporte a funcionalidades tales como la funcionalidad pulsar para hablar (MCPTT, p. ej., un servicio parecido a un "walkie-talkie"), compartir vídeos y acceder a vídeos almacenados en la red (MCVideo), y en MCData el envío/recepción de mensajería de servicio de datos cortos (SDS) y entrega de archivos (FD), entre otros servicios. Actualmente, los servicios MC están definidos para funcionar en redes LTE y, típicamente, están destinados a organizaciones que incluyen agencias gubernamentales tales como servicios de seguridad, policía, bomberos y rescate, así como organizaciones comerciales tales como empresas de servicios públicos y transporte. La señalización del servicio MC (p. ej., señalización de llamadas, señalización de sesiones, señalización de mensajes, señalización de transferencia de archivos, señalización de emisión en continuo, entre otras opciones) se basa en una red central basada en SIP, que en algunos casos puede ser una red central IMS 3GPP.

Los servidores de servicios MC, a los que también se puede hacer referencia como servidores de MCX en esta divulgación, pueden incluir uno o una pluralidad de dichos servidores tales como un servidor MCPTT, un servidor MCVideo, un servidor MCData, entre otras opciones. Un servidor de servicio MC típicamente manejará la mayor parte de la señalización del servicio MC y la lógica del servicio MC.

Un servidor de gestión de ubicación recibe y almacena datos/información de ubicación del usuario, proporciona información de ubicación del usuario a servidores de servicios MC y puede adquirir información de ubicación proporcionada por operadores de red móvil terrestre pública (PLMN).

En algunos escenarios de implementación, los operadores comerciales de PLMN pueden operar la red central IMS/SIP para el servicio MC de una agencia de seguridad pública mientras que la capa de aplicación del servicio MC, el servidor del servicio MC (que podría ser un servidor MCPTT, un servidor MCVideo, un servidor MCData, ubicación servidor de administración, etc.) y otras entidades de red de la capa de aplicación pueden operarse mediante una agencia de seguridad pública o un proveedor de servicios de seguridad pública como la Autoridad de la Red de Primera Respuesta (FirstNet) de los Estados Unidos. Algunas comunicaciones de seguridad pública se consideran altamente confidenciales, no solo en términos de la comunicación de medios real (p. ej., voz, vídeo, mensajes, flujo de datos, archivos, etc.), sino también en términos de las identidades de las partes implicadas en una llamada y la naturaleza de esa llamada.

Todos los servicios MC utilizan un núcleo IMS/SIP. Típicamente, las agencias de seguridad pública ofrecen estos servicios a través del propio núcleo IMS/SIP de la agencia de seguridad pública (que puede compartirse con otras agencias de seguridad pública), el núcleo IMS/SIP de otra empresa o por medio de un IMS que pertenece a una portadora/PLMN. Sin embargo, en los dos últimos casos, el núcleo IMS/SIP utilizado típicamente será un núcleo IMS/SIP aislado que en general se despliega con el fin de ofrecer servicios MC a la agencia de seguridad pública y sus usuarios.

Identidad (ID) del servicio de misión crítica (MC)

El ID del servicio MC se define en la especificación técnica (TS) 23.280 de 3GPP, "Common functional architecture to support mission critical services; Stage 2", como se proporciona, por ejemplo, en la versión 15.0.0 de junio de 2017. El ID del servicio MC se define como "un nombre genérico para la ID de usuario de un usuario de misión crítica dentro de un servicio MC específico. El ID del servicio MC podría reemplazarse por el ID MCPTT, el ID MCVideo o el ID MCData según el contexto".

Cada uno del MCPTT ID, MCVideo ID y MCData ID: son una instancia de un ID de servicio MC dentro del servicio MCPTT, servicio MCVideo y servicio MCData, respectivamente; son globalmente únicos dentro de cada servicio; proporcionan una identidad a un usuario dentro del servicio respectivo; pueden identificar el sistema MC principal/doméstico del usuario de MC asociado; y están formateados como URI.

Pueden existir otras instancias del ID del servicio MC, y las soluciones contenidas en la presente memoria no se limitan necesariamente a los servicios MCPTT, MCVideo y MCData. Existen atributos asociados con instancias del ID del servicio MC configurado en los servicios MC que se relacionan con el usuario humano del servicio MC. Típicamente, esta información identifica al usuario del servicio MC por nombre o rol, y también puede identificar la organización o agencia de un usuario. El servidor de servicios MC puede utilizar dichos atributos asociados con una instancia de un ID de servicio MC para tomar decisiones de autorización sobre el servicio MC concedido al usuario. Por ejemplo, el servicio MC podría utilizar automáticamente un atributo que identifique el rol de un usuario como responsable de incidentes para concederle derechos administrativos adicionales, tales como la capacidad de crear grupos, conceder acceso a grupos de conversación privilegiados, entre otras opciones.

Autenticación y autorización de usuario del servicio MC

En todos los servicios MC, se lleva a cabo un procedimiento de autenticación del servicio MC a nivel de aplicación antes de que el usuario realice un registro en el núcleo IMS/SIP y antes de que el usuario obtenga la autorización del servicio MC. Este procedimiento autentica al usuario del servicio MC para un sistema MC y proporciona un testigo de seguridad que utilizará el UE durante un registro inicial posterior del núcleo IMS/SIP. La autenticación y autorización

se realizan para proporcionar acceso a los servicios MC del usuario de MC, incluidos los servidores de servicios MC necesarios.

La funcionalidad de autenticación y autorización se proporciona en una entidad móvil (ME), por ejemplo, como direcciones de servidor, y es independiente de la UICC. Tal como se usa en la presente memoria, una entidad móvil también podría denominarse dispositivo móvil o equipo de usuario (UE).

Se proporciona una descripción general del procedimiento de autorización y autenticación de usuarios de MC en 3GPP TS 33.180, "Security of the Mission Critical Service". Una parte de esta especificación técnica se describe a continuación con respecto a la figura 3.

A continuación, se hace referencia a la figura 3, que muestra las etapas genéricas para la autenticación y autorización del usuario de MCX. En particular, en la realización de la figura 3, un UE 310 de MCX puede comunicarse con una red LTE y una red 312 de núcleo de paquete mejorado (EPC). Además, el UE 310 puede comunicarse con un servidor 314 de gestión de ID y un núcleo 316 SIP. El núcleo 316 SIP puede ser un IMS. El dominio MCX se muestra en el bloque 318 en la realización de la figura 3.

El UE 310 de MCX primero realiza la autenticación LTE y el procedimiento de vinculación, como se muestra en el bloque 320. La autenticación se especifica, por ejemplo, en 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture", como se proporciona, por ejemplo, en la versión 15.0.0 de junio de 2017.

A continuación, el UE 310 de MCX realiza las etapas siguientes para completar la autenticación del usuario, la autorización del usuario, el registro del servicio MCX y el enlace de identidad entre las identidades de la capa de señalización y los ID del servicio MC. El UE 310 de MCX puede realizar autenticación de usuario de MCX, como se muestra con la flecha 322, y el registro y autenticación SIP, como se muestra con la flecha 324. Las etapas de las flechas 322 y 324 se pueden realizar en cualquier orden o en paralelo. Además, en escenarios donde el orden tiene un impacto en los enlaces de identidad entre una identidad de capa de señalización y el ID de servicio MC, se puede realizar un nuevo registro en el núcleo SIP para actualizar la identidad de capa de señalización registrada.

Por lo tanto, según la realización de la figura 3, el UE 310 de MCX realiza una autenticación de usuario de MCX como se muestra en la flecha 322 con el servidor 314 de gestión de identidad.

Con referencia a la figura 4, el servidor 314 de gestión de identidad está ubicado en el núcleo 410 de servicios comunes de MC y se comunica con un cliente 412 de gestión de identidad ubicado en el UE 310 de MCX. Estas entidades establecen las bases para la autenticación y autorización de usuarios de MCX.

El punto de referencia CSC-1, entre el cliente 412 de gestión de identidad en el UE y el servidor 314 de gestión de identidad, proporciona la interfaz para la autenticación del usuario. El CSC-1 es una interfaz directa de protocolo de transferencia de hipertexto (HTTP) entre el cliente 412 de gestión de identidad en el UE 310 y el servidor 314 de gestión de identidad. El cliente 412 de gestión de identidad admite OpenID Connect 1.0, como se define por ejemplo en OpenID Connect Core 1.0 que incorpora el conjunto de erratas 1.

La autenticación de usuario de MCX, la autorización de servicio de usuario de MCX, OpenID Connect 1.0 y el perfil OpenID Connect para el servicio MCX/MC forman la base de la arquitectura de gestión de identidad.

En consonancia con los estándares OpenID Connect 1.0 y OAuth 2.0, el CSC-1 incluye dos interfaces de gestión de identidad; el punto de conexión de autorización y el punto de conexión del testigo. Los estándares OAuth 2.0, por ejemplo, incluyen IETF RFC 6749, "The OAuth 2.0 Authorization Framework" y IETF RFC 6750, "The OAuth 2.0 Authorization Framework: Bearer Token Usage". Estos puntos de conexión están separados e independientes entre sí y requieren direcciones IP separadas e independientes. El servidor del punto de conexión de autorización y el servidor del punto de conexión de testigo pueden denominarse colectivamente servidor de gestión de identidad.

La conexión HTTP entre el cliente 412 de gestión de identidad y el servidor de gestión de identidad puede protegerse usando el protocolo de transferencia de hipertexto (HTTP) sobre seguridad de la capa de transporte (TLS), que también puede denominarse protocolo seguro de transferencia de hipertexto (HTTPS).

Para prestar soporte a la autenticación de usuario de MCX, el servidor 314 de gestión de identidad se proporciona con el ID de MC del usuario y los ID de servicio de MC (el ID de servicio de MC puede ser el mismo que el ID de MC). Se crea y mantiene una correlación entre el ID de MC y los ID de servicio de MC en el servidor 314 de gestión de identidad. Cuando un usuario de MCX desea autenticarse con el sistema MCX, el ID de MC y las credenciales se proporcionan a través del cliente 412 de gestión de identidad al servidor 314 de gestión de identidad. El servidor 314 de gestión de identidad recibe y verifica el ID de MC y las credenciales y, si son válidos, devuelve por lo menos uno de: un testigo de identificación, un testigo de actualización y un testigo de acceso al cliente 412 de gestión de identidad específico para las credenciales. El cliente 412 de gestión de identidad aprende los ID de servicio MC del usuario a partir del testigo de identificación. La Tabla 3 a continuación muestra los testigos MCX y su utilización.

Tipo de testigo	Consumidor del testigo	Descripción
Testigo de identificación	Cliente(s) de UE	Contiene el ID del servicio MC para por lo menos un servicio autorizado (ID MCPTT, ID MCVideo, ID MCData). Asimismo, puede contener otra información relacionada con el usuario que sea útil para el cliente.
Testigo de acceso	KMS, servidor MCPTT, etc. (Servidor de recursos)	Testigo de corta duración (definible en el IdMS) que transmite la identidad del usuario. Este testigo contiene el ID del servicio MC para por lo menos un servicio autorizado (ID MCPTT, ID MCVideo, ID MCData).
Testigo de actualización	Servidor de gestión de ID (servidor de autorización)	Permite que el UE obtenga un nuevo testigo de acceso sin obligar al usuario a que inicie sesión nuevamente.

TABLA 3: TESTIGOS DE MCX

Para prestar soporte a la autorización del usuario de MCX, los testigos de acceso obtenidos durante la autenticación del usuario se utilizan para obtener servicios MCX para el usuario. La autorización de servicio de usuario de MCX se define en la cláusula 5.1.3 de 3GPP TS 33.180.

Para prestar soporte al modelo funcional de identidad de los servicios MCX/MC, los ID de servicio MC: se suministran en el servidor de gestión de identidad y se asignan a los ID de MC; se suministran en el servicio de gestión de claves (KMS) y se asignan a las claves asociadas a la identidad; se suministran en la base de datos de usuarios del servicio MCX/MC y se asignan a un perfil de usuario; y se suministran en los servidores de gestión de grupo (GMS) y se asignan a los ID de grupo.

Se encuentran más detalles sobre la arquitectura de autorización de usuario en la cláusula 5.1.3 de 3GPP TS 33.180.

A continuación, se hace referencia a la figura 5, que muestra el marco de autenticación del usuario. El marco utiliza el punto de referencia CSC-1 que se muestra en la figura 4.

En la realización de la figura 5, el procedimiento de autenticación de usuario de la flecha 322 de la figura 3 se detalla más en 3 subetapas que comprenden el marco de autenticación del usuario de MCX.

Específicamente, como se muestra con la flecha 510, el UE 310 de MCX y el servidor 314 de gestión de identidad establecen un túnel seguro. Las etapas posteriores aprovechan este túnel.

En la flecha 520, se realiza un proceso de autenticación de usuario en el que el UE 310 de MCX proporciona una identidad de usuario al servidor 314 de gestión de identidad. En la flecha 530, se entregan las credenciales que identifican de forma única al usuario de MCX al cliente de MCX.

Después de los mensajes en la flecha 530, el cliente de MCX usa las credenciales obtenidas a partir del mensaje en la flecha 530 para realizar la autorización del servicio de usuario de MCX en la flecha 328 de la figura 3.

El marco que admite los mensajes de las flechas 520 y 530 utiliza OpenID Connect 1.0.

En referencia de nuevo a la figura 3, para la autenticación de registro SIP en la flecha 324, se pueden utilizar procesos tales como los descritos anteriormente con respecto a la figura 2.

El núcleo 316 SIP puede entonces realizar un registro de terceros con el dominio 318 MCX, como se muestra en el ejemplo de la figura 3 con la flecha 326.

Posteriormente, la autorización del servicio de usuario de MCX se puede realizar entre el UE 310 de MCX y el dominio 310 de MCX, como se muestra con la flecha 328.

Como se describe anteriormente, la autenticación y autorización de usuario de servicios MC/MCX utiliza el marco OpenID, que incluye un testigo de identificación y un testigo de acceso, entre posiblemente otros testigos. Los testigos se obtienen según el marco OAuth 2.0.

A continuación, se hace referencia a la figura 6, que describe el marco de autenticación del usuario de MCX mediante el uso del protocolo OpenID Connect. Específicamente, la figura 6 muestra las etapas mediante las cuales un equipo 310 de usuario de MCX se autentica en el servidor 314 de gestión de identidad, lo que da como resultado un conjunto de credenciales entregadas al UE que identifican de forma única los ID del servicio MC. Los medios por los cuales estas credenciales se envían desde el UE a los servicios MCX se describen en la cláusula 5.1.3 de 3GPP TS 33.180.

El marco de autenticación admite soluciones de autenticación de usuarios extensibles basadas en la política del proveedor de servicios MCX, con autenticación de usuario basada en nombre de usuario/contraseña como procedimiento admitido. Son posibles otros procedimientos de autenticación de usuarios tales como biometría, SecureID, entre otras opciones.

Así, como se observa en la figura 6, el UE 310 establece un túnel seguro con el servidor 314 de gestión de identidad, como se muestra con la flecha 610.

A continuación, el UE 310 envía una petición de autenticación de OpenID Connect en la flecha 620 al servidor 314 de gestión de identidad. La petición puede contener una indicación de los procedimientos de autenticación admitidos por el UE 310.

A continuación, se realiza la autenticación de usuario, como se muestra en el bloque 630. Las credenciales principales para la autenticación del usuario (p. ej., datos biométricos, seguridad, OTP, nombre de usuario/contraseña) se basan en la política del proveedor de servicios MCX.

En un ejemplo, el servidor 314 de gestión de identidad envía un mensaje HTML, p. ej., un formulario HTML al UE 310 donde solicita al usuario su nombre de usuario y la contraseña, mostrado con la flecha 632.

En respuesta, el UE 310 envía el nombre de usuario y la contraseña (proporcionada por el usuario) al servidor 314 de gestión de identidad, como se muestra con la flecha 634.

El servidor 314 de gestión de identidad envía a continuación una respuesta de autenticación de OpenID Connect, mostrada con la flecha 640, al UE 310 que contiene un código de autorización.

El UE 310 envía una petición de testigo de OpenID Connect, mostrada con la flecha 650, al servidor 314 de gestión de identidad, que pasa el código de autorización.

El servidor 314 de gestión de identidad envía entonces una respuesta de testigo de OpenID Connect, como se muestra con la flecha 660, al UE 310 que contiene un testigo de identificación y un testigo de acceso (cada uno de los cuales identifica de forma única al usuario del servicio MCX). El UE 310 consume el testigo de identificación para personalizar el cliente de MCX para el usuario de MCX, y el UE 310 utiliza el testigo de acceso para comunicar la identidad del usuario de MCX al servidor o servidores de MCX. Así, es en los mensajes de la flecha 660 donde se devuelven los testigos.

En la Tabla 4 siguiente se proporciona un mensaje de ejemplo en la flecha 660 que muestra el contenido.

```
HTTP/1.1 200 OK

Content-Type: application/json

Cache-Control: no-cache, no-store

Pragma: no-cache



{

"access_token":"S1AV32hkKG",

"token_type":"Bearer",

"expires_in":3600,

"refresh_token":"tGzv3J0kFOXG5Qx2T1KWIA",

"id_token":"eyJO... NiJ9.eyJic…     161jI ifX0.DeWt4Qu…     ZXso"
}
```

TABLA 4: Contenido del mensaje de ejemplo

La Tabla 4 muestra un mensaje que contiene un testigo_acceso, que comprende una cadena de caracteres. También contiene un testigo_id, que aparece como una cadena de caracteres. Sin embargo, si se descodifica la cadena de caracteres, será lo que se muestra en la Tabla 5 a continuación.

El testigo_id y testigo_acceso forman parte del marco de OpenID Connect, donde los testigos se describen mediante "notificaciones JSON". Las "notificaciones JSON" también pueden denominarse atributos. OpenID tiene un conjunto estándar de notificaciones JSON que se pueden ampliar para incluir otras notificaciones JSON adicionales.

El testigo_id se parece al concepto de una tarjeta de identidad y se describe en un perfil JWT. El testigo_id contiene atributos que identifican al usuario, que incluyen, por ejemplo, un nombre, dirección, números de teléfono, entre otros datos.

```
{
"sub": "248289761001",
"name":"Jane Doe",
"given_name":"Jane",
"family_name":"Doe",
"preferred_username":"j.doe",
"email": "janedoe@example.com"
"picture":"http://example.com/janedoe/me.jpg"
}
```

TABLA 5: Ejemplo de testigo_id usando el esquema de una notificación JSON

La Tabla 5 muestra un esquema de notificación JSON de ejemplo para un testigo_id. A continuación, esto se codifica como una cadena alfanumérica y se envía en el testigo_id como se muestra en la Tabla 4 como una cadena de caracteres.

UICC

Una UICC se identifica mediante una Identificación de tarjeta de circuito integrado (ICCID). Solo existe un ICCID por UICC. Se almacena en un archivo básico (EF) identificado como EF_{ICCID}, como se especifica en ETSI TS 102 221, "Smart Cards; UICC-Terminal interface; Physical and logical characteristics", como se encuentra por ejemplo en la versión 8.2.0 (junio de 2009).

Cuando un dispositivo o UE o ME o terminal se inicializa y decide que necesita seleccionar una aplicación, instancia o perfil UICC, el dispositivo examinará el archivo EF_{DIR} y seleccionará una aplicación de ese archivo. Esto se proporciona, por ejemplo, en 3GPP TS 31.103, "Characteristics of the IP Multimedia Services Identity Module (ISIM) application", como se proporciona, por ejemplo, en la versión 14.2.0 de junio de 2017. En la Tabla 6 a continuación se proporciona un extracto de esta TS.

5.1.1.1 Selección de aplicación ISIM Si el terminal desea participar en la operación IMS, después de la activación de la UICC (véase TS 31.101), el terminal deberá seleccionar una aplicación ISIM, si aparece una aplicación ISIM en el archivo EF_{DIR}, utilizando SELECT por nombre de DF como se define en TS 31.101.

TABLA 6: Extracto de 3GPP TS 31.103

El archivo EF_{DIR} contiene una lista de identificadores de aplicaciones (AID) y cadenas de etiquetas asociadas. El archivo EF_{DIR} se define en 3GPP TS 31.101, "Technical Specification Group Terminals; UICC-Terminal Interface; Physical and Logical Characteristics", como se encuentra, por ejemplo, en la versión 14.1.0 de marzo de 2017. En la Tabla 7 a continuación se muestra un extracto.

13 Archivos independientes de la aplicación

13.1 EF_{DIR}

El EF_{DIR} es un archivo fijo lineal según la MF y está bajo la responsabilidad del emisor.

Tabla 13.1: EF_{DIR} a nivel de MF

Identificador: “2F00”	Estructura: Lineal fija		Imperativo	
SFI: Imperativo				
Tamaño del registro: X bytes		Actividad de actualización: baja		
Condiciones de acceso: LEER ALW ACTUALIZAR ADM DESACTIVAR ADM ACTIVAR ADM				
Bytes	Descripción		I/O	Longitud
1 a X	Objeto TLV de plantilla de aplicación		I	X bytes

El EF consiste en uno o más registros, y cada registro puede contener una entrada. Cada entrada en el EF_{DIR} es un objeto de datos (DO) de plantilla de aplicación tal como se define en ISO/IEC 7816-4. Una plantilla de aplicación DO es un objeto BER-TLV construido con una longitud máxima de 127 bytes y tiene un DO AID imperativo. Dentro del alcance de la presente memoria, todos los demás DO son opcionales.

En la tabla 13.2 se muestra la codificación de los DO imperativos y los DO opcionales que tiene especial significado para el presente documento. Todos los demás DO cumplen con la norma ISO/IEC 7816-4.

Tabla 13.2: Codificación de una entrada de plantilla de aplicación

Longitud	Descripción	Estado
1	Etiqueta de plantilla de aplicación = “61”	I
1	Longitud de la plantilla de aplicación = “03”-“7F”	I
1	Etiqueta de identificador de aplicación = “4F”	I
1	Longitud del AID = “01”-“10”	I
“01” a “10”	Valor AID. Véase ETSI TS 101 220.	I
1	Etiqueta a nivel de aplicación = “50”	O
1	Longitud a nivel de aplicación	O
nota 1	Valor a nivel de aplicación	O
NOTA 1: La etiqueta de la aplicación es un DO que contiene una cadena de bytes proporcionada por el proveedor de la aplicación para mostrarla al usuario a modo de información, p. ej., el nombre del operador. La parte del valor de la etiqueta de la aplicación se codificará según el anexo A. Se recomienda que el número de bytes en la etiqueta de la aplicación no supere los 32. NOTA 2: Otros DO de ISO/IEC 816-4 también pueden estar presentes, a discreción del emisor de la aplicación.				

TABLA 7: Extracto de 3GPP TS 31.101

Un AID tiene dos componentes, el primero es un "Identificador de proveedor de aplicaciones registrado" (RID), que tiene cinco bytes de longitud, y el segundo es una "extensión del identificador de aplicación de propiedad" (PIX), que tiene hasta once bytes de longitud. El RID identifica 3GPP (su valor/codificación es "A000000087"), los primeros nueve bytes del PIX identifican la aplicación, p. ej., USIM, ISIM, etc., y los dos últimos bytes están disponibles para "datos específicos del proveedor de aplicaciones". El AID está estandarizada en ETSI TS 101 220, "Smart Cards; ETSI numbering system for telecommunication application providers", como se encuentra por ejemplo en la versión 11.0.0 de junio de 2011.

Datos ISIM

Los requisitos de datos ISIM se especifican en 3GPP TS 33.203, "3G security; Access security for IP-based services", por ejemplo, en la versión 14.1.0 de junio de 2017.

La cláusula 8.1 de esta TS identifica los requisitos de la aplicación ISIM para prestar soporte a la seguridad del acceso al IMS. No identifica ningún dato o función que pueda ser necesaria en la aplicación ISIM para fines no relacionados con la seguridad.

En la cláusula 8.1 se especifica que la aplicación ISIM incluirá: la identidad de usuario privada de multimedios IP (IMPI); por lo menos una identidad de usuario pública de multimedios IP (IMPU); nombre de dominio de la red originaria; asistencia para la comprobación de números de secuencia en el contexto del dominio IMS; para el ISIM se aplica el mismo marco de algoritmos especificado para el USIM; y una clave de autenticación.

Autenticación ISIM

La autenticación ISIM se define, por ejemplo, en 3GPP TS 33.203 y, en particular, en la sección 6.1.1. Una secuencia de mensajes y un flujo de información de cómo un UE con un ISIM se registra en el IMS y qué parámetros se utilizan en esa operación se muestra a continuación con respecto a la figura 7.

Antes de que un usuario pueda acceder a los servicios IM, es necesario registrar por lo menos una IMPU y autenticar la IMPI en el IMS a nivel de aplicación. Para registrarse, el UE envía un mensaje de REGISTRO SIP hacia el servidor de registro SIP, es decir, la S-CSCF, que realizará la autenticación del usuario junto con el HSS. Los flujos de mensajes son los mismos independientemente de si el usuario ya tiene una IMPU registrada o no.

Así, como se observa en la figura 7, el UE 710 se comunica con la P-CSCF 712. Además, una red incluye la I-CSCF 714 así como el HSS 716 y la S-CSCF 718.

El procedimiento de registro incluye que el UE 710 envíe un mensaje de registro 720 a la P-CSCF 712. Tal como se utiliza en la figura 7, SMn significa mensaje SIP n y CMm significa mensaje Cx m lo cual tiene relación con el proceso de autenticación.

A continuación, el mensaje de registro se reenvía en el mensaje 722 a la I-CSCF 714.

Basándose en el mensaje recibido 722, la I-CSCF 714 realiza una selección Cx con el HSS 716, como se muestra en el bloque 724.

La I-CSCF 714 puede enviar un mensaje de registro 730 a la S-CSCF 718.

La S-CSCF 718, en respuesta al mensaje 730, realiza un procedimiento 732 de entrada de CX con el HSS 716.

A partir de la entrada de CX, la S-CSCF 718 puede utilizar un vector de autenticación (AV) para autenticar y acordar una clave con el usuario. Si la S-CSCF 718 no tiene un AV válido, entonces la S-CSCF 718 envía una petición 740 de AV al HSS 716 en CM1 junto con el número m de AV deseados, donde m es por lo menos uno.

Cada vector de autenticación consiste en los componentes siguientes: un número aleatorio RAND, una respuesta prevista XRES, una clave de cifrado CK, una clave de integridad IK y un testigo de autenticación AUTN. Cada vector de autenticación es bueno para una autenticación y acuerdo de claves entre la S-CSCF 718 y el usuario IMS (según lo identificado por el IMPI).

Por ejemplo, la respuesta 742 enviada de regreso a la S-CSCF 718 puede tener la forma Cx-AV-Req-Resp(IMPI,RAND1||AUTN1||XRES1||CK1||IK1,....,RANDn||AUTNn||XRESn||CKn||IKn).

En base a la respuesta, la S-CSCF 718 envía una pregunta de autenticación al UE a través de la I-CSCF 714, como se muestra en el mensaje 750. Cuando la S-CSCF 718 necesita enviar una pregunta de autenticación al usuario, selecciona el siguiente vector de autenticación de la matriz ordenada, es decir, los vectores de autenticación en un S-CSCF concreto se utilizan según el principio de primero en entrar/primero en salir. Sin embargo, esto no excluye el uso de los procedimientos normales de retransmisión de la capa de transacción SIP.

El mensaje 750 puede tener el formato SM4:4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK).

El mensaje 750 se reenvía a la P-CSCF 712 en el mensaje 752. Cuando la P-CSCF recibe el mensaje 752, almacena la(s) clave(s) (IK y CK) y reenvía el resto del mensaje sin las claves al UE 710 en el mensaje 754. El mensaje 754 puede adoptar la forma SM6:4xx Auth_Challenge(IMPI, RAND, AUTN). Tras recibir la pregunta en el mensaje 754, el UE toma el AUTN, que incluye un MAC y el SQN. La UE calcula el XMAC y comprueba que XMAC=MAC y que el SQN esté en el intervalo correcto según 3GPP TS 33.102. Si ambas comprobaciones son correctas, el UE utiliza el RES y algunos otros parámetros para calcular una respuesta de autenticación.

Esta respuesta se coloca en el encabezado de autorización y se envía de regreso al registrador en el mensaje 760 de registro. Cabe destacar que en esta etapa el UE también calcula las claves de sesión CK e IK. En particular, el UE 710 envía un mensaje 760 de registro a la P-CSCF 712. El mensaje 760 puede tener el formato SM7: REGISTRO (IMPI, respuesta de autenticación).

A continuación, el mensaje de registro se reenvía en el mensaje 762 a la I-CSCF 714.

Basándose en el mensaje recibido 762, la I-CSCF 714 realiza una consulta de Cx con el HSS 716, como se muestra en el bloque 764.

La I-CSCF 714 puede enviar un mensaje de registro 766 a la S-CSCF 718.

La S-CSCF 718 puede entonces realizar un procedimiento 770 de entrada de CX con el HSS 716 y un procedimiento 772 de extracción de CX con el HSS 716, y proporcionar una respuesta 2xx, p. ej., "200 OK", mensaje 780 de regreso a la I-CSCF 714.

La I-CSCF 714 luego reenvía el mensaje de respuesta 2xx a la P-CSCF 712 5 como el mensaje 782. La P-CSCF 712 luego reenvía el mensaje de respuesta 2xx como el mensaje 784 de regreso al UE 710. El mensaje de respuesta 2xx 784 indica al UE 710 que se ha registrado satisfactoriamente para los servicios IMS.

Conectividad de datos LTE

Un UE que desee utilizar conectividad o servicios de datos celulares puede aprovechar por lo menos una red de acceso radioeléctrico terrestre (E-UTRAN) del sistema de telecomunicaciones móviles universal (UMTS) evolucionado, un núcleo de paquete mejorado (EPC) y una red de datos por paquetes (PDN). La combinación de una E-UTRAN y un EPC se conoce como sistema de paquetes mejorado (EPS). En un sistema 5G, esto se compone de una o ambas de una radio de próxima generación (NG) y una red central de NG.

A continuación, se hace referencia a la figura 8. En el ejemplo de la figura 8, el UE 810 se conecta con una PDN 820 mediante el uso de una conexión 822 PDN. Dichas conexiones PDN pueden, en algunas realizaciones, denominarse contextos de protocolo de datos por paquetes (PDP) en redes de segunda generación (2G) o tercera generación (3G), o denominarse sesiones de unidad de datos por paquetes (PDU) en redes de quinta generación (5G). La conexión 822 PDN se puede usar para transmitir y recibir datos tales como datos del plano de control o señalización, datos del plano de usuario, medios de voz/audio, medios de vídeo entre otras opciones de datos, entre el UE 810 y el PDN 820. Una conexión 822 PDN proporciona un mecanismo para que un UE se comunique con una PDN.

La conexión 822 PDN típicamente es a través de una E-UTRAN 832 y un EPC 834, como se proporciona en la figura 8. Sin embargo, en otras realizaciones la conectividad puede ser a través de una red de área local inalámbrica (WLAN) y un EPC, y la presente divulgación no se limita a una conexión 822 PDN en particular.

El E-UTRAN 832 y el EPC 834 típicamente, pero no siempre, pertenecen a un operador de red móvil/PLMN o a una portadora de telefonía móvil, mientras que la PDN 820 puede pertenecer a un operador u otra entidad. Por ejemplo, la PDN puede pertenecer a una corporación, una agencia de seguridad pública o una red empresarial.

El EPS 830 puede consistir únicamente en una HPLMN (primer proveedor de servicios) o puede consistir además en una HPLMN y una VPLMN (segundo proveedor de servicios), utilizándose esta última para itinerancia. Dichas HPLMN y VPLMN no se muestran en la figura 8 por motivos de brevedad.

La EPS 830 puede consistir en diversas entidades. Estos incluyen uno o más de un nodo B mejorado (eNB), entidad de gestión de la movilidad (MME), pasarela de servicio (S-GW), pasarela de PDN (P-GW) y/o servidor del abonado de origen (HSS), entre otros nodos de red.

La conexión 822 PDN proporciona una ruta para datos entre un UE 810 y una PDN 120. Durante el establecimiento de la conexión de PDN, la PDN 820 se identifica mediante un nombre de punto de acceso (APN) y después mediante otros parámetros en la conexión de PDN establecida. El APN puede identificar un nodo de pasarela (p. ej., P-GW, un nodo de soporte de servicio general de radio por paquetes (GPRS) de pasarela (GGSN), entre otros, en el EPC 834 que permite el acceso a la PDN 820.

Como se define en la especificación técnica (TS) 23.003 del Proyecto de asociación de tercera generación (3GPP), "*Numbering, addressing and identification*", como se proporciona, por ejemplo, en la versión 14.3.0 de marzo de 2017, un APN consiste en una porción de identidad de red (NI) y una identidad de operador (OI). Tanto la parte NI como la OI consisten en de una cadena de caracteres separados por puntos. Los caracteres entre los puntos se denominan "etiquetas".

En una realización, el contenido de la porción NI puede no estar definido, mientras que el contenido de la porción OI está estrictamente definido. La red en general añade la porción OI al final de un NI. Los nodos de red que pueden realizar esta función incluyen, entre otros, el nodo de soporte del servicio GPRS (SGSN), MME, S-GW, P-GW, entre otros.

En otras realizaciones, el UE puede proporcionar tanto la NI como la OI si el UE desea solicitar específicamente la conexión a una PDN en una red móvil terrestre pública (PLMN) específica y, en ausencia de que el UE proporcione la OI, la red utiliza lógica definida para decidir la OI que se añadirá a la NI. Esta lógica definida se puede encontrar, por ejemplo, en 3GPP TS 23.060, "*General Packet Radio Service (GPRS); Service description; Stage 2*", como se proporciona por ejemplo en la versión 14.4.0 de junio de 2017.

Un UE está en itinerancia cuando no está vinculado a una PLMN que sea su HPLMN o una HPLMN extendida (EHPLMN). Cuando el UE está en itinerancia, una conexión de PDN puede conectarse a una PDN en la VPLMN o HPLMN. Una conexión a una PDN en la VPLMN a veces se denomina "itinerancia con desvío local" (LBO). Una conexión a una PDN en la HPLMN mientras el UE está en itinerancia se denomina a veces "encaminamiento inicial" o encaminamiento inicial de interfaz S8 ("S8HR").

Un UE puede tener más de una conexión de PDN si el UE necesita conectarse a más de una PDN. Una conexión de PDN consiste en uno o más portadores EPS, a los que se puede hacer referencia sencillamente como "portadores", para que los datos se transmitan y reciban entre el UE y la red. Un portador de EPS dentro de una conexión de PDN se considera el "portador por defecto" o "portador de EPS por defecto" y normalmente es el que se crea en el momento del establecimiento de la conexión de PDN. El resto de los portadores de EPS, además del portador de EPS por defecto, se conocen como "portadores de EPS dedicados" o sencillamente "portadores dedicados" y se utilizan para proporcionar una calidad de servicio (QoS) diferente a los datos de los portadores de EPS por defecto.

Cada portador de EPS tiene un identificador de clase de QoS (QCI). Se puede encontrar una lista completa de QCI, por ejemplo, en la subcláusula 6.1.7.2 de 3GPP TS 23.203, "Policy and charging control architecture", como se proporciona, por ejemplo, en la versión 14.4.0 de junio de 2017. Además del QCI, se puede usar otra información, tal como una plantilla de flujo de tráfico, para decidir qué datos pasan por qué portador de EPS en algunas realizaciones.

En algunas realizaciones, un UE puede configurarse, preconfigurarse o suministrarse con APN para diferentes servicios, características o funciones. En otras realizaciones, se puede utilizar un APN "bien conocido" además de dichos APN suministrados o en lugar de los APN suministrados. Un APN bien conocido es un APN cuyo valor está estandarizado o especificado como un valor específico. Un ejemplo de un APN bien conocido es el "APN bien conocido del IMS", también denominado en algunos documentos "APN IMS". Algunos servicios basados en IMS desplegados por HPLMN aprovechan la conexión APN a un APN bien conocido del IMS.

Los detalles del conocido APN bien conocido del IMS se definen, por ejemplo, en el documento de referencia permanente (PRD) IR.88 de la Asociación del sistema global para comunicaciones móviles (GSM) (GSMA), "*LTE Roaming Guidelines*", versión 9.0 de enero de 2013. Fundamentalmente, el APN bien conocido del IMS tiene un valor de "IMS" y es utilizado por servicios como voz sobre evolución a Largo Plazo (VoLTE), como se define por ejemplo en GSMA PRD IR.92, "*IMS Profile for Voice and SMS*", como se proporciona, por ejemplo, en la versión 11.0 de junio de 2017, y en servicios de comunicación enriquecidos (RCS), como se define, por ejemplo, en GSMA PRD RCC.07, "*Rich Communication Suite 6.0 Advanced Communications Services and Client Specification*", como por ejemplo se proporciona en la versión 7.0 de marzo de 2016, entre otros.

El UE establece una conexión de PDN con el APN bien conocido del IMS, asegurando que el portador de EPS por defecto para esta conexión de PDN tenga un valor QCI específico de "5", lo cual es apropiado para señalizar mensajes como se define en 3GPP TS 23.401, "*General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access*, como se proporciona, por ejemplo, en la versión 15.0.0 de junio de 2017, y en 3GPP TS 23.203. El UE puede entonces establecer uno o más portadores de EPS dedicados para medios de voz/audio y vídeo según sea necesario, con valores QCI de uno y dos respectivamente. Una conexión de PDN al APN bien conocido del IMS puede denominarse conexión de PDN IMS.

A pesar de que el valor del APN bien conocido del IMS está estandarizado, la conexión de PDN IMS proporciona una conexión a una PDN en la HPLMN del UE o en la VPLMN del UE. Es decir, la PDN a la que está conectado un UE puede diferir de otro UE si el otro UE tiene una HPLMN diferente y/o está vinculado a una PLMN diferente, lo que puede depender de si el UE está en itinerancia. Por ejemplo, los UE pueden tener diferentes módulos de identidad de abonado (SIM), módulos de identidad de abonado universal (USIM) o módulos de identidad de abonado IMS (ISIM).

Quinta generación (5G)

5G es la próxima generación de sistemas de comunicaciones inalámbricas. Consiste en una RAN y una red central. Un operador/portador de 5G puede configurar su RAN y/o redes centrales para que admitan múltiples segmentos de red/redes virtuales, por lo que una plataforma de hardware común proporciona diferentes funcionalidades. Un segmento de red se identifica mediante una S-NSSAI (información de asistencia para la selección de segmentos de red única), que actualmente se define en 3GPP TS 23.501, "System Architecture for the 5G System", según lo dispuesto en la versión 1.1.0 de julio de 2017. En la Tabla 8 a continuación se proporciona un extracto de esta TS.

5.15.2 Identificación y selección de un segmento de red: la S-NSSAI y la NSSAI

5.15.2.1 General

Una S-NSSAI (información de asistencia para la selección de segmentos de red única) identifica un segmento de red.

Una S-NSSAI comprende:

- Un tipo de segmento/servicio (SST), que se refiere al comportamiento previsto de segmento de red en términos de características y servicios;
- Un diferenciador de segmentos (SD) que es información opcional que complementa los tipos de segmento/servicio para diferenciar entre múltiples segmentos de red del mismo tipo de segmento/servicio.

La S-NSSAI puede tener valores estándar o valores de PLMN específicos. Las S-NSSAI con valores específicos de PLMN están asociadas al ID de PLMN de la PLMN que las asigna. El UE no utilizará una S-NSSAI en procedimientos de estrato de acceso en ninguna PLMN distinta de aquella a la que está asociada la S-NSSAI.

La NSSAI es una colección de S-NSSAI (información de asistencia para la selección de segmentos de red única). Puede haber como máximo 8 S-NSSAI en la NSSAI enviada en los mensajes de señalización entre el UE y la red. Cada S-NSSAI ayuda a la red a seleccionar una instancia de segmento de red concreto. La misma instancia de segmento de red puede seleccionarse mediante diferentes S-NSSAI.

Según las necesidades operativas o de despliegue del operador, se pueden desplegar múltiples instancias de segmento de red de una S-NSSAI determinada en la misma o en diferentes áreas de registro. Cuando se despliegan múltiples instancias de segmento de red de una S-NSSAI determinada en la misma área de registro, la instancia de AMF que presta servicio al UE puede lógicamente pertenecer a más de una instancia de segmento de red de esa S-NSSAI, es decir, esta instancia de AMF puede ser común a múltiples instancias de segmento de red de esa S-NSSAI. Cuando una S-NSSAI se admite en más de una instancia de segmento de red en una PLMN, cualquiera de las instancias de segmento de red que admiten la misma S-NSSAI en un área determinada puede prestar servicio, como resultado del procedimiento de selección de instancias de segmento de red definido en la cláusula 5.15.5, a un UE al que se le permite utilizar esta S-NSSAI. Tras la asociación con una S-NSSAI, el UE es atendido por la misma instancia de segmento de red para esa S-NSSAI hasta que se produzcan casos en los que, p. ej., la instancia de segmento de red ya no sea válida en un área de registro determinada, o se produzca un cambio en la NSSAI permitida por el UE, etc. En dichos casos, se aplican los procedimientos mencionados en la cláusula 5.15.5.2.2 o la cláusula 5.15.5.2.3.

La selección de una(s) instancia(s) de segmento de red que prestan servicio a un UE y las funciones de red en el plano de control de red central y en el plano de usuario correspondientes a la instancia del segmento de red es responsabilidad del 5GC.

La (R)AN puede utilizar la NSSAI solicitada en la señalización del estrato de acceso para manejar la conexión del plano de control del UE antes de que el 5GC informe a la (R)AN de la NSSAI permitida. La RAN no utiliza la NSSAI solicitada para el encaminamiento cuando el UE proporciona también una ID de usuario temporal.

Cuando un UE se registra con éxito, el CN informa a la (R)AN y proporciona toda la NSSAI permitida para los aspectos del plano de control.

Cuando se establece una sesión de PDU para una S-NSSAI determinada utilizando una instancia de segmento de red específica, el CN proporciona a la (R)AN la S-NSSAI correspondiente a esta instancia de segmento de red para permitir que la RAN realice funciones de acceso específicas.

NOTA: los detalles de cómo la RAN utiliza la información NSSAI se describen en 3GPP TS 38.300.

TABLA 8: Extracto de 3GPP TS 23.501

Una vez que un UE se ha registrado con un segmento de red, puede establecer una sesión de PDU.

A continuación, se hace referencia a la figura 9, que muestra el establecimiento de la unidad de datos por paquetes (PDU) en una red 5G. En particular, el UE 910 está en una PLMN visitada que incluye la red de acceso (radioeléctrico) ((R)AN) 911, la función de gestión de acceso y movilidad (AMF) 912, la función de plano de usuario visitado (V-UPF) 913 y la función de gestión de sesiones visitadas (V-SMF) 914. Además, en la PLMN doméstica del UE 910 hay una función de plano de usuario doméstico (H-UPF) 915, una función de gestión de sesiones domésticas (H-SMF) 916, una función de control de políticas domésticas (H-PCF) 917 y un sistema de gestión de datos unificada (UDM) 918.

Primero se envía una petición 920 de establecimiento de sesión de PDU desde el UE 910 a la AMF visitada 912. Esto se define, por ejemplo, en la cláusula 4.3.2.2.1 de 3GPP TS 23.502, "Procedures for the 5G System", como se proporciona, por ejemplo, en la versión 0.5.0 de julio de 2017.

A continuación, la AMF 912 realiza una selección de SMF, como se muestra en el bloque 922. La AMF 912 realiza las funciones de la cláusula 4.3.2.2.1, con la adición de que la AMF también selecciona una SMF en la HPLMN. La AMF almacena una asociación del ID de sesión de PDU y el ID de SMF en la VPLMN.

La AMF 912 puede entonces enviar una petición de gestión de sesión (SM) con una petición 924 de establecimiento de sesión de PDU a la V-SMF 914. Esto es parecido a las etapas de la cláusula 4.3.2.2.1, con la adición de que la AMF también proporciona la identidad de la SMF en la HPLMN que ha seleccionado en el bloque 922. El identificador de AMF identifica de forma única la AMF que presta servicio al UE. La H-SMF 916 se proporciona cuando la sesión de PDU tiene encaminamiento inicial. La información N1 SM contiene la petición de establecimiento de sesión de la PDU recibida del UE.

La V-SMF 914 puede entonces seleccionar una UPF, como se muestra en el bloque 926. Dicha selección se describe, por ejemplo, en 3GPP TS 23.501, cláusula 6.3.3.

La V-SMF 914 inicia entonces un procedimiento de establecimiento de sesión N4 con una petición 930 con la V-UPF 913 seleccionada. En particular, la petición 930 se envía a la V-UPF 913. Si la SMF asigna información del túnel de la red central (CN), la información del túnel CN se proporciona a la V-UPF en esta petición.

La V-UPF 913 confirma enviando una respuesta 932 de establecimiento de sesión N4 de regreso a la V-SMF 914. Si la V-UPF asigna información del túnel CN, la información del túnel CN se proporciona a la V-SMF 914 en esta respuesta. Al recibir la respuesta 932, la V-SMF 914 puede crear una petición de sesión de PDU 934 y enviarla a la H-SMF 916. Dicha petición puede incluir la identidad permanente del abonado, el nombre de la red de datos (DNN), la S-NSSAI, el ID de sesión de la PDU, el ID de V-SMF, información de túnel V-CN, tipo de PDU, opciones de configuración de protocolo, información de ubicación del usuario, contenedor de petición de red de datos (DN) de SM PDU, entre otra información.

La H-SMF 916 puede entonces enviar una petición 936 de datos de abonado al UDM 918 y el UDM 918 puede entonces enviar de regreso una respuesta 938 de datos de abonado. Esto permite la autorización de autenticación de sesión de PDU como se muestra en el bloque 940.

La H-SMF 916 puede entonces realizar una selección de PCF, como se muestra en el bloque 950, y puede realizar además el establecimiento 952 de sesión PDU-CAN. La H-SMF 916 luego realiza la selección UPF en el bloque 954 y luego puede realizar la modificación de sesión de unidad de datos por paquetes - red de acceso celular (PDU-CAN) como se muestra con la flecha 956. La H-SMF 916 puede entonces realizar la petición 960 de establecimiento de sesión N4 con la H-UPF 915 y puede recibir a cambio una respuesta 962 de establecimiento de sesión N4.

En este punto, pueden producirse los primeros datos 964 de enlace descendente.

La H-SMF 916 puede entonces crear una respuesta 966 de sesión de PDU a la V-SMF 914. Esto puede incluir la regla de calidad de servicio (QoS) autorizada, el modo de continuidad de servicio y sesión (SSC), información del túnel de la red central local (H-CN) que contiene la información del túnel para el tráfico de enlace ascendente hacia la H-UPF, entre otra información. Se pueden incluir múltiples reglas de QoS autorizadas en la respuesta 966 de creación de sesión de PDU. Además, la H-SMF 916 puede enviar a la V-SMF 913 una indicación si a la VPLMN se le permite insertar una capa cruzada (CL) de enlace ascendente o un punto de bifurcación para una sesión de PDU hacia esta DNN.

La V-SMF 914 puede entonces enviar una confirmación de petición de SM con el mensaje de aceptación de establecimiento de sesión de la PDU 970 a la AMF 912.

Tras recibir el mensaje, la AMF 912 puede entonces realizar una petición de sesión de PDU N2 con la (R)AN 911, como se muestra en el mensaje 972.

Entonces puede producirse la reconfiguración del control de recursos radioeléctricos (RRC), como se muestra con la flecha 974, y se envía una confirmación 976 de petición de sesión de PDU N2 de regreso a la AMF 912.

Posteriormente, los primeros datos 980 de enlace ascendente pueden enviarse a la H-UPF 915. La AMF 912 puede entonces proporcionar una petición de SM con información NG2 en el mensaje 982 a la V-SMF 914.

La V-SMF 914 inicia un procedimiento de modificación de sesión N4 con la V-UPF, como se muestra con el mensaje 982 de petición de establecimiento de sesión N4. La V-SMF proporciona reglas de detección, cumplimiento y notificación de paquetes que se instalarán en la V-UPF para esta sesión de PDU, incluida información del túnel de AN, información del túnel H-CN e información del túnel V-CN.

La V-UPF 913 proporciona una respuesta de modificación o establecimiento de sesión N4 a la V-SMF 914, que se muestra como respuesta 986 en la realización de la figura 9. Después de la respuesta 986, la V-UPF 913 entrega cualquier paquete de enlace descendente al UE que se pueda haber almacenado en la memoria intermedia para la sesión de PDU.

Posteriormente, se proporcionan los primeros datos de enlace descendente como se muestra en el mensaje 990. La V-SMF 914 puede proporcionar una confirmación 992 de petición de SM a la AMF 912. Posteriormente, la configuración de la dirección IPv6 puede producirse cuando la H-SMF 916 envía un mensaje al UE, a través de la H-UPF 915, la V-UPF 913. En el caso de PDU tipo IPv6, la H-SMF 916 genera un anuncio de encaminador IPv6 y lo envía al UE a través de N4 y la H-UPF y la V-UPF.

Después de la configuración 994 de dirección IPv6, la H-SMF 916 puede registrar la dirección en el UDM 918. El UDM almacena la identidad H-SMF y el DNN asociado.

Uso de múltiples ISIM para conectarse a múltiples IMS

Según una realización de la presente divulgación, una entidad móvil o equipo de usuario puede recibir múltiples instancias de aplicación UICC, p. ej., un ISIM. Las múltiples instancias del ISIM pueden, aunque no necesariamente, residir en la UICC.

El ME puede entonces elegir la aplicación UICC, p. ej., qué ISIM utilizar para autenticarse en diferentes IMS basándose en una indicación de con qué servicio(s) o aplicación(es) está asociada la aplicación UICC, p. ej., ISIM. Obsérvese que la descripción que sigue hará referencia al ISIM; sin embargo, también podría haber otras aplicaciones UICC que el ME decida utilizar y el ISIM se utiliza como ejemplo ilustrativo.

Los ISIM en esta realización tienen diferentes identificadores de aplicación (AID), que permiten al ME elegir a qué ISIM acceder. Dentro del ME existe un enlace entre el AID y la aplicación de ME que utiliza ese AID específico. Este enlace puede proporcionarse dentro del ME o ser dinámica.

Si el enlace es dinámico, el ME selecciona una aplicación ISIM, por ejemplo, usando el comando SELECT, que contiene el AID de un ISIM. A continuación, el ME determina si el ISIM seleccionado tiene una indicación de que el ISIM se va a utilizar para un servicio/aplicación específicos. La determinación puede incluir la etapa de descargar algunos o todos los contenidos de la aplicación UICC, p. ej., el ISIM en la memoria de ME.

Si existe la indicación, se puede crear un enlace entre el ISIM seleccionado y el servicio/aplicación.

Si no existe una indicación, el ME selecciona la aplicación ISIM siguiente y repite el proceso, y el ME puede, aunque no es necesario, crear un "enlace por defecto". Específicamente, el ME puede enlazar el ISIM sin ninguna indicación a todos los servicios excepto aquellos que tienen un ISIM y una aplicación enlazados. En el caso de no crear un enlace, el ME podrá eliminar parte o la totalidad del contenido de la aplicación UICC que se almacenó para la etapa de determinación.

La indicación ISIM puede realizarse a través de uno de los siguientes:

Un campo explícito en la aplicación en la UICC. Por ejemplo, puede ser un campo que contenga un código de servicio dedicado (p. ej., un determinado valor o posición dentro de una cadena de bits para VoLTE, otro valor para RCS, otro valor para servicios MC, etc.); o

Campos existentes en la aplicación en la UICC que contienen datos específicos. Estos pueden incluir, por ejemplo:

- ICSI (identificador de servicio de comunicación IMS)
- IARI (identificador de referencia de aplicación IMS)
- APN (nombre del punto de acceso)
- S-NSSAI (información de asistencia para la selección de segmentos de red única)

A continuación, se hace referencia a la figura 10, que muestra el flujo de información para el uso de múltiples ISIM. En particular, en la realización de la figura 10, el ME lee todas las aplicaciones UICC y determina el propósito de esas aplicaciones UICC si el archivo de identificador de aplicación (AID) (EF_{AIDAPP}) está presente. A continuación, el ME utiliza las identidades de usuario públicas y privadas asociadas con esa aplicación UICC si el ME desea registrarse en la red para esos servicios. Las respuestas de autenticación se encaminarán a la aplicación UICC adecuada.

Así, en la realización de la figura 10, el ME 1010 tiene tres ISIM, también denominados aplicaciones UICC. Estos se muestran como ISIM 1012, 1014 y 1016.

Además, en la realización de la figura 10, dos redes IMS, concretamente las redes 1020 y 1022, proporcionan servicios IMS. Las redes pueden proporcionar servicios IMS o SIP y pueden ser un núcleo SIP en algunas realizaciones.

En el mensaje 1030, el ME 1010 selecciona el ISIM 1012 y puede enviar un comando SELECT que contiene el AID para el ISIM 1012.

En respuesta al mensaje 1030, el ME puede leer datos del ISIM 1012, mostrado con la flecha 1032. La lectura, en una realización, consiste en determinar si el archivo identificador de aplicación EF_{AIDAPP} está presente. Si el archivo está presente, el ME puede almacenar en su almacenamiento de memoria interna (p. ej., RAM, memoria flash) los datos del EF_{AIDAPP} junto con otros datos del ISIM 1012.

En el mensaje 1040, el ME 1010 selecciona el ISIM 1014 y puede enviar un comando SELECT que contiene el AID para el ISIM 1014.

En respuesta al mensaje 1040, el ME puede leer datos del ISIM 1014, mostrado con la flecha 1042. La lectura, en una realización, consiste en determinar si el archivo identificador de aplicación EF_{AIDAPP} está presente. Si el archivo está presente, el ME puede almacenar en su almacenamiento de memoria interna (p. ej., RAM, memoria flash) los datos del EF_{AIDAPP} junto con otros datos del ISIM 1014.

En el mensaje 1050, el ME 1010 selecciona el ISIM 1016 y puede enviar un comando SELECT que contiene el AID para el ISIM 1016.

En respuesta al mensaje 1050, el ME puede leer datos del ISIM 1016, mostrado con la flecha 1052. La lectura, en una realización, consiste en determinar si el archivo identificador de aplicación EF_{AIDAPP} está presente. Si el archivo está presente, el ME puede almacenar en su almacenamiento de memoria interna (p. ej., RAM, memoria flash) los datos del EF_{AIDAPP} junto con otros datos del ISIM 1016.

El ME 1010 determina que quiere registrarse en una red para una primera función/servicio, por ejemplo, MCPTT. El ME determina que la primera función está asociada con la aplicación UICC para el ISIM 1012 al determinar que el EF_{AIDAPP} para la aplicación UICC para el ISIM 1012 contiene una indicación o identificador de la primera función en el EF_{AIDAPP}.

Se crea un enlace entre la primera función y la aplicación UICC para el ISIM 1012, que se muestra en el bloque 1054. Durante el enlace, todas las transacciones SIP que están asociadas con las identidades de usuario públicas y/o privadas asociadas con la aplicación UICC (p. ej., ISIM 1012) darán como resultado que el ME envíe todos los datos necesarios a la aplicación UICC para el ISIM 1012. Dichos datos pueden incluir, por ejemplo, respuestas/preguntas de autenticación, entre otras opciones. La determinación se describe con más detalle a continuación.

Como se usa en el ejemplo de la figura 10, una función tal como MCPTT, VoLTE, entre otras funciones, puede identificarse mediante un ICSI, IARI, APN u otro identificador parecido.

Si los datos recuperados del ISIM 1012 y almacenados en el ME 1010 incluyen un $EF_{Segmento}$, el ME selecciona el segmento de red según la NSSAI. A continuación, la ME solicita el establecimiento de una PDU que envía un mensaje que contiene la NSSAI. Si hay un APN asociado con la aplicación, por ejemplo, contra el ID público o privado, EF_{AIDAPP}, entonces el APN se utiliza para establecer las conexiones de PDN y/o la sesión de PDU. Como parte del procedimiento de creación y activación de la conexión de PDN y/o sesión de PDU, se proporcionan al ME una o más direcciones de P-CSCF. Por ejemplo, las direcciones pueden proporcionarse en el elemento de información opciones de configuración de protocolo.

Después de seleccionar y almacenar los datos de los ISIM y crear los enlaces, el ME 1010 puede enviar el mensaje 1060 a la red 1020. Por ejemplo, el mensaje 1060 puede ser un 1.er REGISTRO SIP a la red 1020 que contiene por lo menos una ID de usuario pública o privada que se ha recuperado o almacenado en la aplicación UICC para el ISIM 1012.

El ME 1010 recibe una respuesta 1062 401 que contiene vectores de autenticación desde la red 1020.

El ME 1010 puede entonces enviar algunos de los vectores de autenticación al ISIM 1012, como se muestra en el mensaje 1064.

El ME 1010 recibe la respuesta 1066 a algunos de los vectores de autenticación.

El ME 1010 puede entonces enviar el mensaje 1068 de regreso a la red 1020. El mensaje 1068 puede ser, por ejemplo, un 2.º REGISTRO SIP a la red 1020 que contiene algunos de los datos de la respuesta 1066.

El ME 1010 determina entonces que quiere registrarse en una red 1022 para una segunda función, por ejemplo, VoLTE. El ME 1010 puede determinar que la segunda función está asociada con la aplicación UICC o el ISIM 1016 al determinar que el EF_{AIDAPP} para la aplicación UICC en el ISIM 1016 contiene la segunda función en el EF_{AIDAPP}.

El ME 1010 envía el mensaje 1070 a la red 1022. Por ejemplo, el mensaje 1070 puede ser un 3.er REGISTRO SIP para la red 1022 que contiene por lo menos una ID de usuario pública o privada de la aplicación UICC para el ISIM 1016.

El ME 1010 recibe una respuesta 1072 401 que contiene vectores de autenticación.

Basándose en la respuesta 1072, el ME 1010 envía algunos de los vectores de autenticación en el mensaje 1074 a la aplicación UICC para el ISIM 1016.

El ME 1010 puede entonces recibir la respuesta 1076 a algunos de los vectores de autenticación.

El ME 1010 puede entonces enviar un mensaje 1078 a la red 1022. Por ejemplo, el mensaje 1078 puede ser un 4.º REGISTRO SIP a la red 1022 que contiene algunos de los datos recibidos en la respuesta 1076.

En la realización de la figura 10, la selección del ISIM puede basarse en un campo en la aplicación UICC.

Específicamente, según la presente divulgación, el ME: selecciona un ISIM, determina si el EF_{AIDAPP} está presente, lee el EF_{AIDAPP} y almacena la información de EF_{AIDAPP} en su memoria de almacenamiento interna (p. ej., RAM, memoria flash). Esto sucede, por ejemplo, en los mensajes 1032, 1042 y 1052.

El ME 1010 realiza la operación anterior para más de una aplicación UICC y almacena los archivos leídos en la memoria del ME. Por ejemplo, la operación se puede realizar para todas las aplicaciones ISIM en la UICC.

La estructura de la memoria en el ME 1010 podría verse como la siguiente para cada aplicación UICC, identificada por un AID. A continuación, se hace referencia a la figura 11.

En la realización de la figura 11, el AID 1110 incluye un propósito 1120 de AID, que contiene el EF que almacena el propósito del AID.

Los archivos 1130 almacenados contienen todos los datos que se han leído desde la aplicación AID/UICC.

Posteriormente, una vez que la información se almacena en el ME, el ME determina qué aplicación UICC (ISIM) utilizar. Específicamente, el ME 1010 determina si la aplicación UICC identificada por el AID almacenado debe utilizarse para una aplicación específica o para capacidades específicas. Esta determinación se puede realizar utilizando cualquiera de las formas siguientes.

En una primera realización, el archivo EF_{AIDAPP} respectivo contiene una o más indicaciones de con qué propósito o propósitos debería utilizarse la aplicación UICC identificada por el EF_{AID}. Dichos propósitos pueden estar relacionados, por ejemplo, con funciones IMS concretas, incluidas, entre otras, MCPTT, VoLTE o RCS.

El ME compara la indicación con aplicaciones o capacidades admitidas por el ME.

En una segunda realización, el archivo EF_{AIDAPP} puede contener un ICSI o un grupo de valores ICSI asociados con una aplicación o capacidad del dispositivo. En otras realizaciones, el EF_{AIDAPP} puede contener un IARI, APN, S-NSSAI u otros valores parecidos.

La estructura del archivo EF_{AIDAPP} podría modificarse para admitir los párrafos anteriores. Por ejemplo, en el APÉNDICE A a continuación se proporciona un cambio que se puede realizar en 3GPP TS 31.102 o 31.103.

Así, los párrafos anteriores muestran una opción para proporcionar múltiples servicios IMS en un ME que tiene una pluralidad de ISIM.

Selección de ISIM basada en la autenticación del servicio

En una realización adicional, la red indica un ISIM al ME durante una autenticación y autorización a nivel de aplicación. Por ejemplo, la indicación puede realizarse transmitiendo uno o más de un campo explícito o un campo existente como se enumera en las indicaciones ISIM anteriores, que identifican el ISIM a utilizar.

La indicación ISIM se proporciona en un mensaje desde un nodo de red de autenticación y autorización de servicio tal como el servidor de gestión de identidad al ME en respuesta a una petición de autenticación y autorización de servicio. Los servicios MC o MCX existentes utilizan dicha autenticación y autorización de servicio, por ejemplo, mediante el uso de OpenID Connect. Sin embargo, los procedimientos actuales no proporcionan ninguna indicación de las credenciales ISIM o IMS para que las utilice el ME. En otras palabras, el ME sencillamente utiliza el ISIM disponible para el ME desde la UICC.

Por lo tanto, según una realización de la presente divulgación, se puede proporcionar una indicación explícita. A continuación, se hace referencia a la figura 12.

El ejemplo de la figura 12 es idéntico al ejemplo de la figura 6 anterior, con la excepción de la respuesta del testigo de Open ID Connect (OIDC). Por lo tanto, los números iguales en las figuras 6 y 12 tienen una funcionalidad parecida.

Con respecto al mensaje 1210 de respuesta de testigo OIDC, en la realización de la figura 12, este mensaje es donde se proporcionan el ID y los testigos de acceso, así como una indicación ISIM, al UE 310 de MCX mediante el servidor 314 de gestión de identidad.

La indicación ISIM podría, por ejemplo, añadirse al 3GPP TS 33.180 en la subcláusula 5.1.2.3 como texto en negrita en la Tabla 9 a continuación. Sin embargo, dichos cambios son meramente ilustrativos y también podrían realizarse otros cambios.

El IdMS envía una respuesta de testigo de OpenID Connect al UE que contiene un testigo de identificación, un testigo de acceso (cada uno de los cuales identifica de forma única al usuario del servicio MCX) y una indicación ISIM. El UE consume el testigo de identificación para personalizar el cliente de MCX para el usuario de MCX, el UE utiliza el testigo de acceso para comunicar la identidad del usuario de MCX al servidor o servidores de MCX y el UE utiliza la indicación ISIM para seleccionar un ISIM/conjunto de credenciales/parámetros ISIM que se utilizará al realizar un registro posterior en el núcleo IMS/SIP

TABLA 9: Indicación ISIM en 3GPP TS 33.180

Así, con la realización de la figura 10, después de leer y almacenar la información en el ME, si la aplicación MCPTT determina que quiere autenticarse con la red, el ME puede enviar un mensaje a la red que contenga por lo menos uno de:

1.er conjunto de datos que consiste en por lo menos uno de

- 0 a muchos ICCID
- 0 a muchos AID
- 0 a muchas identidades de usuario asociadas con ICCID o AID

Ubicación del UE, que puede ser un sistema de posicionamiento global (GPS); sistema mundial de navegación por satélite (GNSS); ID de célula; índice de avance de temporización (TAI), identificador de área de ubicación (LAI), identificador de la zona de encaminamiento (RAI), entre otros. El mensaje en respuesta de la red puede, por ejemplo, implementarse cambiando las especificaciones 3GPP. Por ejemplo, la Tabla 10 a continuación muestra un cambio que se puede realizar con respecto a la cláusula 5.1.3.2.1 de 3GPP TS 33.180.

5.1.3.2 Autorización de servicio de usuario de MCX con servidor de MCX 5.1.3.2.1General Dependiendo de la implementación, la autorización del servicio de usuario de MCX se puede realizar enviando el testigo de acceso al servidor de MCX a través de los puntos de referencia SIP-1 y SIP-2 mediante el uso de un mensaje de REGISTRO SIP o un mensaje de PUBLICACIÓN SIP. La cláusula 5.1.3.2.2 describe cómo utilizar el mensaje de REGISTRO SIP para transportar el testigo de acceso al servidor de MCX y la cláusula 5.1.3.2.3 describe cómo utilizar el mensaje de PUBLICACIÓN SIP para transportar el testigo de acceso al servidor de MCX. Durante el registro SIP inicial, el mensaje de REGISTRO SIP no se retrasará por falta de un testigo de acceso. Si no hay un testigo de acceso disponible, entonces el registro SIP continuará sin la inclusión del testigo de acceso y el testigo de acceso se transmitirá al servidor de MCX según la etapa C-3 en la figura 5.1.3.1-1. Si se recibe un testigo de acceso después de que el UE haya enviado un REGISTRO SIP y el testigo de acceso indica que se debe usar una identidad de usuario privada diferente asociada con una aplicación UICC diferente a la que se ha utilizado para el REGISTRO SIP inicial, entonces el UE anulará el registro de la identidad de usuario privada en el REGISTRO SIP inicial y volverá a registrarse con la nueva identidad de usuario privada indicada por el testigo de acceso. Si un testigo de acceso está disponible antes del registro SIP, o si el UE anula el registro y se requiere un nuevo registro SIP, el mensaje de REGISTRO SIP puede incluir el testigo de acceso sin requerir que el usuario se vuelva a autenticar. El testigo de acceso se puede enviar a través de SIP al servidor de MCX para volver a enlazar una IMPU y un ID de servicio MC (ID de MCPTT, ID de MCVideo o ID de MCData) si cualquiera de ellos ha cambiado (p. ej., la IMPU es diferente debido a la anulación del registro de SIP/nuevo registro de SIP), o el usuario cierra sesión y otro usuario inicia sesión en el mismo UE).

TABLA 10: Ejemplo de cambio en el 3GPP TS 33.180

La adición, que se muestra en negrita en la Tabla 10, establece que el ME debe volver a registrarse si se recibe un testigo diferente al utilizado originalmente para un REGISTRO SIP. Sin embargo, dichos cambios son meramente ilustrativos y también podrían realizarse otros cambios.

Además, durante el REGISTRO SIP, un mensaje desde el UE de MCX al núcleo SIP puede incluir el IMPI que se ha identificado por el testigo de acceso.

La Tabla 11 a continuación muestra una estructura para dicho mensaje. La Tabla 11 proporciona cambios que se pueden realizar, por ejemplo, en 3GPP TS 33.180.

B.1.1 Testigo de identificación

B.1.1.0 General

El testigo de identificación será un testigo web JSON (JWT) y contendrá las notificaciones de testigo de MCX y estándar siguientes. Las notificaciones de testigo proporcionan información relacionada con la autenticación del usuario de MCX por parte del servidor IdM, así como notificaciones adicionales. Esta cláusula describe el estándar requerido y las notificaciones de MC para el perfil de MCX Connect.

B.1.1.3 Notificaciones de UICC

El perfil de UICC Connect amplía las notificaciones estándar de OpenID Connect con las notificaciones adicionales que se muestran en la tabla B.1.1.3-1.

Tabla B.1.1.3-1: Notificaciones UICC de testigos de identificación

Parámetro	Descripción
ICCID	Opcional. Contiene el ICCID obtenido a partir del EF_{ICCID}. Opcionalmente, si hay más de una UICC presente, el ICCID de cada UICC.
AID	AID opcionales obtenidos a partir de EF_{DIR}. Opcionalmente, si hay una o más de una UICC, los AID de cada UICC.
Private_User_Identity	Identidades de usuario opcionales de la aplicación identificadas por el AID

NOTA: a cada instancia del parámetro se adjuntará un valor numérico que representa la instancia siguiente.

B.3.1.3 Petición de testigo

Para intercambiar el código de autorización por un testigo de identificación, un testigo de acceso y un testigo de actualización, el cliente de MCX realiza una petición al punto de conexión de testigo del servidor de autorización enviando los parámetros siguientes utilizando el formato "application/x-www-form-urlencoded", con una codificación de caracteres UTF-8 en el cuerpo de entidad de la petición HTTP. Obsérvese que la autenticación del cliente es OBLIGATORIA en las aplicaciones nativas (que utilizan PKCE) para poder intercambiar el código de autorización por un testigo de acceso. Suponiendo que se utilizan secretos de cliente, el secreto de cliente se envía en el encabezado de autorización HTTP. Los parámetros estándar de petición de testigo se muestran en la tabla B.3.1.3-1.

Tabla B.3.1.3-1: Parámetros obligatorios estándar de petición de testigo

Parámetro	Valores
grant_type	OBLIGATORIO. El valor se establecerá en "authorization_code".
code	OBLIGATORIO. El código de autorización recibido previamente del servidor IdM como resultado de la petición de autorización y la posterior autenticación satisfactoria del usuario de MCX.
client_id	OBLIGATORIO. El identificador del cliente que realiza la petición de API. Deberá coincidir con el valor que se ha registrado previamente con el proveedor de OAuth durante la fase de despliegue del registro del cliente, o según se ha suministrado a través de un portal de desarrollo.
redirect_uri	OBLIGATORIO. El valor será idéntico al parámetro "redirect_uri" incluido en la petición de autorización.
code_verifier	OBLIGATORIO. Una cadena criptográficamente aleatoria que se utiliza para correlacionar la petición de autorización con la petición de testigo.
ICCID (véase la NOTA)	Opcional. Contiene el ICCID obtenido a partir del EF_{ICCID}. Opcionalmente, si hay más de una UICC presente, el ICCID de cada UICC.
AID (véase la NOTA)	AID opcionales obtenidos a partir de EF_{DIR}. Opcionalmente, si hay una o más de una UICC, los AID de cada UICC.
Private_User_Identity	Identidades de usuario opcionales de la aplicación identificadas por el AID
NOTA: A cada instancia del parámetro se adjuntará un valor numérico que representa la instancia siguiente.	

Un ejemplo de una petición de testigo para MCX Connect podría ser este.

EJEMPLO:

POST /as/token.oauth2 HTTP/1.1

Host: idM.server.com:8031

Cache-Control: no-cache

Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&code=Splx10BeZQQYbYS6WxSbIA&client_id=myNativeApp&code_verifier=0x123456789abcdef&redirect_uri=http://app.mcptt/cb&ICCID1=kkjgshfdjhr4t5345&AID(1)=1kjgslkjfdsgoi9w&Private_User_Id=user@domain.net

B.3.1.4 Respuesta del testigo

Si la petición del testigo de acceso es válida y está autorizada, el servidor IdM devuelve un testigo de identificación, un testigo de acceso y un testigo de actualización al cliente de MCX; en caso contrario, devolverá un error.

Un ejemplo de una respuesta satisfactoria podría ser este:

EJEMPLO:

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8

Cache-Control: no-store

Pragma: no-cache

{

"access_token":"eyJhbGciOiJSUzIlNiJ9.eyJtY3B0dF9pZCI6ImFsaWN1QG9yZy5jb20iLCJleHAiOjEONTM1MDYxMjEsInNjb3BlIjpbIm9wZW5pZCIsIjNncHA6bWNwdHQ6cHROX3N1cnZlcadLCJjbGllbnRfaWQi0iJtY3B0dF9jbGllbnQifQ.XYlqai4YKSZCKRNMLipGC_5nV4BE79llpvjexWjlqqcqiEx6AmHHIRoOmhcxeCESrXei9krom9e8Goxr_hgF3szvgbw18JRbFuv97XgepDLjEq4jL3Cbu41Q9b0WdXAdFmeEbiB8wo_xggiGwv6IDR1b3TgAAsdjkRxSK4ctlKPaOJSRmM7MKMcKhlug3BEkSC9-aXBTSIv5fAGN-ShDbPyHycBpjzKWXByMIR5PaCg-9fwjELXZXdRwz8C6JbRM8aqzhdt4CVhQ3-Arip-S9CKd0tu-qhHfF2ryJDR1g8ZBiihdPH8mJs-qpTFep_l-kON3mL0_g54xVm1MwNOXQA",

"refresh_token":"Y7NSzUJuS0Jp7G4SKpBKSOJVHIZxFbxqsqCIZhOEk9",

"id_token":"eyJhbGciOiJSUzIlNiJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwiYXVkIjoibWNwdHRfY2xpZW50IiwiaXNzIjoiSWRNUy5zZXJ2ZXIuY29tOjkwMzEiLCJpYXQi0jEONTM0OTgxNTgsImV4cCI6MTQlMzQ5ODQ1OCwibWNwdHRfaWQi
OiJhbGhZUBvcmcuY29tIn0.Dpn7AhIMaqMEgg12NYUUSGSFJMPG8M2li9FLtPotDltlywU2emBws8z5JLw81SXQnoLqZ8ZF8tlhZ1W7uuMbufF4Wsr7PAadZixz3CnV2wxFV9qR_VA1-0ccDTPukUsRHsic0SgZ3albcYKd6VsehFe_GDwfqysYzD7yPwCfPZo",

"token_type": "Bearer",

"expires_in": 7199

}

El cliente de MCX ahora puede validar al usuario con el testigo de identificación y configurarse para el usuario (p. ej., extraer el ID del servicio MC a partir del testigo de identificación). A continuación, el cliente de MCX utiliza el testigo de acceso para realizar peticiones autorizadas a los servidores de recursos MCX (servidor MCPTT, servidor MCVideo, servidor MCData, KMS, etc.) en nombre del usuario final. Anexo C (informativo): Flujo detallado de OpenID Connect

TABLA 11: Ejemplo de cambio en el 3GPP TS 33.180

Como se observa en la Tabla 11 anterior, los cambios se muestran en negrita y añaden los parámetros ICCID y AID a las notificaciones de UICC. Además, los parámetros para una petición de testigo pueden incluir el ICCID y el AID. Sin embargo, dichos cambios son meramente ilustrativos y también podrían realizarse otros cambios. Además, en diversas realizaciones, pueden existir múltiples instancias de los parámetros de la Tabla 11 en los mensajes y flujos de información descritos en la presente memoria.

Además, se pueden realizar cambios en el flujo de autenticación y registro de usuario de MC. A continuación, se hace referencia a la figura 13.

En la realización de la figura 13, un usuario 1310 de MC desea obtener servicios mediante el uso de un UE 1311 de MC. El UE 1311 de MC comprende cliente(s) de MCX 1312, cliente 1313 de gestión de ID y un cliente 1314 SIP.

El UE 1311 de MC se comunica por medio de una PLMN 1316, que proporciona acceso 1318 LTE.

La funcionalidad SIP proporcionada a través de un núcleo 1320 SIP primario que comprende una P-CSCF 1321 y una S-CSCF 1322. El núcleo 1320 SIP primario puede proporcionar servicios IMS y, en las realizaciones descritas en la presente memoria, los términos se pueden usar de forma intercambiable.

El sistema de misión crítica lo proporciona el sistema 1324 de MCX primario que incluye el servidor 1325 de MCX y el servidor 1326 de gestión de ID.

El UE 1311 se vincula a una red y establece conectividad IP (p. ej., por medio de una o más conexiones PDN a una o más PDN), como se muestra en el bloque 1330. El UE puede establecer la seguridad de la red como se define, por ejemplo, en 3GPP TS 33.401. Además, se puede detectar un núcleo 1320 SIP primario, que incluye una P-CSCF 1321 y una S-CSCF 1322.

Posteriormente, el cliente 1314 de UE IMS/SIP puede autenticarse con el núcleo 1320 IMS/SIP primario. Esto se muestra, por ejemplo, con la flecha 1340 en la realización de la figura 13 y la autenticación se produce específicamente con la S-SCSF 1322. El núcleo 1320 SIP envía un registro SIP de terceros, como se muestra con la flecha 1342 al servidor, al servidor o servidores 1325 de aplicaciones de MCX, y notifica a los servidores del registro SIP del UE de MC. El mensaje de registro de terceros incluye la IMPU registrada y el URI o dirección IP SIP S-CSCF.

El cliente 1313 de gestión de identidad en el UE 1311 emite una petición de autenticación HTTPS al servidor de gestión de identidad basado en OIDC 1326 en forma de un mensaje 1350 HTTPS GET. El cliente incluye un valor de código de la pregunta en esta petición.

El cliente 1313 de gestión de identidad puede solicitar al usuario 1310 de MC las credenciales, que se proporcionan como se muestra en la flecha 1352. La identidad del usuario de MC y las credenciales asociadas se proporcionan luego al servidor 1326 de gestión de identidad como se muestra con la flecha 1354. Las credenciales se autentican correctamente y, opcionalmente, se autoriza mediante el servidor 1326 de gestión de identidad.

Como parte del mensaje 1350 o de la autenticación en la flecha 1354, el UE puede incluir información en el mensaje enviado al servidor 1326 de gestión de identidad. Dicha información puede incluir, por ejemplo, el ICCID obtenido a partir del EF_{ICCID}. Si hay más de una UICC presente, entonces se puede proporcionar el ICCID de cada UICC en dicho mensaje.

El mensaje 1350 o autenticación en la flecha 1354 puede incluir además los identificadores de aplicación obtenidos a partir del EF_{DIR}. Además, si hay más de una UICC presente, se pueden proporcionar los AID de cada UICC.

El mensaje 1350 o la autenticación de usuario en la flecha 1354 pueden proporcionar además identidades de usuario de las aplicaciones identificadas por el AID.

Además, la ubicación del UE o ME puede proporcionarse en dichos mensajes. Dicha ubicación puede, por ejemplo, encontrarse mediante el uso de un sistema GNSS o la información puede derivarse a partir de la PLMN de servicio cuando el UE está dentro de la cobertura de la tecnología del acceso radioeléctrico (RAT) 3GPP.

El servidor 1326 de gestión de identidad puede solicitar opcionalmente el consentimiento del usuario para conceder el acceso del cliente de MCX al servicio MCX en el servidor de MCX, como se muestra con la flecha 1360, y enviar un mensaje al cliente 1312 de MCX. Al recibir el mensaje, el cliente 1312 de MCX puede presentar, mediante el uso de una interfaz de usuario del UE, una indicación. Dicha indicación puede ser, por ejemplo, una indicación visual, una indicación audible o una indicación por vibración, entre otras opciones. En respuesta a la indicación, se puede recibir una entrada en el equipo de usuario.

Posteriormente, el servidor 1326 de gestión de identidad puede generar un código de autorización que está asociado con el código de la pregunta proporcionado por el cliente. El servidor 1326 de gestión de identidad puede enviar un mensaje HTTP de redireccionamiento del navegador con la respuesta de autorización que contiene el código de autorización como respuesta 1362.

En el UE 1311, el cliente 1313 de gestión de identidad realiza un HTTPS Post 1364 para intercambiar el código de autorización por un testigo de acceso. En el mensaje 1364, el cliente incluye la cadena del verificador de código. Esta cadena está asociada criptográficamente con el valor del código de la pregunta proporcionado en la petición de autorización del mensaje 1350.

El servidor 1326 de gestión de identidad verifica el cliente 1313 de gestión de identidad basándose en la cadena del verificador de código recibida y emite una respuesta, p. ej., un mensaje 200 OK, mostrado con la flecha 1366 en la realización de la figura 13. El mensaje 1366 incluye el testigo de acceso y el testigo de identificación que son específicos del usuario de MC y los servicios MCX incluidos en él.

El testigo de identificación puede contener una notificación de testigo web JSON que contiene por lo menos uno de un ICCID, AID o identidad de usuario asignado por el servidor 1326 de gestión de identidad que el UE debería utilizar para acceder a un sistema. Dicho sistema podría incluir, entre otros, MCPTT, RCS, IMS portador, entre otras opciones. El servidor 1326 de gestión de identidad verifica el cliente 1313 de gestión de identidad calculando el código de la pregunta a partir de la cadena del verificador de código recibida y la compara con el valor del código de la pregunta proporcionado por el cliente en el mensaje 1350.

El testigo de acceso y el testigo de identificación proporcionados en el mensaje 1366 se ponen a disposición del cliente 1312 de MCX, como se muestra con la flecha 1370.

Después de esto, el UE 1311 de MC realiza un registro y autenticación con el sistema identificado en el mensaje 1366 utilizando la información recibida en el Testigo_id. Dicha información incluye la aplicación identificada por el AID si se recibe un AID, o la identidad del usuario si se recibe la identidad del usuario. Como apreciarán los expertos en la materia, si se recibe la identidad del usuario, esto implica que también se utiliza un AID/aplicación específica para acceder al sistema.

El núcleo 1320 SIP puede enviar un registro SIP de terceros (no se muestra) al servidor de MC y notificar al servidor de MC del registro SIP del UE 1311 de MC. El mensaje de registro de terceros incluye la dirección IP o URI SIP S-CSCF y el IMPU registrado y la notificación del testigo web JSON para el testigo de acceso.

Posteriormente, el UE 1311 de MC realiza la autorización del servicio MCX del usuario, mostrada con la flecha 1380. Por lo tanto, como se observa en la realización de la figura 13, el UE 1311 puede proporcionar credenciales de una pluralidad de ISIM a un servidor 1326 de gestión de identidad y puede recibir, en respuesta, identificadores de aplicación para usar con esa información.

Por lo tanto, lo anterior proporciona a un ME o UE mensajes que indican qué ISIM utilizar.

Uso de múltiples credenciales dentro de un único ISIM para la autenticación en múltiples IMS

Según una realización adicional de la presente divulgación, en lugar de usar múltiples ISIM, se puede usar un único ISIM con múltiples identidades.

En esta realización, para cada identidad de usuario almacenada en el ISIM hay uno o ambos de un puntero de algoritmo suministrado y un puntero de aplicación.

Cuando el ME selecciona la aplicación UICC (p. ej., ISIM) y accede a los datos, el ME determinará qué archivos o datos dentro de un archivo deben utilizarse y con qué aplicación. Los datos pueden incluir, por ejemplo, la identidad del usuario, entre otros datos parecidos. Las aplicaciones pueden incluir aplicaciones IMS tales como VoLTE, ViLTE, VoWifi, RCS, servicios de MC/MCX, MCPTT, MCVideo, MCData, entre otras opciones.

El ME realiza un registro SIP con la red mediante el uso de las identidades de usuario asociadas con la aplicación que ha activado el registro SIP. En respuesta al registro SIP, el ME recibirá vectores de autenticación de la red y el ME enviará los vectores de autenticación utilizando el comando AUTHENTICATE a la aplicación UICC seleccionada. El ME también incluirá la identidad del usuario que se ha incluido en el registro SIP.

Al recibir el comando AUTHENTICATE que contiene los vectores de autenticación y la identidad del usuario, la aplicación ISIM enviará los vectores de autenticación al algoritmo de autenticación asociado con la identidad de usuario recibida que estaba en el comando AUTHENTICATE.

Por lo tanto, a continuación, se hace referencia a la figura 14. En la realización de la figura 14, un ME 1410 lee una aplicación UICC, que se muestra como el ISIM 1412. Esa aplicación contiene múltiples conjuntos de parámetros, tales como algoritmos, nombres de dominio doméstico, IMPU, entre otras opciones, que deben utilizarse para fines de autenticación en el núcleo IMS/SIP. El proceso de lectura de la UICC incluye que el ME determine qué algoritmo está asociado con qué identidad de usuario. Por ejemplo, esto se puede hacer en base a un archivo EF_{IMPI} existente que se extiende para indicar qué algoritmo utilizar y para qué aplicación se debe utilizar la identidad del usuario (p. ej., identificador de acceso a la red (NAI)). De forma alternativa, el ME determina qué algoritmo está asociado con qué identidad de usuario utilizando un nuevo archivo que contiene el NAI y el algoritmo que se utilizar con ese NAI. La aplicación a utilizar puede estar implícita en el nombre del archivo o en una indicación contenida en el archivo.

A continuación, el ME 1410 envía un mensaje a la red que contiene el NAI. Al recibir los vectores de autenticación, parte de los vectores de autenticación junto con un algoritmo a utilizar o un NAI se envía a la aplicación UICC.

Así, en referencia de nuevo a la figura 14, el ME 1410 puede querer los servicios IMS de la red 1420 o la red 1422. Por lo tanto, al inicializar la UICC, p. ej., cuando se enciende el ME, puede seleccionar una aplicación UICC usando un comando de selección que se muestra como el mensaje 1430 que contiene el identificador de aplicación para la aplicación seleccionada.

El ME puede entonces leer los datos, como se muestra con la flecha 1432, de la aplicación seleccionada en la UICC y almacenar el contenido de la aplicación seleccionada en el ME. A continuación, una aplicación en el ME determina que desea registrarse en una red para la función seleccionada. Por ejemplo, la función seleccionada pueden ser servicios de misión crítica.

El ME determina que la función seleccionada está asociada con una aplicación al determinar el EF_{IMPI} de la aplicación o un archivo básico para la identidad de usuario privada IMS de la aplicación Y (EF_{IMPIY}) contiene la función seleccionada.

Se crea un enlace entre la función seleccionada y la aplicación, mostrado en el bloque 1434. La etapa de enlace implica todas las transacciones SIP que están asociadas con la identidad de usuario privada en el EF_{IMPI} o el EF_{IMPIY} que están asociadas con la aplicación y esto dará como resultado que el ME envíe los datos necesarios a la aplicación. Ejemplos de dichos datos incluyen respuestas o preguntas de autenticación, entre otros datos parecidos.

Una función puede incluir diversas funciones que incluyen servicios MCX, VoLTE, RCS, entre otras opciones. La función podrá identificarse mediante un ICSI, IARI, APN, entre otros identificadores.

En la realización de la figura 14, el ME envía un mensaje 1440 de registro, tal como una petición de REGISTRO SIP, a la red 1420 que contiene por lo menos una de una identidad de usuario pública o una identidad de usuario privada que se ha recuperado de, o almacenado en, la aplicación UICC asociada a la función seleccionada. También se puede incluir una indicación del algoritmo.

En respuesta al mensaje 1440 de registro, el ME 1410 recibe una respuesta 401 en el mensaje 1442 que contiene una pregunta de autenticación y vectores. También podrá incluirse la indicación del algoritmo a utilizar.

El ME 1410 puede enviar algunos de los datos recibidos del mensaje 1442 a la aplicación seleccionada (ISIM 1412) en el mensaje 1444 usando un comando definido, por ejemplo, en el APÉNDICE B a continuación. Por ejemplo, dicho comando puede definirse en la sección 7.1.2.1 del APÉNDICE B. El comando contiene el identificador de usuario enviado en el mensaje 1440 de registro o un algoritmo que se ha enviado en el mensaje 1440 o se ha recibido en la respuesta 1442 que está asociada con la identificación del usuario. Esta asociación también podría haberse hecho cuando el ME leyó los archivos EF_{IMPI} o EF_{IMPIY}.

En base a la pregunta, el ISIM 1412 devuelve una respuesta 1446 que contiene algunos de los vectores de autenticación.

A continuación, el ME puede enviar un mensaje 1448 de registro, que puede ser, por ejemplo, una segunda petición de REGISTRO SIP, a la red 1420 que contiene algunos de los datos que se recibieron en la respuesta 1446.

Posteriormente, una aplicación en el ME 1410 determina que quiere registrarse en una red para una segunda función, por ejemplo, VoLTE. El ME 1410 determina que la segunda función está asociada con una aplicación en el ISIM 1412 al determinar que el EF_{IMPI} o EF_{IMPIY} en el ISIM 1412 contiene la segunda función en el EF_{IMPI} o EF_{IMPIY}. Se crea un enlace entre la segunda función y el ISIM 1412, como se muestra en el bloque 1449. En la etapa de enlace, todas las transacciones SIP que están asociadas con la identidad de usuario privada en el EF_{IMPI} o EF_{IMPIY} están asociadas con el ISIM 1412 y darán como resultado que el ME envíe todos los datos necesarios al ISIM 1412, incluidas las respuestas o preguntas de autenticación. Posteriormente, el ME envía un mensaje 1450 de registro, tal como una petición de REGISTRO SIP, a la red 1422. El mensaje 1450 de registro es parecido al mensaje 1440 de registro. En respuesta,

la red 1422 envía una respuesta 401 en el mensaje 1452 al ME 1410.

El ME 1410 puede enviar algunos de los datos recibidos del mensaje 1452 a la aplicación seleccionada (ISIM 1412) en el mensaje 1454 usando un comando definido, por ejemplo, en el APÉNDICE B a continuación. Por ejemplo, dicho comando puede definirse en la sección 7.1.2.1 del APÉNDICE B. El comando contiene el identificador de usuario enviado en el mensaje 1450 de registro o un algoritmo que se ha enviado en el mensaje 1450 o se ha recibido en la respuesta 1452 que está asociada con la identificación del usuario. Esta asociación también podría haberse hecho cuando el ME leyó los archivos EF_{IMPI} o EF_{IMPIY}.

En base a la pregunta, el ISIM 1412 devuelve una respuesta 1456 que contiene algunos de los vectores de autenticación.

A continuación, el ME puede enviar un mensaje 1458 de registro, que puede ser, por ejemplo, una segunda petición de REGISTRO SIP, a la red 1422 que contiene algunos de los datos que se recibieron en la respuesta 1456.

En base a los párrafos anteriores, un único ISIM puede contener credenciales de múltiples servicios que pueden distinguirse en función de las identidades, por ejemplo, en el EF_{IMPI} o EF_{IMPIY}.

Los módulos, entidades móviles y equipos y dispositivos de usuario descritos anteriormente pueden ser cualquier dispositivo informático o nodo de red. Dicho dispositivo informático o nodo de red puede incluir cualquier tipo de dispositivo electrónico, incluidos, entre otros, dispositivos móviles tales como teléfonos inteligentes o teléfonos celulares. Los ejemplos pueden incluir además equipos de usuario fijos o móviles, tales como dispositivos de Internet de las cosas (IoT), terminales, dispositivos de domótica, equipos médicos en entornos hospitalarios o domésticos, dispositivos de seguimiento de inventario, dispositivos de monitorización ambiental, dispositivos de gestión de energía, dispositivos de gestión de infraestructura, vehículos o dispositivos para vehículos, dispositivos electrónicos fijos, entre otros. Vehículos incluye vehículos de motor (p. ej., automóviles, automóviles, camiones, autobuses, motocicletas, etc.), aeronaves (p. ej., aviones, vehículos aéreos no tripulados, sistemas de aeronaves no tripuladas, drones, helicópteros, etc.), naves espaciales (p. ej., aviones espaciales, lanzaderas, cápsulas espaciales, estaciones espaciales, satélites, etc.), embarcaciones (p. ej., barcos, botes, aerodeslizadores, submarinos, etc.), vehículos ferroviarios (p. ej., trenes y tranvías, etc.) y otros tipos de vehículos, incluido cualquier combinación de cualquiera de los anteriores, ya sean existentes actualmente o que surjan más adelante.

En la figura 15 se muestra un diagrama simplificado de un dispositivo informático. El dispositivo informático de la figura 15 podría ser cualquier UE, ME u otro nodo como se describe anteriormente.

En la figura 15, el dispositivo 1510 incluye un procesador 1520 y un subsistema 1530 de comunicaciones, donde el procesador 1520 y el subsistema 1530 de comunicaciones cooperan para realizar los procedimientos de las realizaciones descritas anteriormente. El subsistema 1520 de comunicaciones puede, en algunas realizaciones, comprender múltiples subsistemas, por ejemplo, para diferentes tecnologías radioeléctricas.

El procesador 1520 está configurado para ejecutar lógica programable, que puede almacenarse, junto con los datos, en el dispositivo 1910, y se muestra en el ejemplo de la figura 15 como la memoria 1540. La memoria 1540 puede ser cualquier medio de almacenamiento tangible, no transitorio, legible por ordenador. El medio de almacenamiento legible por ordenador puede ser un medio tangible o transitorio/no transitorio tal como óptico (p. ej., CD, DVD, etc.), magnético (p. ej., cinta), unidad de memoria flash, disco duro u otra memoria conocida en la técnica.

De forma alternativa, o además de la memoria 1540, el dispositivo 1510 puede acceder a datos o lógica programable desde un medio de almacenamiento externo, por ejemplo, a través del subsistema 1530 de comunicaciones.

El subsistema 1530 de comunicaciones permite que el dispositivo 1510 se comunique con otros dispositivos o elementos de red y puede variar según el tipo de comunicación que se realiza. Además, el subsistema 1530 de comunicaciones puede comprender una pluralidad de tecnologías de comunicaciones, incluida cualquier tecnología de comunicaciones por cable o inalámbrica.

Las comunicaciones entre los diversos elementos del dispositivo 1510 pueden realizarse a través de un bus interno 1560 en una realización. Sin embargo, son posibles otras formas de comunicación.

Además, si la estación informática es una entidad móvil, a continuación, se describe un ejemplo de equipo móvil con respecto a la figura 16.

La entidad 1600 móvil puede comprender un dispositivo de comunicación inalámbrica bidireccional que tiene capacidades de comunicación de voz o datos, o ambas. La entidad 1600 móvil en general tiene la capacidad de comunicarse con otros sistemas informáticos. Dependiendo de la funcionalidad exacta proporcionada, se puede hacer referencia a la entidad móvil como un dispositivo de mensajería de datos, un buscapersonas bidireccional, un dispositivo de correo electrónico inalámbrico, un teléfono inteligente, un teléfono celular con capacidades de mensajería de datos, un dispositivo de Internet inalámbrico, un dispositivo inalámbrico, un dispositivo móvil, un equipo de usuario, un módem celular integrado o un dispositivo de comunicación de datos, como ejemplos.

Cuando la entidad 1600 móvil está habilitada para comunicación bidireccional, puede incorporar un subsistema 1611 de comunicación, que incluye un receptor 1612 y un transmisor 1614, así como componentes asociados tales como uno o más elementos de antena 1616 y 1618, osciladores locales (LO) 1613, y un módulo de procesamiento tal como un procesador de señales digitales (DSP) 1620. Como resultará evidente para los expertos en el campo de las comunicaciones, el diseño particular del subsistema 1611 de comunicación dependerá de la red de comunicación en la que se pretende que opere la entidad móvil.

Los requisitos de acceso a la red también variarán según el tipo de red 1619. En algunas redes, el acceso a la red está asociado con un abonado o usuario de la entidad 1600 móvil. Una entidad móvil puede interactuar con un módulo de identidad de usuario (RUIM) integrado o extraíble o una tarjeta de módulo de identidad de abonado (SIM) o una SIM UMTS (USIM) para operar en una red. La interfaz 1644 USIM/SIM/RUIM normalmente es parecida a una ranura para tarjetas en la que se puede insertar y expulsar una tarjeta USIM/SIM/RUIM. La tarjeta USIM/SIM/RUIM puede tener memoria y contener muchas configuraciones 1651 clave y otra información 1653 tal como identificación e información relacionada con el abonado. En otros casos, en lugar de una red 1619, la entidad 1600 móvil puede comunicarse con un nodo sin acceso, tal como un vehículo, infraestructura de carretera, otra entidad móvil u otra comunicación entre pares. Cuando se hayan completado los procedimientos de activación o registro de red requeridos, la entidad 1600 móvil puede enviar y recibir señales de comunicación a través de la red 1619. Como se ilustra en la figura 16, la red 1619 puede incluir múltiples estaciones de base que se comunican con la entidad móvil.

Las señales recibidas por la antena 1616 a través de la red 1619 de comunicación se introducen en el receptor 1612, que puede realizar funciones de receptor tan comunes como amplificación de señal, conversión descendente de frecuencia, filtrado, selección de canal y similares. La conversión analógica a digital (A/D) de una señal recibida permite realizar funciones de comunicación más complejas, tales como la desmodulación y la descodificación, en el DSP 1620. De forma parecida, las señales a transmitir se procesan, incluyendo modulación y codificación, por ejemplo, mediante el DSP 1620 y se introducen al transmisor 1614 para la conversión digital a analógica (D/A), conversión ascendente de frecuencia, filtrado, amplificación y transmisión sobre la red 1619 de comunicación a través de la antena 1618. El DSP 1620 no solo procesa señales de comunicación, sino que también proporciona control del receptor y del transmisor. Por ejemplo, las ganancias aplicadas a las señales de comunicación en el receptor 1612 y el transmisor 1614 pueden controlarse de forma adaptativa a través de algoritmos de control automático de ganancia implementados en el DSP 1620.

La entidad 1600 móvil en general incluye un procesador 1638 que controla el funcionamiento general del dispositivo. Las funciones de comunicación, incluidas las comunicaciones de datos y voz, se realizan a través del subsistema 1611 de comunicación. El procesador 1638 también interactúa con subsistemas de dispositivos adicionales tales como la pantalla 1622, la memoria flash 1624, la memoria de acceso aleatorio (RAM) 1626, los subsistemas 1628 de entrada/salida (E/S) auxiliares, puerto serie 1630, uno o más teclados o teclados numéricos 1632, altavoz 1634, micrófono 1636, otro subsistema 1640 de comunicación tal como un subsistema de comunicaciones de corto alcance o subsistema DSRC, y cualquier otro subsistema de dispositivo en general designado como 1642. El puerto serie 1630 podría incluir un puerto USB, un puerto de diagnóstico integrado (OBD) u otro puerto conocido por los expertos en la materia.

Algunos de los subsistemas que se muestran en la figura 16 realizan funciones relacionadas con la comunicación, mientras que otros subsistemas pueden proporcionar funciones "residentes" o en el dispositivo. En particular, algunos subsistemas, tales como el teclado 1632 y la pantalla 1622, por ejemplo, pueden utilizarse tanto para funciones relacionadas con la comunicación, como introducir un mensaje de texto para su transmisión sobre una red de comunicación, como para funciones residentes en el dispositivo, como una calculadora o una lista de tareas.

El software del sistema operativo utilizado por el procesador 1638 puede almacenarse en un almacén persistente tal como una memoria flash 1624, que en su lugar puede ser una memoria de solo lectura (ROM) o un elemento de almacenamiento parecido (no se muestra). Los expertos en la materia apreciarán que el sistema operativo, las aplicaciones específicas del dispositivo o partes de los mismos se pueden cargar temporalmente en una memoria volátil tal como la RAM 2026. Las señales de comunicación recibidas también pueden almacenarse en la RAM 1626.

Como se muestra, la memoria flash 1624 puede segregarse en diferentes áreas tanto para los programas informáticos 1658 como para el almacenamiento de datos de programas 1650, 1652, 1654 y 1656. Estos diferentes tipos de almacenamiento indican que cada programa puede asignar un parte de la memoria flash 1624 para sus propios requisitos de almacenamiento de datos. El procesador 1638, además de sus funciones de sistema operativo, puede permitir la ejecución de aplicaciones de software en la entidad móvil. Normalmente se instalará en la entidad 1600 móvil durante la fabricación un conjunto predeterminado de aplicaciones que controlan las operaciones básicas, incluidas potencialmente aplicaciones de comunicación de voz y datos, por ejemplo. Otras aplicaciones podrían instalarse posteriormente o de forma dinámica.

Las aplicaciones y el software pueden almacenarse en cualquier medio de almacenamiento legible por ordenador. El medio de almacenamiento legible por ordenador puede ser un medio tangible o transitorio/no transitorio tal como óptico (p. ej., CD, DVD, etc.), magnético (p. ej., cinta) u otra memoria conocida en la técnica.

Una aplicación de software puede ser una aplicación de gestión de información personal (PIM) que tiene la capacidad de organizar y gestionar elementos de datos relacionados con el usuario de la entidad móvil tales como, entre otros, correo electrónico, mensajes, eventos de calendario, correos de voz, citas y elementos de tareas. También se pueden cargar aplicaciones adicionales, incluidas aplicaciones de productividad, aplicaciones de redes sociales, juegos, entre otras, en la entidad 1600 móvil a través de la red 1619, un subsistema 1628 de E/S auxiliar, un puerto serie 1630, un subsistema 1640 de comunicaciones de corto alcance o cualquier otro subsistema 1642 adecuado, e instalado por un usuario en la RAM 1626 o un almacén no volátil (no se muestra) para su ejecución por el procesador 1638. Dicha flexibilidad en la instalación de aplicaciones aumenta la funcionalidad del dispositivo y puede proporcionar funciones mejoradas en el dispositivo, funciones relacionadas con la comunicación o ambas.

En un modo de comunicación de datos, una señal recibida tal como un mensaje de texto o la descarga de una página web se procesará por el subsistema 1611 de comunicación y se introducirá en el procesador 1638, que puede procesar aún más la señal recibida para enviarla a la pantalla 1622, o de forma alternativa a un dispositivo 1628 de E/S auxiliar.

Un usuario de la entidad 1600 móvil también puede escribir elementos de datos tales como mensajes, por ejemplo, usando el teclado 1632, que puede ser un teclado alfanumérico completo o un teclado de tipo telefónico, ya sea físico o virtual, entre otros, junto con la pantalla 1622 y posiblemente un dispositivo 1628 de E/S auxiliar. A continuación, dichos elementos escritos pueden transmitirse sobre una red de comunicación a través del subsistema 1611 de comunicación.

Cuando se proporcionan comunicaciones de voz, el funcionamiento global de la entidad 1600 móvil es parecido, excepto que las señales recibidas típicamente pueden enviarse a un altavoz 1634 y las señales para la transmisión pueden generarse mediante un micrófono 1636. También se pueden implementar subsistemas de E/S de voz o audio alternativos, tales como un subsistema de grabación de mensajes de voz, en la entidad 1600 móvil. Aunque la salida de voz o señal de audio se logra preferiblemente principalmente a través del altavoz 1634, la pantalla 1622 también se puede usar para proporcionar una indicación de la identidad de una parte que llama, la duración de una llamada de voz u otra información relacionada con una llamada de voz, por ejemplo.

El puerto serie 1630 en la figura 16 puede implementarse en una entidad móvil para la cual puede ser deseable la sincronización con el ordenador de sobremesa de un usuario (no se muestra), pero es un componente opcional del dispositivo. Dicho puerto 1630 puede permitir a un usuario establecer preferencias a través de un dispositivo externo o aplicación de software y puede ampliar las capacidades de la entidad 1600 móvil proporcionando información o descargas de software a la entidad 1600 móvil de otra manera que no sea a través de una red de comunicación inalámbrica. Como apreciarán los expertos en la materia, el puerto serie 1630 se puede utilizar además para conectar la entidad móvil a un ordenador para que actúe como módem o para cargar una batería en la entidad móvil.

Otros subsistemas 1640 de comunicaciones, tales como un subsistema de comunicaciones de corto alcance, son un componente adicional que puede proporcionar comunicación entre la entidad 1600 móvil y diferentes sistemas o dispositivos, que no necesariamente tienen que ser dispositivos parecidos. Por ejemplo, el subsistema 1640 puede incluir un dispositivo de infrarrojos y circuitos y componentes asociados o un Bluetooth™ o un módulo de comunicación por Bluetooth™ de bajo consumo de energía para proporcionar comunicación con sistemas y dispositivos habilitados de forma parecida. El subsistema 1640 puede incluir además una radio WUR. El subsistema 1640 puede incluir además una radio DSRC. El subsistema 1640 puede incluir además comunicaciones no celulares tales como wifi o WiMAX, o comunicaciones de campo cercano, y según las realizaciones anteriores dicha radio puede ser capaz de dividirse en algunas circunstancias.

Las realizaciones descritas en la presente memoria son ejemplos de estructuras, sistemas o procedimientos que tienen elementos correspondientes a elementos de las técnicas de esta solicitud. Esta descripción escrita puede permitir a los expertos en la materia hacer y utilizar realizaciones con elementos alternativos que también corresponden a los elementos de las técnicas de esta solicitud. El alcance previsto de las técnicas de esta solicitud incluye por lo tanto otras estructuras, sistemas o procedimientos que no difieren de las técnicas de esta solicitud como se describen en la presente memoria, e incluye además otras estructuras, sistemas o procedimientos con diferencias insustanciales de las técnicas de esta solicitud como se describen en la presente memoria.

Aunque las operaciones se representan en un orden particular en los dibujos, esto no debe entenderse como que se requiere que dichas operaciones se realicen en el orden particular mostrado o en orden secuencial, o que se realicen todas las operaciones ilustradas, para lograr los resultados deseables. En determinadas circunstancias, puede emplearse el procesamiento en paralelo y multitarea. Además, no debe entenderse que la separación de diversos componentes del sistema en la implementación descrita anteriormente requiere dicha separación en todas las implementaciones, y debe entenderse que los componentes y sistemas del programa descritos en general pueden integrarse juntos en un producto de software de señal o empaquetarse en múltiples productos de software.

Asimismo, las técnicas, sistemas, subsistemas y procedimientos descritos e ilustrados en las diversas implementaciones como discretos o separados pueden combinarse o integrarse con otros sistemas, módulos, técnicas o procedimientos. Otros elementos que se muestran o se analizan como acoplados o acoplados directamente o en comunicación entre sí pueden estar acoplados indirectamente o comunicarse a través de alguna interfaz, dispositivo o componente intermedio, ya sea eléctrica, mecánicamente o de otro modo. Un experto en la materia puede constatar

y realizar otros ejemplos de cambios, sustituciones y alteraciones.

Si bien la descripción detallada anterior ha mostrado, descrito y señalado las características novedosas fundamentales de la divulgación aplicadas a diversas implementaciones, se entenderá que los expertos en la materia pueden realizar diversas omisiones, sustituciones y cambios en la forma y los detalles del sistema ilustrado. Además, el orden de las etapas del procedimiento no está implícito en el orden en que aparecen en las reivindicaciones.

Cuando los mensajes se envían hacia/desde un dispositivo electrónico, dichas operaciones pueden no ser inmediatas o directamente desde el servidor. Pueden entregarse de forma síncrona o asíncrona desde un servidor u otra infraestructura de sistema informático que admita los dispositivos/procedimientos/sistemas descritos en la presente memoria. Las etapas anteriores pueden incluir, total o parcialmente, comunicaciones síncronas/asíncronas hacia/desde el dispositivo/infraestructura. Además, la comunicación desde el dispositivo electrónico puede ser hacia uno o más puntos de conexión en una red. Estos puntos de conexión pueden ser atendidos por un servidor, un sistema informático distribuido, un procesador de flujo, etc. Las redes de entrega de contenido (CDN) también pueden proporcionar comunicación a un dispositivo electrónico. Por ejemplo, en lugar de una respuesta típica del servidor, el servidor también puede proporcionar o indicar datos a la red de entrega de contenido (CDN) para esperar la descarga por parte del dispositivo electrónico en un momento posterior, tal como una actividad posterior del dispositivo electrónico. Así, los datos pueden enviarse directamente desde el servidor u otra infraestructura, tal como una infraestructura distribuida o una CDN, como parte del sistema o separada del mismo.

Típicamente, los medios de almacenamiento pueden incluir cualquiera o alguna combinación de los siguientes: un dispositivo de memoria de semiconductor tal como una memoria de acceso aleatorio dinámica o estática (una DRAM o SRAM), una memoria de solo lectura borrable y programable (EPROM), una memoria de solo lectura programable y borrable eléctricamente (EEPROM) y memoria flash; un disco magnético tal como un disco fijo, flexible y extraíble; otro medio magnético que incluye cinta; un medio óptico tal como un disco compacto (CD) o un disco de vídeo digital (DVD); u otro tipo de dispositivo de almacenamiento. Obsérvese que las instrucciones analizadas anteriormente se pueden proporcionar en un medio de almacenamiento legible por ordenador o por máquina, o de forma alternativa, se pueden proporcionar en múltiples medios de almacenamiento legibles por ordenador o por máquina distribuidos en un sistema grande que tiene posiblemente una pluralidad de nodos. Dicho medio o medios de almacenamiento legibles por ordenador o por máquina se consideran que forman parte de un artículo (o artículo de fabricación). Un artículo o artículo de fabricación puede referirse a cualquier componente único o múltiple fabricado. El medio o medios de almacenamiento pueden ubicarse en la máquina que ejecuta las instrucciones legibles por máquina, o ubicarse en un sitio remoto desde el cual se pueden descargar instrucciones legibles por máquina a través de una red para su ejecución.

APÉNDICE A – Cambios en el 3GPP TS 31.102/103

4.2.X EF_{AIDAPP} (Aplicación del AID)

Este EF contiene uno o más propósitos de la aplicación UICC.

Identificador: “6Fxx”	Estructura: transparente		Opcional
SFI: “xx”			
Tamaño del archivo: 1 byte		Actividad de actualización: baja	
Condiciones de acceso: LEER PIN ACTUALIZAR ADM DESACTIVAR ADM ACTIVAR ADM			
Bytes	Descripción	I/O	Longitud
1	Aplicación del AID	I	1

Aplicación del AID

Codificación:

b8	b7	b6	b5	b4	b3	b2	b1	
					X	X	0	servicios de MC
					X	X	1	VoLTE (servicios de HPLMN)
					0	0	1	RCS
					0	1	1	RFU
					1	1	1	RFU
RFU (véase TS 31.101 [3])								

Solución alternativa para codificar la aplicación en el EF_{IMPI} existente

Se apreciará que se podría implementar una combinación de lo anterior y lo siguiente.

4.2.X $EF_{Segmento}$ (Segmento de la aplicación)

Este EF contiene el propósito del AID.

Identificador: “6Fxx”	Estructura: transparente		Opcional
SFI: “xx”			
Tamaño del archivo: 1 byte		Actividad de actualización: baja	
Condiciones de acceso: LEER PIN ACTUALIZAR ADM DESACTIVAR ADM ACTIVAR ADM			
Bytes	Descripción	I/O	Longitud
1-X	SST	I	X
X+1 a X+Y	SD	O	Y

4.2.X EF_{AIDAPP} (Aplicación del AID)

Este EF contiene el propósito del AID.

Identificador: “6Fxx”	Estructura: transparente	Opcional	
SFI: “xx”			
Tamaño del archivo: 1 byte		Actividad de actualización: baja	
Condiciones de acceso: LEER PIN ACTUALIZAR ADM DESACTIVAR ADM ACTIVAR ADM			
Bytes	Descripción	I/O	Longitud
X+1	Número de ICSI	O	1
X+2	Objeto ICSI TLV	O	1

Objeto ICSI TLV:

Contenido:

- El contenido y la codificación se definen a continuación:

Codificación de los objetos ICSI TLV

Longitud	Descripción	Valor	Estado
1 byte	TAG ICSI TLV	“KK”	I
1 byte	Longitud del ICSI	Y	I
Y bytes	Valor del ICSI	-	I

- Codificación:

Identificador del servicio de comunicación IMS: se codificará según lo especificado en TS 24.229.

Los bytes no utilizados se establecerán en 'FF'

Nota: las realizaciones anteriores podrían combinarse para tener un único archivo que tenga un ID de aplicación y luego una lista de ICSI o IARI en el que el ICSI/IARI represente las capacidades que se admiten con el tipo de aplicación general.

En lo anterior, también es posible añadir un campo APN si es necesario; el ME puede utilizarlo si es necesario para establecer la conexión PDN a la red de datos para esa aplicación (p. ej., VoLTE, MCPTT, RCS, etc.). Véase la figura 17 para una posible forma de codificar el APN.

APÉNDICE B – Cambios en el 3GPP TS 31.102/103

4.2.2 EF_{IMPI} (Identidad de usuario privada IMS)

Este EF contiene la identidad de usuario privada del usuario.

Identificador: “6F02”	Estructura: transparente	Imperativo
SFI: “02”		
Tamaño del archivo: X bytes	Actividad de actualización: baja	
Condiciones de acceso: LEER PIN ACTUALIZAR ADM DESACTIVAR ADM ACTIVAR ADM		

Bytes	Descripción	I/O	Longitud
1 a X	Objeto de datos NAI TLV	I	X bytes
X+1	Longitud en bytes del algoritmo	O	1
X+2	Algoritmo para utilizar con el IMPI	O	1
X+3	Longitud en bytes de la aplicación	O	1
X+4	Aplicación para el IMPI	O	1
X+5 a X+Y	Punto de acceso a la red	O	Y

Algoritmo para utilizar con el IMPI

Codificación:

b8	b7	b6	b5	b4	b3	b2	b1	
					X	X	0	Algoritmo 1
					X	X	1	Algoritmo 2
					0	0	1	Algoritmo 3
					0	1	1	Algoritmo 4
					1	1	1	Algoritmo 5
RFU (véase TS 31.101 [3])								

Algoritmo para utilizar con el IMPI

Codificación:

b8	b7	b6	b5	b4	b3	b2	b1	
					X	X	0	servicios de MC
					X	X	1	VoLTE (servicios de HPLMN)
					0	0	1	RCS
					0	1	1	?
					1	1	1	?
RFU (véase TS 31.101 [3])								

Punto de acceso a la red

Contiene un APN que usa el ME cuando utiliza la codificación NAI

Véase APN en 3GPP TS 23.003

Solución alternativa para codificar la aplicación en el EF_{IMPI} existente

Se apreciará que se podría implementar una combinación de lo anterior y lo siguiente.

4.2.X EF_{IMPIY} (Identidad de usuario privada IMS para la aplicación Y)

Este EF contiene la identidad de usuario privada del usuario que se utilizará para una aplicación Y alternativa.

Identificador: “6Fxx”	Estructura: transparente	Imperativo
SFI: “xx”		
Tamaño del archivo: X bytes	Actividad de actualización: baja	
Condiciones de acceso: LEER PIN ACTUALIZAR ADM DESACTIVAR ADM ACTIVAR ADM		

Bytes	Descripción	I/O	Longitud
1 a X	Objeto de datos NAI TLV	I	X bytes
X+1	Longitud en bytes del algoritmo	O	1
X+2	Algoritmo para utilizar con el IMPI	O	1
X+3 a X+Y	Punto de acceso a la red	O	Y

Algoritmo para utilizar con el IMPI

Codificación:

b8	b7	b6	b5	b4	b3	b2	b1	
					X	X	0	Algoritmo 1
					X	X	1	Algoritmo 2
					0	0	1	Algoritmo 3
					0	1	1	Algoritmo 4
					1	1	1	Algoritmo 5
RFU (véase TS 31.101 [3])								

Punto de acceso a la red

Contiene un APN que usa el ME cuando utiliza la codificación NAI

Véase APN en 3GPP TS 23.003

7.1.2.1 Contexto de seguridad IMS AKA

Byte(s)	Descripción	Longitud
1	Longitud de RAND (L1)	1
2 a (L1+1)	RAND	L1
(L1+2)	Longitud de AUTN (L2)	1
(L1+3) a (L1+L2+2)	AUTN	L2
	Longitud de la ID de usuario	1
	ID de usuario	
Implementación alternativa		
	Longitud del algoritmo	1
	Algoritmo	L4

La codificación de AUTN se describe en TS 33.102 [4]. El bit más significativo de RAND está codificado en el bit 8 del byte 2. El bit más significativo de AUTN está codificado en el bit 8 del byte (L1+3).

Parámetros/datos de respuesta, caso 1, comando satisfactorio:

La codificación de la ID de usuario es como se describe en el apartado 4.2.2.

5

REIVINDICACIONES

1. Un procedimiento en una entidad (1010) móvil que permite el uso de múltiples servicios de multimedios, IMS, sobre protocolo de Internet, IP, comprendiendo el procedimiento:

leer (1032, 1042, 1052) datos de un primer módulo de identidad de abonado IMS, ISIM, de una pluralidad de módulos de identidad de abonado IMS, ISIM, (1012, 1014, 1016) asociados con la entidad móvil; estando ubicados los ISIM en la entidad (1010) móvil;

la lectura comprende determinar si un archivo identificador de aplicación, EF_{AIDAPP}, está presente en el primer ISIM;

si el archivo identificador de aplicación, EF_{AIDAPP}, está presente y almacena los datos del archivo identificador de aplicación, EF_{AIDAPP}, en una memoria interna de la entidad (1010) móvil; y

crear (1054) un enlace en la memoria interna de la entidad móvil para enlazar (1054) una función en la entidad móvil a un ISIM de la pluralidad de ISIM, en el que la creación comprende:

seleccionar los datos del archivo identificador de aplicación, EF_{AIDAPP}, del primer ISIM;

determinar si una indicación en los datos del archivo identificador de aplicación, EF_{AIDAPP}, del primer ISIM (1012,1014,1016) incluyen una indicación para la función;

si la indicación en los datos del archivo identificador de aplicación, EF_{AIDAPP}, incluyen la indicación de la función, determinar que el primer ISIM será el que se enlazará a la función y enlazar el primer ISIM a la función; y

si la indicación en los datos del archivo identificador de aplicación, EF_{AIDAPP}, no incluyen la función, seleccionar los datos del archivo identificador de aplicación, EF_{AIDAPP}, de un ISIM diferente de la pluralidad de ISIM,

en el que cuando se invoca la función seleccionada, se utiliza el ISIM enlazado a la función seleccionada.

2. El procedimiento de la reivindicación 1, en el que la indicación es un campo explícito en los datos del archivo identificador de aplicación, EF_{AIDAPP}.

3. El procedimiento de la reivindicación 1, en el que la indicación es un identificador de servicio de comunicación IMS.

4. El procedimiento de la reivindicación 1, en el que la indicación es un identificador de referencia de aplicación IMS.

5. El procedimiento de la reivindicación 1, en el que la indicación es un nombre de punto de acceso.

6. El procedimiento de la reivindicación 1, en el que la pluralidad de ISIM están asociados con una tarjeta de circuito integrado universal, UICC, en la entidad móvil.

7. Una entidad móvil que permite el uso de múltiples servicios de multimedios, IMS, sobre protocolo de Internet, IP, comprendiendo la entidad móvil:

un procesador; y

un sistema de comunicaciones,

en el que la entidad móvil está configurada para llevar a cabo el procedimiento de una cualquiera de las reivindicaciones 1 a 6.

8. Un medio legible por ordenador para almacenar código de instrucción que permite el uso de múltiples servicios de multimedios, IMS sobre protocolo de Internet, IP, que, cuando se ejecutan por un procesador (1638) de una entidad móvil, hacen que la entidad (1600) móvil:

lleve a cabo el procedimiento de una cualquiera de las reivindicaciones 1 a 6.

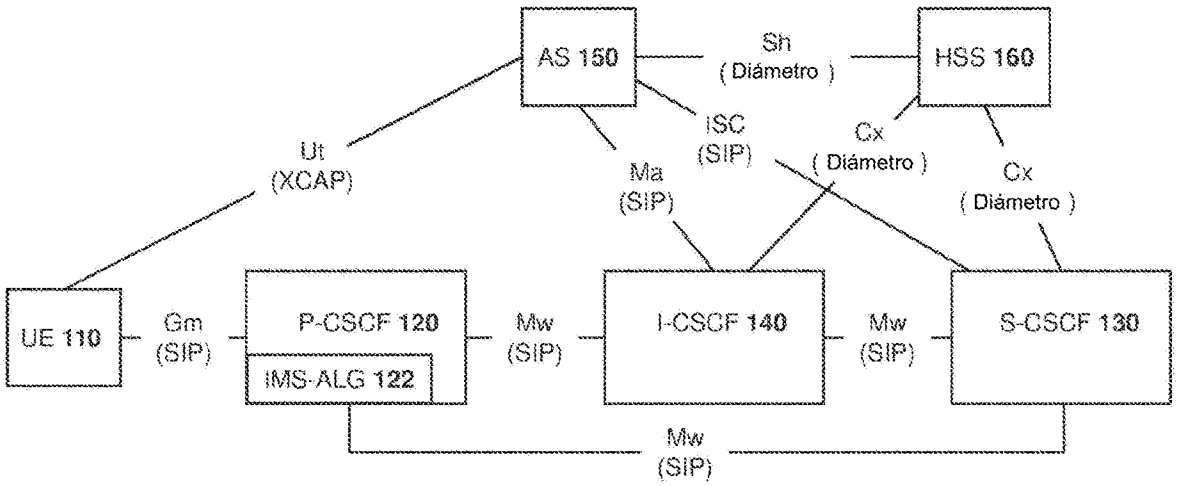
AS 150
Sh
(Diámetro)
HSS 160
ISC
(SIP)
Cx
(Diámetro)
Ut
(XCAP)
Ma
(SIP)
Cx
(Diámetro)
UE 110
Gm
(SIP)
P-CSCF 120
IMS-ALG 122
Mw
(SIP)
I-CSCF 140
Mw
(SIP)
S-CSCF 130
Mw
(SIP)

FIG. 1

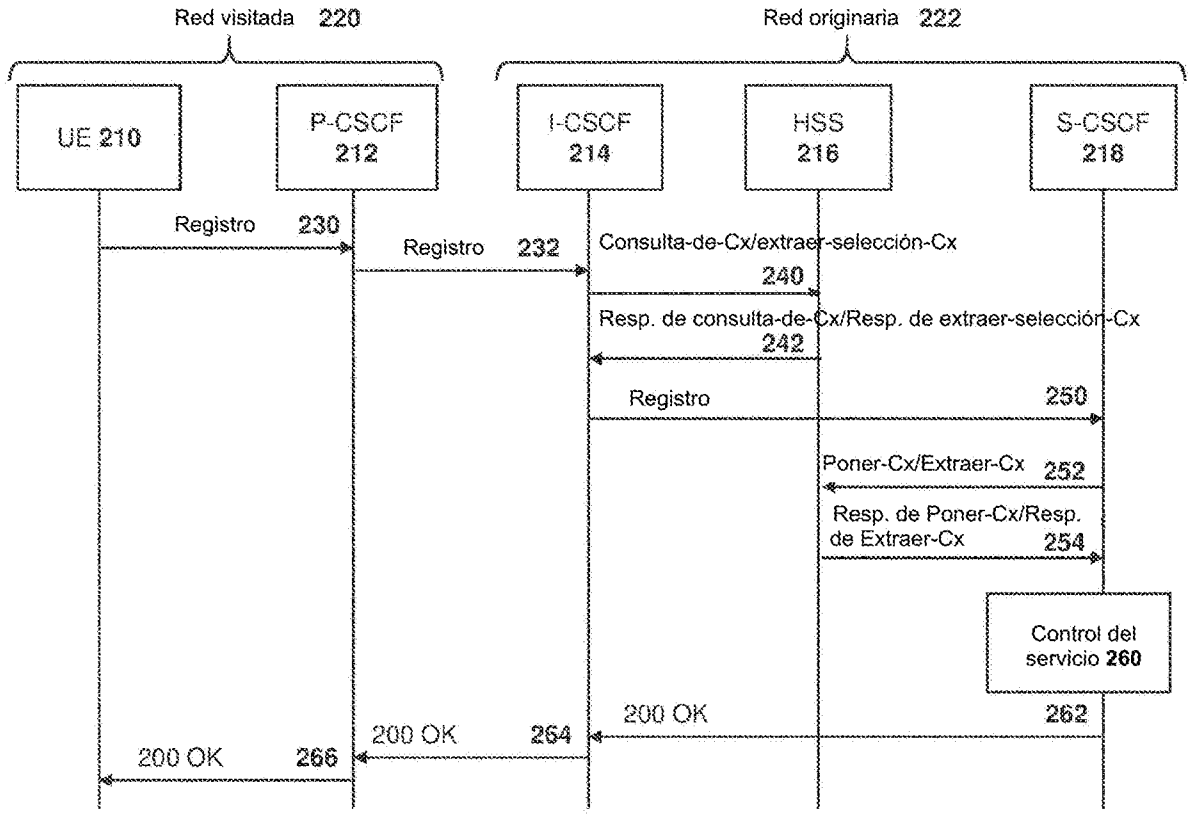
Red visitada 220
Red originaria 222
UE 210
P-CSCF 212
I-CSCF 214
HSS 216
S-CSCF 218
Registro 230
Registro 232
Consulta-de-Cx/extraer-selección-Cx 240
Resp. de consulta-de-Cx/Resp. de extraer-selección-Cx 242
Registro 250
Poner-Cx/Extraer-Cx 252
Resp. de Poner-Cx/Resp. de Extraer-Cx 254
Control del servicio 260
200 OK 262
200 OK 264
200 OK 266

FIG. 2

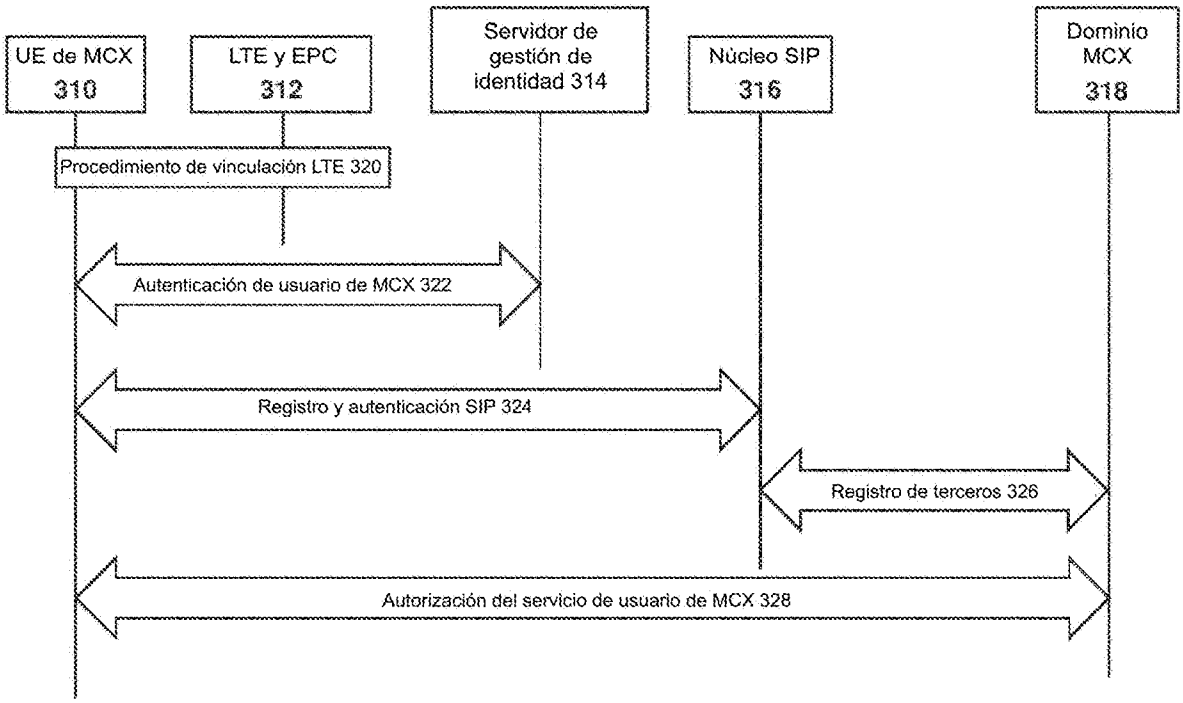
UE de MCX
310
LTE y EPC
312
Servidor de gestión de identidad 314
Núcleo SIP
316
Dominio MCX
318
Procedimiento de vinculación LTE 320
Autenticación de usuario de MCX 322
Registro y autenticación SIP 324
Registro de terceros 326
Autorización del servicio de usuario de MCX 328

FIG. 3

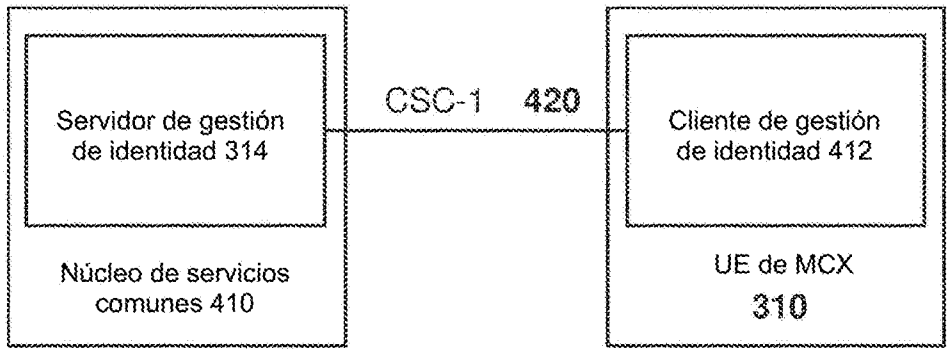
Servidor de gestión de identidad 314
CSC-1 420
Cliente de gestión de identidad 412
Núcleo de servicios comunes 410
UE de MCX 310

FIG. 4

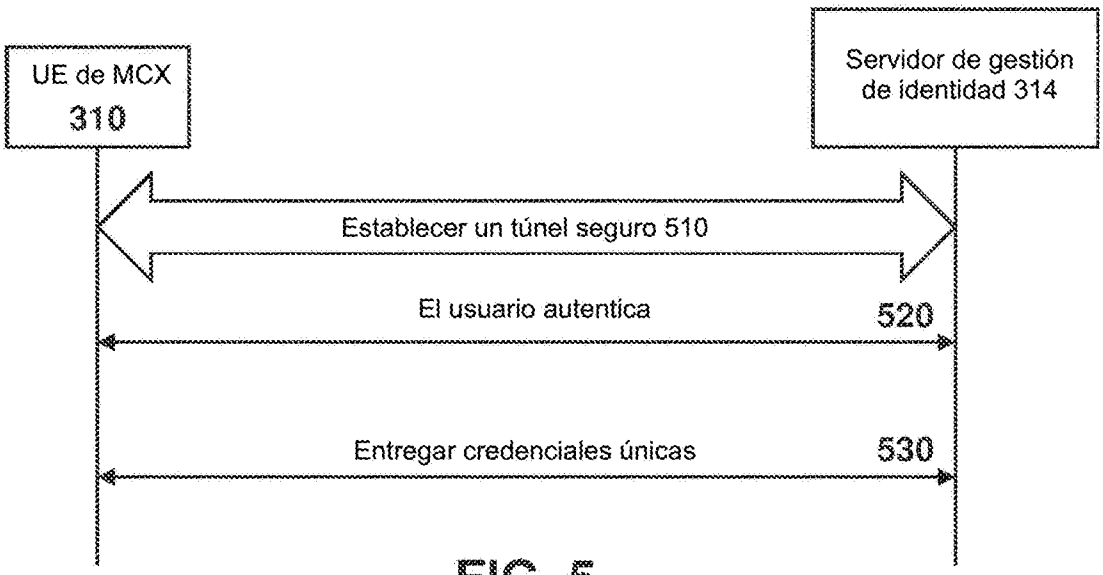
UE de MCX 310
Servidor de gestión de identidad 314
Establecer un túnel seguro 510
El usuario autentica
520
Entregar credenciales únicas
530

FIG. 5

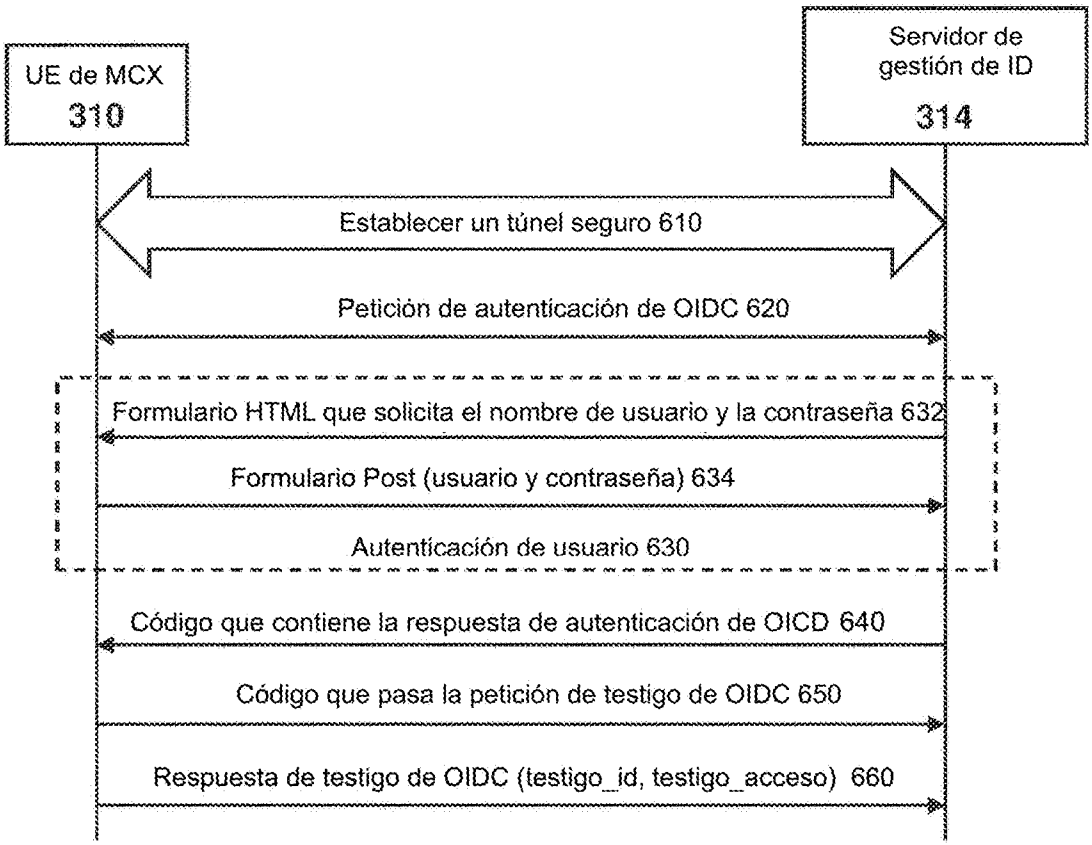
UE de MCX
310
Servidor de gestión de ID
314
Establecer un túnel seguro 610
Petición de autenticación de OIDC 620
Formulario HTML que solicita el nombre de usuario y la contraseña 632
Formulario Post (usuario y contraseña) 634
Autenticación de usuario 630
Código que contiene la respuesta de autenticación de OICD 640
Código que pasa la petición de testigo de OIDC 650
Respuesta de testigo de OIDC (testigo_id, testigo_acceso) 660

FIG. 6

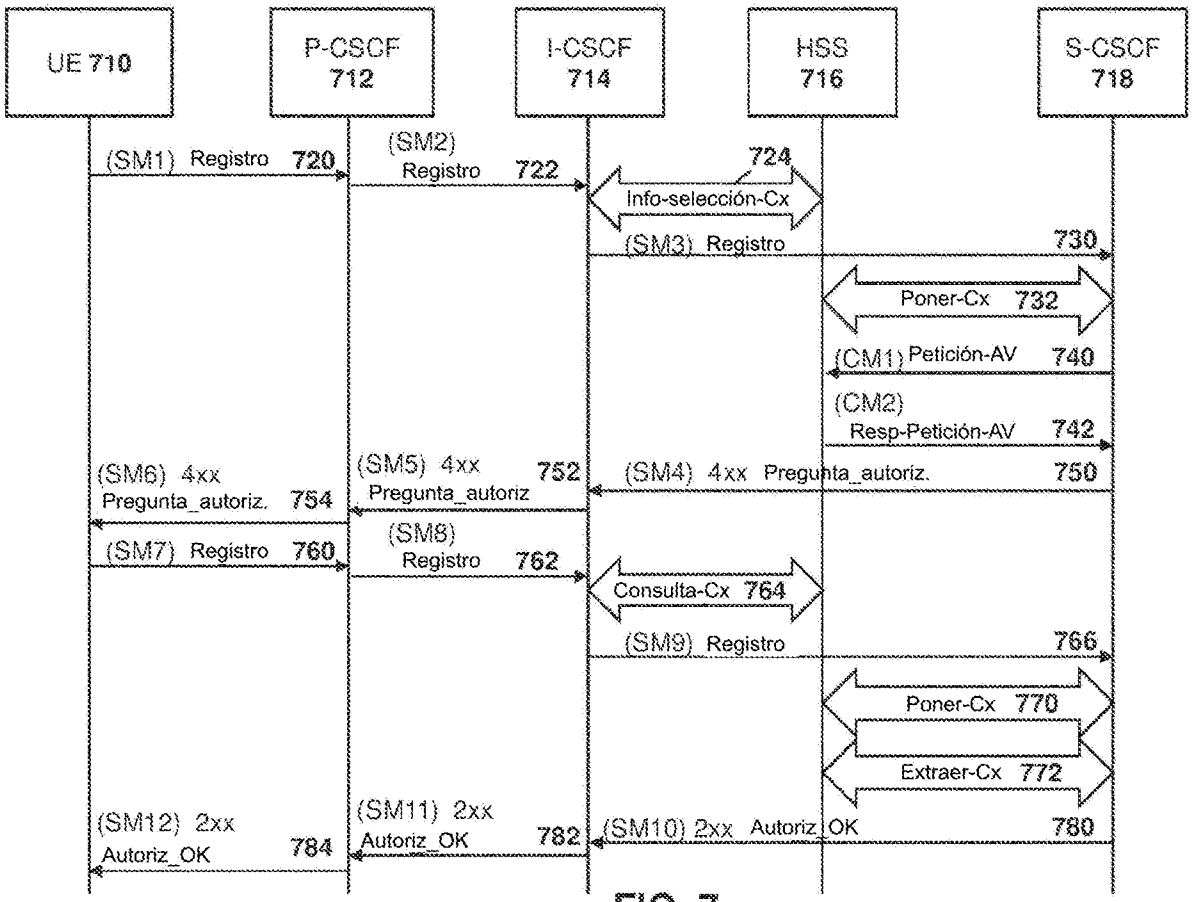
UE 710
P-CSCF 712
I-CSCF 714
HSS 716
S-CSCF 718
(SM1) Registro 720
(SM2) Registro 722
724
Info-selección-Cx
(SM3) Registro 730
Poner-Cx 732
(CM1) Petición-AV 740
(CM2) Resp-Petición-AV 742
(SM6) 4xx Pregunta_autoriz. 754
(SM5) 4xx Pregunta_autoriz 752
(SM4) 4xx Pregunta_autoriz. 750
(SM7) Registro 760
(SM8) Registro 762
Consulta-Cx 764
(SM9) Registro 766
Poner-Cx 770
Extraer-Cx 772
(SM12) 2xx Autoriz_OK 784
(SM11) 2xx Autoriz_OK 782
(SM10) 2xx Autoriz_OK 780

FIG. 7

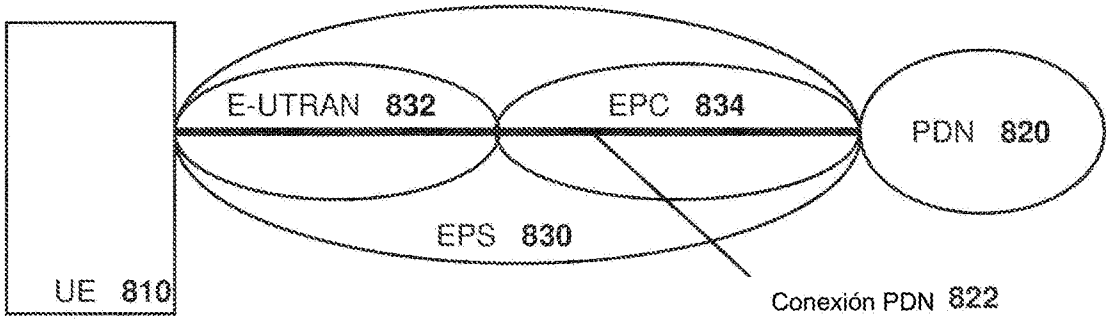

FIG. 8

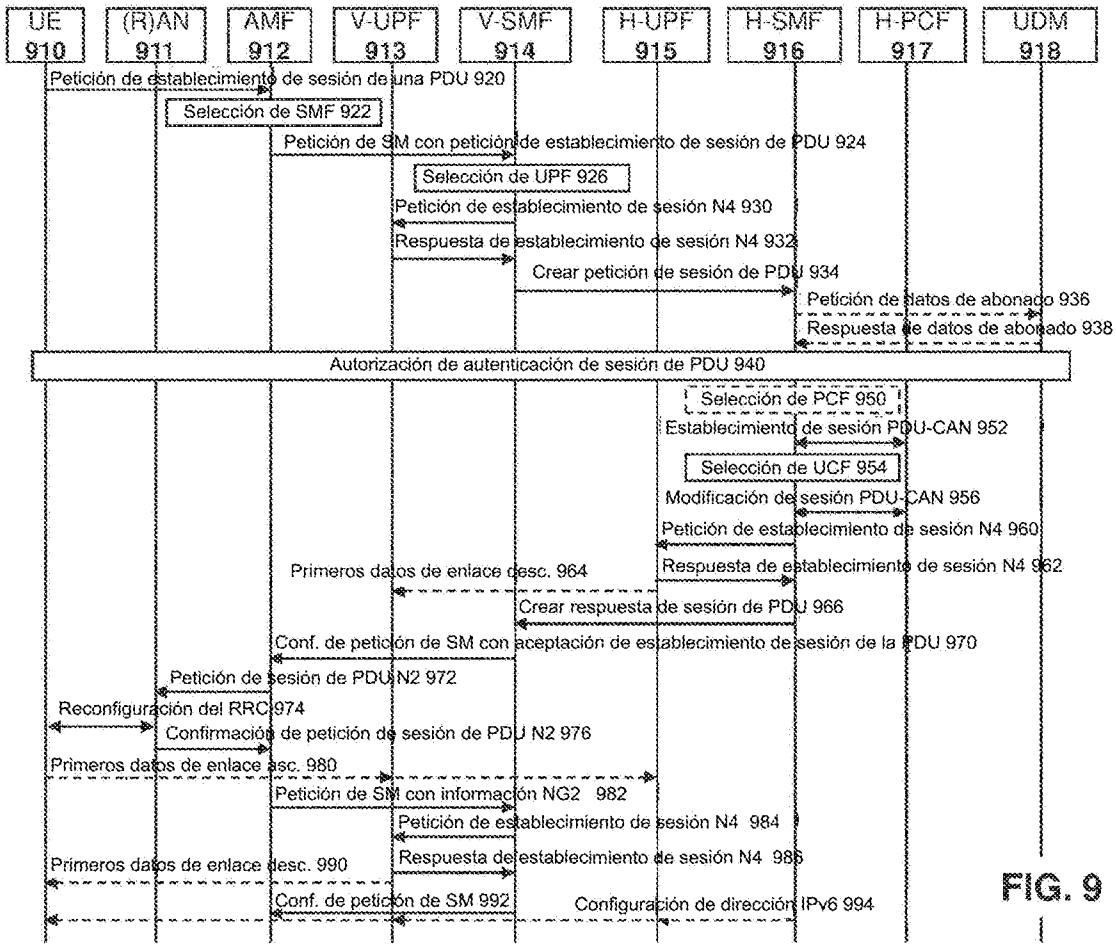
UE 910
(R)AN 911
AMF 912
V-UPF 913
V-SMF 914
H-UPF 915
H-SMF 916
H-PCF 917
UDM 918
Petición de establecimiento de sesión de una PDU 920
Selección de SMF 922
Petición de SM con petición de establecimiento de sesión de PDU 924
Selección de UPF 926
Petición de establecimiento de sesión N4 930
Respuesta de establecimiento de sesión N4 932
Crear petición de sesión de PDU 934
Petición de datos de abonado 936
Respuesta de datos de abonado 938
Autorización de autenticación de sesión de PDU 940
Selección de PCF 950
Establecimiento de sesión PDU-CAN 952
Selección de UCF 954
Modificación de sesión PDU-CAN 956
Petición de establecimiento de sesión N4 960
Respuesta de establecimiento de sesión N4 962
Primeros datos de enlace desc. 964
Crear respuesta de sesión de PDU 966
Conf. de petición de SM con aceptación de establecimiento de sesión de la PDU 970
Petición de sesión de PDU N2 972
Reconfiguración del RRC 974
Confirmación de petición de sesión de PDU N2 976
Primeros datos de enlace asc. 980
Petición de SM con información NG2 982
Petición de establecimiento de sesión N4 984
Respuesta de establecimiento de sesión N4 986
Primeros datos de enlace desc. 990
Conf. de petición de SM 992
Configuración de dirección IPv6 994

FIG. 9

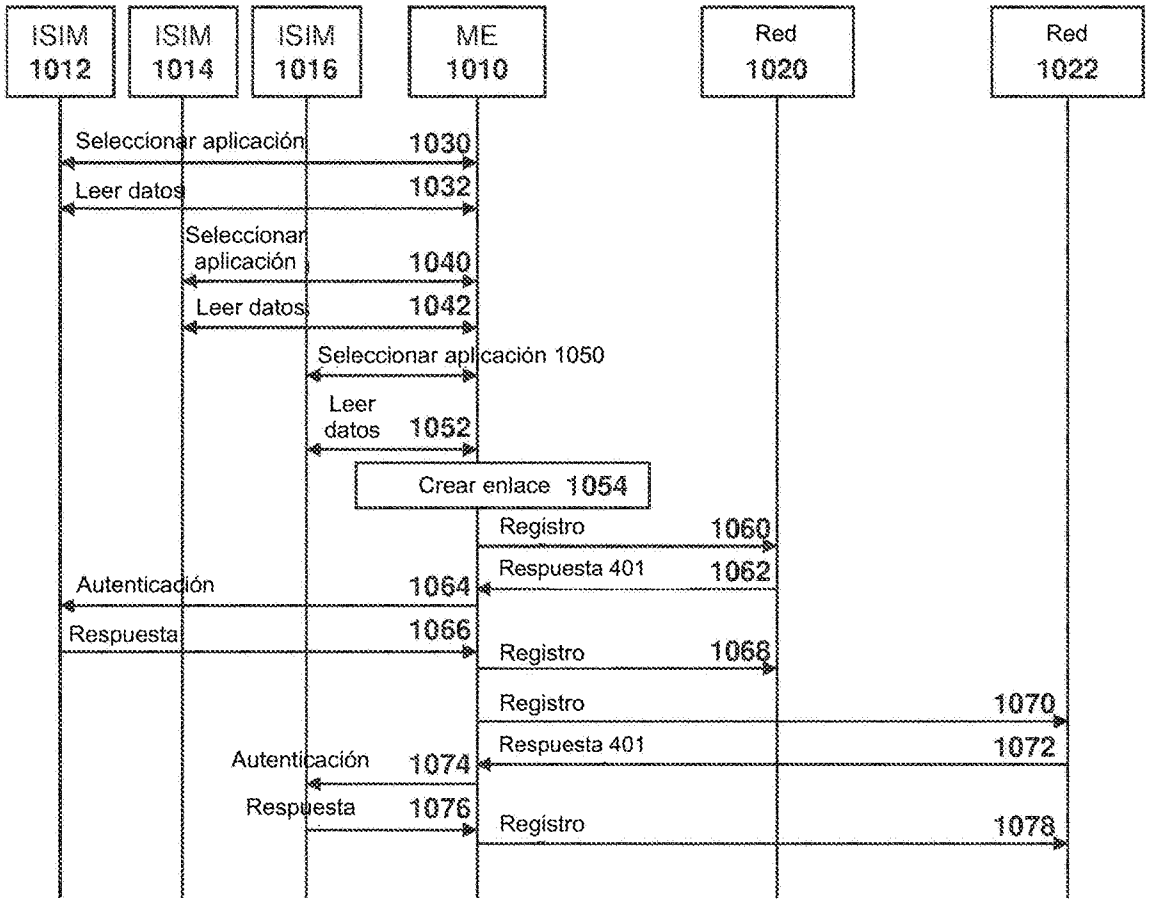
ISIM 1012
ISIM 1014
ISIM 1016
ME 1010
Red 1020
Red 1022
Seleccionar aplicación 1030
Leer datos 1032
Seleccionar aplicación 1040
Leer datos 1042
Seleccionar aplicación 1050
Leer datos 1052
Crear enlace 1054
Registro 1060
Respuesta 401 1062
Autenticación 1064
Respuesta 1066
Registro 1068
Registro 1070
Respuesta 401 1072
Autenticación 1074
Respuesta 1076
Registro 1078

FIG. 10

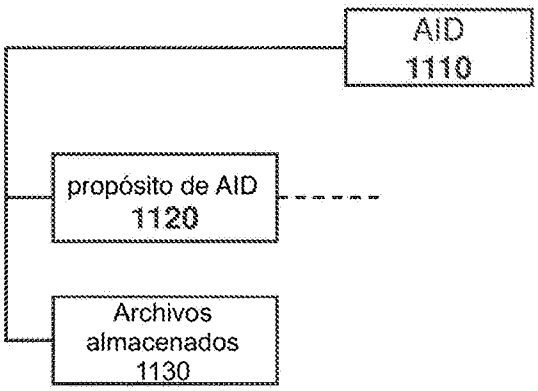
AID
1110
propósito de AID
1120
Archivos
almacenados
1130

FIG. 11

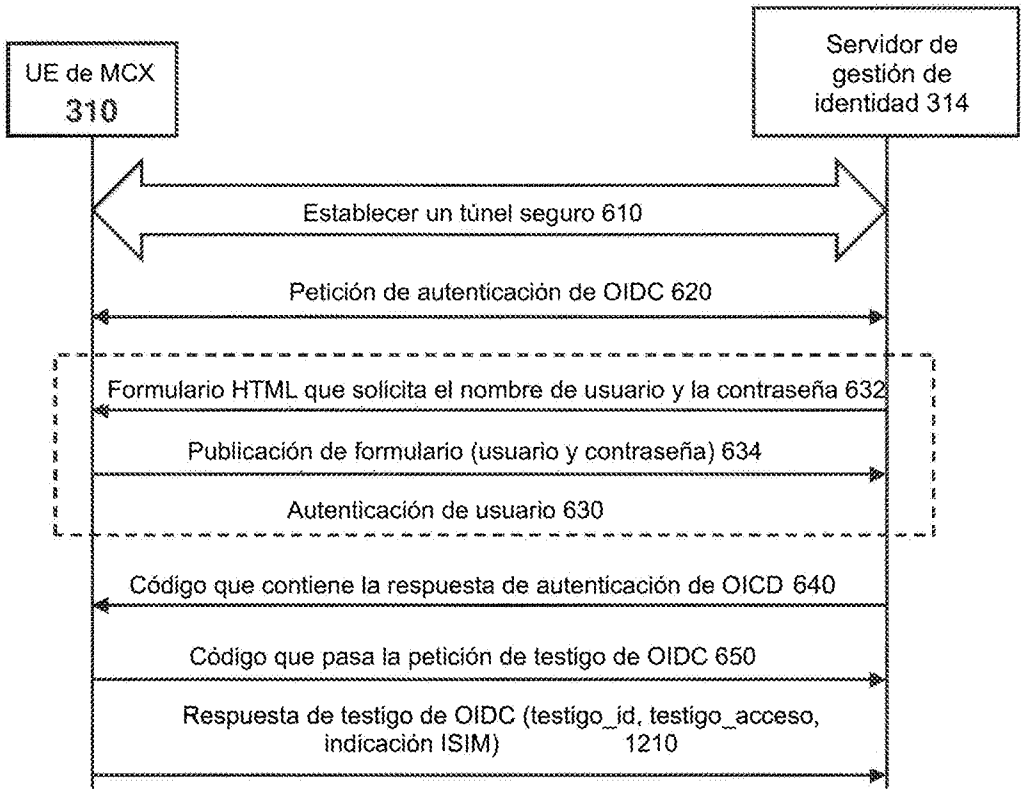
UE de MCX
310
Servidor de
gestión de
identidad 314
Establecer un túnel seguro 610
Petición de autenticación de OIDC 620
Formulario HTML que solicita el nombre de usuario y la contraseña 632
Publicación de formulario (usuario y contraseña) 634
Autenticación de usuario 630
Código que contiene la respuesta de autenticación de OICD 640
Código que pasa la petición de testigo de OIDC 650
Respuesta de testigo de OIDC (testigo_id, testigo_acceso,
indicación ISIM) 1210

FIG. 12

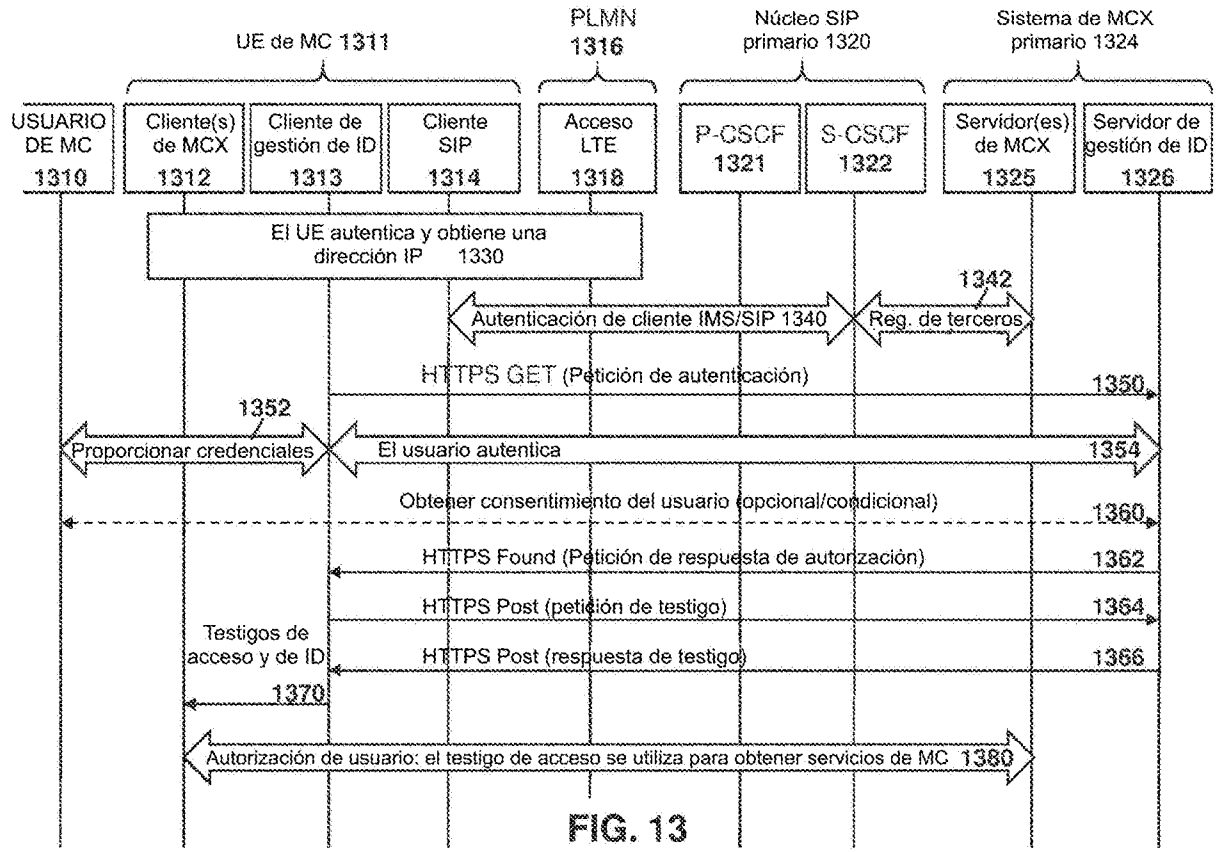
UE de MC 1311
PLMN 1316
Núcleo SIP primario 1320
Sistema de MCX primario 1324
USUARIO DE MC 1310
Cliente(s) de MCX 1312
Cliente de gestión de ID 1313
Cliente SIP 1314
Acceso LTE 1318
P-CSCF 1321
S-CSCF 1322
Servidor(es) de MCX 1325
Servidor de gestión de ID 1326
El UE autentica y obtiene una dirección IP 1330
1342
Autenticación de cliente IMS/SIP 1340
Reg. de terceros
HTTPS GET (Petición de autenticación)
1350
1352
Proporcionar credenciales
El usuario autentica
1354
Obtener consentimiento del usuario (opcional/condicional)
1360
HTTPS Found (Petición de respuesta de autorización)
1362
HTTPS Post (petición de testigo)
1364
Testigos de acceso y de ID
HTTPS Post (respuesta de testigo)
1366
1370
Autorización de usuario: el testigo de acceso se utiliza para obtener servicios de MC 1380

FIG. 13

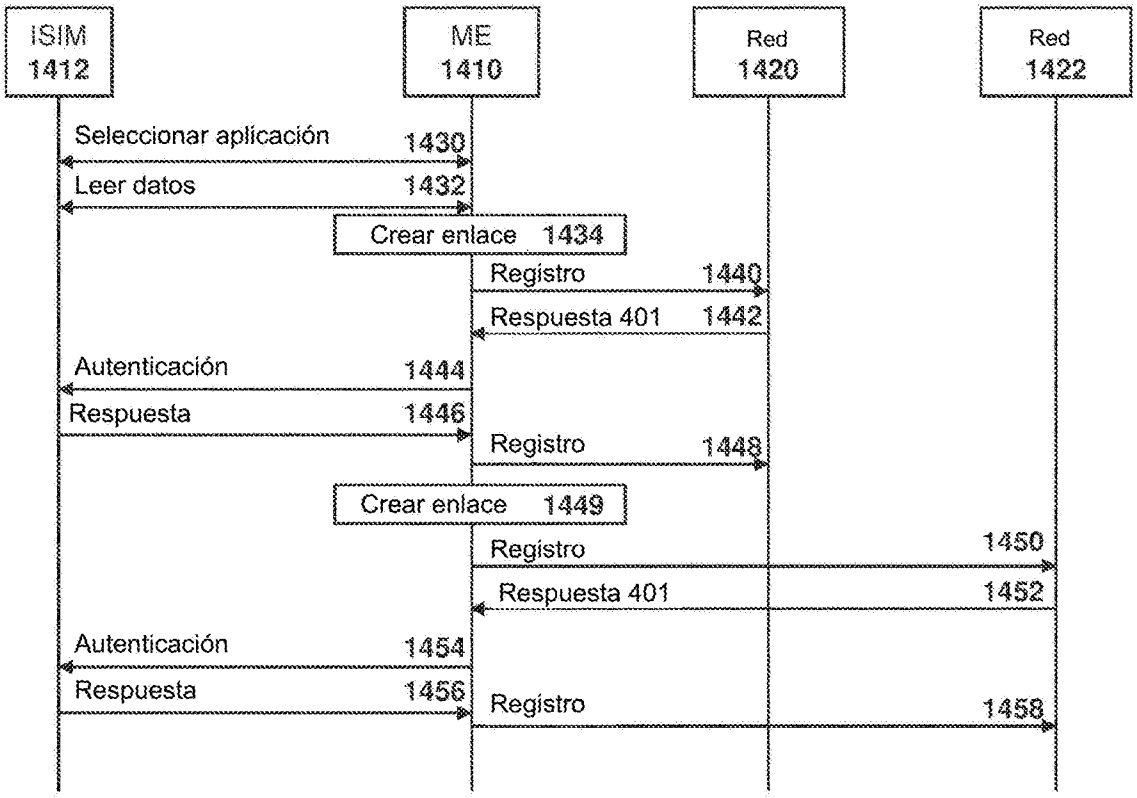
ISIM
1412
ME
1410
Red
1420
Red
1422
Seleccionar aplicación 1430
Leer datos 1432
Crear enlace 1434
Registro 1440
Respuesta 401 1442
Autenticación 1444
Respuesta 1446
Registro 1448
Crear enlace 1449
Registro 1450
Respuesta 401 1452
Autenticación 1454
Respuesta 1456
Registro 1458

FIG. 14

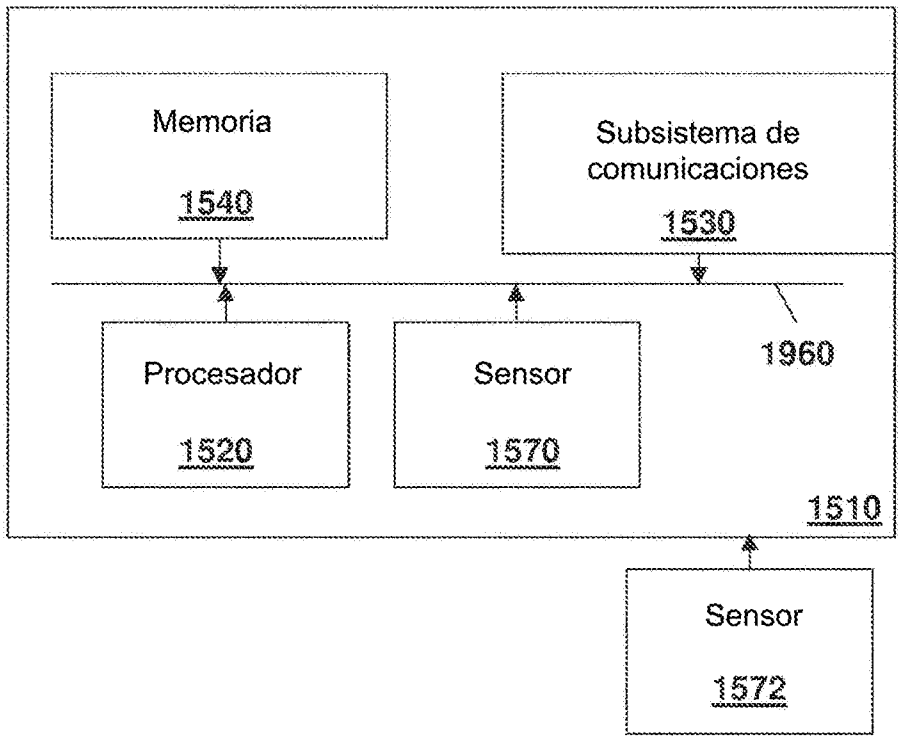
Memoria
1540
Subsistema de comunicaciones
1530
1960
Procesador
1520
Sensor
1570
1510
Sensor
1572

FIG. 15

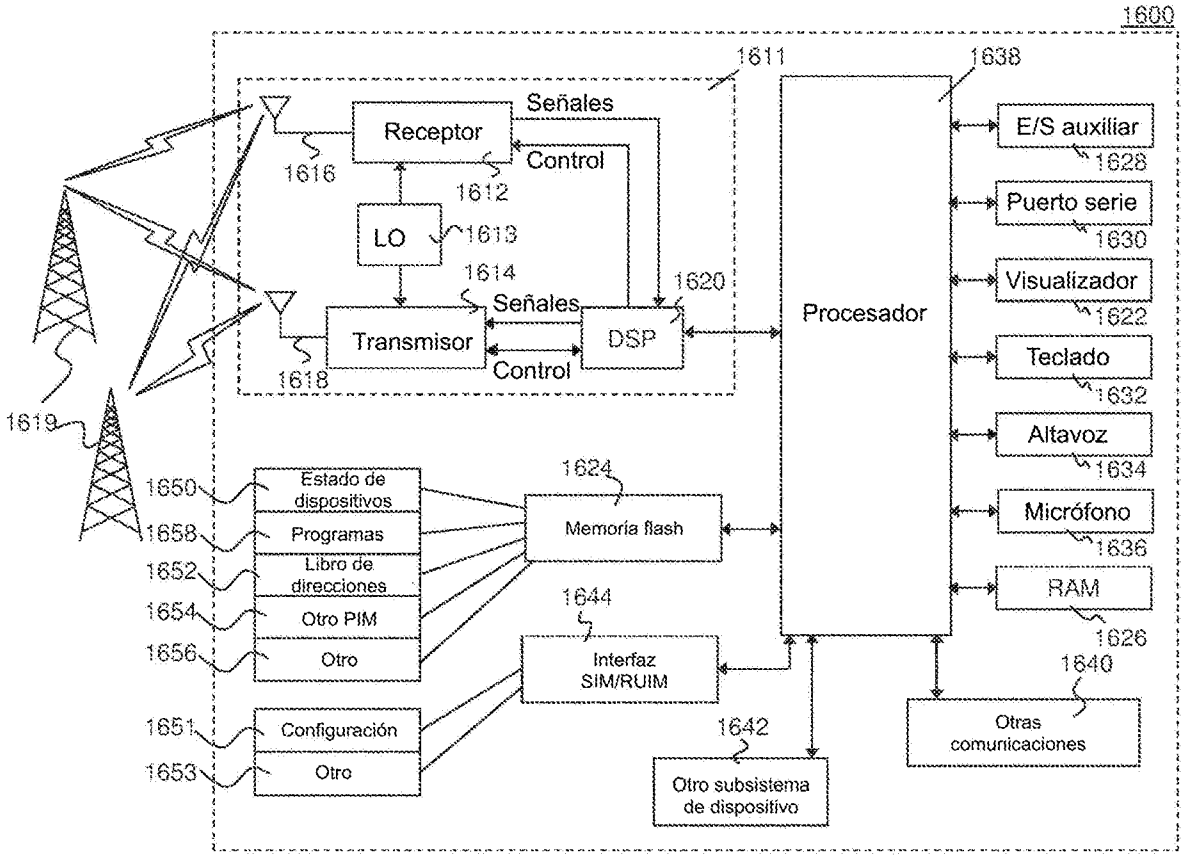
1600
1611
1638
Señales
Receptor
Control
1616
1612
LO
1613
1614
Señales
1620
Transmisor
DSP
Control
1618
Procesador
1619
E/S auxiliar
1628
Puerto serie
1630
Visualizador
1622
Teclado
1632
Altavoz
1634
Micrófono
1636
RAM
1626
1624
1650
Estado de dispositivos
1658
Programas
1652
Libro de direcciones
1654
Otro PIM
1656
Otro
Memoria flash
1644
Interfaz SIM/RUIM
1640
Otras comunicaciones
1642
Otro subsistema de dispositivo
1651
Configuración
1653
Otro

FIG. 16