

**AUTENTICACIÓN DE UN DISPOSITIVO DE COMUNICACIÓN INALÁMBRICA CON UN
SERVIDOR DE AUTENTICACIÓN EXTERNA**

CAMPO TÉCNICO

5 La presente solicitud se refiere en general a una red de comunicación inalámbrica, y se refiere más particularmente a la autenticación de un dispositivo de comunicación inalámbrica con un servidor de autenticación externa a la red de comunicación inalámbrica.

ANTECEDENTES

10 Una red de comunicación inalámbrica realiza un procedimiento para autenticar y autorizar un dispositivo de comunicación inalámbrica como requisito previo para proporcionar un servidor de comunicación inalámbrica a ese dispositivo. En algunos casos, como cuando la red de comunicación inalámbrica es una red no pública independiente (SNPN), la red de comunicación inalámbrica puede soportar la autenticación y autorización de un dispositivo de comunicación inalámbrica basándose en credenciales de un servidor de autorización externo que es externo a
15 la red de comunicación inalámbrica, es decir, en un Titular de Credenciales (CH). Dicha autenticación y autorización puede denominarse autenticación y autorización primarias, es decir, no son secundarias como puede ser el caso de la autenticación y autorización específicas de segmentos de red.

20 Sin embargo, existen desafíos a la hora de explotar la autenticación y autorización externas y al mismo tiempo preservar la privacidad del identificador. Por ejemplo, existen desafíos al explotar la autenticación externa cuando un dispositivo de comunicación inalámbrica activa la autenticación primaria utilizando un identificador anónimo para preservar la privacidad.

RESUMEN

25 Algunas realizaciones en el presente documento facilitan la autenticación de un dispositivo de comunicación inalámbrica con un servidor de autenticación externa que es externo a una red de comunicación inalámbrica. Según algunas realizaciones, el servidor de autenticación externa envía, a la red de comunicación inalámbrica, un identificador afirmado por el servidor de autenticación externa que identifica como auténtico el dispositivo de comunicación inalámbrica, por ejemplo, un identificador que es, o está asociado con, el identificador autenticado por el
30 servidor de autenticación externa. La red de comunicación inalámbrica puede entonces autenticar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en ese identificador afirmado. De esta manera, incluso si el dispositivo de comunicación inalámbrica activa la autenticación usando un identificador anónimo, la red de comunicación inalámbrica aún puede conocer un identificador no-anónimo para el dispositivo de
35 comunicación inalámbrica después de la autenticación. De este modo, algunas realizaciones

facilitan ventajosamente la autenticación externa y al mismo tiempo preservan la privacidad del identificador.

Más particularmente, las realizaciones del presente documento incluyen un método realizado por un servidor de autenticación en una red de comunicación inalámbrica. El método comprende iniciar la autenticación primaria de un dispositivo de comunicación inalámbrica con un servidor de autenticación externa que es externo a la red de comunicación inalámbrica. El método también comprende recibir señalización que indica que la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa fue exitosa y que incluye un identificador afirmado por el servidor de autenticación externa que identifica como auténtico el dispositivo de comunicación inalámbrica. En algunas realizaciones, el método comprende además autenticar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en el identificador incluido en la señalización recibida.

En algunas realizaciones, iniciar la autenticación primaria comprende iniciar la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa usando un identificador anónimo que no identifica el dispositivo de comunicación inalámbrica. En una de dichas realizaciones, el identificador incluido en la señalización recibida es un identificador no-anónimo. Por ejemplo, en algunas realizaciones, el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo y el identificador no-anónimo es un SUPI no-anónimo.

Alternativa o adicionalmente, iniciar la autenticación primaria puede comprender iniciar la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa usando un identificador presentado que el dispositivo de comunicación inalámbrica ha presentado como identificación del dispositivo de comunicación inalámbrica a la red de comunicación inalámbrica. En este caso, autenticar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en el identificador incluido en la señalización recibida puede comprender confirmar que el identificador presentado corresponde al identificador incluido en la señalización recibida. En una realización, dicha confirmación comprende transmitir el identificador presentado a un equipo de red que implementa una función de Gestión Unificada de Datos, UDM, y realizar dicha confirmación basándose en una respuesta recibida del equipo de red que implementa la función de UDM.

En algunas realizaciones, la autenticación primaria se inicia como parte de un procedimiento para registrar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica. En una de dichas realizaciones, el método comprende además registrar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en la autenticación exitosa del dispositivo de comunicación inalámbrica con la red de

comunicación inalámbrica.

En algunas realizaciones, la red de comunicación inalámbrica es una red no pública independiente.

Las realizaciones en el presente documento también incluyen un método realizado en un
5 servidor de autenticación externa para una red de comunicación inalámbrica. El método comprende realizar una autenticación primaria de un dispositivo de comunicación inalámbrica con el servidor de autenticación externa para que el dispositivo de comunicación inalámbrica acceda a la red de comunicación inalámbrica. El método comprende además transmitir, a un
10 servidor de autenticación en la red de comunicación inalámbrica, una señalización que indica que la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa tuvo éxito y que incluye un identificador afirmado por el servidor de autenticación externa que identifica como auténtico el dispositivo de comunicación inalámbrica.

En algunas realizaciones, el método comprende además recibir señalización que activa el
servidor de autenticación externa para realizar la autenticación primaria del dispositivo de
15 comunicación inalámbrica con el servidor de autenticación externa. En una de dichas realizaciones, la señalización incluye un identificador anónimo para el dispositivo de comunicación inalámbrica. En algunas realizaciones, por ejemplo, el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

En algunas realizaciones, el identificador incluido en la señalización transmitida es un
20 identificador no-anónimo. En una de dichas realizaciones, el identificador no-anónimo es un SUPI no-anónimo.

En algunas realizaciones, la red de comunicación inalámbrica es una red no pública independiente.

Las realizaciones en el presente documento incluyen además un método realizado por un
25 nodo de red en una red de comunicación inalámbrica. El método comprende recibir, desde un servidor de autenticación en la red de comunicación inalámbrica, una solicitud de autenticación primaria de un dispositivo de comunicación inalámbrica con un servidor de autenticación externa para el acceso del dispositivo de comunicación inalámbrica a la red de comunicación inalámbrica. El método comprende además transmitir, al servidor de autenticación en la red de comunicación
30 inalámbrica, una respuesta que indica que la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa tuvo éxito y que incluye un identificador afirmado por el servidor de autenticación externa que identifica como auténtico al dispositivo de comunicación inalámbrica.

En algunas realizaciones, la solicitud incluye un identificador anónimo para el dispositivo
35 de comunicación inalámbrica, y el identificador incluido en la señalización transmitida es un

identificador no-anónimo. En una realización, por ejemplo, el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo y el identificador no-anónimo es un SUPI no-anónimo.

5 En algunas realizaciones, la red de comunicación inalámbrica es una red no pública independiente.

En algunas realizaciones, el servidor de autenticación implementa una función de servidor de autenticación, AUSF, y/o el nodo de red implementa una Función de Autorización y Autenticación Específica del Segmento de Red, NSSAAF.

10 Las realizaciones en el presente documento también incluyen un método realizado por un nodo de red en una red de comunicación inalámbrica. El método comprende recibir, desde un servidor de autenticación en la red de comunicación inalámbrica, una solicitud de datos de autenticación para un dispositivo de comunicación inalámbrica. El método comprende además transmitir, al servidor de autenticación, una respuesta que indica que la autenticación primaria del dispositivo de comunicación inalámbrica se va a ejecutar con un servidor de autenticación
15 externa que es externo a la red de comunicación inalámbrica y que incluye un identificador que se va a presentar al servidor de autenticación externa.

En algunas realizaciones, la solicitud incluye un identificador anónimo para el dispositivo de comunicación inalámbrica, y el identificador incluido en la respuesta es el identificador anónimo del dispositivo de comunicación inalámbrica. En una realización, por ejemplo, el
20 identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

En algunas realizaciones, el método comprende además decidir, basándose en una parte del dominio del identificador anónimo, que la autenticación primaria del dispositivo de comunicación inalámbrica se ejecutará con el servidor de autenticación externa a la red de comunicación inalámbrica.

25 En algunas realizaciones, la red de comunicación inalámbrica es una red no pública independiente.

Las realizaciones en el presente documento también incluyen los aparatos correspondientes, programas de computador y portadoras de esos programas de computador.

30 Por ejemplo, las realizaciones del presente documento incluyen un servidor de autenticación configurado para su uso en una red de comunicación inalámbrica. El servidor de autenticación que comprende circuitos de comunicación y circuitos de procesamiento. Los circuitos de procesamiento están configurados para iniciar la autenticación primaria de un dispositivo de comunicación inalámbrica con un servidor de autenticación externa que es externo a la red de comunicación inalámbrica, recibir señalización que indica que la autenticación
35 primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa fue

exitosa y que incluye un identificador afirmado por el servidor de autenticación externa que identifica como auténtico el dispositivo de comunicación inalámbrica, y autenticar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en el identificador incluido en la señalización recibida.

5 Las realizaciones del presente documento también incluyen un servidor de autenticación externa para una red de comunicación inalámbrica. El servidor de autenticación externa comprende circuitos de comunicación y circuitos de procesamiento. Los circuitos de procesamiento están configurados para realizar la autenticación primaria de un dispositivo de comunicación inalámbrica con el servidor de autenticación externa para el acceso del dispositivo
10 de comunicación inalámbrica a la red de comunicación inalámbrica, y para transmitir, a un servidor de autenticación en la red de comunicación inalámbrica, señalización que indica que la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa fue exitosa y eso incluye un identificador afirmado por el servidor de autenticación externa que identifica como auténtico el dispositivo de comunicación inalámbrica.

15 Las realizaciones en el presente documento incluyen además un nodo de red configurado para su uso en una red de comunicación inalámbrica. El nodo de red comprende circuitos de comunicación y circuitos de procesamiento. Los circuitos de procesamiento están configurados para recibir, desde un servidor de autenticación en la red de comunicación inalámbrica, una solicitud de autenticación primaria de un dispositivo de comunicación inalámbrica con un servidor
20 de autenticación externa para el acceso del dispositivo de comunicación inalámbrica a la red de comunicación inalámbrica. Los circuitos de procesamiento también están configurados para transmitir, al servidor de autenticación en la red de comunicación inalámbrica, una respuesta que indica que la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa tuvo éxito y que incluye un identificador afirmado por el servidor de
25 autenticación externa que identifica como auténtico el dispositivo de comunicación inalámbrica.

Las realizaciones en el presente documento incluyen además un nodo de red configurado para su uso en una red de comunicación inalámbrica. El nodo de red comprende circuitos de comunicación y circuitos de procesamiento. Los circuitos de procesamiento están configurados para recibir, desde un servidor de autenticación en la red de comunicación inalámbrica, una
30 solicitud de datos de autenticación para un dispositivo de comunicación inalámbrica, y para transmitir, al servidor de autenticación, una respuesta que indica que la autenticación primaria del dispositivo de comunicación inalámbrica debe ejecutarse con un servidor de autenticación externa que es externo a la red de comunicación inalámbrica y que incluye un identificador para ser presentado al servidor de autenticación externa.

35

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 es un diagrama esquemático de bloques de un dispositivo de comunicación inalámbrica 10 según algunas realizaciones.

5 La Figura 2 es un diagrama de bloques de autenticación a través de un Titular de Credenciales en un 5GS según algunas realizaciones.

La Figura 3 es un diagrama de flujo de llamadas de autenticación con un servidor de autenticación externa según algunas realizaciones.

10 La Figura 4 es un diagrama de flujo de llamadas de autenticación con un servidor de autenticación externa según algunas realizaciones, donde un dispositivo de comunicación inalámbrica utiliza un identificador anónimo.

La Figura 5 es un diagrama de flujo de llamadas de autenticación con un servidor de autenticación externa según algunas realizaciones donde un dispositivo de comunicación inalámbrica utiliza un servidor identificador no-anónimo.

15 La Figura 6 es un diagrama de flujo lógico de un método realizado por un servidor de autenticación según algunas realizaciones.

La Figura 7 es un diagrama de flujo lógico de un método realizado por un servidor de autenticación externa según algunas realizaciones.

La Figura 8 es un diagrama de flujo lógico de un método realizado por un nodo de red (por ejemplo, implementando una NSSAAF) según algunas realizaciones.

20 La Figura 9 es un diagrama de flujo lógico de un método realizado por un nodo de red (por ejemplo, implementando una UDM) según algunas realizaciones.

La Figura 10 es un diagrama de bloques de un servidor de autenticación según algunas realizaciones.

25 La Figura 11 es un diagrama de bloques de un servidor de autenticación externa según algunas realizaciones.

La Figura 12 es un diagrama de bloques de un nodo de red (por ejemplo, que implementa una NSSAAF) según algunas realizaciones.

La Figura 13 es un diagrama de bloques de un nodo de red (por ejemplo, implementando una UDM) según algunas realizaciones.

30 La Figura 14 es un diagrama de bloques de un sistema de comunicación según algunas realizaciones.

La Figura 15 es un diagrama de bloques de un equipo de usuario según algunas realizaciones.

La Figura 16 es un diagrama de bloques de un nodo de red según algunas realizaciones.

35 La Figura 17 es un diagrama de bloques de un servidor según algunas realizaciones.

La Figura 18 es un diagrama de bloques de un entorno de virtualización según algunas realizaciones.

DESCRIPCIÓN DETALLADA

La Figura 1 muestra una red de comunicación inalámbrica 10 según algunas realizaciones. En algunas realizaciones, la red de comunicación inalámbrica 10 es una red no pública independiente (SNPN). Independientemente, la red de comunicación inalámbrica 10 está configurada para proporcionar servicio de comunicación inalámbrica a un dispositivo de comunicación inalámbrica 12, por ejemplo, que tiene una suscripción a la red de comunicación inalámbrica 10. Como requisito previo para proporcionar dicho servicio al dispositivo de comunicación inalámbrica 12, la red de comunicación inalámbrica 10 está configurada para autenticar y autorizar el dispositivo de comunicación inalámbrica 12, por ejemplo, como parte de un procedimiento para registrar el dispositivo de comunicación inalámbrica 12 con la red de comunicación inalámbrica 10.

Como se muestra al respecto, un servidor de autenticación 14 en la red de comunicación inalámbrica 10 está configurado para iniciar la autenticación primaria del dispositivo de comunicación inalámbrica 12 con un servidor de autenticación externa 20 que es externo a la red de comunicación inalámbrica 10. El servidor de autenticación externa 20 puede estar, por ejemplo, fuera del control y/o gestión del operador de la red de comunicación inalámbrica. En algunas realizaciones, el servidor de autenticación 14 inicia dicha autenticación primaria a través de uno o más nodos de red 16 en la red de comunicación inalámbrica 10. Como se muestra, por ejemplo, el servidor de autenticación 14 transmite una solicitud de autenticación 22 a un nodo de red 16, por ejemplo, implementando una Función de Autorización y Autenticación Específica de Segmento de Red (NSSAAF). En este caso, la solicitud de autenticación 22 puede indicar o solicitar que la autenticación primaria se realice con una red externa, y el nodo de red 16 puede seleccionar el servidor de autenticación externa 20 para tal fin.

El servidor de autenticación 14 según algunas realizaciones recibe señalización 24 en respuesta a la solicitud de autenticación 22, por ejemplo, a través del nodo de red 16. La señalización 24 indica que la autenticación primaria del dispositivo de comunicación inalámbrica 12 con el servidor de autenticación externa 20 tuvo éxito. En particular, la señalización 24 también incluye un identificador 26 afirmado por el servidor de autenticación externa 20 que identifica como auténtico el dispositivo de comunicación inalámbrica 12. Por ejemplo, en algunas realizaciones, el identificador afirmado 26 es el identificador realmente autenticado por el servidor de autenticación externa 20 como identificador del dispositivo de comunicación inalámbrica 12. El identificador 26 puede ser, por ejemplo, un ID de Protocolo de Autenticación Extensible (EAP). En otras realizaciones, el identificador afirmado 26 puede estar asociado con el identificador

realmente autenticado por el servidor de autenticación externa 20 como identificador del dispositivo de comunicación inalámbrica 12. El identificador 26 puede ser, por ejemplo, un identificador público (por ejemplo, un Identificador de Suscripción Pública Genérico, GPSI) asignado al ID de EAP. De cualquier manera, el identificador afirmado 26 identifica el dispositivo de comunicación inalámbrica 12, por ejemplo, de una manera no anónima.

El servidor de autenticación 14 en algunas realizaciones puede así autenticar el dispositivo de comunicación inalámbrica 12 con la red de comunicación inalámbrica 10 basándose en el identificador 26 incluido en la señalización recibida 24.

En particular, cuando el servidor de autenticación externa 20 proporciona el identificador afirmado 26 al servidor de autenticación 14 en la red de comunicación inalámbrica 10, algunas realizaciones permiten la autenticación incluso si el dispositivo de comunicación inalámbrica 12 inicia la autenticación primaria usando un identificador anónimo, por ejemplo, un Identificador Oculto de Suscripción (SUCI) anónimo, o Identificador Permanente de Suscripción (SUPI) anónimo. De hecho, si el dispositivo de comunicación inalámbrica 12 inicia la autenticación primaria utilizando un identificador anónimo, el servidor de autenticación 14 según las realizaciones en el presente documento aprende la identidad no anónima del dispositivo de comunicación inalámbrica 12 desde el servidor de autenticación externa 20 (mediante el servidor de autenticación externa 20 informando al servidor de autenticación 14 del identificador afirmado 26) y de este modo es capaz de autenticar el dispositivo de comunicación inalámbrica 12 con la red de comunicación inalámbrica 10.

Considere ahora un ejemplo de algunas realizaciones donde la red de comunicación inalámbrica 10 se ejemplifica como una red no pública independiente (SNPN), donde el dispositivo de comunicación inalámbrica 12 se ejemplifica como un equipo de usuario (UE), donde el servidor de autenticación 14 se ejemplifica como implementando una Función de Servidor de Autenticación (AUSF), y donde el servidor de autenticación externa 20 se ejemplifica implementando un Servidor de Contabilidad de Autorización de Autenticación (AAA-S).

El Acceso del UE de soporte de SNPN que utiliza credenciales propiedad de un titular de credenciales separado de la SNPN. La AUSF en una SNPN puede admitir autenticación y autorización primaria de los UE que utilizan credenciales de un servidor de AAA en un Titular de Credenciales (CH). La Figura 2 muestra la arquitectura del sistema 5G para la SNPN con un titular de credenciales que utiliza un servidor de AAA para la autenticación y autorización primaria.

Si la Gestión de Datos Unificada (UDM) decide que la autenticación primaria la realiza el servidor de AAA en el CH en función de los datos de suscripción del UE y el SUPI del UE, que

la UDM oculta del SUCI recibido de la AUSF, entonces la UDM indica a la AUSF que se requiere autenticación primaria mediante un servidor de AAA en un CH. La AUSF descubrirá y seleccionará la NSSAAF y luego reenviará mensajes EAP a la NSSAAF. La NSSAAF selecciona el servidor de AAA según el nombre de dominio correspondiente a la parte del dominio SUPI, retransmite mensajes EAP entre la AUSF y el servidor de AAA (o proxy AAA) y realiza la conversión de protocolo relacionada. El servidor de AAA actúa como servidor de EAP a efectos de autenticación primaria.

El SUPI se utiliza para identificar el UE durante la autenticación primaria y la autorización hacia el servidor de AAA. La Función de Acceso y Movilidad (AMF) y la Función de Gestión de Sesión (SMF) recuperarán los datos de suscripción del UE de la UDM utilizando el SUPI.

Si el UE proporciona un SUCI basado en un SUPI que la UDM puede ocultar en la SNPN, el SUPI resultante se puede proporcionar al AAA-S a través de la AUSF. En este caso, el SUPI se utiliza entre la AUSF en la SNPN y el AAA-S en el CH para identificar el UE durante el procedimiento de autenticación primaria.

Sin embargo, el UE puede, por otro lado, proporcionar un "SUCI anónimo" durante el registro del UE que activa el procedimiento de autenticación principal, por ejemplo, como se describe en la TS 33.501 v17.2.1 del 3GPP que define el uso del Protocolo de Autenticación Extensible (EAP) – Seguridad de la Capa de Transporte (TLS) para la autenticación primaria. Tal puede ser el caso en un sistema 5G (5GS), por ejemplo, como se describe en el Anexo informativo B de la TS 33.501 v17.2.1, o en el contexto de dispositivos sin capacidad 5G (N5GC) detrás de Puertas de Enlace Residenciales (RG) en redes privadas o en escenarios de implementación aislados con acceso por cable, por ejemplo, como se describe en el Anexo O informativo de la TS 33.501 v17.2.1. Independientemente, en tales realizaciones, durante el registro del UE que desencadena el procedimiento de autenticación principal, el UE hace uso de un SUPI/SUCI, que omite la parte del nombre de usuario del Identificador de Acceso a la Red (NAI) (denominado en adelante "SUPI/SUCI anónimo").

Sin embargo, el "esquema nulo" podría usarse en la capa de Estrato Sin Acceso (NAS) y al mismo tiempo preservar la privacidad del identificador de suscripción, omitiendo la parte del nombre de usuario del NAI como se describe en la cláusula 2.3 de RFC 4282. Sería análogo a usar un identificador anónimo en el EAP, lo que significa que solo la parte del reino de NAI se incluye en SUCI, que se envía en la capa NAS. Por tanto, el SUCI formado todavía se puede utilizar para enrutar la solicitud de autenticación a la AUSF.

En los casos en los que se utiliza un identificador anónimo, la UDM no es capaz de resolver ningún SUPI para el SUCI anónimo proporcionado por el UE y es responsable de que la AUSF actúe como servidor del EAP para solicitar el SUPI al UE durante la ejecución de EAP-

TLS. Si el SUPI recibido de la UDM es anónimo, la AUSF deriva el SUPI del identificador del cliente en el certificado de cliente TLS.

Algunas realizaciones hacen que la AUSF/UDM en la SNPN sea consciente del SUPI del UE incluso en este caso en el que se utiliza un identificador anónimo, es decir, incluso cuando la función del servidor de EAP la proporciona el AAA-S en el CH en lugar de la AUSF.

Algunas realizaciones también prevén la posibilidad de que el SUPI del UE en la SNPN podría intercambiarse con el servidor de AAA externo del CH. Se espera que cuando la SNPN y el CH pertenezcan a la misma organización, sea aceptable utilizar el SUPI como identificador de usuario para la autenticación del EAP bajo el control del AAA-S en el CH. Sin embargo, el CH puede ser proporcionado por una organización diferente a la SNPN e incluso el CH puede brindar sus servicios a múltiples SNPN. Entonces, dependiendo de la relación de confianza entre el CH/AAA-S y la SNPN, podría haber casos que requieran que el identificador de usuario utilizado por el AAA-S en el CH durante el procedimiento de autenticación primaria no sea el SUPI utilizado dentro de la SNPN para el resto de los procedimientos.

Según las realizaciones del presente documento, en el caso de que el UE aplique un SUCI anónimo al registrarse en la SNPN, la AUSF/UDM en la SNPN no puede conocer el SUPI real del UE basándose en el mensaje inicial del UE. Sólo después de una autenticación realizada entre el UE y la AAA del CH, la AAA aprende la identidad del UE (ID del UE). En algunas realizaciones, el ID del UE se devuelve a la AUSF junto con un resultado de autenticación exitoso. Luego, la UDM/AUSF aprende el SUPI del ID del UE.

Según otras realizaciones, en el caso de que no se utilicen SUPI anonimizados, el UE aplica un SUCI real al registrarse en la SNPN. La AUSF/UDM en la SNPN puede entonces resolver el SUPI real del UE desde el UE. Pero dado que la autenticación del UE depende de la AAA de CH, solo después de la autenticación por parte de la AAA de CH y que la AAA envíe el ID del UE autenticado de vuelta a la SNPN, entonces la UDM/AUSF puede estar segura de que es el SUPI real del UE autenticado. Por lo tanto, también en este caso el ID del UE en algunas realizaciones se devuelve desde la AAA de CH a la AUSF de SNPN después de una autenticación exitosa.

En ambos casos, el ID del UE enviado de vuelta por la AAA a la AUSF/UDM puede ser un SUPI si la AAA/CH es de confianza para la SNPN o, en caso contrario, un ID de asociación. Esta ID de asociación puede basarse en un ID del UE público, es decir, un GPSI.

La Figura 3 muestra la autenticación primaria con un dominio externo según algunas realizaciones.

0. El UE se configurará con credenciales del titular de las credenciales, por ejemplo, SUPI que contiene un identificador específico de la red y credenciales para cualquier método del EAP de generación de claves.

Además, se supone que existe una relación de confianza entre la SNPN y el servidor de AAA titular de las credenciales. Estas entidades deben autenticarse mutuamente y la información transferida en la interfaz debe tener confidencialidad, integridad y protección de reproducción.

1. El UE seleccionará la SNPN e iniciará el registro del UE en la SNPN.

Para la construcción del SUCI, se pueden utilizar los métodos de la cláusula 6.12 de la TS 33.501 v17.2.1. Si la clave pública de la red doméstica de la SNPN no está proporcionada en el UE, el UE creará un SUCI utilizando un esquema nulo con SUPI anonimizado como se describe en el Anexo B de la TS 33.501 v17.2.1.

2. La AMF dentro de la SNPN iniciará una autenticación primaria para el UE utilizando una operación de servicio Nausf_UEAuthentication_Authenticate con la AUSF. La AMF seleccionará una AUSF en función del Identificador de Red Local (HNI) del SUCI (es decir, dominio para el tipo SUPI del NSI) presentado por el UE como se especifica en la TS 23.501 v17.1.1. En este caso, se utiliza "SUCI anónimo" en el paso 1, el ámbito de la "SUCI anónimo" facilitará la selección de la AUSF/UDM en la SNPN correspondiente propietaria de la suscripción para el UE de la SNPN.

3. La AUSF iniciará una operación de servicio Nudm_UEAuthentication_Get. La AUSF seleccionará una UDM también utilizando el SUCI/SUPI proporcionado por la AMF como se especifica en la TS 23.501 v17.1.1.

NOTA 1: Se utilizará SUPI en lugar de SUCI en el caso de una nueva autenticación.

4. En caso de que la UDM reciba un SUCI, la UDM deberá resolver el SUCI al SUPI antes de verificar el método de autenticación aplicable al SUPI. La UDM decide ejecutar la autenticación primaria con una entidad externa basada en los datos de suscripción o mirando la parte del dominio del SUPI en formato NAI. Cuando se utiliza SUCI anónimo, la UDM aún puede decidir, basándose en la parte del dominio de SUPI, tal vez en combinación con los datos de suscripción, que la autenticación primaria se ejecutará con una entidad externa. Alternativamente, la AUSF puede omitir la interacción con la UDM y decidir ejecutar la autenticación primaria basada en la configuración local de la parte del dominio del SUPI.

5. La UDM proporcionará a la AUSF el SUPI del UE e indicará a la AUSF que ejecute la autenticación primaria con un titular de Credenciales externo. Cuando se utiliza un SUCI anónimo, la UDM devuelve un SUPI anónimo a la AUSF. Dependiendo de la relación de confianza con el servidor de AAA, la UDM puede proporcionar al usuario SUPI (si el servidor de AAA es confiable para la SNPN) y adicionalmente un identificador alternativo (por ejemplo, GPSI)

adecuado para ser presentado o comunicado con el servidor de AAA.

6. Según la indicación de la UDM, la AUSF seleccionará una NSSAAF como se define en la TS 23.501 v17.1.1 de 3GPP e iniciará una operación de servicio Nnssaaf_AIWF_Authenticate hacia esa NSSAAF como se define en la sección 14.4.x de la TS 23.501 v17.1.1. En algunas realizaciones, este paso ejemplifica la señalización 22 en la Figura 1, por ejemplo, para iniciar la autenticación primaria. Dependiendo de la relación de confianza con el servidor de AAA, la AUSF incluye el SUPI o GPSI como ID de UE en el mensaje. Tenga en cuenta que el SUPI puede ser un SUPI anónimo si se recibe en el paso 5.

7. La NSSAAF seleccionará el servidor de AAA según el nombre de dominio correspondiente a la parte del dominio del ID del UE proporcionado por la UDM a la AUSF en el paso 5 (por ejemplo, SUPI, SUPI anónimo o ID/GPSI alternativo). La NSSAAF realizará la conversión de protocolos relacionados y retransmitirá mensajes al servidor de AAA. Tenga en cuenta que la NSSAAF puede enviar opcionalmente el ID del UE recibido en el mensaje (no se muestra en el flujo).

8. El UE y el servidor de AAA realizarán una autenticación mutua. El servidor de AAA actuará como servidor de EAP a efectos de autenticación primaria. Cuando se utiliza SUCI/SUPI anónimo o un ID del UE/GPSI alternativo a SUPI, el servidor de AAA solicita un identificador al UE utilizando una solicitud de ID de EAP antes de ejecutar el método de autenticación del EAP.

9. Después de una autenticación exitosa, el MSK y el ID de UE autenticado (SUPI o UEID/GPSI alternativo) se proporcionarán desde el servidor de AAA al NSSAAF. El servidor de AAA puede derivar el ID del UE autenticado a partir del ID de EAP a partir de la autenticación, o utilizar el ID de EAP como ID del UE autenticado. Alternativamente, si la NSSAF ha proporcionado el ID del UE en el paso 7, el servidor de AAA puede verificar la coincidencia del ID del UE recibido y el ID autenticado y determinar el resultado de la autenticación basándose en el resultado de la coincidencia (por ejemplo, si se debe enviar el éxito del EAP).

10. La NSSAAF devuelve el MSK y el ID del UE recibida en el paso 6 y/o el ID del UE autenticada recibida en el paso 9 (SUPI o UEID/GPSI alternativa) a la AUSF utilizando el mensaje de respuesta de operación del servicio Nnssaaf_AIWF_Authenticate. En algunas realizaciones, este paso ejemplifica la señalización 24 que recibe el servidor de autenticación 14 en la Figura 1, por ejemplo, donde el identificador afirmado 26 en la Figura 1 se ejemplifica como el ID del UE autenticado.

11. La AUSF verifica la coincidencia del SUPI recibido en el paso 5 con el UEID/SUPI autenticado para determinar el resultado de la autenticación en SNPN. Si se recibe SUPI anónimo o no se recibe SUPI desde el paso 5, la AUSF verificará la UDM del perfil de autenticación y suscripción del UE en función del UEID/SUPI autenticado recibido. Por ejemplo,

si el UEID autenticado es GPSI, la AUSF invocará el servicio de UDM para traducir el GPSI a SUPI utilizando una operación de servicio Nudm_SDM_Get (traducción de identificador).

12. La AUSF utilizará los 256 bits más significativos de MSK como K_{AUSF} . La AUSF también derivará K_{SEAF} del K_{AUSF} como se define en el Anexo A.6 de la TS 33.501 v17.2.1.

5 13. La AUSF enviará la indicación exitosa junto con el SUPI del UE a la AMF junto con el K_{SEAF} resultante.

14. La AMF enviará el éxito del EAP en un mensaje NAS.

15. El UE derivará la K_{AUSF} desde MSK como se describe en el paso 12.

10 Las Figuras 4 y 5 ilustran los diferentes casos dependiendo del tipo del SUCI proporcionado por la UE. Los pasos de las Figuras 4 y 5 son los mismos que los descritos anteriormente con respecto a la Figura 3, excepto donde se indica a continuación.

El GPSI se utiliza cuando no se confía en el AAA-S. De lo contrario, el SUPI puede compartirse entre la AUSF y el AAA-S.

15 La Figura 4 en particular muestra la autenticación primaria con un dominio externo cuando se utiliza un SUCI anónimo. Entonces, en comparación con la Figura 3, el UE proporciona un SUCI anónimo (A-SUCI) en formato NAI en la Solicitud de Registro (Paso 1) a la AMF, que se propaga a la AUSF y la UDM. En consecuencia, la UDM devuelve un SUPI anónimo (A-SUPI) a la AUSF en el Paso 5 correspondiente al A-SUCI. Aquí, dado que se confía en el AAA-S, no se utiliza el GPSI.

20 Con el A-SUPI recibido de la UDM, la AUSF envía el A-SUPI a la NSSAAF en su solicitud de autenticación (Paso 6). El AAA-S autentica el UE y devuelve el SUPI o GPSI como ID del UE autenticado (Paso 9), que se transmite a la AUSF (Paso 10). Si se devuelve un GPSI, la AUSF traduce el GPSI al SUPI del UE con asistencia de la UDM. Luego la operación continúa como se describe en la Figura 3.

La Figura 5 muestra la autenticación primaria con un dominio externo cuando se utiliza un SUCI no-anónimo. En este ejemplo, la UDM devuelve un GPSI a la AUSF (Paso 5) correspondiente al SUCI no-anónimo proporcionado por el UE en el Paso 1. La UDM también devuelve el SUPI no-anónimo correspondiente al SUCI no-anónimo.

30 En una realización, la AUSF proporciona correspondientemente el GPSI a la NSSAAF en su solicitud de autenticación (Paso 6), por ejemplo, en caso de que no se confíe en el AAA-S. En este caso, el GPSI se transmite al AAA-S. El AAA-S puede entonces devolver un GPSI en función del cual se autentica el UE (Paso 9). Dado que la AUSF ya comprende la relación entre el GPSI y el SUPI del Paso 5, la AUSF no necesita emplear la asistencia de la UDM para traducir el GPSI devuelto a un SUPI. En consecuencia, la operación puede realizarse como se

describe anteriormente en la Figura 3.

En otra realización, por el contrario, la AUSF proporciona el SUPI a la NSSAAF en su solicitud de autenticación (Paso 6), por ejemplo, en caso de que se confíe en el AAA-S. En este caso, el SUPI se retransmite al AAA-S. Luego, el AAA-S puede devolver un SUPI en función del cual se autentica el UE (Paso 9), momento en el cual la operación puede continuar como se describe anteriormente en la Figura 3.

En vista de las modificaciones y variaciones anteriores, la Figura 6 representa un método realizado por un servidor de autenticación 14 en una red de comunicación inalámbrica 10 de acuerdo con realizaciones particulares. El método incluye iniciar la autenticación primaria de un dispositivo de comunicación inalámbrica 12 con un servidor de autenticación externa 20 que es externo a la red de comunicación inalámbrica 10 (Bloque 600). El método también comprende recibir señalización 24 que indica que la autenticación primaria del dispositivo de comunicación inalámbrica 12 con el servidor de autenticación externa 20 tuvo éxito y que incluye un identificador 26 afirmado por el servidor de autenticación externa 20 que identifica como auténtico el dispositivo de comunicación inalámbrica 12 (Bloque 610). El identificador 26 por ejemplo, puede ser, o estar asociado con, un identificador autenticado basándose en cuál servidor de autenticación externa 20 autenticó el dispositivo de comunicación inalámbrica 12 a través de la autenticación primaria. Independientemente, el método en algunas realizaciones también comprende autenticar el dispositivo de comunicación inalámbrica 12 con la red de comunicación inalámbrica 10 basándose en el identificador 26 incluido en la señalización recibida 24 (Bloque 620).

Aspectos adicionales del método de la Figura 6 se enumeran en las REALIZACIONES DEL GRUPO A en el presente documento.

Por ejemplo, en algunas realizaciones, dicho inicio comprende iniciar la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa utilizando un identificador anónimo que no identifica el dispositivo de comunicación inalámbrica. En un ejemplo, el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

En algunas realizaciones, el identificador incluido en la señalización recibida es un identificador no-anónimo. Por ejemplo, en una realización, el identificador no-anónimo es un SUPI no-anónimo.

En algunas realizaciones, el identificador incluido en la señalización recibida es un identificador público que identifica el dispositivo de comunicación inalámbrica ante una red externa a la red de comunicación inalámbrica. Por ejemplo, en una realización, el identificador público es un Identificador de Suscripción Pública Genérico, GPSI. De forma alternativa o

adicional, en algunas realizaciones, el método comprende además traducir, o solicitar la traducción, del identificador público a un identificador que identifique el dispositivo de comunicación inalámbrica en la red de comunicación inalámbrica.

5 En algunas realizaciones, el identificador incluido en la señalización recibida es, o está asociado con, un identificador autenticado basándose en el cual el servidor de autenticación externa autenticó el dispositivo de comunicación inalámbrica a través de la autenticación primaria. Por ejemplo, en una realización, el identificador autenticado es una Identidad del Protocolo de Autenticación Extensible, EAP.

10 En algunas realizaciones, dicho inicio comprende iniciar la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa utilizando un identificador presentado que el dispositivo de comunicación inalámbrica ha presentado como identificación del dispositivo de comunicación inalámbrica a la red de comunicación inalámbrica. En una de dichas realizaciones, autenticar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en el identificador incluido en la señalización recibida
15 comprende confirmar que el identificador presentado corresponde al identificador incluido en la señalización recibida.

En algunas realizaciones, la autenticación primaria se inicia como parte de un procedimiento para registrar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica. En una de dichas realizaciones, el método comprende además
20 registrar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en la autenticación exitosa del dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica. Por ejemplo, cuando la autenticación exitosa del dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica es un requisito previo para el registro del dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica, el
25 procedimiento para registrar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica puede resultar de hecho en el registro del dispositivo de comunicación inalámbrica, siempre y cuando se cumpla cualquier otro requisito para el registro (por ejemplo, autorización). Por otra parte, si falla la autenticación del dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica, también falla el procedimiento para registrar el
30 dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica.

En algunas realizaciones, la red de comunicación inalámbrica es una red no pública independiente.

En algunas realizaciones, el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

La Figura 7 representa un método realizado por un servidor de autenticación externa 20 que es externo a una red de comunicación inalámbrica 10 de acuerdo con otras realizaciones particulares. El método incluye realizar la autenticación primaria de un dispositivo de comunicación inalámbrica 12 con el servidor de autenticación externa 20 para el acceso del dispositivo de comunicación inalámbrica 12 a la red de comunicación inalámbrica 10 (Bloque 700). El método también comprende transmitir, a un servidor de autenticación 14 en la red de comunicación inalámbrica 10, señalización 24 que indica que la autenticación primaria del dispositivo de comunicación inalámbrica 12 con el servidor de autenticación externa 20 tuvo éxito y que incluye un identificador 26 afirmado por el servidor de autenticación externa 20 que identifica como auténtico el dispositivo de comunicación inalámbrica 12 (Bloque 710).

Aspectos adicionales del método de la Figura 7 se enumeran en las REALIZACIONES DEL GRUPO B del presente documento.

En algunas realizaciones, el método comprende además recibir señalización que activa el servidor de autenticación externa para realizar la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa, en donde la señalización incluye un identificador anónimo para el dispositivo de comunicación inalámbrica. En una realización, el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

En algunas realizaciones, el identificador incluido en la señalización transmitida es un identificador no-anónimo. Por ejemplo, el identificador no-anónimo es un SUPI no-anónimo.

En algunas realizaciones, el identificador incluido en la señalización transmitida es un identificador público que identifica el dispositivo de comunicación inalámbrica ante una red externa a la red de comunicación inalámbrica. Por ejemplo, el identificador público es un Identificador de Suscripción Pública Genérico, GPSI.

En algunas realizaciones, el identificador incluido en la señalización transmitida es, o está asociado con, un identificador autenticado basándose en el cual el servidor de autenticación externa autenticó el dispositivo de comunicación inalámbrica a través de la autenticación primaria. Por ejemplo, el identificador autenticado es una Identidad del Protocolo de Autenticación Extensible, EAP.

En algunas realizaciones, la red de comunicación inalámbrica es una red no pública independiente.

En algunas realizaciones, el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

La Figura 8 representa un método realizado por un nodo de red 16 (por ejemplo, implementando una NSSAAF) en una red de comunicación inalámbrica 10 de acuerdo con otras

realizaciones particulares. El método incluye recibir, desde un servidor de autenticación 14 en la red de comunicación inalámbrica 10, una solicitud de autenticación primaria de un dispositivo de comunicación inalámbrica 12 con un servidor de autenticación externa 20 para el acceso por parte del dispositivo de comunicación inalámbrica 12 a la red de comunicación inalámbrica 10 (Bloque 800). El método también comprende transmitir, al servidor de autenticación 13 en la red de comunicación inalámbrica 10, una respuesta que indica que la autenticación primaria del dispositivo de comunicación inalámbrica 12 con el servidor de autenticación externa 20 tuvo éxito y que incluye un identificador 26 afirmado por el servidor de autenticación externa 20 que identifica como auténtico el dispositivo de comunicación inalámbrica 12 (Bloque 810).

Aspectos adicionales del método de la Figura 8 se enumeran en las REALIZACIONES DEL GRUPO C del presente documento.

Por ejemplo, en algunas realizaciones, la solicitud incluye un identificador anónimo para el dispositivo de comunicación inalámbrica. Por ejemplo, el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

En algunas realizaciones, el identificador incluido en la señalización transmitida es un identificador no-anónimo. Por ejemplo, el identificador no-anónimo es un SUPI no-anónimo.

En algunas realizaciones, el identificador incluido en la señalización transmitida es un identificador público que identifica el dispositivo de comunicación inalámbrica ante una red externa a la red de comunicación inalámbrica. Por ejemplo, el identificador público es un Identificador de Suscripción Pública Genérico, GPSI. En algunas realizaciones,

En algunas realizaciones, el identificador incluido en la señalización transmitida es, o está asociado con, un identificador autenticado basándose en el cual el servidor de autenticación externa autenticó el dispositivo de comunicación inalámbrica a través de la autenticación primaria. Por ejemplo, el identificador autenticado es una Identidad del Protocolo de Autenticación Extensible, EAP.

En algunas realizaciones, la red de comunicación inalámbrica es una red no pública independiente.

En algunas realizaciones, el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

En algunas realizaciones, el nodo de red implementa una Función de Autorización y Autenticación Específica del Segmento de Red, NSSAAF.

La Figura 9 representa un método realizado por un nodo de red (por ejemplo, implementando una UDM) en una red de comunicación inalámbrica de acuerdo con otras realizaciones particulares. El método incluye recibir, desde un servidor de autenticación en la red de comunicación inalámbrica, una solicitud de datos de autenticación para un dispositivo de

comunicación inalámbrica (Bloque 900). El método también comprende transmitir, al servidor de autenticación, una respuesta que indica que la autenticación primaria del dispositivo de comunicación inalámbrica se va a ejecutar con un servidor de autenticación externa que es externo a la red de comunicación inalámbrica y que incluye un identificador que se va a presentar al servidor de autenticación externa. (Bloque 910).

Algunos aspectos adicionales del método de la Figura 9 se enumeran en las REALIZACIONES DEL GRUPO D del presente documento.

Por ejemplo, en algunas realizaciones, el identificador incluido en la respuesta es un identificador anónimo para el dispositivo de comunicación inalámbrica. En algunas realizaciones, el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

En algunas realizaciones, el identificador incluido en la respuesta es un identificador público que identifica el dispositivo de comunicación inalámbrica ante una red externa a la red de comunicación inalámbrica. En un ejemplo, el identificador público es un Identificador de Suscripción Pública Genérico, GPSI.

En algunas realizaciones, la solicitud incluye un identificador anónimo para el dispositivo de comunicación inalámbrica. En una de dichas realizaciones, el método comprende además decidir, basándose en una parte del dominio del identificador anónimo, que la autenticación primaria del dispositivo de comunicación inalámbrica se ejecutará con el servidor de autenticación externa a la red de comunicación inalámbrica.

En algunas realizaciones, la red de comunicación inalámbrica es una red no pública independiente.

En algunas realizaciones, el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

Las realizaciones en el presente documento también incluyen un método realizado por un nodo de red en una red de comunicación inalámbrica. El método comprende recibir una solicitud para traducir un identificador público, que identifica el dispositivo de comunicación inalámbrica en una red externa a la red de comunicación inalámbrica, a un identificador no público que identifica el dispositivo de comunicación inalámbrica en la red de comunicación inalámbrica. El método también comprende traducir el identificador público al identificador no público y transmitir una respuesta que incluye el identificador no público.

En algunas realizaciones, el identificador público es un Identificador de Suscripción Pública Genérico, GPSI.

En algunas realizaciones, el identificador no público es un Identificador Permanente de Suscripción, SUPI.

En algunas realizaciones, la red de comunicación inalámbrica es una red no pública

independiente.

En algunas realizaciones, la solicitud se recibe desde un servidor de autenticación. En algunas realizaciones, el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

5 Las realizaciones en el presente documento también incluyen los aparatos correspondientes. Las realizaciones en el presente documento, por ejemplo, incluyen un servidor de autenticación 14 configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el servidor de autenticación 14.

10 Las realizaciones también incluyen un servidor de autenticación 14 que comprende circuitos de procesamiento y circuitos de suministro de energía. Los circuitos de procesamiento están configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el servidor de autenticación 14. El circuito de suministro de energía está configurado para suministrar energía al servidor de autenticación 14.

15 Las realizaciones incluyen además un servidor de autenticación 14 que comprende circuitos de procesamiento. Los circuitos de procesamiento están configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el servidor de autenticación 14. En algunas realizaciones, el servidor de autenticación 14 comprende además circuitos de comunicación.

20 Las realizaciones incluyen además un servidor de autenticación 14 que comprende circuitos de procesamiento y memoria. La memoria contiene instrucciones ejecutables por los circuitos de procesamiento mediante las cuales el servidor de autenticación 14 es configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el servidor de autenticación 14.

25 Las realizaciones también incluyen un servidor de autenticación externa 20 que comprende circuitos de procesamiento y circuitos de suministro de energía. Los circuitos de procesamiento están configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el servidor de autenticación externa 20. El circuito de suministro de energía está configurado para suministrar energía al servidor de autenticación externa 20.

30 Las realizaciones incluyen además un servidor de autenticación externa 20 que comprende circuitos de procesamiento. Los circuitos de procesamiento están configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el servidor de autenticación externa 20. En algunas realizaciones, el servidor de autenticación externa 20 comprende además circuitos de comunicación.

35 Las realizaciones incluyen además un servidor de autenticación externa 20 que

comprende circuitos de procesamiento y memoria. La memoria contiene instrucciones ejecutables por los circuitos de procesamiento mediante las cuales el servidor de autenticación externa 20 es configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el servidor de autenticación externa 20.

5 Las realizaciones en el presente documento también incluyen un nodo de red 16 configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el nodo de red 16.

Las realizaciones también incluyen un nodo de red 16 que comprende circuitos de procesamiento y circuitos de suministro de energía. Los circuitos de procesamiento están
10 configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones descritas anteriormente para el nodo de red 16. El circuito de suministro de energía está configurado para suministrar energía al nodo de red 16.

Las realizaciones incluyen además un nodo de red 16 que comprende circuitos de procesamiento. Los circuitos de procesamiento están configurados para realizar cualquiera de
15 los pasos de cualquiera de las realizaciones descritas anteriormente para el nodo de red 16. En algunas realizaciones, el nodo de red 16 comprende además circuitos de comunicación.

Las realizaciones incluyen además un nodo de red 16 que comprende circuitos de procesamiento y memoria. La memoria contiene instrucciones ejecutables por los circuitos de procesamiento mediante las cuales el nodo de red 16 es configurado para realizar cualquiera de
20 los pasos de cualquiera de las realizaciones descritas anteriormente para el nodo de red 16.

Más particularmente, los aparatos descritos anteriormente pueden realizar los métodos del presente documento y cualquier otro procesamiento implementando cualquier medio, módulo, unidad o circuito funcional. En una realización, por ejemplo, los aparatos comprenden los respectivos circuitos o circuitería configurados para realizar los pasos mostrados en las
25 figuras del método. Los circuitos o circuitería a este respecto pueden comprender circuitos dedicados a realizar cierto procesamiento funcional y/o uno o más microprocesadores junto con la memoria. Por ejemplo, los circuitos pueden incluir uno o más microprocesadores o microcontroladores, así como otro hardware digital, que puede incluir procesadores de señales digitales (DSP), lógica digital de propósito especial y similares. Los circuitos de procesamiento
30 pueden configurarse para ejecutar código de programa almacenado en la memoria, que puede incluir uno o varios tipos de memoria, como Memoria de solo lectura (ROM), memoria de acceso aleatorio, memoria caché, dispositivos de memoria flash, dispositivos de almacenamiento óptico, etc. El código de programa almacenado en la memoria incluye instrucciones de programa para ejecutar uno o más protocolos de telecomunicaciones y/o comunicaciones de datos, así como
35 instrucciones para llevar a cabo una o más de las técnicas descritas en este documento en varias

realizaciones. En realizaciones que emplean memoria, la memoria almacena código de programa que, cuando es ejecutado por uno o más procesadores, lleva a cabo las técnicas descritas en el presente documento.

La Figura 10, por ejemplo, ilustra un servidor de autenticación 14 implementado de acuerdo con una o más realizaciones. Como se muestra, el servidor de autenticación 14 incluye circuitos de procesamiento 1010 y circuitos de comunicación 1020. Los circuitos de comunicación 1020 están configurados para transmitir y/o recibir información hacia y/o desde uno o más nodos, por ejemplo, a través de cualquier tecnología de comunicación. Los circuitos de procesamiento 1010 están configurados para realizar el procesamiento descrito anteriormente, por ejemplo, en la Figura 6, tal como ejecutando instrucciones almacenadas en la memoria 1030. Los circuitos de procesamiento 1010 a este respecto pueden implementar ciertos medios, unidades o módulos funcionales.

La Figura 11 ilustra un servidor de autenticación externa 20 implementado de acuerdo con una o más realizaciones. Como se muestra, el servidor de autenticación externa 20 incluye circuitos de procesamiento 1110 y circuitos de comunicación 1120. Los circuitos de comunicación 1120 están configurados para transmitir y/o recibir información hacia y/o desde uno o más nodos, por ejemplo, a través de cualquier tecnología de comunicación. Los circuitos de procesamiento 1110 están configurados para realizar el procesamiento descrito anteriormente, por ejemplo, en la Figura 7, tal como ejecutando instrucciones almacenadas en la memoria 1130. Los circuitos de procesamiento 1110 a este respecto pueden implementar ciertos medios, unidades o módulos funcionales.

La Figura 12 ilustra un nodo de red 16 implementado de acuerdo con una o más realizaciones. El nodo de red 16 puede, por ejemplo, implementar una NSSAAF. Como se muestra, el nodo de red 16 incluye circuitos de procesamiento 1210 y circuitos de comunicación 1220. Los circuitos de comunicación 1220 están configurados para transmitir y/o recibir información hacia y/o desde uno o más nodos, por ejemplo, a través de cualquier tecnología de comunicación. Los circuitos de procesamiento 1210 están configurados para realizar el procesamiento descrito anteriormente, por ejemplo, en la Figura 8, tal como ejecutando instrucciones almacenadas en la memoria 1230. Los circuitos de procesamiento 1210 a este respecto pueden implementar ciertos medios, unidades o módulos funcionales.

La Figura 13 ilustra un nodo de red 1300 implementado de acuerdo con una o más realizaciones. El nodo de red 1300 puede, por ejemplo, implementar una UDM. Como se muestra, el nodo de red 1300 incluye circuitos de procesamiento 1310 y circuitos de comunicación 1320. Los circuitos de comunicación 1320 están configurados para transmitir y/o recibir información hacia y/o desde uno o más nodos, por ejemplo, a través de cualquier

tecnología de comunicación. Los circuitos de procesamiento 1310 están configurados para realizar el procesamiento descrito anteriormente, por ejemplo, en la Figura 9, tal como ejecutando instrucciones almacenadas en la memoria 1330. Los circuitos de procesamiento 1310 a este respecto puede implementar ciertos medios, unidades o módulos funcionales.

5 Los expertos en la técnica también apreciarán que las realizaciones del presente documento incluyen además los programas de computador correspondientes.

Un programa de computador comprende instrucciones que, cuando se ejecutan en al menos un procesador de un aparato, hacen que el aparato lleve a cabo cualquiera de los procesamientos respectivos descritos anteriormente. Un programa de computador a este
10 respecto puede comprender uno o más módulos de código correspondientes a los medios o unidades descritos anteriormente.

Las realizaciones incluyen además una portadora que contiene dicho programa de computador. Esta portadora puede comprender una de una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por computador.

15 A este respecto, las realizaciones en el presente documento también incluyen un producto de programa de computador almacenado en un medio no transitorio legible por computador (almacenamiento o grabación) y que comprende instrucciones que, cuando se ejecutan mediante un procesador de un aparato, hacen que el aparato funcione como se describe anteriormente.

20 Las realizaciones incluyen además un producto de programa de computador que comprende partes de código de programa para realizar los pasos de cualquiera de las realizaciones del presente documento cuando el producto de programa de computador se ejecuta mediante un dispositivo de cómputo. Este producto de programa de computador puede almacenarse en un medio de grabación legible por computador.

25 La Figura 14 muestra un ejemplo de un sistema de comunicación 1400 de acuerdo con algunas realizaciones.

En el ejemplo, el sistema de comunicación 1400 incluye una red de telecomunicaciones 1402 que incluye una red de acceso 1404, tal como una red de acceso por radio (RAN), y una red central 1406, que incluye uno o más nodos de red central 1408. La red de acceso 1404
30 incluye uno o más nodos de red de acceso, tales como los nodos de red 1410a y 1410b (uno o más de los cuales pueden denominarse generalmente nodos de red 1410), o cualquier otro nodo o nodo de acceso del Proyecto de Asociación de Tercera Generación (3GPP) similar o punto de acceso no-3GPP. Los nodos de red 1410 facilitan la conexión directa o indirecta del equipo de usuario (UE), tal como conectando los UE 1412a, 1412b, 1412c y 1412d (uno o más de los cuales

pueden denominarse generalmente UE 1412) a la red central 1406 a través de una o más conexiones inalámbricas.

Ejemplos de comunicaciones inalámbricas a través de una conexión inalámbrica incluyen transmitir y/o recibir señales inalámbricas usando ondas electromagnéticas, ondas de radio, ondas infrarrojas y/u otros tipos de señales adecuadas para transmitir información sin el uso de alambres, cables u otros materiales conductores. Además, en diferentes realizaciones, el sistema de comunicación 1400 puede incluir cualquier número de redes cableadas o inalámbricas, nodos de red, UE y/o cualquier otro componente o sistema que pueda facilitar o participar en la comunicación de datos y/o señales ya sea a través de cables o conexiones inalámbricas. El sistema de comunicación 1400 puede incluir y/o interactuar con cualquier tipo de comunicación, telecomunicaciones, datos, celular, red de radio y/u otro tipo de sistema similar.

Los UE 1412 pueden ser cualquiera de una amplia variedad de dispositivos de comunicación, incluyendo dispositivos inalámbricos dispuestos, configurados y/u operables para comunicarse de forma inalámbrica con los nodos de red 1410 y otros dispositivos de comunicación. De manera similar, los nodos de red 1410 están dispuestos, son capaces, configurados y/u operables para comunicarse directa o indirectamente con los UE 1412 y/o con otros nodos o equipos de red en la red de telecomunicaciones 1402 para permitir y/o proporcionar acceso a la red, tales como acceso a la red inalámbrica, y/o para realizar otras funciones, tales como administración en la red de telecomunicaciones 1402.

En el ejemplo representado, la red central 1406 conecta los nodos de red 1410 a uno o más anfitriones, tales como el anfitrión 1416. Estas conexiones pueden ser directas o indirectas a través de una o más redes o dispositivos intermediarios. En otros ejemplos, los nodos de red pueden estar acoplados directamente a anfitriones. La red central 1406 incluye un nodo de red central más (por ejemplo, el nodo de red central 1408) que está estructurado con componentes de hardware y software. Las características de estos componentes pueden ser sustancialmente similares a las descritas con respecto a los UE, nodos de red y/o anfitriones, de modo que las descripciones de los mismos sean generalmente aplicables a los componentes correspondientes del nodo de red central 1408. Los nodos de red central de ejemplo incluyen funciones de uno o más de un Centro de Conmutación Móvil (MSC), una Entidad de Gestión de Movilidad (MME), un Servidor de Abonado Doméstico (HSS), una Función de Gestión de Acceso y Movilidad (AMF), una Función de Gestión de Sesión (SMF) y una Función de Autenticación de Servidor (AUSF), Función de Desocultación de Identificador de Suscripción (SIDF), Gestión de Datos Unificada (UDM), Proxy de Protección de Borde de Seguridad (SEPP), Función de Exposición de Red (NEF) y/o Función de Plano de Usuario (UPF).

El anfitrión 1416 puede estar bajo propiedad o control de un proveedor de servicios distinto de un operador o proveedor de la red de acceso 1404 y/o de la red de telecomunicaciones 1402, y puede ser operado por el proveedor de servicios o en nombre del proveedor de servicios. El servidor 1416 puede alojar una variedad de aplicaciones para proporcionar uno o más servicios. Ejemplos de dichas aplicaciones incluyen contenido de audio/vídeo en vivo y pregrabado, servicios de recopilación de datos, como la recuperación y compilación de datos sobre diversas condiciones ambientales detectadas por una pluralidad de UE, funcionalidad de análisis, redes sociales, funciones para controlar o interactuar de otro modo con dispositivos remotos, funciones para un centro de alarma y vigilancia, o cualquier otra función similar realizada por un servidor.

En conjunto, el sistema de comunicación 1400 de la Figura 14 permite la conectividad entre los UE, los nodos de red y los anfitriones. En ese sentido, el sistema de comunicación puede configurarse para operar de acuerdo con reglas o procedimientos predefinidos, tales como estándares específicos que incluyen, entre otros: Sistema Global de Comunicaciones Móviles (GSM); Sistema Universal de Telecomunicaciones Móviles (UMTS); Evolución a Largo Plazo (LTE) y/u otros estándares 2G, 3G, 4G, 5G adecuados o cualquier estándar de generación futura aplicable (por ejemplo, 6G); estándares de red de área local inalámbrica (WLAN), como los estándares 802.11 (WiFi) del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE); y/o cualquier otro estándar de comunicación inalámbrica apropiado, como la interoperabilidad mundial para acceso por microondas (WiMax), Bluetooth, Z-Wave, Comunicación de Campo Cercano (NFC), ZigBee, LiFi y/o cualesquiera estándares de red de área amplia de bajo consumo (LPWAN) como LoRa y Sigfox.

En algunos ejemplos, la red de telecomunicaciones 1402 es una red celular que implementa características estandarizadas del 3GPP. En consecuencia, la red de telecomunicaciones 1402 puede soportar la división de red para proporcionar diferentes redes lógicas a diferentes dispositivos que están conectados a la red de telecomunicaciones 1402. Por ejemplo, la red de telecomunicaciones 1402 puede proporcionar servicios de Comunicación de Baja Latencia Ultra Confiable (URLLC) a algunos UE, mientras proporciona servicios de Banda Ancha Móvil Mejorada (eMBB) a otros UE, y/o servicios de Comunicación de Tipo de Máquina Masiva (mMTC)/IoT Masiva a incluso más UE.

En algunos ejemplos, los UE 1412 están configurados para transmitir y/o recibir información sin interacción humana directa. Por ejemplo, un UE puede diseñarse para transmitir información a la red de acceso 1404 en un horario predeterminado, cuando se activa por un evento interno o externo, o en respuesta a solicitudes de la red de acceso 1404. Además, un UE puede configurarse para funcionar en modo de RAT única o múltiple o de múltiples estándares.

Por ejemplo, un UE puede operar con cualquiera o una combinación de Wi-Fi, NR (Nueva Radio) y LTE, es decir, estar configurado para conectividad dual multiradio (MR-DC), como Nueva Radio de E-UTRAN (Red de Acceso de Radio de UMTS Evolucionado Terrestre) – Conectividad Dual (EN-DC).

En el ejemplo, el concentrador 1414 se comunica con la red de acceso 1404 para facilitar la comunicación indirecta entre uno o más UE (por ejemplo, UE 1412c y/o 1412d) y nodos de red (por ejemplo, el nodo de red 1410b). En algunos ejemplos, el concentrador 1414 puede ser un controlador, enrutador, fuente de contenido y análisis, o cualquiera de los otros dispositivos de comunicación descritos en el presente documento con respecto a los UE. Por ejemplo, el concentrador 1414 puede ser un enrutador de banda ancha que permite el acceso a la red central 1406 para los UE. Como otro ejemplo, el concentrador 1414 puede ser un controlador que envía comandos o instrucciones a uno o más actuadores en los UE. Los comandos o instrucciones pueden recibirse desde los UE, los nodos de red 1410 o mediante código ejecutable, script, proceso u otras instrucciones en el concentrador 1414. Como otro ejemplo, el concentrador 1414 puede ser un recolector de datos que actúa como almacenamiento temporal para datos del UE y, en algunas realizaciones, puede realizar análisis u otro procesamiento de los datos. Como otro ejemplo, el concentrador 1414 puede ser una fuente de contenido. Por ejemplo, para un UE que es un dispositivo, pantalla, altavoz u otro dispositivo de entrega de medios de VR, el concentrador 1414 puede recuperar activos de VR, vídeo, audio u otros medios o datos relacionados con información sensorial a través de un nodo de red, que el concentrador 1414 luego proporciona al UE directamente, después de realizar el procesamiento local, y/o después de agregar contenido local adicional. En otro ejemplo más, el concentrador 1414 actúa como un servidor proxy u orquestador para los UE, en particular si uno o más de los UE son dispositivos IoT de baja potencia.

El concentrador 1414 puede tener una conexión constante/persistente o intermitente con el nodo de red 1410b. El concentrador 1414 también puede permitir un esquema y/o programación de comunicación diferente entre el concentrador 1414 y los UE (por ejemplo, UE 1412c y/o 1412d), y entre el concentrador 1414 y la red central 1406. En otros ejemplos, el concentrador 1414 está conectado a la red central 1406 y/o uno o más UE a través de una conexión por cable. Además, el concentrador 1414 puede configurarse para conectarse a un proveedor de servicios M2M a través de la red de acceso 1404 y/o a otro UE a través de una conexión directa. En algunos escenarios, los UE pueden establecer una conexión inalámbrica con los nodos de red 1410 mientras todavía están conectados a través del concentrador 1414 mediante una conexión por cable o inalámbrica. En algunas realizaciones, el concentrador 1414 puede ser un concentrador dedicado, es decir, un concentrador cuya función principal es enrutar

comunicaciones hacia/desde los UE desde/hacia el nodo de red 1410b. En otras realizaciones, el concentrador 1414 puede ser un concentrador no dedicado, es decir, un dispositivo que es capaz de operar para enrutar las comunicaciones entre los UE y el nodo de red 1410b, pero que además es capaz de operar como un punto de inicio y/o final de comunicación para ciertos canales de datos.

La Figura 15 muestra un UE 1500 de acuerdo con algunas realizaciones. Como se usa en el presente documento, un UE se refiere a un dispositivo capaz, configurado, dispuesto y/u operable para comunicarse de forma inalámbrica con nodos de red y/u otros UE. Los ejemplos de un UE incluyen, entre otros, un teléfono inteligente, un teléfono móvil, un teléfono celular, un teléfono de voz sobre IP (VoIP), un teléfono inalámbrico de bucle local, un computador de escritorio, un asistente digital personal (PDA), cámaras inalámbricas, una consola o dispositivo de juegos, dispositivo de almacenamiento de música, dispositivo de reproducción, dispositivo terminal portátil, punto final inalámbrico, estación móvil, tableta, computador portátil, equipo integrado en computador portátil (LEE), equipo montado en computador portátil (LME), dispositivo inteligente, equipo inalámbrico en las instalaciones del cliente (CPE), dispositivo inalámbrico montado en un vehículo o montado/integrado en un vehículo, etc. Otros ejemplos incluyen cualquier UE identificado por el Proyecto de Asociación de Tercera Generación (3GPP), incluyendo un UE de Internet de las cosas de banda estrecha (NB-IoT), un UE de comunicación de tipo máquina (MTC), y/o un UE de MTC mejorado (eMTC).

Un UE puede admitir comunicación de dispositivo a dispositivo (D2D), por ejemplo implementando un estándar 3GPP para comunicación de enlace lateral, Comunicación Dedicada de Corto Alcance (DSRC), vehículo a vehículo (V2V), vehículo a infraestructura (V2I), o vehículo a todo (V2X). En otros ejemplos, un UE puede no tener necesariamente un usuario en el sentido de un usuario humano que posea y/o opere el dispositivo relevante. En cambio, un UE puede representar un dispositivo que está destinado a la venta o a la operación por parte de un usuario humano, pero que no puede, o que inicialmente no puede estar asociado con un usuario humano específico (por ejemplo, un controlador de riego inteligente). Alternativamente, un UE puede representar un dispositivo que no está destinado a la venta ni a la operación por parte de un usuario final, pero que puede asociarse u operarse en beneficio de un usuario (por ejemplo, un medidor de energía inteligente).

El UE 1500 incluye circuitos de procesamiento 1502 que están acoplados operativamente a través de un bus 1504 a una interfaz de entrada/salida 1506, una fuente de energía 1508, una memoria 1510, una interfaz de comunicación 1512 y/o cualquier otro componente, o cualquier combinación de los mismos. Ciertos UE pueden utilizar todos o un subconjunto de los componentes que se muestran en la Figura 15. El nivel de integración entre los componentes

puede variar de un UE a otro UE. Además, ciertos UE pueden contener múltiples instancias de un componente, como múltiples procesadores, memorias, transceptores, transmisores, receptores, etc.

Los circuitos de procesamiento 1502 están configurados para procesar instrucciones y datos y pueden configurarse para implementar cualquier máquina de estado secuencial operativa para ejecutar instrucciones almacenadas como programas de computador legibles por máquina en la memoria 1510. Los circuitos de procesamiento 1502 pueden implementarse como una o más máquinas de estado implementadas por hardware (por ejemplo, en lógica discreta, matrices de puertas programables en campo (FPGA), circuitos integrados de aplicación específica (ASIC), etc.); lógica programable junto con el firmware adecuado; uno o más programas de computador almacenados, procesadores de uso general, como un microprocesador o un procesador de señales digitales (DSP), junto con el software adecuado; o cualquier combinación de los anteriores. Por ejemplo, los circuitos de procesamiento 1502 pueden incluir múltiples unidades centrales de procesamiento (CPU).

En el ejemplo, la interfaz de entrada/salida 1506 puede configurarse para proporcionar una interfaz o interfaces a un dispositivo de entrada, un dispositivo de salida o uno o más dispositivos de entrada y/o salida. Ejemplos de dispositivo de salida incluyen un altavoz, una tarjeta de sonido, una tarjeta de vídeo, una pantalla, un monitor, una impresora, un actuador, un emisor, una tarjeta inteligente, otro dispositivo de salida o cualquier combinación de los mismos. Un dispositivo de entrada puede permitir a un usuario capturar información en el UE 1500. Ejemplos de un dispositivo de entrada incluyen una pantalla sensible al tacto o sensible a la presencia, una cámara (por ejemplo, una cámara digital, una cámara de video digital, una cámara web, etc.), un micrófono, un sensor, un mouse, una bola de seguimiento, un pad direccional, un trackpad, una rueda de desplazamiento, una tarjeta inteligente y similares. La pantalla sensible a la presencia puede incluir un sensor táctil capacitivo o resistivo para detectar la entrada de un usuario. Un sensor puede ser, por ejemplo, un acelerómetro, un giroscopio, un sensor de inclinación, un sensor de fuerza, un magnetómetro, un sensor óptico, un sensor de proximidad, un sensor biométrico, etc., o cualquier combinación de los mismos. Un dispositivo de salida puede usar el mismo tipo de puerto de interfaz que un dispositivo de entrada. Por ejemplo, se puede utilizar un puerto de Bus Serie Universal (USB) para proporcionar un dispositivo de entrada y un dispositivo de salida.

En algunas realizaciones, la fuente de energía 1508 está estructurada como una batería o paquete de baterías. Se pueden usar otros tipos de fuentes de energía, tales como una fuente de energía externa (por ejemplo, un tomacorriente), un dispositivo fotovoltaico o una celda de energía. La fuente de energía 1508 puede incluir además circuitos de energía para entregar

energía desde la propia fuente de energía 1508, y/o una fuente de energía externa, a las diversas partes del UE 1500 a través de circuitos de entrada o una interfaz tal como un cable de energía eléctrica. La entrega de energía puede ser, por ejemplo, para cargar la fuente de energía 1508. Los circuitos de energía pueden realizar cualquier formateo, conversión u otra modificación de la energía de la fuente de energía 1508 para hacer que la energía sea adecuada para los respectivos componentes del UE 1500 al que se suministra la energía.

La memoria 1510 puede ser o estar configurada para incluir memoria tal como memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de solo lectura programable (PROM), memoria de solo lectura programable y borrrable (EPROM), memoria de solo lectura programable y borrrable electrónicamente (EEPROM), discos magnéticos, discos ópticos, discos duros, cartuchos extraíbles, unidades flash, etc. En un ejemplo, la memoria 1510 incluye uno o más programas de aplicación 1514, tales como un sistema operativo, una aplicación de navegador web, un widget, un motor de dispositivo u otra aplicación, y los datos correspondientes 1516. La memoria 1510 puede almacenar, para uso del UE 1500, cualquiera de una variedad de diversos sistemas operativos o combinaciones de sistemas operativos.

La memoria 1510 puede configurarse para incluir una serie de unidades de disco físicas, tales como una matriz redundante de discos independientes (RAID), memoria flash, unidad flash USB, unidad de disco duro-externa, unidad de almacenamiento en miniatura, lápiz de memoria, unidad de llave, unidad de memoria de alta densidad. unidad de disco óptico de disco versátil digital (HD-DVD), unidad de disco duro interna, unidad de disco óptico Blu-Ray, unidad de disco óptico de almacenamiento de datos digitales holográficos (HDDS), módulo de memoria externo mini dual en línea (DIMM), memoria de acceso aleatorio dinámica síncrona (SDRAM), SDRAM micro-DIMM externa, memoria de tarjeta inteligente como un módulo resistente a manipulaciones en forma de una tarjeta de circuitos integrados universal (UICC) que incluye uno o más módulos de identidad de abonado (SIM), como un USIM y/o ISIM, otra memoria o cualquier combinación de las mismas. La UICC puede ser, por ejemplo, una UICC incorporada (eUICC), una UICC integrada (iUICC) o una UICC extraíble comúnmente conocida como "tarjeta SIM". La memoria 1510 puede permitir que el UE 1500 acceda a instrucciones, programas de aplicación y similares, almacenados en medios de memoria transitorios o no transitorios, para descargar datos o cargar datos. Un artículo de fabricación, tal como uno que utiliza un sistema de comunicación, puede incorporarse tangiblemente como o en la memoria 1510, que puede ser o comprender un medio de almacenamiento legible por dispositivo.

Los circuitos de procesamiento 1502 pueden configurarse para comunicarse con una red de acceso u otra red utilizando la interfaz de comunicación 1512. La interfaz de comunicación 1512 puede comprender uno o más subsistemas de comunicación y puede incluir o estar

acoplada comunicativamente a una antena 1522. La interfaz de comunicación 1512 puede incluir uno o más transceptores utilizados para comunicarse, tal como comunicándose con uno o más transceptores remotos de otro dispositivo capaz de comunicación inalámbrica (por ejemplo, otro UE o un nodo de red en una red de acceso). Cada transceptor puede incluir un transmisor 1518 y/o un receptor 1520 apropiado para proporcionar comunicaciones de red (por ejemplo, ópticas, eléctricas, asignaciones de frecuencia, etc.). Además, el transmisor 1518 y el receptor 1520 pueden acoplarse a una o más antenas (por ejemplo, la antena 1522) y pueden compartir componentes de circuitos, software o firmware, o alternativamente implementarse por separado.

En la realización ilustrada, las funciones de comunicación de la interfaz de comunicación 1512 pueden incluir comunicación celular, comunicación Wi-Fi, comunicación LPWAN, comunicación de datos, comunicación de voz, comunicación multimedia, comunicaciones de corto alcance tales como Bluetooth, comunicación de campo cercano, comunicación basada en ubicación tal como el uso del sistema de posicionamiento global (GPS) para determinar una ubicación, otra función de comunicación similar, o cualquier combinación de las mismas. Las comunicaciones pueden implementarse de acuerdo con uno o más protocolos y/o estándares de comunicación, tales como IEEE 802.11, Acceso Multiplexado por División de Código (CDMA), Acceso Múltiple por División de Código de Banda Ancha (WCDMA), GSM, LTE, Nueva Radio (NR), UMTS, WiMax, Ethernet, protocolo de control de transmisión/protocolo de Internet (TCP/IP), red óptica síncrona (SONET), Modo de Transferencia Asíncrona (ATM), QUIC, Protocolo de Transferencia de Hipertexto (HTTP), etc.

Independientemente del tipo de sensor, un UE puede proporcionar una salida de datos capturados por sus sensores, a través de su interfaz de comunicación 1512, a través de una conexión inalámbrica a un nodo de red. Los datos capturados por los sensores de un UE se pueden comunicar a través de una conexión inalámbrica a un nodo de red a través de otro UE. La salida puede ser periódica (p. ej., una vez cada 15 minutos si informa la temperatura detectada), aleatoria (p. ej., para igualar la carga de los informes de varios sensores), en respuesta a un evento desencadenante (p. ej., cuando se detecta humedad y se envía una alerta), en respuesta a una solicitud (por ejemplo, una solicitud iniciada por un usuario) o una transmisión continua (p. ej., una transmisión de video en vivo de un paciente).

Como otro ejemplo, un UE comprende un actuador, un motor o un interruptor, relacionado con una interfaz de comunicación configurada para recibir entrada inalámbrica desde un nodo de red a través de una conexión inalámbrica. En respuesta a la entrada inalámbrica recibida, los estados del actuador, el motor o el interruptor pueden cambiar. Por ejemplo, el UE puede comprender un motor que ajusta las superficies de control o rotores de un dron en vuelo según

la entrada recibida o un brazo robótico que realiza un procedimiento médico según la entrada recibida.

Un UE, cuando tiene la forma de un dispositivo de Internet de las cosas (IoT), puede ser un dispositivo para su uso en uno o más dominios de aplicaciones, comprendiendo estos dominios, entre otros, tecnología portátil urbana, aplicaciones industriales extendidas y atención médica. Algunos ejemplos no limitativos de dicho dispositivo de IoT son un dispositivo que se encuentra o que está integrado en: un refrigerador o congelador conectado, un televisor, un dispositivo de iluminación conectado, un medidor de electricidad, un robot aspirador, un altavoz inteligente controlado por voz, una cámara de seguridad para el hogar, un detector de movimiento, un termostato, un detector de humo, un sensor de puerta/ventana, un sensor de inundación/humedad, una cerradura eléctrica, un timbre conectado, un sistema de aire acondicionado como una bomba de calor, un vehículo autónomo, un sistema de vigilancia, un dispositivo de monitoreo del clima, un dispositivo de monitoreo de estacionamiento de vehículos, una estación de carga de vehículos eléctricos, un reloj inteligente, un rastreador de actividad física, una pantalla montada en la cabeza para Realidad Aumentada (AR) o Realidad Virtual (VR), un dispositivo portátil para uso táctil para aumento o mejora sensorial, un rociador de agua, un dispositivo de seguimiento de animales o artículos, un sensor para monitorear una planta o un animal, un robot industrial, un vehículo aéreo no tripulado (UAV) y cualquier tipo de dispositivo médico, como un monitor de frecuencia cardíaca o un robot quirúrgico controlado remotamente. Un UE en forma de dispositivo de IoT comprende circuitos y/o software dependiendo de la aplicación prevista del dispositivo de IoT, además de otros componentes como se describe en relación con el UE 1500 que se muestra en la Figura 15.

Como otro ejemplo específico más, en un escenario de IoT, un UE puede representar una máquina u otro dispositivo que realiza monitoreo y/o mediciones, y transmite los resultados de dicho monitoreo y/o mediciones a otro UE y/o un nodo de red. En este caso, el UE puede ser un dispositivo de M2M, que en un contexto de 3GPP puede denominarse dispositivo de MTC. Como ejemplo particular, el UE puede implementar el estándar NB-IoT de 3GPP. En otros escenarios, un UE puede representar un vehículo, tal como un automóvil, un autobús, un camión, un barco y un avión, u otro equipo que sea capaz de monitorear y/o informar sobre su estado operativo u otras funciones asociadas con su operación.

En la práctica, se puede utilizar cualquier número de UE juntos con respecto a un único caso de uso. Por ejemplo, un primer UE podría estar integrado en un dron y proporcionar la información de velocidad del dron (obtenida a través de un sensor de velocidad) a un segundo UE que es un controlador remoto que opera el dron. Cuando el usuario realiza cambios desde el control remoto, el primer UE puede ajustar el acelerador del dron (por ejemplo, controlando un

actuador) para aumentar o disminuir la velocidad del dron. El primer y/o segundo UE también pueden incluir más de una de las funcionalidades descritas anteriormente. Por ejemplo, un UE podría comprender el sensor y el actuador, y manejar la comunicación de datos tanto para el sensor de velocidad como para los actuadores.

5 La Figura 16 muestra un nodo de red 1600 de acuerdo con algunas realizaciones. Tal como se utiliza en el presente documento, nodo de red se refiere a equipo capaz, configurado, dispuesto y/u operable para comunicarse directa o indirectamente con un UE y/o con otros nodos o equipos de red, en una red de telecomunicaciones. Los ejemplos de nodos de red incluyen, entre otros, puntos de acceso, AP, (por ejemplo, puntos de acceso de radio), estaciones base, 10 BS, (por ejemplo, estaciones base de radio, Nodo B, Nodo B evolucionado, eNB, y Nodos B de NR, gNB).

Las estaciones base pueden clasificarse según la cantidad de cobertura que brindan (o, dicho de otra manera, su nivel de potencia de transmisión) y, por lo tanto, dependiendo de la cantidad de cobertura proporcionada, pueden denominarse estaciones base femto, estaciones 15 base pico, estaciones base micro, o estaciones base macro. Una estación base puede ser un nodo de retransmisión o un nodo donante de retransmisión que controla un retransmisor. Un nodo de red también puede incluir una o más (o todas) partes de una estación base de radio distribuida, como unidades digitales centralizadas y/o unidades de radio remotas (RRU) a veces denominadas cabezas de radio remotas (RRH). Tales unidades de radio remotas pueden o no 20 estar integradas con una antena como una antena de radio integrada. Las partes de una estación base de radio distribuida también pueden denominarse nodos en un sistema de antena distribuida (DAS).

Otros ejemplos de nodos de red incluyen nodos de acceso 5G de múltiples puntos de transmisión (multi-TRP), equipos de radio multiestándar (MSR) como BS de MSR, controladores 25 de red como controladores de red de radio (RNC) o controladores de estaciones base (BSC), estaciones transceptoras base (BTS), puntos de transmisión, nodos de transmisión, entidades de coordinación de múltiples celdas/multidifusión (MCE), nodos de operación y mantenimiento (O&M), nodos del Sistema de Soporte de Operaciones (OSS), nodos de Red Autoorganizada (SON), nodos de posicionamiento (por ejemplo, Centros de Ubicación Móviles de Servicio 30 Evolucionado (E-SMLC)) y/o Pruebas de Minimización Conducción (MDT).

El nodo de red 1600 incluye circuitos de procesamiento 1602, una memoria 1604, una interfaz de comunicación 1606 y una fuente de energía 1608. El nodo de red 1600 puede estar compuesto de múltiples componentes separados físicamente (por ejemplo, un componente de NodeB y un componente de RNC, o un componente de BTS y un componente de BSC, etc.), 35 cada uno de los cuales puede tener sus propios componentes respectivos. En ciertos escenarios

en los que el nodo de red 1600 comprende múltiples componentes separados (por ejemplo, componentes de BTS y BSC), uno o más de los componentes separados pueden compartirse entre varios nodos de red. Por ejemplo, un único RNC puede controlar múltiples NodeB. En tal escenario, cada par único de NodeB y RNC puede, en algunos casos, considerarse un único
5 nodo de red independiente. En algunas realizaciones, el nodo de red 1600 puede configurarse para soportar múltiples tecnologías de acceso por radio (RAT). En tales realizaciones, algunos componentes pueden duplicarse (por ejemplo, una memoria separada 1604 para diferentes RAT) y algunos componentes pueden reutilizarse (por ejemplo, una misma antena 1610 puede ser compartida por diferentes RAT). El nodo de red 1600 también puede incluir múltiples conjuntos
10 de los diversos componentes ilustrados para diferentes tecnologías inalámbricas integradas en el nodo de red 1600, por ejemplo, GSM, WCDMA, LTE, NR, WiFi, Zigbee, Z-wave, LoRaWAN, Identificación por Radiofrecuencia (RFID) o tecnologías inalámbricas Bluetooth. Estas tecnologías inalámbricas se pueden integrar en el mismo chip o en un conjunto de chips diferente o en otros componentes dentro del nodo de red 1600.

15 Los circuitos de procesamiento 1602 pueden comprender una combinación de uno o más de un microprocesador, controlador, microcontrolador, unidad de procesamiento central, procesador de señales digitales, circuitos integrados de aplicación específica, conjunto de puertas programables en campo o cualquier otro dispositivo, recurso o combinación de equipo de computo, recurso adecuado, o combinación de hardware, software y/o lógica codificada
20 operable para proporcionar, ya sea solo o junto con otros componentes del nodo de red 1600, tales como la memoria 1604, para proporcionar la funcionalidad del nodo de red 1600.

En algunas realizaciones, los circuitos de procesamiento 1602 incluyen un sistema en un chip (SOC). En algunas realizaciones, los circuitos de procesamiento 1602 incluyen uno o más circuitos transceptores de radiofrecuencia (RF) 1612 y circuitos de procesamiento de banda base
25 1614. En algunas realizaciones, los circuitos transceptores de radiofrecuencia (RF) 1612 y los circuitos de procesamiento de banda base 1614 pueden estar en chips (o conjuntos de chips), placas o unidades independientes, tales como unidades de radio y unidades digitales. En realizaciones alternativas, parte o la totalidad de los circuitos transceptores de RF 1612 y los circuitos de procesamiento de banda base 1614 pueden estar en el mismo chip o conjunto de
30 chips, tarjetas o unidades.

La memoria 1604 puede comprender cualquier forma de memoria volátil o no volátil legible por computador que incluye, entre otros, almacenamiento persistente, memoria de estado sólido, memoria montada de forma remota, medios magnéticos, medios ópticos, memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), medios de almacenamiento masivo (por
35 ejemplo, un disco duro), medios de almacenamiento extraíbles (por ejemplo, una unidad flash,

un disco compacto, CD, o un disco de video digital, DVD), y/o cualquier otro dispositivo o dispositivos de memoria no volátiles, no transitorios, legibles y/o ejecutables por computador que almacenan información, datos y/o instrucciones que pueden usarse mediante circuitos de procesamiento 1602. La memoria 1604 puede almacenar cualquier instrucción, dato o información adecuada, incluyendo un programa de computador, software, una aplicación que incluya uno o más de lógica, reglas, código, tablas, etc. y/u otras instrucciones capaces de ser ejecutadas por los circuitos de procesamiento 1602 y utilizadas por el nodo de red 1600. La memoria 1604 puede usarse para almacenar cualquier cálculo realizado por los circuitos de procesamiento 1602 y/o cualquier dato recibido a través de la interfaz de comunicación 1606. En algunas realizaciones, los circuitos de procesamiento 1602 y la memoria 1604 están integrados.

La interfaz de comunicación 1606 se utiliza en comunicación por cable o inalámbrica de señalización y/o datos entre un nodo de red, red de acceso y/o UE. Tal como se ilustra, la interfaz de comunicación 1606 comprende puerto(s)/terminal(es) 1616 para enviar y recibir datos, por ejemplo, hacia y desde una red a través de una conexión por cable. La interfaz de comunicación 1606 también incluye circuitos frontales de radio 1618 que pueden acoplarse a, o en ciertas realizaciones ser parte de, la antena 1610. Los circuitos frontales de radio 1618 comprenden filtros 1620 y amplificadores 1622. Los circuitos frontales de radio 1618 pueden conectarse a una antena 1610 y a los circuitos de procesamiento 1602. Los circuitos frontales de radio pueden configurarse para acondicionar señales comunicadas entre la antena 1610 y los circuitos de procesamiento 1602. Los circuitos frontales de radio 1618 pueden recibir datos digitales que se enviarán a otros nodos de red o UE a través de una conexión inalámbrica. Los circuitos frontales de radio 1618 pueden convertir los datos digitales en una señal de radio que tiene el canal y los parámetros de ancho de banda apropiados usando una combinación de filtros 1620 y/o amplificadores 1622. La señal de radio puede entonces transmitirse a través de la antena 1610. De manera similar, al recibir datos, la antena 1610 puede recopilar señales de radio que luego se convierten en datos digitales mediante los circuitos frontales de radio 1618. Los datos digitales pueden pasarse a los circuitos de procesamiento 1602. En otras realizaciones, la interfaz de comunicación puede comprender diferentes componentes y/o diferentes combinaciones de componentes.

En ciertas realizaciones alternativas, el nodo de red 1600 no incluye circuitos frontales de radio separados 1618; en cambio, los circuitos de procesamiento 1602 incluyen circuitos frontales de radio y están conectados a la antena 1610. De manera similar, en algunas realizaciones, todos o algunos de los circuitos transceptores de RF 1612 son parte de la interfaz de comunicación 1606. En otras realizaciones más, la interfaz de comunicación 1606 incluye uno o más puertos o terminales 1616, los circuitos frontales de radio 1618 y los circuitos transceptores

de RF 1612, como parte de una unidad de radio (no mostrada), y la interfaz de comunicación 1606 se comunica con los circuitos de procesamiento de banda base 1614, que es parte de una unidad digital (no mostrada).

5 La antena 1610 puede incluir una o más antenas, o conjuntos de antenas, configuradas para enviar y/o recibir señales inalámbricas. La antena 1610 puede estar acoplada a los circuitos frontales de radio 1618 y puede ser cualquier tipo de antena capaz de transmitir y recibir datos y/o señales de forma inalámbrica. En ciertas realizaciones, la antena 1610 está separada del nodo de red 1600 y se puede conectar al nodo de red 1600 a través de una interfaz o puerto.

10 La antena 1610, la interfaz de comunicación 1606 y/o los circuitos de procesamiento 1602 pueden configurarse para realizar cualquier operación de recepción y/o ciertas operaciones de obtención descritas en el presente documento como realizadas por el nodo de red. Cualquier información, datos y/o señales pueden recibirse desde un UE, otro nodo de red y/o cualquier otro equipo de red. De manera similar, la antena 1610, la interfaz de comunicación 1606 y/o los circuitos de procesamiento 1602 pueden configurarse para realizar cualquier operación de
15 transmisión descrita en el presente documento como realizada por el nodo de red. Cualquier información, datos y/o señales pueden transmitirse a un UE, otro nodo de red y/o cualquier otro equipo de red.

La fuente de energía 1608 proporciona energía a los diversos componentes del nodo de red 1600 en una forma adecuada para los componentes respectivos (por ejemplo, a un nivel de
20 voltaje y corriente necesario para cada componente respectivo). La fuente de energía 1608 puede comprender, además, o estar acoplada a, circuitos de administración de energía para suministrar energía a los componentes del nodo de red 1600 para realizar la funcionalidad descrita en el presente documento. Por ejemplo, el nodo de red 1600 puede conectarse a una fuente de energía externa (por ejemplo, la red eléctrica, una toma de electricidad) a través de
25 circuitos de entrada o una interfaz tal como un cable eléctrico, mediante el cual la fuente de energía externa suministra energía a los circuitos de alimentación de la fuente de energía 1608. Como ejemplo adicional, la fuente de energía 1608 puede comprender una fuente de energía en forma de una batería o paquete de baterías que está conectada o integrada en circuitos de energía. La batería puede proporcionar energía de respaldo en caso de que falle la fuente de
30 energía externa.

Las realizaciones del nodo de red 1600 pueden incluir componentes adicionales además de los mostrados en la Figura 16 para proporcionar ciertos aspectos de la funcionalidad del nodo de red, incluyendo cualquiera de las funciones descritas en el presente documento y/o cualquier funcionalidad necesaria para soportar el tema descrito en el presente documento. Por ejemplo,
35 el nodo de red 1600 puede incluir equipo de interfaz de usuario para permitir la entrada de

información en el nodo de red 1600 y para permitir la salida de información desde el nodo de red 1600. Esto puede permitir a un usuario realizar diagnóstico, mantenimiento, reparación y otras funciones administrativas para el nodo de red 1600.

La Figura 17 es un diagrama de bloques de un anfitrión 1700, que puede ser una realización del anfitrión 1416 de la Figura 14, de acuerdo con diversos aspectos descritos en el presente documento. Como se usa en el presente documento, el anfitrión 1700 puede ser o comprender varias combinaciones de hardware y/o software, incluyendo un servidor independiente, un servidor Blade, un servidor implementado en la nube, un servidor distribuido, una máquina virtual, un contenedor o recursos de procesamiento en una granja de servidores. El anfitrión 1700 puede proporcionar uno o más servicios a uno o más UE.

El anfitrión 1700 incluye circuitos de procesamiento 1702 que están acoplados operativamente a través de un bus 1704 a una interfaz de entrada/salida 1706, una interfaz de red 1708, una fuente de energía 1710 y una memoria 1712. Se pueden incluir otros componentes en otras realizaciones. Las características de estos componentes pueden ser sustancialmente similares a las descritas con respecto a los dispositivos de las figuras anteriores, tales como las Figuras 15 y 16, de manera que las descripciones de estos son generalmente aplicables a los componentes correspondientes del anfitrión 1700.

La memoria 1712 puede incluir uno o más programas de computador que incluyen uno o más programas de aplicación de anfitrión 1714 y datos 1716, que pueden incluir datos de usuario, por ejemplo, datos generados por un UE para el anfitrión 1700 o datos generados por el anfitrión 1700 para un UE. Las realizaciones del anfitrión 1700 pueden utilizar solo un subconjunto o todos los componentes mostrados. Los programas de aplicación de anfitrión 1714 pueden implementarse en una arquitectura basada en contenedores y pueden proporcionar soporte para códecs de vídeo (por ejemplo, Codificación de Vídeo Versátil (VVC), Codificación de Vídeo de Alta Eficiencia (HEVC), Codificación de Vídeo Avanzada (AVC), MPEG, VP9) y códecs de audio (por ejemplo, FLAC, Codificación de Audio Avanzada (AAC), MPEG, G.711), incluyendo la transcodificación para múltiples clases, tipos o implementaciones diferentes de los UE (por ejemplo, teléfonos, computadores de escritorio, sistemas de visualización portátiles, sistemas de visualización frontal). Los programas de aplicación de anfitrión 1714 también pueden proporcionar autenticación de usuario y verificaciones de licencia y pueden informar periódicamente el estado, las rutas y la disponibilidad de contenido a un nodo central, tal como un dispositivo dentro o en el borde de una red central. En consecuencia, el servidor 1700 puede seleccionar y/o indicar un servidor diferente para servicios over-the-top para un UE. Los programas de aplicación anfitriona 1714 pueden soportar varios protocolos, tales como el protocolo HTTP Live Streaming (HLS), el Protocolo de Mensajería en Tiempo Real (RTMP), el

Protocolo de Transmisión en Tiempo Real (RTSP), el Streaming Adaptativo Dinámico sobre HTTP (MPEG-DASH), etc.

La Figura 18 es un diagrama de bloques que ilustra un entorno de virtualización 1800 en el que se pueden virtualizar funciones implementadas por algunas realizaciones. En el presente contexto, virtualizar significa crear versiones virtuales de aparatos o dispositivos que pueden incluir la virtualización de plataformas de hardware, dispositivos de almacenamiento y recursos de red. Como se usa en el presente documento, la virtualización se puede aplicar a cualquier dispositivo descrito en el presente documento, o componentes del mismo, y se relaciona con una implementación en la que al menos una parte de la funcionalidad se implementa como uno o más componentes virtuales. Algunas o todas las funciones descritas en el presente documento pueden implementarse como componentes virtuales ejecutados por una o más máquinas virtuales (VM) implementadas en uno o más entornos virtuales 1800 alojados por uno o más nodos de hardware, tal como un dispositivo de cómputo de hardware que opera como un nodo de red, UE, nodo de red central o anfitrión. Además, en realizaciones en las que el nodo virtual no requiere conectividad de radio (por ejemplo, un nodo o anfitrión de red central), entonces el nodo puede estar completamente virtualizado.

Las aplicaciones 1802 (que alternativamente pueden denominarse instancias de software, dispositivos virtuales, funciones de red, nodos virtuales, funciones de red virtual, etc.) se ejecutan en el entorno de virtualización Q400 para implementar algunas de las características, funciones y/o beneficios de algunas de las realizaciones descritas en el presente documento.

El hardware 1804 incluye circuitos de procesamiento, memoria que almacena software y/o instrucciones ejecutables mediante circuitos de procesamiento de hardware y/u otros dispositivos de hardware como se describe en el presente documento, tales como una interfaz de red, una interfaz de entrada/salida, etc. Los circuitos de procesamiento pueden ejecutar software para crear instancias de una o más capas de virtualización 1806 (también denominadas hipervisores o monitores de máquinas virtuales (VMM)), proporcionar VM 1808a y 1808b (una o más de las cuales pueden denominarse generalmente VM 1808), y/o realizar cualquiera de las funciones, características y/o beneficios descritos en relación con algunas realizaciones descritas en el presente documento. La capa de virtualización 1806 puede presentar una plataforma operativa virtual que aparece como hardware de red para las VM 1808.

Las VM 1808 comprenden procesamiento virtual, memoria virtual, red o interfaz virtual y almacenamiento virtual, y pueden ejecutarse mediante una capa de virtualización correspondiente 1806. Se pueden implementar diferentes realizaciones de la instancia de un dispositivo virtual 1802 en una o más VM 1808, y las implementaciones se pueden realizar de diferentes maneras. La virtualización del hardware se denomina en algunos contextos

virtualización de funciones de red (NFV). La NFV se puede utilizar para consolidar muchos tipos de equipos de red en hardware de servidor de alto volumen estándar de la industria, conmutadores y almacenamiento físicos, que se pueden ubicar en centros de datos y equipos en las instalaciones del cliente.

5 En el contexto de NFV, una VM 1808 puede ser una implementación de software de una máquina física que ejecuta programas como si se estuvieran ejecutando en una máquina física no virtualizada. Cada una de las VM 1808, y esa parte del hardware 1804 que ejecuta esa VM, ya sea hardware dedicado a esa VM y/o hardware compartido por esa VM con otras VM, forma elementos de red virtual separados. Aún en el contexto de NFV, una función de red virtual es
10 responsable de manejar funciones de red específicas que se ejecutan en una o más VM 1808 sobre el hardware 1804 y corresponde a la aplicación 1802.

 El hardware 1804 puede implementarse en un nodo de red independiente con componentes genéricos o específicos. El hardware 1804 puede implementar algunas funciones mediante virtualización. Alternativamente, el hardware 1804 puede ser parte de un grupo más
15 grande de hardware (por ejemplo, como en un centro de datos o CPE) donde muchos nodos de hardware trabajan juntos y se administran a través de la administración y orquestación 1810, que, entre otras cosas, supervisa la administración del ciclo de vida de las aplicaciones 1802. En algunas realizaciones, el hardware 1804 está acoplado a una o más unidades de radio, cada una de las cuales incluye uno o más transmisores y uno o más receptores que pueden estar
20 acoplados a una o más antenas. Las unidades de radio pueden comunicarse directamente con otros nodos de hardware a través de una o más interfaces de red apropiadas y pueden usarse en combinación con los componentes virtuales para proporcionar un nodo virtual con capacidades de radio, tal como un nodo de acceso de radio o una estación base. En algunas realizaciones, se puede proporcionar alguna señalización con el uso de un sistema de control
25 1812 que se puede usar alternativamente para la comunicación entre nodos de hardware y unidades de radio.

 Aunque los dispositivos de cómputo descritos en el presente documento (por ejemplo, UE, nodos de red, anfitriones) pueden incluir la combinación ilustrada de componentes de hardware, otras realizaciones pueden comprender dispositivos de cómputo con diferentes
30 combinaciones de componentes. Debe entenderse que estos dispositivos de cómputo pueden comprender cualquier combinación adecuada de hardware y/o software necesario para realizar las tareas, características, funciones y métodos aquí descritos. La determinación, el cálculo, la obtención u operaciones similares descritas en el presente documento se pueden realizar mediante circuitos de procesamiento, que pueden procesar información, por ejemplo,
35 convirtiendo la información obtenida en otra información, comparando la información obtenida o

la información convertida con información almacenada en el nodo de red, y /o realizando una o más operaciones con base en la información obtenida o información convertida, y como resultado de dicho procesamiento tomar una determinación. Además, si bien los componentes se representan como cajas individuales ubicadas dentro de una caja más grande, o anidadas dentro de múltiples cajas, en la práctica, los dispositivos de cómputo pueden comprender múltiples componentes físicos diferentes que forman un único componente ilustrado, y la funcionalidad puede dividirse entre componentes separados. Por ejemplo, se puede configurar una interfaz de comunicación para incluir cualquiera de los componentes descritos en el presente documento, y/o la funcionalidad de los componentes se puede dividir entre los circuitos de procesamiento y la interfaz de comunicación. En otro ejemplo, se pueden implementar funciones no intensivas desde el punto de vista computacional de cualquiera de dichos componentes en software o firmware y se pueden implementar funciones computacionalmente intensivas en hardware.

En determinadas realizaciones, parte o toda la funcionalidad descrita en el presente documento puede proporcionarse por circuitos de procesamiento que ejecutan instrucciones almacenadas en la memoria, que en determinadas realizaciones puede ser un producto de programa de computador en forma de un medio de almacenamiento no transitorio legible por computador. En realizaciones alternativas, parte o la totalidad de la funcionalidad se puede proporcionar mediante circuitos de procesamiento sin ejecutar instrucciones almacenadas en un medio de almacenamiento legible por dispositivo separado o discreto, tal como de manera cableada. En cualquiera de esas realizaciones particulares, ya sea que se ejecuten instrucciones almacenadas en un medio de almacenamiento no transitorio legible por computador o no, los circuitos de procesamiento se pueden configurar para realizar la funcionalidad descrita. Los beneficios proporcionados por dicha funcionalidad no se limitan solo a los circuitos de procesamiento ni a otros componentes del dispositivo de cómputo, sino que los disfruta el dispositivo cómputo en su conjunto y/o los usuarios finales y una red inalámbrica en general.

Algunas realizaciones de ejemplo de las técnicas y aparatos descritos en el presente documento incluyen, entre otros, los siguientes ejemplos:

Realizaciones del Grupo A

A1. Un método realizado por un servidor de autenticación en una red de comunicación inalámbrica, comprendiendo el método:

iniciar la autenticación primaria de un dispositivo de comunicación inalámbrica con un servidor de autenticación externa que es externo a la red de comunicación inalámbrica;

recibir señalización que indica que la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa tuvo éxito y

que incluye un identificador afirmado por el servidor de autenticación externa que identifica como auténtico el dispositivo de comunicación inalámbrica; y autenticar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en el identificador incluido en la señalización recibida.

5
A2. El método de la realización A1, caracterizado porque dicha iniciación comprende iniciar la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa utilizando un identificador anónimo que no identifica el dispositivo de comunicación inalámbrica.

10
A3. El método de la realización A2, caracterizado porque el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

A4. El método de cualquiera de las realizaciones A1-A3, caracterizado porque el identificador
15 incluido en la señalización recibida es un identificador no-anónimo.

A5. El método de la realización A4, caracterizado porque el identificador no-anónimo es un SUPI no-anónimo.

20
A6. El método de cualquiera de las realizaciones A1-A4, caracterizado porque el identificador incluido en la señalización recibida es un identificador público que identifica el dispositivo de comunicación inalámbrica ante una red externa a la red de comunicación inalámbrica.

A7. El método de la realización A6, caracterizado porque el identificador público es un
25 Identificador de Suscripción Pública Genérico, GPSI.

A8. El método de cualquiera de las realizaciones A6-A7, que comprende además traducir o solicitar la traducción del identificador público a un identificador que identifica el dispositivo de comunicación inalámbrica en la red de comunicación inalámbrica.

30
A9. El método de cualquiera de las realizaciones A1-A8, caracterizado porque el identificador incluido en la señalización recibida es, o está asociado con, un identificador autenticado basándose en el cual el servidor de autenticación externa autenticó el dispositivo de comunicación inalámbrica a través de la autenticación primaria.

35

A10. El método de la realización A9, caracterizado porque el identificador autenticado es una Identidad del Protocolo de Autenticación Extensible, EAP.

A11. El método de cualquiera de las realizaciones A1-A10, caracterizado porque dicha iniciación comprende iniciar la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa utilizando un identificador presentado que el dispositivo de comunicación inalámbrica ha presentado como identificación del dispositivo de comunicación inalámbrica a la red de comunicación inalámbrica, y caracterizado porque autenticar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basándose en el identificador incluido en la señalización recibida comprende confirmar que el identificador presentado corresponde al identificador incluido en la señalización recibida.

A12. El método de cualquiera de las realizaciones A1-A11, en donde la autenticación primaria se inicia como parte de un procedimiento para registrar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica, y en donde el método comprende además registrar el dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica basado en la autenticación exitosa del dispositivo de comunicación inalámbrica con la red de comunicación inalámbrica.

A13. El método de cualquiera de las realizaciones A1-A12, caracterizado porque la red de comunicación inalámbrica es una red no pública independiente.

A14. El método de cualquiera de las realizaciones A1-A13, caracterizado porque el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

Realizaciones del Grupo B

B1. Un método realizado por un servidor de autenticación externa para una red de comunicación inalámbrica, comprendiendo el método:

realizar la autenticación primaria de un dispositivo de comunicación inalámbrica con el servidor de autenticación externa para el acceso del dispositivo de comunicación inalámbrica a la red de comunicación inalámbrica; y
transmitir, a un servidor de autenticación en la red de comunicación inalámbrica, una señalización que indica que la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa tuvo éxito y que incluye un identificador afirmado por el servidor de autenticación externa que

identifica como auténtico el dispositivo de comunicación inalámbrica.

5 B2. El método de la realización B1, que comprende además recibir señalización que activa el servidor de autenticación externa para realizar la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa, caracterizado porque la señalización incluye un identificador anónimo para el dispositivo de comunicación inalámbrica.

10 B3. El método de la realización B2, caracterizado porque el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

B4. El método de cualquiera de las realizaciones B1-B3, caracterizado porque el identificador incluido en la señalización transmitida es un identificador no-anónimo.

15 B5. El método de la realización B4, caracterizado porque el identificador no-anónimo es un SUPI no-anónimo.

20 B6. El método de cualquiera de las realizaciones B1-B4, caracterizado porque el identificador incluido en la señalización transmitida es un identificador público que identifica el dispositivo de comunicación inalámbrica ante una red externa a la red de comunicación inalámbrica.

B7. El método de la realización B6, caracterizado porque el identificador público es un Identificador de Suscripción Pública Genérico, GPSI.

25 B8. El método de cualquiera de las realizaciones B1-B7, caracterizado porque el identificador incluido en la señalización transmitida es, o está asociado con, un identificador autenticado basándose en el cual el servidor de autenticación externa autenticó el dispositivo de comunicación inalámbrica a través de la autenticación primaria.

30 B9. El método de la realización B8, caracterizado porque el identificador autenticado es una Identidad del Protocolo de Autenticación Extensible, EAP.

B10. El método de cualquiera de las realizaciones B1-B9, caracterizado porque la red de comunicación inalámbrica es una red no pública independiente.

35 B11. El método de cualquiera de las realizaciones B1-B10, caracterizado porque el servidor de

autenticación implementa una Función de Servidor de Autenticación, AUSF.

Realizaciones del Grupo C

- 5 C1. Un método realizado por un nodo de red en una red de comunicación inalámbrica, comprendiendo el método:
- recibir, desde un servidor de autenticación en la red de comunicación inalámbrica, una solicitud de autenticación primaria de un dispositivo de comunicación inalámbrica con un servidor de autenticación externa para el acceso del dispositivo de comunicación inalámbrica a la red de comunicación inalámbrica; y
- 10 transmitir, al servidor de autenticación en la red de comunicación inalámbrica, una respuesta que indica que la autenticación primaria del dispositivo de comunicación inalámbrica con el servidor de autenticación externa tuvo éxito y que incluye un identificador afirmado por el servidor de autenticación externa que identifica como auténtico el dispositivo de comunicación inalámbrica.
- 15
- C2. El método de la realización C1, caracterizado porque la solicitud incluye un identificador anónimo para el dispositivo de comunicación inalámbrica.
- C3. El método de la realización C2, caracterizado porque el identificador anónimo es un
- 20 Identificador Permanente de Suscripción, SUPI, anónimo.
- C4. El método de cualquiera de las realizaciones C1-C3, caracterizado porque el identificador incluido en la señalización transmitida es un identificador no-anónimo.
- 25 C5. El método de la realización C4, caracterizado porque el identificador no-anónimo es un SUPI no-anónimo.
- C6. El método de cualquiera de las realizaciones C1-C4, caracterizado porque el identificador incluido en la señalización transmitida es un identificador público que identifica el dispositivo de
- 30 comunicación inalámbrica ante una red externa a la red de comunicación inalámbrica.
- C7. El método de la realización C6, caracterizado porque el identificador público es un Identificador de Suscripción Pública Genérico, GPSI.
- 35 C8. El método de cualquiera de las realizaciones C1-C7, caracterizado porque el identificador

incluido en la señalización transmitida es, o está asociado con, un identificador autenticado basándose en el cual el servidor de autenticación externa autenticó el dispositivo de comunicación inalámbrica a través de la autenticación primaria.

- 5 C9. El método de la realización C8, caracterizado porque el identificador autenticado es una Identidad del Protocolo de Autenticación Extensible, EAP.

C10. El método de cualquiera de las realizaciones C1-C9, caracterizado porque la red de comunicación inalámbrica es una red no pública independiente.

- 10 C11. El método de cualquiera de las realizaciones C1-C10, caracterizado porque el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

- C12. El método de cualquiera de las realizaciones C1-C11, caracterizado porque el nodo de red
15 implementa una Función de Autorización y Autenticación Específica del Segmento de Red, NSSAAF.

Realizaciones del Grupo D

- 20 D1. Un método realizado por un nodo de red en una red de comunicación inalámbrica, comprendiendo el método:

recibir, desde un servidor de autenticación en la red de comunicación inalámbrica, una solicitud de datos de autenticación para un dispositivo de comunicación inalámbrica; y

- 25 transmitir, al servidor de autenticación, una respuesta que indica que la autenticación primaria del dispositivo de comunicación inalámbrica se ejecutará con un servidor de autenticación externa que es externo a la red de comunicación inalámbrica y que incluye un identificador que se presentará al servidor de autenticación externa.

- 30 D2. El método de la realización D1, caracterizado porque el identificador incluido en la respuesta es un identificador anónimo para el dispositivo de comunicación inalámbrica.

D3. El método de la realización D2, caracterizado porque el identificador anónimo es un Identificador Permanente de Suscripción, SUPI, anónimo.

D4. El método de cualquiera de las realizaciones D1-D3, caracterizado porque el identificador incluido en la respuesta es un identificador público que identifica el dispositivo de comunicación inalámbrica ante una red externa a la red de comunicación inalámbrica.

5 D5. El método de la realización D4, caracterizado porque el identificador público es un Identificador de Suscripción Pública Genérico, GPSI.

D6. El método de cualquiera de las realizaciones D1-D5, caracterizado porque la solicitud incluye un identificador anónimo para el dispositivo de comunicación inalámbrica.

10 D7. El método de la realización D6, que comprende además decidir, basándose en una parte del dominio del identificador anónimo, que la autenticación primaria del dispositivo de comunicación inalámbrica se ejecutará con el servidor de autenticación externa a la red de comunicación inalámbrica.

15 D8. El método de cualquiera de las realizaciones D1-D7, caracterizado porque la red de comunicación inalámbrica es una red no pública independiente.

20 D9. El método de cualquiera de las realizaciones D1-D8, caracterizado porque el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

DD1. Un método realizado por un nodo de red en una red de comunicación inalámbrica, comprendiendo el método:

25 recibir una solicitud para traducir un identificador público, que identifica el dispositivo de comunicación inalámbrica en una red externa a la red de comunicación inalámbrica, a un identificador no público que identifica el dispositivo de comunicación inalámbrica en la red de comunicación inalámbrica;
traducir el identificador público al identificador no público; y
transmitir una respuesta que incluye el identificador no público.

30 DD2. El método de la realización DD2, caracterizado porque el identificador público es un Identificador de Suscripción Pública Genérico, GPSI.

35 DD3. El método de cualquiera de las realizaciones DD1-DDD2, caracterizado porque el identificador no público es un Identificador Permanente de Suscripción, SUPI.

DD4. El método de cualquiera de las realizaciones DD1-DD2, caracterizado porque la red de comunicación inalámbrica es una red no pública independiente.

- 5 DD5. El método de cualquiera de las realizaciones DD1-DD4, caracterizado porque la solicitud se recibe desde un servidor de autenticación.

DD6. El método de la realización DD5, caracterizado porque el servidor de autenticación implementa una Función de Servidor de Autenticación, AUSF.

10

Realizaciones del Grupo E

E1. Un servidor de autenticación configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo A.

- 15 E2. Un servidor de autenticación que comprende circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo A.

E3. Un servidor de autenticación que comprende:

circuitos de comunicación; y

- 20 circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo A.

E4. Un servidor de autenticación que comprende:

circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo A;

- 25 circuitos de suministro de energía configurados para suministrar energía al servidor de autenticación.

E5. Un servidor de autenticación que comprende:

30 circuitos de procesamiento y memoria, donde la memoria contiene instrucciones ejecutables por los circuitos de procesamiento mediante los cuales el servidor de autenticación es configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo A.

- 35 E6. Un programa de computador que comprende instrucciones que, cuando las ejecuta al

menos un procesador de un servidor de autenticación, hace que el servidor de autenticación lleve a cabo los pasos de cualquiera de las realizaciones del Grupo A.

5 E7. Una portadora que contiene el programa de cómputo de la realización E6, caracterizado porque la portadora es una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por computador.

10 E8. Un servidor de autenticación externo configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo B.

E9. Un servidor de autenticación externa que comprende circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo B.

15 E10. Un servidor de autenticación externa que comprende:
circuitos de comunicación; y
circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo B.

20 E11. Un servidor de autenticación externa que comprende:
circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo B;
circuitos de suministro de energía configurados para suministrar energía al servidor de autenticación externa.

25 E12. Un servidor de autenticación externa que comprende:
circuitos de procesamiento y memoria, donde la memoria contiene instrucciones ejecutables por los circuitos de procesamiento mediante los cuales el servidor de autenticación externa es configurado para realizar cualquiera de los pasos de
30 cualquiera de las realizaciones del Grupo B.

E13. Un programa de computador que comprende instrucciones que, cuando las ejecuta al menos un procesador de un servidor de autenticación, hacen que el servidor de autenticación externa lleve a cabo los pasos de cualquiera de las realizaciones del Grupo B.

35

E14. Una portadora que contiene el programa de cómputo de la realización E13, caracterizado porque la portadora es una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por computador.

5 E15. Un nodo de red configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo C o del Grupo D.

E16. Un nodo de red que comprende circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo C o del Grupo D.

10

E17. Un nodo de red que comprende:

circuitos de comunicación; y

circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo C o del Grupo D.

15

E18. Un nodo de red que comprende:

circuitos de procesamiento configurados para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo C o del Grupo D;

circuitos de suministro de energía configurados para suministrar energía al nodo de red.

20

E19. Un nodo de red que comprende:

circuitos de procesamiento y memoria, donde la memoria contiene instrucciones ejecutables por los circuitos de procesamiento mediante los cuales el nodo de red es configurado para realizar cualquiera de los pasos de cualquiera de las realizaciones del Grupo C o del Grupo D.

25

E20. Un programa de computador que comprende instrucciones que, cuando las ejecuta al menos un procesador de un nodo de red, hace que el nodo de red lleve a cabo los pasos de cualquiera de las realizaciones del Grupo C o del Grupo D.

30

E21. Una portadora que contiene el programa de cómputo de la realización E20, caracterizado porque la portadora es una señal electrónica, una señal óptica, una señal de radio o un medio de almacenamiento legible por computador.

35