(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **3 015 684**

(51) Int. Cl.:

H04W 12/02 (2009.01)
H04W 12/04 (2011.01)
H04W 12/06 (2011.01)
H04W 12/10 (2011.01)
H04W 12/72 (2011.01)
H04W 12/75 (2011.01)
H04L 9/40 (2012.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.07.2018 E 23209200 (7)**

(97) Fecha y número de publicación de la concesión europea: **05.03.2025 EP 4297340**

(54) Título: **Identificador oculto de suscripción**

(30) Prioridad:

25.07.2017 US 201762536632 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.05.2025

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.00%)
164 83 Stockholm, SE

(72) Inventor/es:

TORVINEN, VESA;
SAARINEN, PASI;
NAKARMI, PRAJWOL KUMAR;
CASTELLANOS ZAMORA, DAVID;
BEN HENDA, NOAMEN y
WIFVESSON, MONICA

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Identificador oculto de suscripción

Campo técnico

La invención se refiere a métodos realizados por un servidor de autenticación y un equipo de usuario (UE), respectivamente. Además, también se describen un UE y un servidor de autenticación.

Antecedentes

Es importante mantener la confidencialidad del identificador de suscripción a largo plazo de un equipo de usuario (UE) (por ejemplo, una IMSI (Identidad de Abonado Móvil Internacional)). Los sistemas 3GPP de primera generación (por ejemplo, 4G/LTE, 3G/UMTS, 2G/GSM) incluían un mecanismo parcial para la confidencialidad del identificador de suscripción a largo plazo usando uno o más identificadores de suscripción a corto plazo. El GUTI (ID Temporal Único Global) y el C-RNTI (Identificador Temporal de Red de Celdas de Radio) son ejemplos de identificadores de suscripción a corto plazo en sistemas 4G/LTE. Sin embargo, el mecanismo parcial heredado puede exponer el identificador de suscripción a largo plazo en texto sin cifrar a través de la interfaz aérea. Por ejemplo, los denominados "receptores IMSI" podrían simplemente solicitar el identificador a largo plazo del UE, por ejemplo, usando mensajes de solicitud/respuesta de identificador.

El Proyecto de Asociación de 3ª Generación (3GPP) analiza actualmente cómo se puede mejorar la seguridad, así como la privacidad, en las redes de comunicaciones. Con respecto a 5G, la TS 3GPP 33.501 V0.2.0 menciona un Identificador Permanente de Suscripción (SUPI) y se observa que el SUPI puede estar oculto, por ejemplo en forma de seudónimo o SUPI cifrado con clave pública.

El documento US 2013/003971 A1 describe un método para determinar una entidad de red con base en un identificador, en donde el identificador contiene una parte cifrada. Se puede enviar una solicitud a la entidad de red para ayudar en el descifrado del identificador.

El documento WO 2016/209126 A1 describe un método de protección de la confidencialidad de un identificador asociado mediante un primer nodo de red con un abonado usado por una entidad móvil en una red de comunicaciones. El primer nodo de red recibe una solicitud para la autenticación de un UE desde un segundo nodo de red en una red de servicio. El primer nodo de red genera entonces un seudónimo asociado con el identificador.

Compendio

Un objetivo de la invención es facilitar la seguridad en la comunicación entre un UE y una red de comunicaciones.

Un primer aspecto de la invención se refiere a un método realizado por un servidor de autenticación en una red doméstica de un UE para obtener un SUPI que comprende un número de identificación de abonado móvil (MSIN), un código de país móvil (MCC) y un código de red móvil (MNC). El método comprende:

recibir, desde el UE, a través de una solicitud de autenticación de una Función de Anclaje de Seguridad un identificador oculto de suscripción, SUCI, que comprende

una parte cifrada en la que el MSIN del SUPI está cifrado, y

una parte de texto sin cifrar que comprende un identificador de red doméstica para la red doméstica, un identificador de clave pública para una clave pública de la red doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado usado por el UE para cifrar el MSIN en el SUCI, y en donde el identificador de red doméstica es el MCC y el MNC;

determinar un servidor de desocultación que se utiliza para descifrar la parte cifrada del SUCI;

enviar el SUCI al servidor de desocultación, y

recibir el SUPI en respuesta.

En una realización, el método puede comprender además recibir el SUCI desde el UE como parte de un procedimiento de registro para registrar el UE en una red de comunicación inalámbrica.

El método puede comprender además enviar el SUCI y una solicitud de un vector de autenticación para autenticar el UE al servidor de desocultación determinado en el mismo mensaje.

El método puede comprender además recibir el vector de autenticación y el SUPI, del servidor de desocultación determinado en la misma respuesta.

Un segundo aspecto se refiere a un método realizado por un UE. El método comprende:

generar un SUCI, que comprende una parte cifrada en la que un MSIN de un SUPI está cifrada, y una parte de texto sin cifrar que comprende un identificador de red doméstica para una red doméstica del UE, un identificador de clave pública para una clave pública de la red doméstica del UE y un identificador de esquema de cifrado que identifica un esquema de cifrado usado por el UE para cifrar el MSIN en el SUCI, y donde el identificador de red doméstica es un MCC del SUPI y un MNC del SUPI;

transmitir el SUCI, a través de una solicitud de autenticación de una Función de Anclaje de Seguridad a un servidor de autenticación en la red doméstica para reenviar el SUCI a un servidor de desocultación capaz de descifrar el SUPI a partir del SUCI.

El SUCI puede transmitirse en una solicitud para registrarse en una red de comunicación inalámbrica.

La generación del SUCI se puede realizar usando un componente de hardware seguro a prueba de manipulaciones del UE para generar el SUCI. En tal caso, la generación del SUCI puede comprender generar el SUCI en base a una clave de privacidad seleccionada entre una pluralidad de claves de privacidad almacenadas en el componente de hardware seguro resistente a la manipulación.

En una realización, la generación del SUCI comprende enviar un tiempo al componente de hardware seguro resistente a la manipulación para usar en la generación del SUCI.

La generación del SUCI comprende en una realización generar el SUCI desde una clave de privacidad que comprende el SUPI.

Transmitir el SUCI al servidor de autenticación comprende, en una realización, transmitir el SUCI al servidor de autenticación en respuesta a un mensaje de solicitud de identificador recibido desde una Función de gestión de Autenticación y Movilidad, AMF, como parte de un procedimiento para registrar el UE en una red de comunicación inalámbrica. En tal realización, el método puede comprender también transmitir una solicitud de registro al AMF, en donde la solicitud de registro comprende un identificador temporal único global 5G, y recibir el mensaje de solicitud de identificador en respuesta.

El método según el segundo aspecto puede comprender además autenticar con éxito con el servidor de autenticación después de la transmisión del SUCI, y recibir un mensaje de aceptación de registro en respuesta.

En una realización de los aspectos primero y segundo, el esquema de cifrado puede ser un esquema de cifrado nulo.

En una realización del primer y segundo aspectos, el esquema de cifrado puede ser un Esquema de Cifrado Integrado de Curva Elíptica, ECIES.

Un tercer aspecto se refiere a un servidor de autenticación para una red doméstica de un UE para obtener un SUPI, que comprende un MSIN, un MCC y un MNC. El servidor de autenticación está configurado para:

recibir desde el UE, a través de una solicitud de autenticación de una Función de Anclaje de Seguridad, un SUCI, que comprende una parte cifrada en la que el MSIN del SUPI está cifrada, y una parte de texto sin cifrar que comprende un identificador de red doméstica para la red doméstica, un identificador de clave pública para la red doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado usado por el UE para cifrar el MSIN en el SUCI, y en donde el identificador de red doméstica es el MCC y el MNC;

determinar un servidor de desocultación que se va a usar para descifrar la parte cifrada del SUCI;

enviar el SUCI al servidor de desocultación, y

recibir el SUPI en respuesta.

Un cuarto aspecto se refiere a un UE configurado para:

generar un SUCI, que comprende una parte cifrada en la que se cifra un MSIN de un SUPI;

y una parte de texto sin cifrar que comprende un identificador de red doméstica para una red doméstica del UE, un identificador de clave pública para una clave pública de la red doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado usado por el UE para cifrar el en el SUCI, y donde el identificador de red doméstica es un MCC del SUPI y un MNC del SUPI; y

transmitir el SUCI, a través de una solicitud de autenticación de una Función de Anclaje de Seguridad, a un servidor de autenticación en la red doméstica para reenviar el SUCI a un servidor de desocultación capaz de descifrar el SUPI.

Breve descripción de los dibujos

La Figura 1 ilustra una red de comunicación inalámbrica ejemplar.

La Figura 2 ilustra un ejemplo en el que un UE cifra su identificador de suscripción a largo plazo como parte de un

procedimiento de conexión.

La Figura 3 ilustra un ejemplo de un Identificador Oculto de Suscripción (SUCI).

La Figura 4 ilustra un ejemplo de una clave de privacidad.

La Figura 5 ilustra un esquema de privacidad de clave pública 3GPP.

La Figura 6 ilustra un ejemplo de un procedimiento de registro.

La Figura 7 ilustra un ejemplo en el que un 5G-USIM/UICC de un UE genera el SUCI.

La Figura 8 ilustra un ejemplo en el que el 5G-USIM/UICC no tiene una clave de privacidad.

La Figura 9 ilustra un ejemplo en el que un ME genera el SUCI.

La Figura 10 ilustra un ejemplo en el que se notifica al ME acerca de una clave de privacidad actualizada.

La Figura 11 ilustra un ejemplo en el que el ME detecta que el 5G-USIM/UICC ha sido reemplazado.

La Figura 12 ilustra un ejemplo de datos de verificación de clave de privacidad.

La Figura 13 ilustra un ejemplo de proceso de registro de UE en el que el UE no tiene una clave de privacidad válida.

La Figura 14 ilustra un proceso de registro de UE de ejemplo en el que es necesario actualizar la clave de privacidad del UE.

La Figura 15 ilustra un ejemplo de cómo la clave de privacidad y los datos de verificación de la clave de privacidad están relacionados entre sí.

La Figura 16 ilustra una realización de hardware para, por ejemplo, un servidor de autenticación.

La Figura 17 ilustra una realización de un servidor de autenticación.

La Figura 18 ilustra una realización de un servidor de autenticación.

La Figura 19 ilustra una realización para, por ejemplo, un servidor de desocultación.

La Figura 20 ilustra una realización de un servidor de desocultación.

La Figura 21 ilustra una realización de un UE.

La Figura 22 ilustra una realización de un UE.

Descripción detallada

La Figura 1 ilustra una red 30 de comunicación inalámbrica de ejemplo que incluye un UE 1, una red 2 de servicio y una red 3 doméstica. El UE y la red doméstica están ambos conectados comunicativamente e intercambian señales entre sí a través de la red de servicio. El UE está configurado con un identificador de suscripción que identifica una suscripción soportada por la red doméstica, y accede a la red doméstica usando la red de servicio.

Los ejemplos típicos del UE 1 incluyen un equipo móvil (ME), terminal móvil, teléfono inteligente, ordenador personal, un ordenador portátil, un ordenador de escritorio, una estación de trabajo, una tableta, un ordenador portable y/o un dispositivo inteligente. Según realizaciones concretas del UE, el UE puede comprender un almacenamiento de memoria general como parte de un ME, y un componente de hardware seguro resistente a la manipulación que proporciona un almacenamiento seguro, como un 5G-USIM (Módulo de Identidad de Abonado Universal), un UICC (Tarjeta de Circuito Integrado Universal), por ejemplo con un 5G-USIM instalado en el mismo y/u otro dispositivo de almacenamiento seguro. Según tales realizaciones, cualquiera de las capacidades atribuidas al UE, generalmente, se puede realizar usando el componente de hardware seguro resistente a la manipulación del UE.

La red 2 de servicio incluye dispositivos físicos y/o medios de señalización capaces de intercambiar señales de comunicación con el UE 1 y la red 3 doméstica. En concreto, la red de servicio puede incluir hardware que proporcione uno o más: puntos de acceso (por ejemplo, una estación base, eNodoB, femtocelda y/o punto de acceso inalámbrico), redes de acceso, servidores de autenticación, Funciones de gestión de Acceso y Movilidad (AMF), Funciones de Anclaje de Seguridad (SEAF), Funciones de Servidor de Autenticación (AUSF) y/o cualquier combinación de los mismos (no mostrado). En concreto, un servidor de autenticación puede proporcionar una o más AMF, SEAF AUSF y/o cualquier combinación de las mismas. Los detalles de estas entidades de red se discutirán con más detalle a continuación.

La red 3 doméstica incluye dispositivos físicos y/o medios de señalización capaces de intercambiar señales de comunicación con el UE 1 a través de la red 2 de servicio. En concreto, la red doméstica puede incluir uno o más:

servidores de desocultación, servidores de autenticación (por ejemplo, como se describe anteriormente), servidores de aprovisionamiento de claves, Funciones de Desocultación de Identificador de Suscripción (SIDF), Funciones de Aprovisionamiento de Claves de Privacidad (PKPF), Gestión de Datos Unificada (UDM) y/o cualquier combinación de los mismos (no mostrado). En concreto, un servidor de desocultación puede proporcionar una o más SIDF, PKPF y/o cualquier combinación de las mismas. Detalles concretos de estas entidades de red también se discutirán con más detalle a continuación.

La red de servicio y/o doméstica incluyen una o más: redes inalámbricas y/o redes móviles. Dichas redes pueden comprender cualquier número de dispositivos de red tales como enrutadores, puertas de enlace, conmutadores, concentradores, cortafuegos y similares (no mostrados) que soportan el intercambio de tales señales de comunicación.

Aunque la Figura 1 ilustra redes domésticas y de servicio separadas, en algunas realizaciones de la presente descripción, la red 3 doméstica es la red 2 de servicio, es decir, en el caso de que el UE no esté en itinerancia. Además, aunque anteriormente se especificaron ejemplos de funciones concretas en la red doméstica o en la red de servicio, esas funciones particulares pueden estar en la otra red doméstica o red de servicio según realizaciones concretas. Además, aunque solo se ilustra un UE 1 en la Figura 1, las redes de servicio y domésticas pueden soportar una pluralidad de UE, según realizaciones concretas.

Una forma de ejemplo de mantener la confidencialidad del identificador de suscripción a largo plazo de un UE es proteger el identificador de suscripción a largo plazo usando una clave pública de la red doméstica. La clave pública de la red doméstica se puede aprovisionar dentro del UE 1 sin un certificado, de modo que no se requiere una infraestructura de clave pública global (PKI) o una autoridad certificadora (CA) (es decir, porque la técnica se usa asimétricamente entre el UE y una función en la red 3 doméstica). En tal ejemplo, se puede esperar que el UE cifre el identificador de suscripción a largo plazo, que luego se transmite hacia la red doméstica, usando la clave pública de la red doméstica.

La Figura 2 ilustra un ejemplo concreto de este tipo en el que el UE cifra su identificador de suscripción a largo plazo como parte de un procedimiento de conexión. Según el ejemplo de la Figura 2, el UE 1 cifra su IMSI, dejando sus partes MCC (Código de País Móvil) y MNC (Código de Red Móvil) en texto sin cifrar, y envía una Solicitud de Conexión a la red 2 de servicio con la IMSI cifrada. Como su identificador (paso 1). La red de servicio identifica la red 3 doméstica del UE usando MCC/MNC de texto sin cifrar y solicita información de autenticación de la red doméstica del UE usando la IMSI cifrada como identificador del UE (paso 2). La red doméstica descifra la IMSI de la IMSI cifrada y obtiene la información de autenticación correspondiente. En respuesta a la solicitud de información de autenticación, la red doméstica envía la información de autenticación del UE junto con la IMSI de texto sin cifrar a la red de servicio (paso 3). La red de servicio realiza un procedimiento de autenticación con el UE para autenticar el UE (paso 4). Si el procedimiento de autenticación tiene éxito, la red de servicio envía un mensaje Aceptación de Conexión al UE (paso 5).

En tal enfoque, la clave pública de la red doméstica puede preprovisionarse en un USIM y/o puede suministrarse usando un procedimiento de aprovisionamiento OTA (Por el Aire). Aunque el enfoque ilustrado en la Figura 2 protege el identificador de suscripción a largo plazo en al menos algunas realizaciones, algunas de tales realizaciones pueden incluir una o más deficiencias. Por ejemplo, el enfoque ilustrado en la Figura 2 puede verse frustrado por USIM heredados que no se pueden cambiar de manera factible, ciertas operadoras domésticas que pueden no admitir el aprovisionamiento OTA y/o USIM que pueden no ser actualizables (por ejemplo, debido a limitaciones técnicas, falta de espacio de almacenamiento u otras limitaciones).

Diversas realizaciones de la presente descripción proporcionan alternativas a al menos algunos aspectos de la realización concreta ilustrada en la Figura 2, que corresponden a la Figura 3-8: Interacciones entre componentes en el documento “Deliverable D3.6 5G-PPP Security enablers open specicifications (v2.0)”. Realizaciones concretas permiten que la clave pública de la red 3 doméstica sea aprovisionada (por ejemplo, nuevamente o renovada) y almacenada en el UE 1, de modo que el UE 1 pueda cifrar su identificador de suscripción con esta clave pública. Además, en realizaciones concretas, la red de núcleo (tal como una red 5GC (núcleo 5G)) activa el aprovisionamiento de la clave pública de la red doméstica sobre los procedimientos de tráfico existentes definidos por 3GPP (por ejemplo, señalización de registro/autenticación, por ejemplo, mensajes de Estrato Sin Acceso entre el UE y un nodo AMF/SEAF en relación con un procedimiento de registro) sin la necesidad de depender de infraestructura adicional y procedimientos fuera de banda tales como realizar un procedimiento de actualización OTA.

Aunque las diversas realizaciones en la presente memoria describirán determinadas características o acciones realizadas por el UE 1, no se debe suponer que dichas características o acciones sean realizadas por cualquier componente concreto del UE a menos que se especifique lo contrario. Por ejemplo, dichas funciones pueden o no ser realizadas por una UICC, USIM, UICC incrustada, UICC integrada u otros circuitos y/o software del UE (por ejemplo, circuitos de banda base en el ME), dependiendo de la realización concreta.

Las realizaciones concretas incluyen un Identificador Permanente de Suscripción (SUPI). Un SUPI es un identificador permanente 5G de texto sin cifrar, único a nivel mundial, asignado a cada suscriptor en un sistema 5G. El SUPI puede estar basado en IMSI o no basado en IMSI. Las realizaciones que incluyen un SUPI basado en IMSI pueden usar la IMSI como se describe en la TS 3GPP 23.003 V15.0.0, por ejemplo. Las realizaciones que incluyen un SUPI no basado en IMSI pueden basarse en un Identificador de Acceso a la Red (NAI) según la identificación de usuario basada en la

RFC 4282 IETF NAI descrita en la TS 3GPP 23.003 V15.0.0. En algunas realizaciones, el SUPI contiene la dirección de la red doméstica (por ejemplo, el MCC y el MNC en el caso de un SUPI basado en IMSI). Tales realizaciones pueden permitir ciertos escenarios de itinerancia, por ejemplo, proporcionando a la red 2 de servicio información útil para identificar la red 3 doméstica del UE. En caso de que el SUPI sea un NAI, también puede contener la IMSI, pero también puede ser no IMSI basado.

Realizaciones concretas incluyen adicional o alternativamente un Identificador Oculto de Suscripción (SUCI), tal como se ilustra en el ejemplo de la Figura 3. Un SUCI es una versión protegida de un SUPI. El SUCI incluye una parte de texto sin cifrar y una parte cifrada.

La parte de texto sin cifrar incluye un identificador de red doméstica que identifica la red doméstica del UE 1. Por ejemplo, el SUCI puede incluir un MCC y MNC de la red doméstica. La parte de texto sin cifrar también puede incluir un identificador de clave pública, un identificador de esquema de cifrado y/o parámetros relacionados con el esquema útiles para descifrar la parte cifrada del SUCI según un esquema de cifrado, como una clave pública efímera del UE u otros parámetros para su uso en el Esquema de Cifrado Integrado de Curva Elíptica (ECIES) u otro esquema de cifrado. El término clave efímera es conocido por las personas expertas en la técnica y se define como una clave cuyo uso está restringido a un período de tiempo corto, como una única conexión (o sesión) de telecomunicaciones, tras lo cual se elimina todo rastro de la misma. Como se discutirá a continuación, el identificador de clave pública es un identificador que puede usarse dentro de la red doméstica para identificar la SIDF correcta en una red doméstica que incluye una pluralidad de SIDF. El ECIES, el identificador de clave pública y las SIDF se describirán con mayor detalle a continuación. Las personas expertas en la materia entenderá que "parte de texto sin cifrar" dentro del contexto del SUCI significa que la información que contiene no está oculta/no es información cifrada.

Cuando la parte cifrada se incluye en el SUCI, el SUCI es una versión protegida de SUPI. La parte cifrada incluye un identificador de suscripción cifrado, como un MSIN (Número de Identificación de Abonado Móvil) o nombre de usuario. El nombre de usuario puede ser la totalidad o una parte de los caracteres que vienen antes de la '@' en un NAI, por ejemplo nombredeusuario@mnc<MNC>.mcc<MCC>.3gppnetwork.org. En este ejemplo, todos los caracteres antes de '@' están cifrados. En el caso de un NAI decorado, que tiene la forma 'realmdomestico!nombredeusuario@otrorealm', solo la parte del nombre de usuario del texto a la izquierda de la '@' está cifrada, ya que el realmdoméstico podría usarse como información de enrutamiento. Por tanto, se puede realizar el descif'a'o de la parte cifrada del SUCI para aprender el SUPI correspondiente. ECIES es un ejemplo de un esquema de cifrad' 'e clave pública que puede usarse para generar un SUCI a partir de u' SUPI y/o un SUPI a partir de un SUCI. Como se discutirá más adelante, la parte cifrada del SUCI puede usar un esquema de cifrado nulo, por ejemplo, si el UE 1 no ha sido provisto con la clave pública de la red doméstica.

Una SIDF es una función ubicada en la red doméstica que se encarga de descifrar el SUCI. Concretamente en la arquitectura 5G, una SIDF puede estar coubicada en la UDM (Gestión de datos unificada). De manera alternativa, se puede decir que la SIDF es parte de la UDM o que lo proporciona la UDM. De manera adicional o alternativa, una SIDF puede ser una entidad separada de la UDM y/o coubicada con una AUSF (Función de Servidor de Autenticación).

La Figura 4 ilustra un ejemplo de una clave de privacidad. Este ejemplo concreto de clave de privacidad incluye una clave pública de la red doméstica. En algunas realizaciones, la clave de privacidad también incluye uno o más parámetros relacionados con el esquema de clave pública, el identificador de suscripción a largo plazo, un campo de asunto que indica una red, dominio o contexto al que pertenece la clave de privacidad (por ejemplo, el asunto puede ser un identificador de red doméstica, como un MCC/MNC), un identificador de esquema de clave pública, valores específicos de dominio relacionados con el esquema de clave pública (por ejemplo, valores para el dominio de curva elíptica en el caso del esquema ECIES), el identificador de clave pública como se discutirá más adelante detalle a continuación, los tiempos de validez que indican cuándo es válida la clave de privacidad (por ejemplo, no es válida antes y/o no es válida después de un tiempo), un campo de uso de clave que indica una o más formas en que se puede usar la clave (por ejemplo, privacidad del identificador de suscripción, segmento selección de privacidad, etc.) y/o una firma digital calculada sobre parte o la totalidad de la clave de privacidad.

En concreto, el campo de uso de la clave puede establecerse para indicar que la clave es útil para la "privacidad de la suscripción", de acuerdo con las realizaciones de la presente descripción. Los usos de la privacidad que están más allá del alcance de la presente descripción pueden indicar de manera adicional o alternativa otros usos para la clave de privacidad. Por ejemplo, la clave privada se puede usar para fines de "privacidad de la Información de Asistencia para la Selección de Segmentos de Red (NSSAI)" en lugar de, o además de, para fines de "privacidad de suscripción". De hecho, tales otros propósitos pueden incluir métodos, dispositivos y sistemas similares en el UE 1 y/o en la red Doméstica para el aprovisionamiento inicial, la actualización y otras características como se describe en la presente memoria. Aunque una clave de privacidad puede, en algunas realizaciones, indicar usos múltiples, otras realizaciones pueden incluir claves de privacidad respectivas para usos respectivos, el campo de uso de clave de cada clave de privacidad indica un uso de clave único (por ejemplo, una de las claves de privacidad puede indicar " privacidad de suscripción" y el otro puede indicar "privacidad de NSSAI"). El campo de uso de clave puede formatearse como un número entero, uno o más valores enumerados, una cadena alfanumérica, una cadena de bits, una cadena delimitada y/o una matriz de cualquiera de los formatos mencionados anteriormente, entre otras cosas.

Un esquema de privacidad de clave pública 3GPP (esquemas 3GPK) es un esquema de clave pública estandarizado

que un UE 1 puede soportar para la interoperabilidad entre el UE y, por ejemplo, un operador móvil. En ausencia de un esquema estandarizado, los proveedores de UE probablemente necesitarían coordinarse con dichos operadores para implementar mecanismos de privacidad. Según realizaciones concretas, el UE debería soportar cualquier esquema permitido y/o estandarizado para que la red doméstica pueda elegir libremente un esquema sin crear ninguna dificultad de interoperabilidad. Uno de estos esquemas en concreto es, por ejemplo, el ECIES. Se pueden adoptar esquemas concretos como estándar, y se les puede dar un identificador (también llamado "registro") para la interoperabilidad. Para cada uno de estos esquemas, también se puede especificar cualquier algoritmo específico que deba ser compatible. Por ejemplo, en el caso de ECIES, se pueden especificar el acuerdo de claves (KA), la función de derivación de claves (KD) (KDF), la integridad simétrica y el cifrado simétrico. También se pueden especificar uno o más parámetros relacionados con dicho esquema, así como (en uno o más casos) sus valores estáticos potenciales. Por ejemplo, en ECIES, los parámetros del dominio de curva elíptica (p, a, b, G, n, h) para una curva sobre un campo principal y/o (m, f (x), a, b, G, n, h) para una curva sobre un campo binario.

La Figura 5 ilustra un esquema 3GPK de ejemplo. A cada esquema adoptado como estándar se le puede asignar un identificador específico. Por ejemplo, al esquema nulo se le puede asignar un 0, a ECIES se le puede asignar un 1, y así sucesivamente. El identificador puede ser, por ejemplo, un identificador de 4 bits. Otras realizaciones pueden formatear el identificador de esquema de otras formas, que incluyen, pero no se limitan a, uno o más números enteros, cadenas numéricas, cadenas alfanuméricas, cadenas de bits y/u otros tipos de datos.

Según las realizaciones de la presente memoria, el UE se registra en la red 30 de comunicación inalámbrica según un procedimiento de registro, tal como el procedimiento de registro de ejemplo ilustrado en la Figura 6. Según el procedimiento de registro de ejemplo ilustrado en la Figura 6, el UE usa una clave pública de la red doméstica para ocultar un identificador de suscripción a largo plazo. Aunque una o más interfaces concretas ilustradas en la Figura 6, como las especificadas por una N seguida de una designación numérica (por ejemplo, N1, N12, N13), estén de acuerdo con la TS 3GPP 23.501, la señalización realizada a través de tales interfaces como se describe en la presente memoria, así como otras de las interfaces en sí mismas (por ejemplo, Nxx), no se conocen ni se describen en ninguna técnica conocida.

Según el ejemplo de la Figura 6, el UE 1 incluye un identificador temporal (por ejemplo, un 5G-GUTI) en una solicitud de registro y envía la solicitud de registro a una AMF/SEAF 4 (paso 1). La AMF/SEAF, al no reconocer el 5G-GUTI, transmite un mensaje de solicitud de identificador al UE para solicitar el identificador del UE (paso 2). El UE responde al mensaje de solicitud de identificador con un mensaje de respuesta de identificador que comprende un SUCI (paso 3). La AMF/SEAF solicita la autenticación del UE desde la AUSF 5 en la red 3 doméstica e incluye el SUCI en la solicitud de autenticación (paso 4). La AUSF usa la información codificada en el SUCI para determinar cuál de una pluralidad de SIDF usar para descifrar al menos parte del SUCI (paso 5). En concreto, la AUSF puede usar el identificador de clave pública que se incluye en el SUCI (o que de otro modo está presente en el mensaje de solicitud de autenticación) para identificar la SIDF 6 correcta. En algunas realizaciones, la AUSF puede usar de manera adicional o alternativa el identificador de esquema para identificar la SIDF correcto. En otras palabras, diferentes SIDF pueden manejar diferentes esquemas de cifrado (por ejemplo, una primera SIDF puede manejar ECIES y una segunda SIDF puede manejar RSA), y la AUSF puede elegir una SIDF apropiada con base en qué esquema es identificado por el SUCI. En una realización alternativa más, la información usada para identificar la SIDF 6 correcta puede ser un parámetro o ID que indica la SIDF 6 y qué parámetro/ID se almacena o proporciona al componente 8 de hardware seguro resistente a la manipulación.

Las realizaciones de la presente descripción pueden incluir múltiples SIDF para evitar tener un solo punto de fallo para las redes que tienen un gran número de abonados, por ejemplo. En consecuencia, las implementaciones distribuidas de SIDF pueden resultar ventajosas para mejorar la tolerancia a fallos, el balanceo de carga y/o la capacidad general de la red. De manera adicional o alternativa, se pueden implementar diferentes instancias de SIDF para manejar diferentes conjuntos de claves públicas de la red doméstica. Por consiguiente, el identificador de clave pública en el SUCI puede usarse para seleccionar la instancia o instancias de SIDF adecuadas, según una o más realizaciones en la presente memoria. De manera alternativa, en realizaciones concretas que solo tienen una SIDF desplegada, el identificador de clave pública puede omitirse del SUCI.

La AUSF 5 envía el SUCI a la SIDF 6 seleccionada (paso 6). Si la SIDF está coubicado en la UDM 7 (de modo que el mensaje Nxx en el paso 6 de la Figura 6 es un mensaje N13, por ejemplo), entonces el mismo mensaje puede usarse para solicitar un vector de autenticación o credenciales de autenticación de la UDM. La SIDF descifra el SUCI para obtener un SUPI correspondiente y devuelve el SUPI a la AUSF (paso 7). Si la SIDF está coubicada en la UDM, entonces se puede usar el mismo mensaje para devolver los vectores/credenciales de autenticación a la AUSF.

La AUSF 5 y el UE 1 intercambian mensajes de autenticación usando vectores/credenciales de autenticación recibidos desde la UDM 7 (paso 8). Si la AUSF aún no ha recibido el vector/credenciales de autenticación requeridos de la UDM (por ejemplo, en el paso 7 discutido anteriormente), la AUSF puede solicitar el vector/credenciales de autenticación de la UDM antes de iniciar la autenticación con el UE (no mostrado). De manera alternativa, la AUSF puede haber delegado la autenticación a la SEAF. En tales realizaciones, la AUSF puede simplemente reenviar el SUPI a la SEAF en este paso, y confiar en la SEAF para realizar la autenticación en el siguiente paso.

Continuando con el ejemplo en el que la AUSF 5 autentica satisfactoriamente el UE 1, la AUSF devuelve el SUPI a la

AMF/SEAF 4 (paso 9). La AMF/SEAF acepta el registro del UE y transmite un mensaje de aceptación del registro al UE (paso 10).

Como se discutió brevemente con anterioridad, las características concretas del UE 1 pueden ser realizadas por un componente 8 de hardware seguro resistente a la manipulación del UE. La Figura 7 ilustra un ejemplo concreto en el que un 5G-USIM/UICC 8a de un UE genera el SUCI. Aunque este ejemplo en concreto usa el término 5G-USIM / UICC, este término no debe considerarse limitativo con respecto a ninguna versión o proveedor de tecnología USIM o UICC, ni este término debe considerarse limitativo con respecto a cualquier generación de red móvil, por ejemplo, 2G/3G/4G/5G.

Según el ejemplo de la Figura 7, un ME 9 solicita un SUCI (paso 1). En algunas de tales realizaciones, esta solicitud SUCI puede incluir la marca de tiempo. En otras de tales realizaciones, la solicitud puede ser simplemente una operación de lectura del 5G-USIM/UICC 8a. Según tales realizaciones en las que existen múltiples claves públicas de la red doméstica, el 5G-USIM/UICC elige la clave de privacidad correspondiente correcta (por ejemplo, en base a la hora) y genera el SUCI usando la clave de privacidad seleccionada (paso 2). De manera alternativa, si existen tales realizaciones en las que solo hay una clave de privacidad, el 5G-USIM/UICC simplemente usa esa clave de privacidad. El 5G-USIM/UICC luego devuelve el SUCI al ME (paso 3).

La Figura 8 ilustra un ejemplo en el que el 5G-USIM/UICC no tiene una clave de privacidad o no es compatible con la función.

Según el ejemplo de la Figura 8, el ME 9 solicita un SUCI con una solicitud (que puede incluir la marca de tiempo, en algunas realizaciones) de manera similar a la descrita anteriormente con respecto a la Figura 7. En este ejemplo, sin embargo, el 5G-USIM/UICC 8a no tiene clave de privacidad o no reconoce el comando porque soporta la función (paso 2). En consecuencia, el 5G-USIM/UICC devuelve un mensaje de error (o datos vacíos) al ME (paso 3).

De manera alternativa al ejemplo de la Figura 8, el ME 9 puede saber que el 5G-USIM/UICC 8a no tiene clave de privacidad o no admite la clave de privacidad por otros medios, según realizaciones concretas. Por ejemplo, el ME puede obtener la versión o la información del proveedor del 5G-USIM/UICC y determinar, con base en esta información, que una clave de privacidad no es compatible o no está presente. Como otro ejemplo, el ME puede determinar que una clave de privacidad no está soportada o no está presente en el 5G-USIM/UICC con base en algún otro mensaje de respuesta del 5G-USIM / UICC.

La Figura 9 ilustra un ejemplo en el que el ME 9 genera el SUCI, pero la clave de privacidad en sí está almacenada en el 5G-USIM/UICC 8a.

Según el ejemplo de la Figura 9, el ME 9 no tiene clave de privacidad y solicita una al 5G-USIM/UICC 8a (paso 1). En algunas realizaciones, la solicitud incluye la marca de tiempo. En otras realizaciones, la solicitud es una operación de lectura directa desde la memoria del 5G-USIM/UICC. El 5G-USIM/UICC luego elige la clave de privacidad (por ejemplo, según la marca de tiempo, si se proporciona en la solicitud) (paso 2). El 5G-USIM/UICC devuelve la clave de privacidad al ME (paso 3). En este punto, el ME puede, en algunas realizaciones (pero no necesariamente en todas las realizaciones) almacenar la clave de privacidad y/o el SUPI en una memoria no volátil del ME (paso 4). El ME genera entonces el SUCI con base en el SUPI y la clave de privacidad (paso 5).

La Figura 10 ilustra un ejemplo en el que el ME 9 recibe una notificación si la clave de privacidad se actualiza en el 5G-USIM/UICC 8a. En este escenario, el ME se suscribe a los cambios en las claves de privacidad y recibe notificaciones cuando hay actualizaciones disponibles. Este escenario asume que el ME almacena la clave de privacidad o solicita al 5G-USIM/UICC la clave de privacidad según sea necesario para obtener la clave de privacidad más reciente.

Según el ejemplo de la Figura 10, el ME 9 envía una solicitud al 5G-USIM/UICC 8a solicitando suscribirse a las actualizaciones de la clave de privacidad (paso 1). La solicitud puede, en algunas realizaciones, incluir un SUPI. El 5G-USIM/UICC acepta la suscripción y transmite un acuse de recibo al ME en respuesta (paso 2). Cuando la red doméstica actualiza la clave o las claves de privacidad o entrega una o más nuevas al 5G-USIM/UICC (paso 3), el 5G-USIM/UICC notifica al ME que hay una o más claves de privacidad nuevas disponibles (paso 4). Aunque la Figura 10 representa el mensaje de notificación que incluye la clave o las claves de privacidad, según otras realizaciones, el ME puede leer de manera alternativa la clave del 5G-USIM/UICC con base en la notificación. El ME reconoce la notificación (paso 5). Entonces, el ME almacena la nueva clave o las nuevas claves de privacidad en la memoria no volátil del ME (paso 6). El ME puede reemplazar los datos de la clave de privacidad existente si el MCC/MNC/MSID en los datos de la clave de privacidad almacenados previamente son idénticos.

La Figura 11 ilustra un ejemplo en el que el UE está encendido y el ME 9 detecta que el 5G-USIM/UICC 8a ha sido reemplazado (por ejemplo, con un 5G-USIM/UICC diferente, o simplemente extraído y reinsertado, según diversas realizaciones). Aunque realizaciones concretas pueden tratar el reemplazo con un 5G-USIM/UICC diferente de la misma manera que una extracción y reinserción (por ejemplo, por razones de seguridad), otras realizaciones pueden responder de manera diferente con base en cuál de estos dos escenarios se detecta.

Según el ejemplo de la Figura 10, el UE 1 se enciende (paso 1). El ME 9 envía un mensaje al 5G-USIM/UICC 8a (paso

2) y el 5G-USIM/UICC responde de una manera que es inconsistente con el momento en que el UE se encendió (paso 3). Por ejemplo, el mensaje de respuesta puede incluir un SUPI diferente al visto previamente por el ME.

El ME 9 determina que el 5G-USIM/UICC 8a ha sido reemplazado (paso 4). Por ejemplo, el 5G-USIM/UICC puede ser diferente de alguna manera de la vez anterior cuando se encendió el UE 1, lo que indica que el 5G-USIM/UICC ha sido reemplazado por uno diferente. De manera alternativa, el ME puede detectar que el 5G-USIM/UICC ha sido reemplazado utilizando una memoria no volátil que se actualiza mediante un mecanismo mecánico, eléctrico o de software, como un sensor óptico, interruptor, sensor de peso, sensor de presión y/o circuitos eléctricos que se activan cuando se quita y/o se inserta el 5G-USIM/UICC, por ejemplo, independientemente de si se ha quitado y vuelto a insertar el mismo 5G-USIM/UICC o uno diferente.

El ME 9 elimina la clave de privacidad que había almacenado previamente de la memoria no volátil (si existe). De manera adicional o alternativa, si el ME almacenó el SUPI del antiguo 5G-USIM/UICC con la clave de privacidad en su memoria, el ME puede decidir eliminar la clave de privacidad de la memoria no volátil con base en una comparación del SUPI devuelto por el nuevo 5G-USIM/UICC 8a con el SUPI almacenado con la clave de privacidad anterior.

Las realizaciones concretas descritas anteriormente describen formas en las que los dispositivos dentro de un sistema de comunicación inalámbrica pueden intercambiar de forma segura un identificador de suscripción, incluyendo la generación y uso de estructuras de datos concretas y esquemas de cifrado/descifrado correspondientes. En concreto, las realizaciones descritas anteriormente permiten que este intercambio seguro se realice como parte del registro del UE 1 en la red 30 de comunicación inalámbrica. Muchas de estas realizaciones suponen que el UE está provisto de una clave de privacidad válida.

Para asegurar que el UE 1 tiene, de hecho, una clave de privacidad válida, realizaciones adicionales de la presente descripción describen formas en las que provisionar el UE. Las realizaciones concretas relacionadas con el aprovisionamiento pueden incluir los Datos de Verificación de Clave de Privacidad (MAC-P). Como se muestra en el ejemplo de la Figura 12, los MAC-P incluyen un código de autenticación de mensajes (MAC). El MAC se calcula en función de la clave de privacidad y una clave de aprovisionamiento (que se explicará con mayor detalle a continuación). Por ejemplo, el MAC puede calcularse sobre los diversos campos de la clave de privacidad, que incluyen, pero no se limitan a, la clave pública de la red doméstica y sus parámetros relacionados como se describe anteriormente, en combinación con la clave de aprovisionamiento.

Los MAC-P puede, según algunas realizaciones, también incluir un identificador de clave de aprovisionamiento (por ejemplo, una RAND) y/o un identificador de algoritmo de protección de integridad. Según algunas realizaciones en las que los MAC-P no incluyen el identificador del algoritmo de protección de integridad, el algoritmo de protección de integridad a ser usado puede identificarse por separado de los MAC-P, o puede usarse una función de derivación de clave (KDF) predefinida como, por ejemplo, HMAC-SHA-256. Los MAC-P pueden incluir de manera adicional o alternativa un campo contador, que puede usarse para identificar los MAC-P de una pluralidad de MAC-P (por ejemplo, en los casos en que se calcula más de unos MAC-P usando la misma clave de aprovisionamiento). La relación entre la clave de privacidad (por ejemplo, como se muestra en la Figura 4) y los MAC-P (por ejemplo, como se muestra en la Figura 12) se explica con más detalle a continuación con respecto a la Figura 15.

La clave de aprovisionamiento es un secreto compartido entre el UE 1 y una PKPF 10 (véase la Figura 13), que se describe con más detalle a continuación. La clave de aprovisionamiento es específica del UE, es decir, es una clave que en la red 3 doméstica está asociada con el UE y/o el USIM, UICC 8a 5G o cualquier otro hardware en el UE/ME en el que se permite un SIM/USIM para ser almacenado. En algunas realizaciones, la clave de aprovisionamiento puede derivarse de la clave maestra de la red doméstica, por ejemplo K_{AUSF} en una red 5G o futura tal como se creó en por ejemplo los AKA 5G, EA'-AKA' y EAP-TLS (Protocolo de Autenticación Extensible - Seguridad de la capa de transporte), que se crea cuando el UE 1 se autentica en la red. En algunas de tales realizaciones, la AUSF puede tener la clave maestra de la red doméstica. Además, se puede crear una nueva clave maestra de red doméstica cuando el UE se vuelve a autenticar.

Según un ejemplo, la clave de aprovisionamiento se puede crear a partir de una CK (clave de cifrado), IK (clave de integridad) (por ejemplo, aplicando una KDF tal como HMAC-SHA-256 u otra función hash segura unidireccional, como SHA -256, o una concatenación de CK e IK). La clave de aprovisionamiento puede, de manera alternativa a una generación directa a partir de la clave maestra o CK/IK, generarse a partir 'e CK" e IK' como se genera a partir de CK e IK en el método EAP'AKA '. En otra alternativa, la clave de aprovisionamiento puede generarse a partir de EMSK (Clave de Sesión Maestra Extendida) en el caso de EAP-TLS como se especifica en RFC5216. Como la misma clave maestra de la red doméstica puede usarse para derivar numerosas claves, las realizaciones de la presente descripción usan al menos un parámetro estándar adicional en combinación con la clave maestra de la red doméstica como entrada para derivar la clave de aprovisionamiento. Por ejemplo, cuando se usa KDF estándar, el FC (Código de Función) se puede usar como entrada (por ejemplo, como se especifica en la TS 33.220, tal como la TS 33.220 V15.0.0) para producir una clave de aprovisionamiento que se distinga de otras claves producidas usando la clave maestra de la red doméstica.

Según otro ejemplo, la clave de aprovisionamiento puede ser una clave que es la misma que, o derivada de, una clave compartida efímera que se comparte entre la SIDF 6 y el UE 1, concretamente cuando el esquema de cifrado usado

es un esquema de clave pública híbrido tal como como el ECIES. Por ejemplo, el ECIES usa un mecanismo de clave pública (por ejemplo, Diffie-Hellman) para un acuerdo de clave que da como resultado una clave compartida, que es efímera, entre la SIDF y el UE. Esa clave compartida efímera, por motivos de seguridad, generalmente se procesa más a través de una función de derivación de clave (por ejemplo, SHA-256) para derivar aún otras claves compartidas derivadas entre la SIDF y el UE (por ejemplo, la clave de cifrado y la clave MAC en el ECIES). Una de estas otras claves compartidas derivadas se utiliza generalmente para el cifrado y se denomina clave de cifrado efímera. Según se aplica a las realizaciones de la presente descripción, una de estas otras claves compartidas derivadas puede usarse, por ejemplo, para generar un SUCI a partir de un SUPI. Además, en algunas realizaciones, otra de las claves compartidas derivadas (por ejemplo, la clave MAC en ECIES), una nueva derivada de una de las claves compartidas derivadas, o aún otra clave derivada de la clave compartida efímera, pueden usarse como la clave de aprovisionamiento. En algunas realizaciones en las que la SIDF tiene, o es capaz de obtener/derivar la clave de aprovisionamiento, la SIDF también puede calcular el MAC o los MAC-P.

La PKPF 10 es una función ubicada en la red 3 doméstica que es responsable de proporcionar la clave de privacidad. Según realizaciones concretas, la PKPF puede ubicarse junto con la AUSF 5, y concretamente en al menos algunas realizaciones en las que la clave de aprovisionamiento se deriva de la clave maestra de la red doméstica que se crea con base a la autenticación primaria entre el UE y la red. En otras realizaciones, la PKPF puede estar colocada con otras entidades 5GC, tales como el UDM 7. Según aún otras realizaciones, la PKPF es su propia entidad separada. En algunas realizaciones, la SIDF 6 y la PKPF se implementan juntas como una única función y no es necesario transferir la clave de aprovisionamiento. En algunas otras realizaciones, la PKPF puede obtener la clave de aprovisionamiento de la SIDF. La PKPF también puede obtener el MAC/MAC-P de la SIDF.

La Figura 13 ilustra un proceso de registro de UE de ejemplo en el que el UE 1 no tiene una clave de privacidad válida. Por ejemplo, el usuario final puede haber insertado un nuevo USIM/UICC en el UE, y este nuevo USIM/UICC no contiene una clave de privacidad.

Según el ejemplo ilustrado en la Figura 13, el UE 1 envía una solicitud de registro a una AMF/SEAF 4, que incluye un SUCI en la solicitud (paso 1). Debido a que el UE inicialmente no tiene clave de privacidad en este escenario, el UE usa un esquema nulo o un método de cifrado nulo para crear el SUCI. El esquema nulo se implementa de manera que devuelve la misma salida que la entrada, y se aplica tanto al cifrado en el UE como al descifrado por la SIDF 6. Además, debido a que el UE no tiene una clave de privacidad que indique el esquema nulo o el método de cifrado nulo (que la red doméstica puede elegir libremente, según realizaciones), se puede usar un indicador explícito o implícito de que falta la clave de privacidad real del UE, según realizaciones concretas. Por ejemplo, como se discutió anteriormente, el SUCI puede usar un esquema de cifrado nulo para la parte cifrada, lo que puede indicar implícitamente que falta la clave de privacidad. De manera alternativa, un indicado" de "clave de privacidad faltante" puede ser, por ejemplo, un valor identificador de clave pública estandarizado o bien conocido, una bandera y/o un indicador de tipo de mensaje (por ejemplo, una solicitud de registro del tipo "provisión de privacidad" o "registro preinicial ").

La AMF/SEAF 4, que ha recibido la solicitud de registro, solicita al UE la autenticación desde la AUSF 5/PKPF 10 (paso 2). La AUSF envía el SUCI (y el indicado" de "clave de privacidad faltante", si se incluyó uno en la solicitud de autenticación) a una SIDF 6 (paso 3). Según las realizaciones en las que la SIDF está coubicada en el UDM 7 (por ejemplo, el mensaje Nxx es un mensaje N13), entonces se puede usar el mismo mensaje para solicitar un vector/credenciales de autenticación desde el UDM.

La SIDF 6 ve que el SUCI está en texto sin cifrar y que al UE 1 le falta una clave de privacidad. Según este ejemplo, la SIDF tiene una política local que establece que todos los SUCI deben protegerse mediante ECIES. En consecuencia, la SIDF devuelve un SUPI a la AUSF, junto con una solicitud para proporcionar la clave de privacidad ECIES al UE (paso 4). En algunas realizaciones, la respuesta incluye múltiples claves de privacidad para ser proporcionadas al UE. Según las realizaciones en las que la SIDF está coubicada en el UDM 7, entonces se puede usar el mismo mensaje para devolver el vector/credenciales de autenticación a la AUSF 5.

Según realizaciones en las que la AUSF 5 no ha recibido aún el vector/credenciales de autenticación desde el UDM 7, la AUSF 5 puede solicitar dicho vector/credenciales de autenticación desde el UDM antes de iniciar la autenticación con el UE (no mostrado). De manera alternativa, según realizaciones en las que la AUSF ya ha recibido el vector/credenciales de autenticación desde el UDM, la AUSF y el UE intercambian mensajes de autenticación usando dichos vectores/credenciales de autenticación (paso 5). De manera alternativa, la AUSF puede haber delegado la autenticación a la AMF/SEAF 4.

Según este ejemplo, la PKPF 10 se ubica junto con la AUSF 5. En consecuencia, tras la autenticación exitosa, la AUSF/PKPF crea una clave de aprovisionamiento que puede usarse para proteger el mensaje de aprovisionamiento de la clave de privacidad al UE 1, es decir, sin la necesidad de intercambiar señalización para transferir la clave de aprovisionamiento. Según otras realizaciones en las que la AUSF y la PKPF no están coubicadas, la AUSF puede solicitar que la clave de aprovisionamiento sea generada por la PKPF y la PKPF puede transferir la clave de aprovisionamiento a la AUSF en respuesta (no mostrado).

La AUSF 5/PKPF 10 protege la clave o las claves de privacidad (recibidas desde la SIDF 6 en el paso 4) con la clave de aprovisionamiento calculando un MAC (por ejemplo, como se describe anteriormente con respecto a la Figura 12)

y construyendo los MAC-P (paso 6). En algunas realizaciones, la clave de privacidad también puede estar cifrada. En algunas realizaciones, la AUSF/PKPF puede recibir el MAC y/o los MAC-P de la SIDF, como se describió anteriormente, concretamente en al menos algunas realizaciones en las que la clave de aprovisionamiento está basada en la clave compartida efímera de, por ejemplo, un esquema ECES. En concreto, como se discutió anteriormente, la SIDF puede haber generado el MAC y/o los MAC-P.

A continuación, la AUSF 5 devuelve el SUPI, la clave o las claves de privacidad y los MAC-P a la AMF/SEAF 4 (paso 7). En algunas realizaciones, el SUPI, la clave o las claves de privacidad y/o los MAC-P se transmiten a la AMF/SEAF en el mismo flujo de mensajes relacionado con el registro para registrar el UE 1 en la red 30 de comunicación inalámbrica. En algunas realizaciones, el SUPI, la clave o las claves de privacidad y/o los MAC-P se transmiten a la AMF/SEAF en un flujo de mensajes separado (no mostrado).

Según realizaciones en las que la AUSF 5 delegó la autenticación del UE 1 a la AMF/SEAF 4, la AMF/SEAF puede autenticar al UE en este punto (no mostrado). En tales realizaciones, la AMF/SEAF puede haber recibido el SUPI, la clave o las claves de privacidad y los MAC-P previamente, por ejemplo, directamente desde la SIDF 6 en el paso 4.

La AMF/SEAF 4 acepta el registro del UE 1 y envía la clave o las claves de privacidad y los MAC-P al UE, por ejemplo, en un mensaje de aceptación del registro (paso 8). A continuación, el UE intenta verificar el MAC y, si tiene éxito, almacena la clave o las claves de privacidad. Para verificar el MAC, el UE crea la misma clave de aprovisionamiento que hizo anteriormente la AUSF 5/PKPF 10. En otras palabras, cuando el UE genera un MAC esperado y luego lo compara con el MAC recibido, se verifica el MAC si se considera que el MAC esperado es el mismo que el MAC recibido.

En algunas realizaciones, el UE 1 luego se desconecta de la red (paso 9), por ejemplo, para iniciar un nuevo procedimiento de registro usando una clave de privacidad provista para ocultar su identidad de abonado, según una de las realizaciones descritas anteriormente. Por ejemplo, desconectarse y volver a registrarse de esta manera puede evitar que un atacante vincule el SUPI a un identificador temporal del UE.

El UE 1 puede, en algunas realizaciones, necesitar ser provisto con una clave de privacidad debido a la expiración o invalidación de una clave de privacidad que fue previamente provista al UE. La Figura 14 ilustra un proceso de registro de UE de ejemplo en el que la clave de privacidad del UE necesita actualizarse, por ejemplo, por alguna razón de seguridad u operativa. Algunas de las razones por las que la clave de privacidad proporcionada previamente puede necesitar ser actualizada, según diversas realizaciones, pueden ser que la privacidad proporcionada previamente puede haber alcanzado (o está llegando) su fecha de caducidad, la seguridad en la red 30 de comunicación inalámbrica se ha visto comprometida de alguna manera, y/o la clave de privacidad está sujeta a actualizaciones periódicas.

Según el ejemplo de la Figura 14, el UE 1 envía una solicitud de registro a una AMF/SEAF 4 (paso 1). La solicitud de registro incluye un SUCI. En este ejemplo, dado que el UE tiene una clave de privacidad, el UE usa un esquema o método de cifrado (por ejemplo, el ECIES) para crear el SUCI, por ejemplo, según una de las realizaciones descritas anteriormente.

La AMF/SEAF 4 solicita la autenticación del UE desde una AUSF 5/PKPF 10 (paso 2). La AUSF envía el SUCI a una SIDF 6 (paso 3). Como en el ejemplo anterior según algunas realizaciones en las que la SIDF está coubicado con el UDM 7, entonces se puede usar el mismo mensaje para solicitar un vector/credenciales de autenticación desde el UDM.

La SIDF 6 ve que el SUCI se cifra con una clave de privacidad que debe actualizarse. Por ejemplo, la SIDF puede detectar que la clave de privacidad ha caducado o está a punto de caducar, o que la clave de privacidad no es válida por cualquier otro motivo, como se explicó anteriormente. La SIDF devuelve un SUPI a la AUSF 5 junto con una solicitud para la provisión de la clave de privacidad ECIES actualizada al UE (paso 4). Según algunas realizaciones, la respuesta puede incluir diversas claves de privacidad. Además, como se discutió anteriormente, según algunas realizaciones en las que la SIDF está coubicada en el UDM, se puede usar el mismo mensaje para devolver el vector/credenciales de autenticación a la AUSF.

La AUSF 5 y el UE 1 intercambian mensajes de autenticación usando vectores/credenciales de autenticación recibidos desde el UDM 7 (paso 5). Como se discutió en ejemplos anteriores, la AUSF puede haber recibido el vector/credenciales de autenticación requeridos desde el UDM ya en el paso 4 (por ejemplo, en algunas realizaciones en las que la SIDF 6 está coubicada en el UDM), o la AUSF puede solicitar dicho vector de autenticación/credenciales del UDM antes de iniciar la autenticación con el UE.

Según realizaciones en las que la PKPF 10 está coubicada con la AUSF 5, la AUSF/PKPF puede crear una clave de aprovisionamiento usada para proteger el mensaje de aprovisionamiento de la clave de privacidad al UE 1 como resultado de una autenticación exitosa. Por ejemplo, el procedimiento de autenticación puede incluir la producción de una clave maestra de red doméstica que puede usarse para derivar la clave de aprovisionamiento. De manera alternativa, en realizaciones en las que la PKPF y la AUSF no están coubicadas, la AUSF y la PKPF pueden intercambiar la clave de provisión a través de mensajes apropiados (no mostrados).

La AUSF 5/PKPF 10 protege la clave o las claves de privacidad (recibidas desde la SIDF 6 en el paso 4) con la clave de aprovisionamiento calculando un MAC y construyendo los MAC-P, por ejemplo, según el ejemplo ilustrado en la Figura 14 (paso 6). Como se discutió anteriormente, en algunas realizaciones, la AUSF/PKPF puede recibir el MAC

y/o los MAC-P de la SIDF, como se describió anteriormente, concretamente en al menos algunas realizaciones en las que la clave de aprovisionamiento se basa en la clave compartida efímera de, por ejemplo, un esquema EICES. En concreto, como se discutió anteriormente, la SIDF puede haber generado el MAC y/o los MAC-P.

Después de una autenticación exitosa, la AUSF 5 envía el SUPI, la clave o las claves de privacidad y los MAC-P a la AMF/SEAF 4 (paso 7), por ejemplo, en el mismo flujo de mensajes relacionado con el registro. Otras realizaciones pueden usar flujos de mensajes separados para uno o más de los SUPI, claves de privacidad o MAC-P. Además, como se discutió anteriormente, la AUSF puede haber delegado la autenticación del UE a la SEAF, en cuyo caso el SUPI, la clave de privacidad y los MAC-P pueden haber sido devueltos a la SEAF ya en el paso 4, y la AUSF realiza la autenticación como se describió anteriormente.

La AMF/SEAF 4 acepta el registro del UE 1 y envía la clave de privacidad y los MAC-P al UE, por ejemplo, en un mensaje de aceptación del registro (paso 8). El UE crea la misma clave de aprovisionamiento a partir de la autenticación primaria que hizo la AUSF 5/PKPF 10, y verifica el MAC en el mensaje. Si la verificación tiene éxito, el UE almacena la clave o las claves de privacidad. La antigua clave de privacidad también puede eliminarse.

Según un ejemplo más, la AUSF 5 genera el MAC y los MAC-P y envía la clave de privacidad y los MAC-P al UE 1 a través del UDM 7 que reenvía la clave o las claves de privacidad y los MAC-P a la AMF, que luego reenvía la) clave o las claves de privacidad y los MAC-P al UE 1. En tal ejemplo, la AUSF puede ser una AUSF de Red Móvil Terrestre Pública Local y la AMF puede ser en ese caso una AMF de Red Móvil Terrestre Pública Visitada (VPLMN). En tal caso, la autenticación puede haber sido delegada por la AUSF a la AMF VPLMN.

Como se discutió anteriormente, el MAC puede calcularse en base a una clave de privacidad (por ejemplo, como se ilustra en la Figura 4) y una clave de aprovisionamiento para generar los MAC-P (por ejemplo, como se ilustra en la Figura 12). En algunas realizaciones en las que se proporcionan múltiples claves de privacidad al UE 1, se puede calcular el mismo MAC sobre todas las claves de privacidad enviadas en el mismo mensaje.

La Figura 15 ilustra un ejemplo de cómo la clave de privacidad y los MAC-P están relacionados entre sí, y qué parámetros se usan como entrada para el cálculo del MAC (o MAC esperado (XMAC), según corresponda). Como se muestra en la Figura 15, la clave de aprovisionamiento y la clave de privacidad se usan para generar un MAC, que luego se puede usar en combinación con otra clave de privacidad para actualizar el MAC, y así sucesivamente hasta que se procesen todas las claves de privacidad. Una vez que se procesan todas las claves de privacidad, la clave de privacidad y el MAC pueden enviarse al UE.

En vista de todo lo anterior, uno o más de los dispositivos o funciones descritas anteriormente pueden implementarse usando el hardware de ejemplo ilustrado en la Figura 16. El hardware de ejemplo incluye los circuitos 11 de procesamiento y los circuitos 12 de comunicación. Los circuitos de procesamiento están acoplados comunicativamente a los circuitos de comunicación, por ejemplo, a través de uno o más buses. Los circuitos de procesamiento pueden comprender uno o más microprocesadores, microcontroladores, circuitos de hardware, circuitos lógicos discretos, registros de hardware, procesadores de señales digitales (DSP), matrices de puertas programables en campo (FPGA), circuitos integrados de aplicaciones específicas (ASIC) o una combinación de los mismos. Por ejemplo, los circuitos de procesamiento pueden ser hardware programable capaz de ejecutar instrucciones de software almacenadas, por ejemplo, como un programa 133 informático legible por máquina en unos circuitos 13 de memoria. Los circuitos de memoria de las diversas realizaciones pueden comprender cualquier medio legible por máquina no transitorio conocido en la técnica o que puedan desarrollarse, ya sean volátiles o no volátiles, incluidos, entre otros, medios de estado sólido (por ejemplo, SRAM, DRAM, DDRAM, ROM, PROM, EPROM, memoria flash, unidad de estado sólido, etc.), dispositivos de almacenamiento extraíbles (por ejemplo, una tarjeta Secure Digital (SD), tarjeta miniSD, tarjeta microSD, lápiz de memoria, unidad de memoria USB, unidad flash USB, cartucho ROM, Disco de Medios Universal), una unidad fija (por ejemplo, unidad de disco duro magnético), o similares, en su totalidad o en cualquier combinación. Según realizaciones concretas en las que el hardware se usa para implementar el UE 1, los circuitos de memoria pueden comprender un componente 8 de hardware seguro a prueba de manipulaciones que proporciona almacenamiento seguro, tal como un 5G-USIM y / o UICC 8a.

Los circuitos 12 de comunicación pueden ser un concentrador de controladores configurado para controlar las rutas de datos de entrada y salida (I/O) del hardware. Tales rutas de datos de I/O pueden incluir rutas de datos para intercambiar señales a través de una red 30 de comunicación inalámbrica. Por ejemplo, los circuitos de comunicación pueden comprender un transceptor configurado para enviar y recibir señales de comunicación dentro y/o entre el UE 1, la red 2 de servicio y/o la red 3 doméstica, por ejemplo, a través de un medio aéreo, eléctrico y/u óptico.

Los circuitos 12 de comunicación pueden implementarse como un componente físico unitario, o como una pluralidad de componentes físicos que están dispuestos de manera contigua o por separado, cualquiera de los cuales puede estar acoplado comunicativamente a cualquier otro, o puede comunicarse con cualquier otro a través de los circuitos 11 de procesamiento. Por ejemplo, los circuitos de comunicación pueden comprender los circuitos del transmisor configurados para enviar señales de comunicación y los circuitos del receptor configurados para recibir señales de comunicación (no mostradas).

Según realizaciones concretas, el hardware ilustrado en la Figura 16 puede configurarse con una pluralidad de

componentes. Estos componentes pueden incluir una pluralidad de unidades de hardware y/o módulos de software acoplados comunicativamente. Una o más de las unidades de hardware pueden ser, por ejemplo, parte de los circuitos 11 de procesamiento. Una o más de las unidades de software pueden estar, por ejemplo, almacenadas en los circuitos 13 de memoria y ser ejecutadas por los circuitos de procesamiento. Por ejemplo, el hardware como el ilustrado en la Figura 16 se puede usar para implementar un servidor 14 de autenticación (por ejemplo, una AMF, SEAF 4, AUSF 5) en una red 3 doméstica de un UE 1 y se puede configurar con los componentes de ejemplo ilustrados en la Figura 17 para obtener un identificador de suscripción, como un SUPI, de un UE. Los componentes de la Figura 17 incluyen una unidad o módulo 15 de determinación y una unidad o módulo 16 de interfaz. La unidad o módulo de determinación está configurada para determinar un servidor 19 de eliminación de desocultación que se usará para descifrar la parte cifrada del SUCI, y con base en la información recibida desde el UE, cuál de una pluralidad de servidores de desocultación usar para descifrar al menos parte de un identificador oculto de suscripción (SUCI) en el que el identificador de suscripción está cifrado. La unidad o módulo de interfaz está configurada para enviar el SUCI al servidor de desocultación determinado y recibir el identificador de suscripción, por ejemplo el SUPI, en respuesta. En otras palabras, el módulo de interfaz está configurado para recibir también el SUCI generado por el UE, donde el SUCI comprende una parte cifrada en la que al menos una parte del SUPI está cifrada, y una parte de texto sin cifrar que comprende un identificador de red doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado usado por el UE para cifrar el SUPI en el SUCI.

Dicho servidor 14 de autenticación puede configurarse de manera adicional o alternativa con los componentes de ejemplo ilustrados en la Figura 18 para provisionar un UE 1. Los componentes de la Figura 18 incluyen una unidad o módulo 17 de obtención, y una unidad o módulo 18 de transmisión. La unidad o módulo de obtención está configurada para obtener un código de autenticación de mensajes (MAC) basado en una clave de aprovisionamiento específica del UE 1 y una clave de privacidad de una red 3 doméstica del UE. La unidad o módulo transmisor está configurado para transmitir la clave de privacidad y el MAC al UE.

Dicho servidor 14 de autenticación puede configurarse además para realizar de manera adicional o alternativa cualquiera de los métodos descritos en la presente memoria con respecto a un servidor de autenticación, por ejemplo, usando cualquiera de los componentes de hardware o software del servidor de autenticación descritos anteriormente. Se puede usar otro hardware consistente con el ejemplo ilustrado en la Figura 16, para implementar un servidor 19 de desocultación (por ejemplo, la SIDF 6) para proporcionar un identificador de suscripción de un UE 1 a un servidor 14 de autenticación, y se puede configurar con los componentes de ejemplo ilustrados en la Figura 19. Los componentes de la Figura 19 incluyen una unidad o módulo 20 de recepción, una unidad o módulo 21 de descifrado, y una unidad o módulo 22 de envío. La unidad o módulo de recepción está configurada para recibir, desde el servidor de autenticación, un SUCI que comprende una parte cifrada en la que al menos una parte del SUPI está cifrada, y una parte de texto sin cifrar que comprende un identificador de red doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado usado por un UE para cifrar el SUPI en el SUC y que es compatible con el servidor de desocultación. La unidad o módulo de descifrado está configurada para descifrar al menos parte del SUCI, usando el esquema de cifrado indicado por el identificador del esquema de cifrado para obtener el SUPI. La unidad o módulo emisor está configurada para enviar el SUPI al servidor de autenticación.

Dicho servidor 19 de desocultación puede configurarse de manera adicional o alternativa con los componentes de ejemplo ilustrados en la Figura 20 para suministrar un UE 1. Los componentes de la Figura 20 incluyen una unidad o módulo 23 de generación, y una unidad o módulo 24 de transmisión. La unidad o módulo de generación está configurada para generar un Identificador Permanente de Suscripción (SUPI) y una clave de privacidad para el UE en respuesta a la recepción, desde un servidor 14 de autenticación, un Identificador Oculto de Suscripción (SUCI) del UE que indica que el UE carece de una clave de privacidad válida. La unidad o módulo transmisor está configurada para el reenvío del SUPI y la clave de privacidad al servidor de autenticación. Por lo tanto, el término "servidor de desocultación" también puede denominarse servidor de desocultación de SUCI.

Dicho servidor 19 de desocultación puede configurarse además para realizar de manera adicional o alternativa cualquiera de los métodos descritos en la presente memoria con respecto a un servidor de desocultación, por ejemplo, usando cualquiera de los componentes de hardware o software del servidor de desocultación descritos anteriormente.

Aún otro hardware consistente con el ejemplo ilustrado en la Figura 16, puede usarse para implementar un UE 1 para notificar de forma segura a una red 30 de comunicación inalámbrica de un identificador de suscripción, y puede configurarse con los componentes de ejemplo ilustrados en la Figura 21. Los componentes de la Figura 21 incluyen una unidad o módulo 25 de generación, y una unidad o módulo 26 de transmisión. La unidad o módulo de generación está configurada para generar un SUCI que comprende una parte cifrada en la que al menos una parte de un SUPI está cifrada, y una parte de texto sin cifrar que comprende un identificador de red doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado usado por el UE para cifrar el SUPI en el SUCI. La unidad o módulo de transmisión está configurada para transmitir el SUCI a un servidor 14 de autenticación para reenviar el SUCI a un servidor 19 de desocultación capaz de descifrar el SUPI.

Tal UE 1 puede configurarse de manera adicional o alternativa con los componentes de ejemplo ilustrados en la Figura 22 para obtener una clave de privacidad. Los componentes de la Figura 22 incluyen una unidad o módulo 27 de recepción y una unidad o módulo 28 de verificación. La unidad o módulo de recepción está configurada para recibir la clave de privacidad y un código de autenticación de mensajes (MAC) desde un servidor 14 de autenticación. La unidad

o módulo de verificación está configurada para verificar la integridad de la clave de privacidad generando una clave de aprovisionamiento y usando la clave de aprovisionamiento y la clave de privacidad para reproducir el MAC recibido desde el servidor de autenticación, siendo la clave de aprovisionamiento un secreto compartido entre el UE y el servidor de autenticación.

Dicho UE 1 puede configurarse además para realizar de manera adicional o alternativa cualquiera de los métodos descritos en la presente memoria con respecto a un UE, por ejemplo, usando cualquiera de los componentes de hardware o software de UE descritos anteriormente.

REIVINDICACIONES

1. Un método realizado por un servidor (14) de autenticación en una red (3) doméstica de un equipo de usuario (1), UE, para obtener un identificador permanente de suscripción, SUPI, que comprende un número de identificación de abonado móvil, un código de país móvil y un código de red móvil, comprendiendo el método:

recibir desde el UE (1), a través de una solicitud de autenticación de una función de anclaje de seguridad, un identificador oculto de suscripción, SUCI, que comprende:

una parte cifrada en la que el número de identificación de abonado móvil está cifrada, y

una parte de texto sin cifrar que comprende un identificador de red doméstica para la red (3) doméstica, un identificador de clave pública para una clave pública de la red (3) doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado utilizado por el UE (1) para cifrar el número de identificación de abonado móvil en el SUCI, y en el que el identificador de red doméstica es el código de país móvil y el código de red móvil,

determinar un servidor (19) de desocultación que se utiliza para descifrar la parte cifrada del SUCI;

enviar el SUCI al servidor (19) de desocultación, y

recibir el SUPI en respuesta.

2. El método según la reivindicación 1, en el que el esquema de cifrado es un esquema de cifrado nulo.

3. El método de una cualquiera de las reivindicaciones 1-2, que comprende además recibir el SUCI del UE (1) como parte de un procedimiento de registro para registrar el UE (1) con una red (30) de comunicación inalámbrica.

4. El método de una cualquiera de las reivindicaciones anteriores, que comprende además enviar el SUCI y una solicitud de un vector de autenticación para autenticar el UE (1) al servidor (19) de desocultación determinado en el mismo mensaje.

5. El método de la reivindicación 4, que comprende además recibir el vector de autenticación y el SUPI desde el servidor (19) de desocultación determinado en la misma respuesta.

6. El método según una cualquiera de las reivindicaciones 1, 3-5, en el que el esquema de cifrado es un Esquema de Cifrado Integrado de Curva Elíptica, ECIES.

7. Un método realizado por un equipo de usuario (1), UE, comprendiendo el método:

generar un identificador oculto de suscripción, SUCI, que comprende

una parte cifrada en la que un número de identificación de abonado móvil de un identificador permanente de suscripción, SUPI, está cifrado, y

una parte de texto sin cifrar que comprende un identificador de red doméstica para una red (3) doméstica del UE (1), un identificador de clave pública para la red (3) doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado utilizado por el UE (1) para cifrar el número de identificación de abonado móvil en el SUCI, y donde el identificador de red doméstica es un código de país móvil del SUPI y un código de red móvil del SUPI;

transmitir el SUCI, a través de una solicitud de autenticación de una función de anclaje de seguridad a un servidor (14) de autenticación en la red doméstica para reenviar el SUCI a un servidor (19) de desocultación capaz de descifrar el NAI a partir del SUCI.

8. El método de la reivindicación 7, en el que el SUCI se transmite en una solicitud de registro en una red (30) de comunicación inalámbrica.

9. El método de una cualquiera de las reivindicaciones 7-8, en el que generar el SUCI comprende usar un componente (8) de hardware seguro a prueba de manipulaciones del UE (1) para generar el SUCI.

10. El método de la reivindicación 9, en el que generar el SUCI comprende generar el SUCI en base a una clave de privacidad seleccionada entre una pluralidad de claves de seguridad almacenadas en el componente (8) de hardware seguro resistente a la manipulación.

11. El método de una cualquiera de las reivindicaciones 9-10, en el que generar el SUCI comprende enviar un tiempo al componente (8) de hardware seguro resistente a la manipulación para usar en la generación

12. El método de una cualquiera de las reivindicaciones 9-11, en el que generar el SUCI comprende generar el SUCI desde una clave de privacidad que comprende el SUPI.

13. El método de una cualquiera de las reivindicaciones 7-12, en el que transmitir el SUCI al servidor (14) de autenticación comprende transmitir el SUCI al servidor (14) de autenticación en respuesta a un mensaje de solicitud de identificador recibido de una Función de gestión de Movilidad y Autenticación (4), AMF, como parte de un procedimiento para registrar el UE (1) en una red (30) de comunicación inalámbrica.

14. El método de la reivindicación 13, que comprende además transmitir una solicitud de registro al AMF (4), en el que la solicitud de registro comprende un identificador temporal único global 5G, y recibir el mensaje de solicitud de identificador en respuesta.

15. El método de una cualquiera de las reivindicaciones 13-14, que comprende además autenticar con éxito con el servidor (14) de autenticación después de transmitir el SUCI, y recibir un mensaje de aceptación de registro en respuesta.

16. El método según una cualquiera de las reivindicaciones 7-15, en el que el esquema de cifrado es un esquema de cifrado nulo.

17. El método según una cualquiera de las reivindicaciones 7-15, en el que el esquema de cifrado es un esquema de Cifrado Integrado de Curva Elíptica.

18. Un servidor (14) de autenticación para una red (3) doméstica de un equipo de usuario (1), UE, para obtener un identificador permanente de suscripción, SUPI, que comprende un número de identificación de abonado móvil, un código de país móvil y un código de red móvil, estando configurado el servidor (14) de autenticación para:

recibir desde el UE (1), a través de una solicitud de autenticación de una función de anclaje de seguridad, un identificador oculto de suscripción, SUCI, que comprende

una parte cifrada en la que el número de identificación de abonado móvil del SUPI está cifrada, y

una parte de texto sin cifrar que comprende un identificador de red doméstica para la red (3) doméstica, un identificador de clave pública para la red (3) doméstica y un identificador de esquema de cifrado que identifica un esquema de cifrado utilizado por el UE (1) para cifrar el número de identificación de abonado móvil en el SUCI, y donde el identificador de red doméstica es el código de país móvil y el código de red móvil,

determinar un servidor (19) de desocultación que se utiliza para descifrar la parte cifrada del SUCI;

enviar el SUCI al servidor (19) de desocultación, y

recibir el SUPI en respuesta.

19. Un equipo de usuario (1), UE, configurado para:

generar un identificador oculto de suscripción, SUCI, que comprende una parte cifrada en la que un número de identificación de abonado móvil de un identificador permanente de suscripción, SUPI, está cifrada, y una parte de texto sin cifrar que comprende un identificador de red doméstica de una red (3) doméstica del UE (1), un identificador de clave pública para una clave pública de la red (3) doméstica, y un identificador de esquema de cifrado que identifica un esquema de cifrado utilizado por el UE (1) para cifrar el SUPI en el SUCI; y en el que el identificador de red doméstica es un código de país móvil del SUPI y un código de red móvil del SUPI; y

transmitir el SUCI, a través de una solicitud de autenticación de una función de anclaje de seguridad, a un servidor (14) de autenticación en la red doméstica para reenviar el SUCI a un servidor (19) de desocultación capaz de descifrar el SUPI.

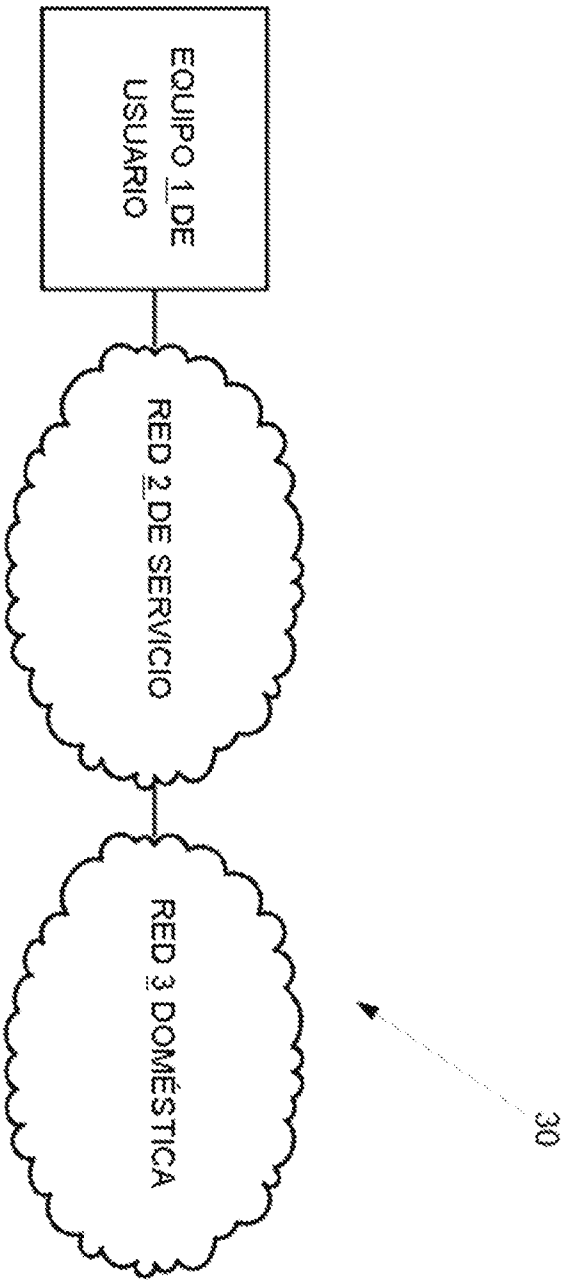


FIG. 1

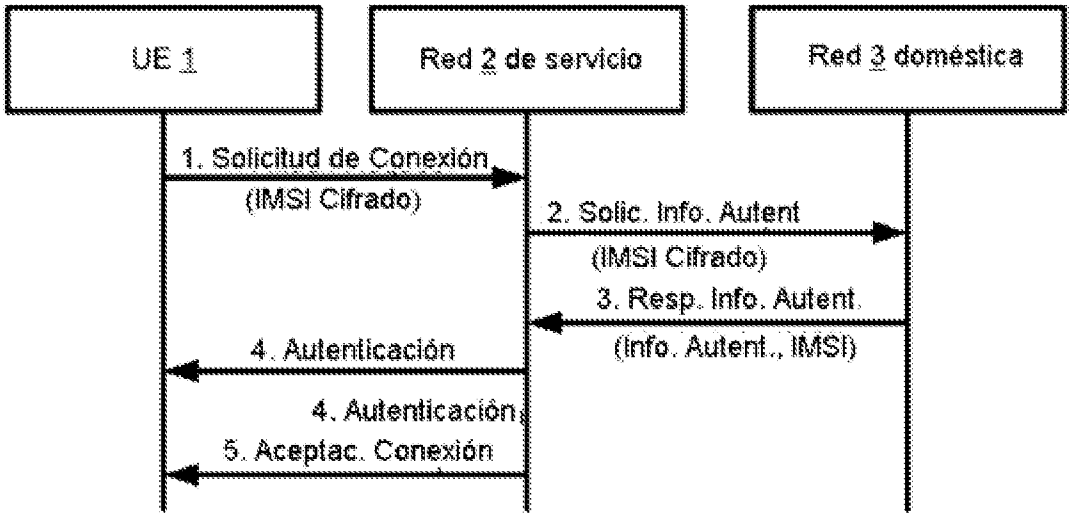

UE 1
Red 2 de servicio
Red 3 doméstica
1. Solicitud de Conexión
(IMSI Cifrado)
2. Solic. Info. Autent
(IMSI Cifrado)
3. Resp. Info. Autent.
(Info. Autent., IMSI)
4. Autenticación
4. Autenticación
5. Aceptac. Conexión

Fig. 2

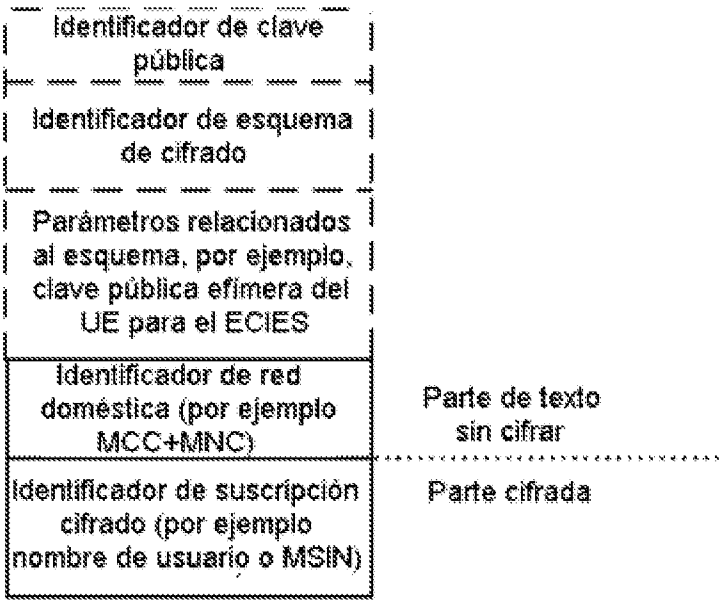

Identificador de clave pública
Identificador de esquema de cifrado
Parámetros relacionados al esquema, por ejemplo, clave pública efímera del UE para el ECIES
Identificador de red doméstica (por ejemplo MCC+MNC)
Identificador de suscripción cifrado (por ejemplo nombre de usuario o MSIN)
Parte de texto sin cifrar
Parte cifrada

Fig. 3


[Identificador de suscripción (por ejemplo, nombre de usuario o MSIN)
Asunto (por ejemplo mCC/MNC o identificador de SIDF
Identificador de esquema: por ejemplo 0 (esquema nulo, 1 (ECIES), etc
Valores específicos de dominio relacionados con el esquema de clave pública
Clave pública
ID de clave pública
Validez (no antes)
Validez (no después)
Uso de clave (privacidad de suscripción)
[Firma Digital]

Fig. 4

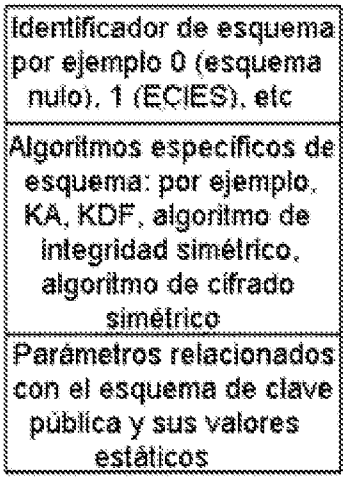
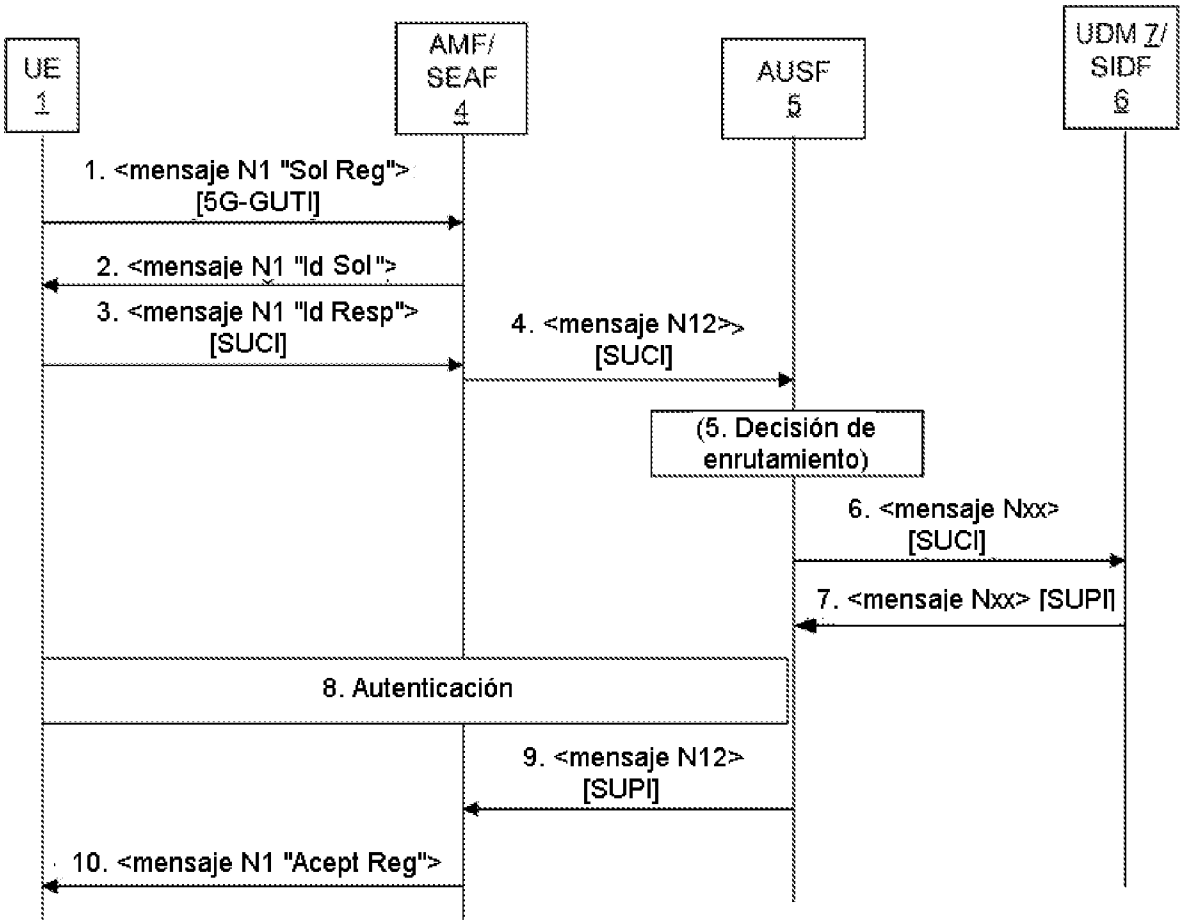

Identificador de esquema por ejemplo 0 (esquema nulo), 1 (ECIES), etc
Algoritmos específicos de esquema: por ejemplo, KA, KDF, algoritmo de integridad simétrico, algoritmo de cifrado simétrico
Parámetros relacionados con el esquema de clave pública y sus valores estáticos

Fig. 5


UE
1
AMF/
SEAF
4
AUSF
5
UDM 7/
SIDF
6
1. <mensaje N1 "Sol Reg">
[5G-GUTI]
2. <mensaje N1 "Id Sol">
3. <mensaje N1 "Id Resp">
[SUCI]
4. <mensaje N12>>
[SUCI]
(5. Decisión de
enrutamiento)
6. <mensaje Nxx>
[SUCI]
7. <mensaje Nxx> [SUPI]
8. Autenticación
9. <mensaje N12>
[SUPI]
10. <mensaje N1 "Acept Reg">
Fig. 6

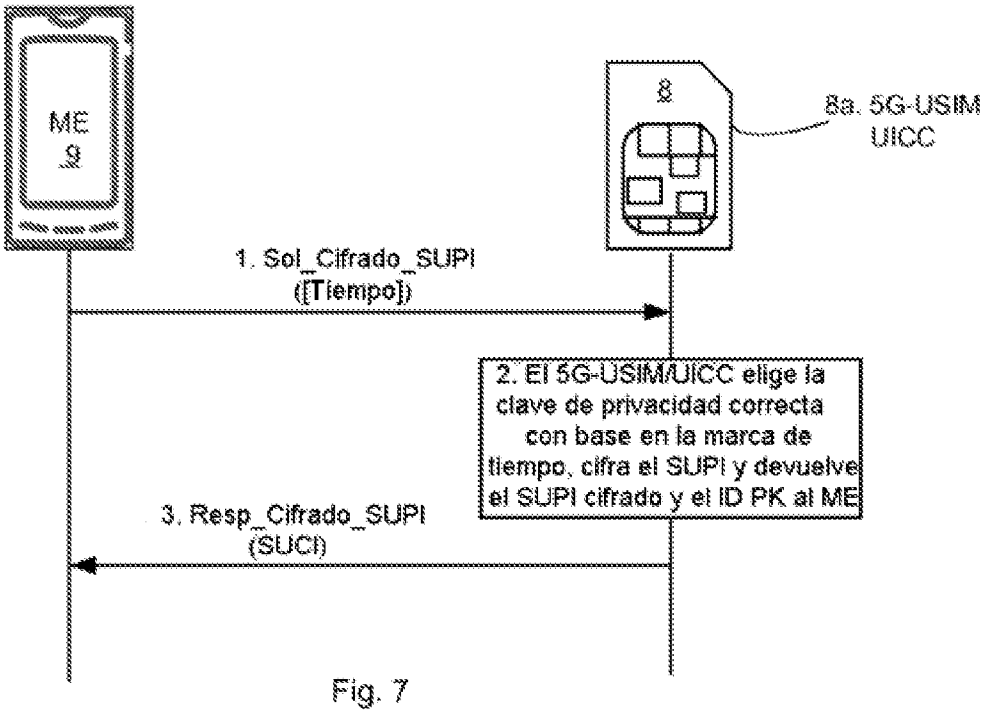

ME
9
8
8a. 5G-USIM
UICC
1. Sol_Cifrado_SUPI
([Tiempo])
2. El 5G-USIM/UICC elige la clave de privacidad correcta con base en la marca de tiempo, cifra el SUPI y devuelve el SUPI cifrado y el ID PK al ME
3. Resp_Cifrado_SUPI
(SUCI)

Fig. 7

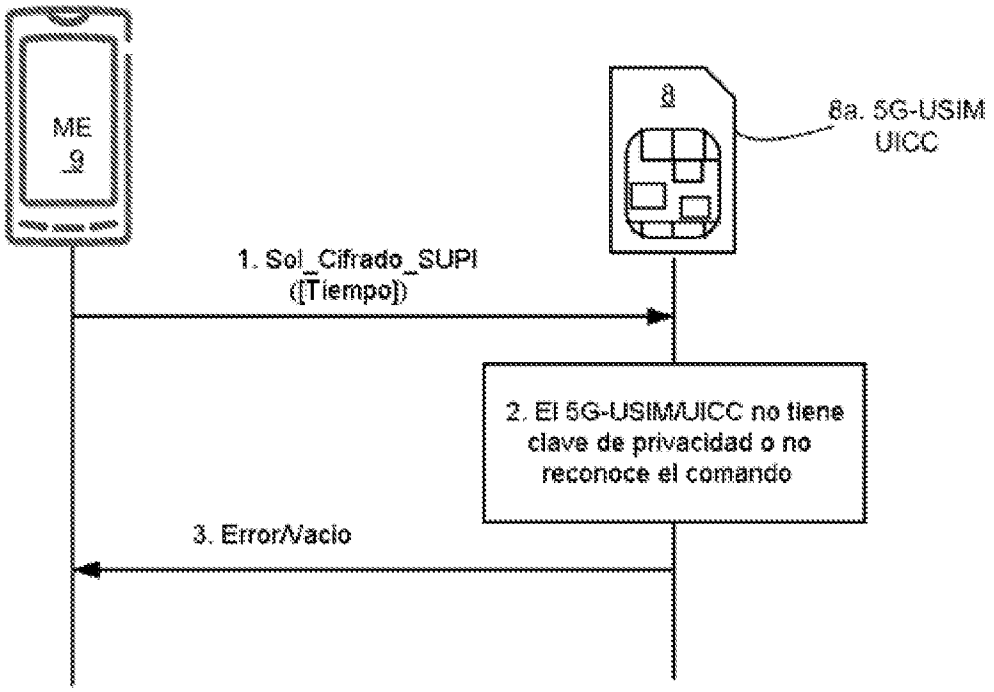

ME
9
8
8a. 5G-USIM
UICC
1. Sol_Cifrado_SUPI
([Tiempo])
2. El 5G-USIM/UICC no tiene clave de privacidad o no reconoce el comando
3. Error/Vacio

Fig. 8

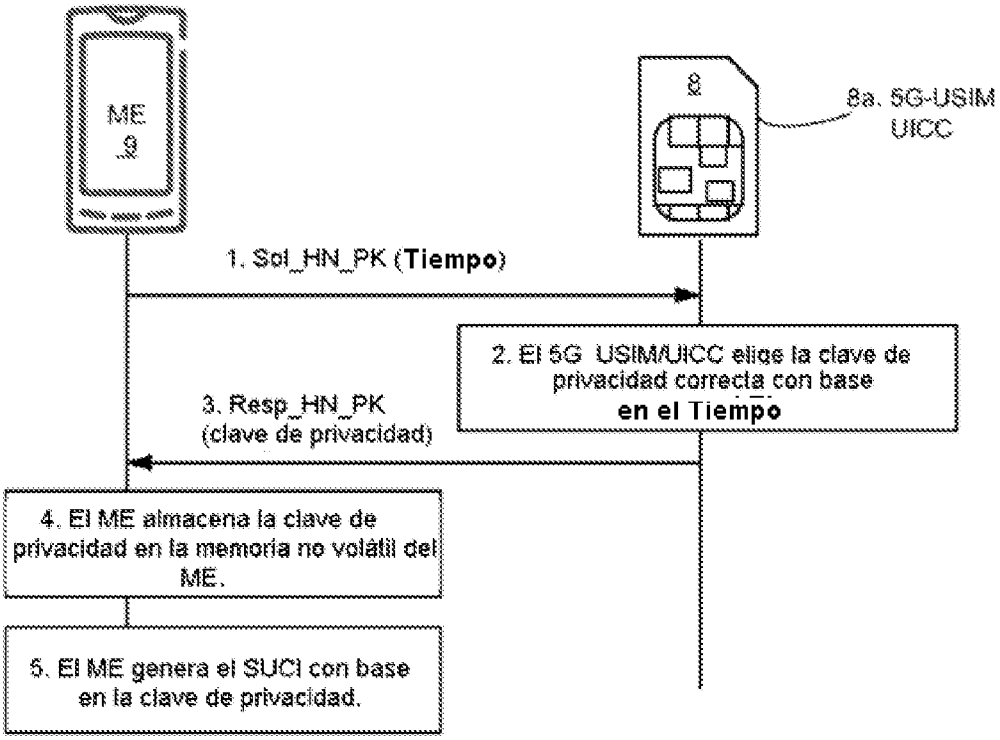

ME
9
8
8a. 5G-USIM
UICC
1. Sol_HN_PK (Tiempo)
2. El 5G USIM/UICC elige la clave de privacidad correcta con base en el Tiempo
3. Resp_HN_PK
(clave de privacidad)
4. El ME almacena la clave de privacidad en la memoria no volátil del ME.
5. El ME genera el SUCI con base en la clave de privacidad.

Fig. 9

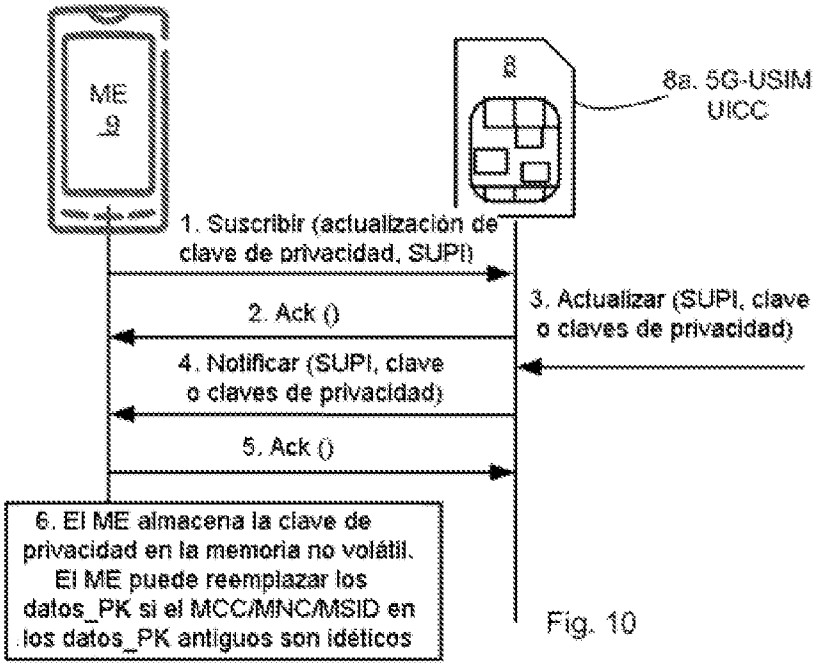

ME
9
8
8a. 5G-USIM
UICC
1. Suscribir (actualización de clave de privacidad, SUPI)
2. Ack ()
3. Actualizar (SUPI, clave o claves de privacidad)
4. Notificar (SUPI, clave o claves de privacidad)
5. Ack ()
6. El ME almacena la clave de privacidad en la memoria no volátil. El ME puede reemplazar los datos_PK si el MCC/MNC/MSID en los datos_PK antiguos son idéticos

Fig. 10

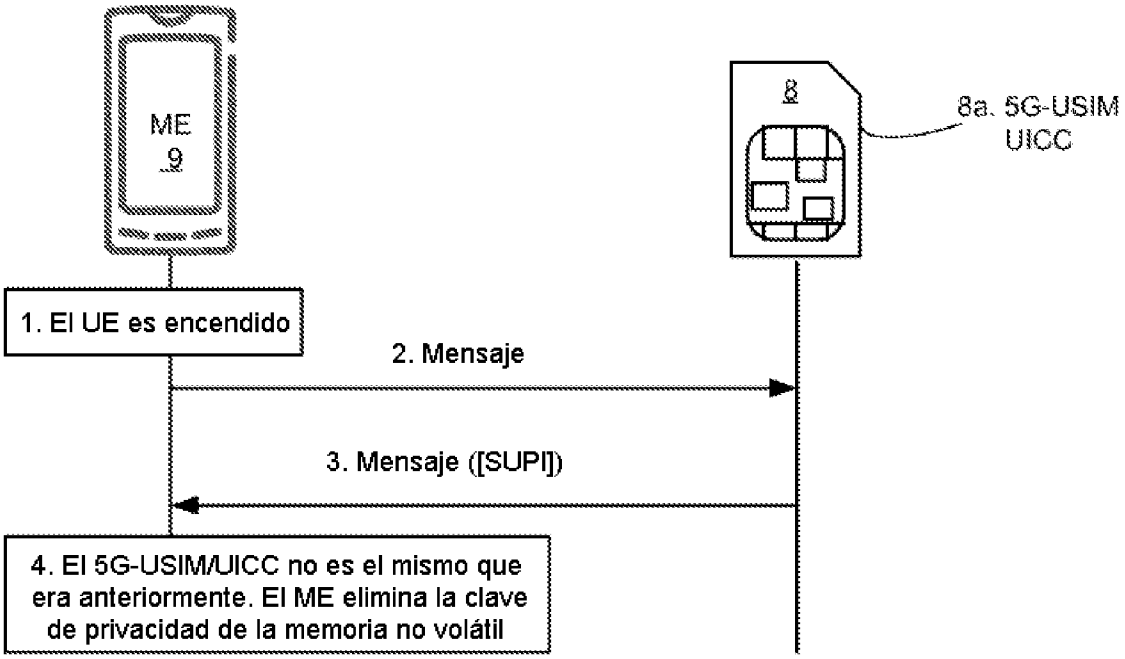

ME
9
8
8a. 5G-USIM
UICC
1. El UE es encendido
2. Mensaje
3. Mensaje ([SUPI])
4. El 5G-USIM/UICC no es el mismo que era anteriormente. El ME elimina la clave de privacidad de la memoria no volátil

Fig. 11

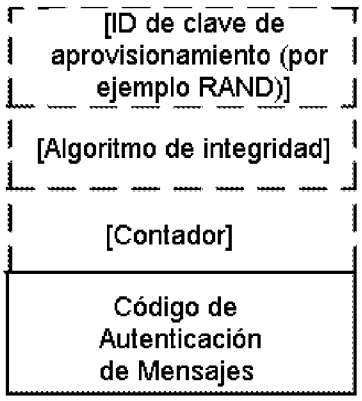

[ID de clave de aprovisionamiento (por ejemplo RAND)]
[Algoritmo de integridad]
[Contador]
Código de Autenticación de Mensajes

Fig. 12

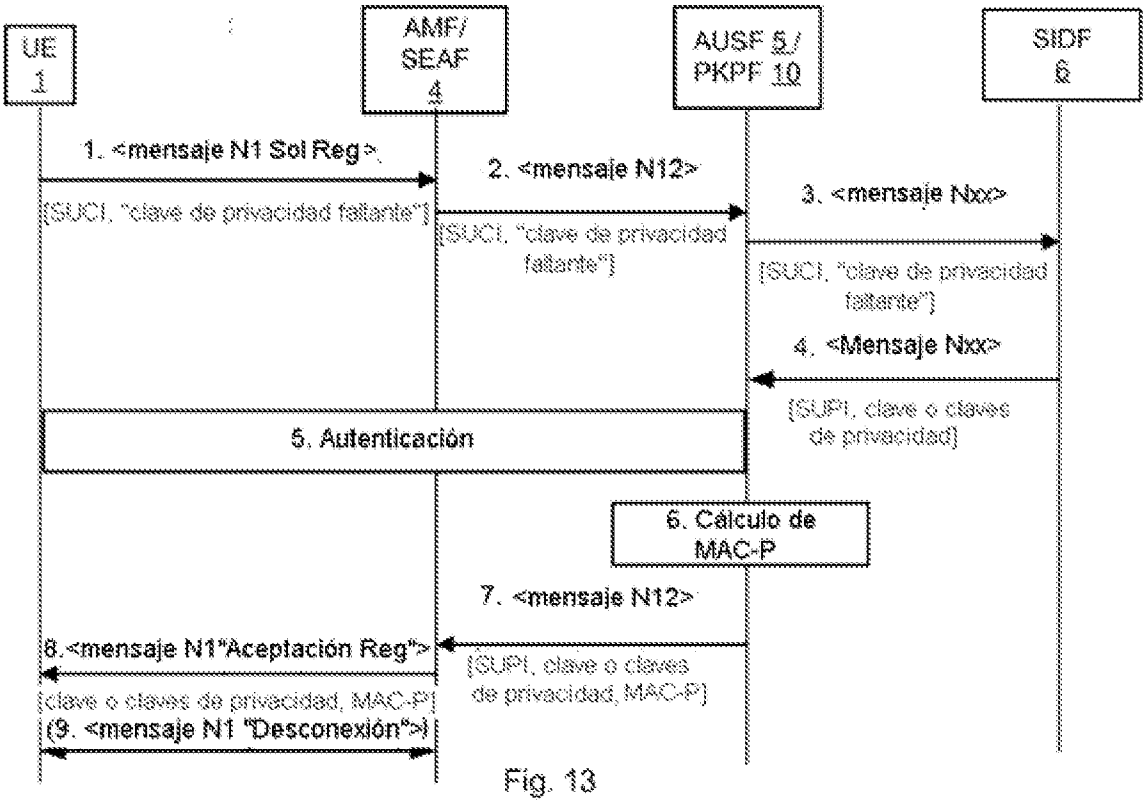

UE 1
AMF/ SEAF 4
AUSF 5/ PKPF 10
SIDF 6
1. <mensaje N1 Sol Reg>
[SUCI, "clave de privacidad faltante"]
2. <mensaje N12>
[SUCI, "clave de privacidad faltante"]
3. <mensaje Nxx>
[SUCI, "clave de privacidad faltante"]
4. <Mensaje Nxx>
[SUPI, clave o claves de privacidad]
5. Autenticación
6. Cálculo de MAC-P
7. <mensaje N12>
[SUPI, clave o claves de privacidad, MAC-P]
8.<mensaje N1"Aceptación Reg">
[clave o claves de privacidad, MAC-P]
(9. <mensaje N1 "Desconexión">)

Fig. 13

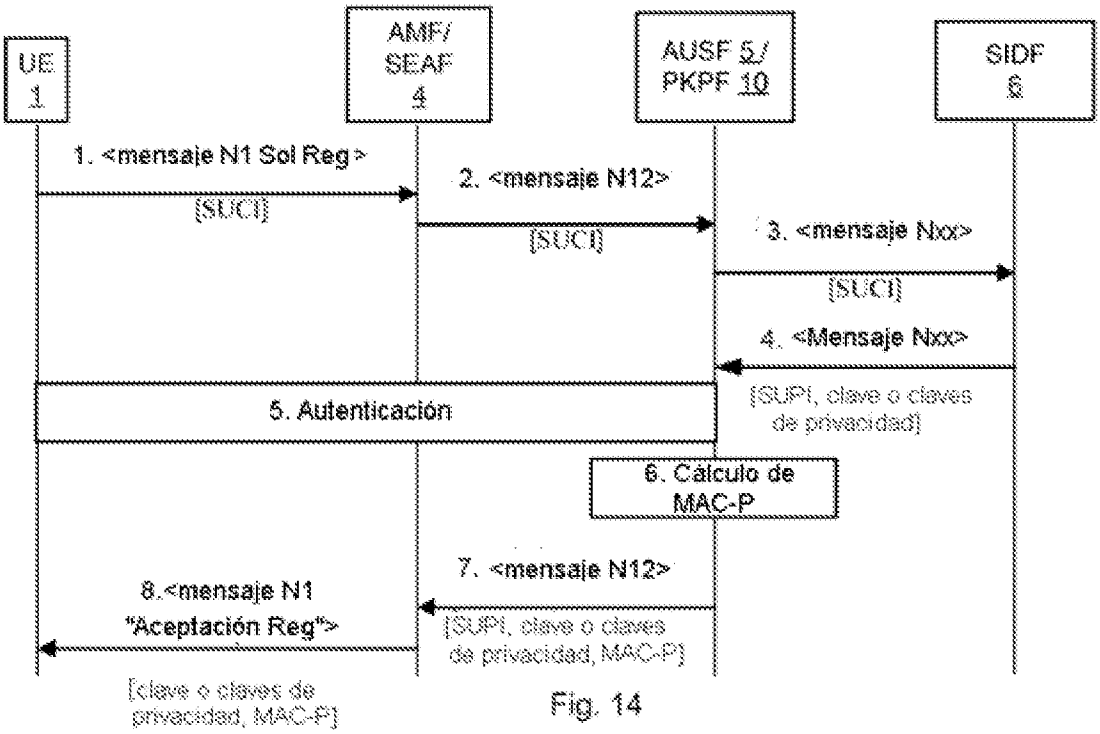

UE 1
AMF/ SEAF 4
AUSF 5/ PKPF 10
SIDF 6
1. <mensaje N1 Sol Reg>
[SUCI]
2. <mensaje N12>
[SUCI]
3. <mensaje Nxx>
[SUCI]
4. <Mensaje Nxx>
[SUPI, clave o claves de privacidad]
5. Autenticación
6. Cálculo de MAC-P
7. <mensaje N12>
[SUPI, clave o claves de privacidad, MAC-P]
8.<mensaje N1 "Aceptación Reg">
[clave o claves de privacidad, MAC-P]

Fig. 14

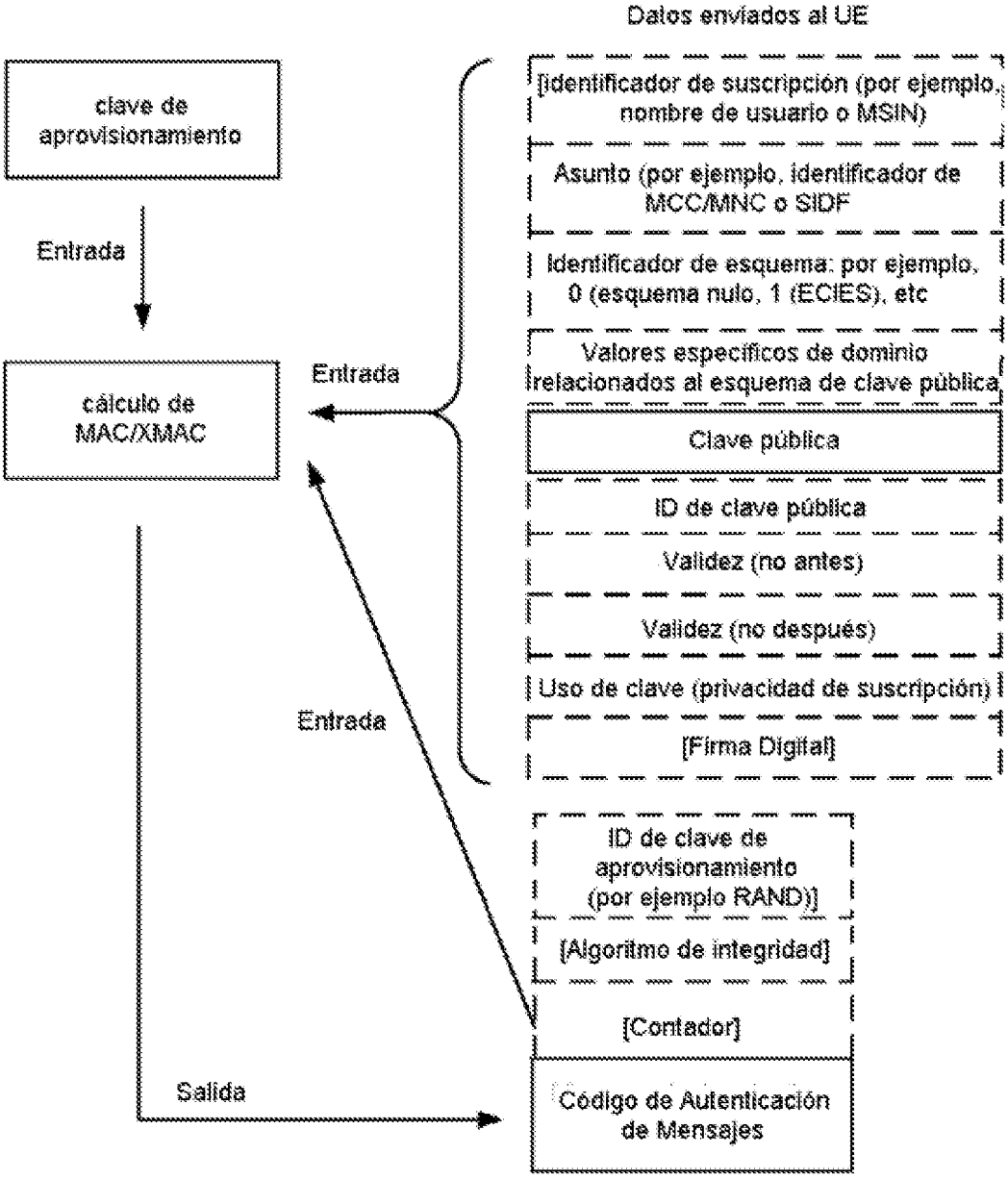

Datos enviados al UE
clave de aprovisionamiento
Entrada
cálculo de MAC/XMAC
Entrada
Entrada
Salida
[identificador de suscripción (por ejemplo, nombre de usuario o MSIN)
Asunto (por ejemplo, identificador de MCC/MNC o SIDF
Identificador de esquema: por ejemplo, 0 (esquema nulo, 1 (ECIES), etc
Valores específicos de dominio relacionados al esquema de clave pública
Clave pública
ID de clave pública
Validez (no antes)
Validez (no después)
Uso de clave (privacidad de suscripción)
[Firma Digital]
ID de clave de aprovisionamiento (por ejemplo RAND)]
[Algoritmo de integridad]
[Contador]
Código de Autenticación de Mensajes

Fig. 15

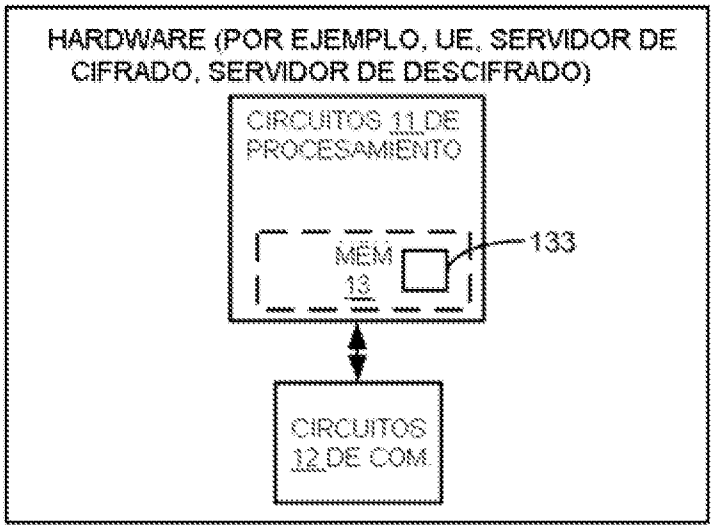


Fig. 16

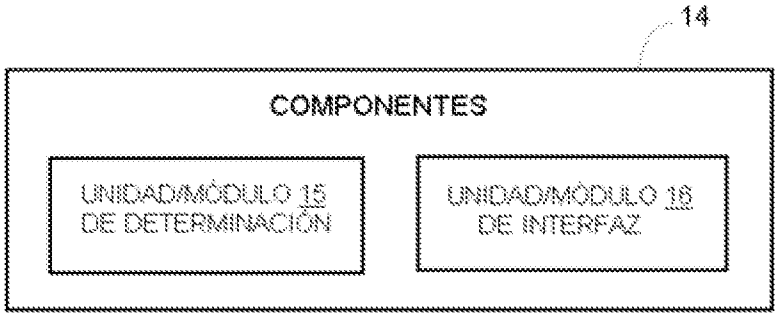


Fig. 17

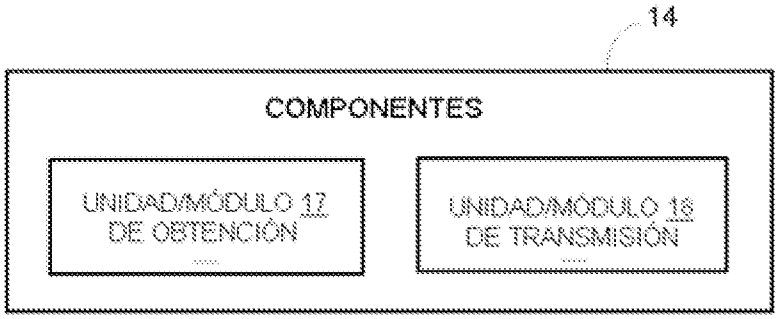


Fig. 18

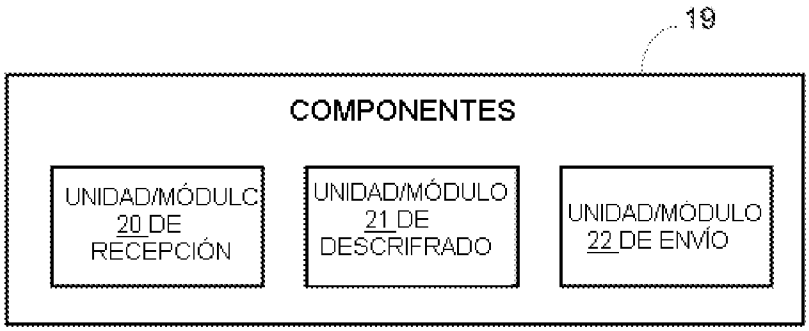


Fig. 19

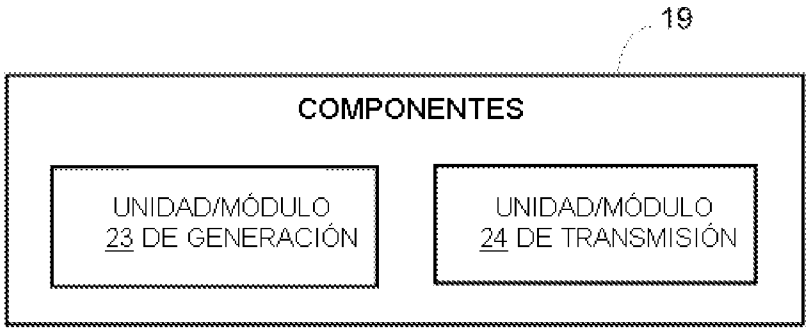


Fig. 20

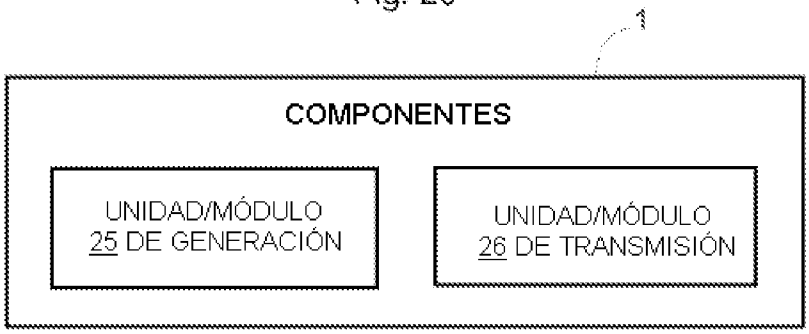


Fig. 21

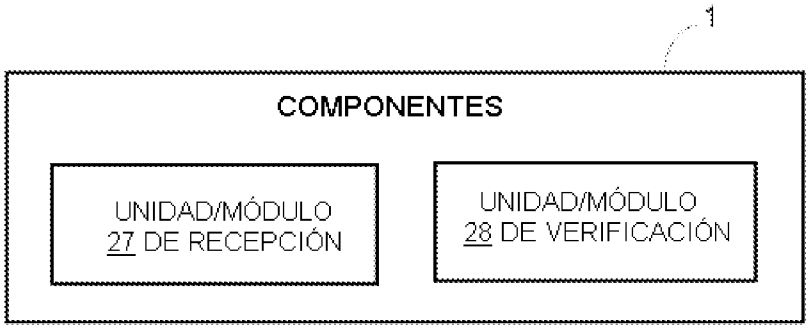


Fig. 22