

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 980 203**

51 Int. Cl.:

H04W 12/00 (2011.01)
H04W 12/04 (2011.01)
H04W 4/80 (2008.01)
H04W 84/12 (2009.01)
H04W 12/43 (2011.01)
H04W 12/50 (2011.01)
H04L 9/40 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 86 Fecha de presentación y número de la solicitud internacional: **29.08.2019** **PCT/EP2019/073029**
87 Fecha y número de publicación internacional: **05.03.2020** **WO20043809**
96 Fecha de presentación y número de la solicitud europea: **29.08.2019** **E 19758764 (5)**
97 Fecha y número de publicación de la concesión europea: **03.04.2024** **EP 3844930**

54 Título: **Acceso a dispositivos no 3GPP a la red central**

30 Prioridad:

30.08.2018 EP 18191757

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
30.09.2024

73 Titular/es:

KONINKLIJKE PHILIPS N.V. (100.0%)
High Tech Campus 52
5656 AG Eindhoven, NL

72 Inventor/es:

BERNSEN, JOHANNES, ARNOLDUS, CORNELIS
y
DEES, WALTER

74 Agente/Representante:

ISERN JARA, Jorge

ES 2 980 203 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Acceso a dispositivos no 3GPP a la red central

5 Campo de la invención

La invención se refiere a un dispositivo sin identidad de abonado, sin SI, dispuesto para la comunicación inalámbrica en una red local de acuerdo con un protocolo de comunicación local. La invención también se refiere a un dispositivo de identidad de abonado, SI, y a procedimientos para su uso en un sistema SI.

10 La presente invención se refiere al campo de la integración de dispositivos de comunicación inalámbrica local en al menos sistemas de comunicación móvil de área regional, también llamados redes centrales, por ejemplo, redes 3G, LTE, 4G o 5G. El acceso a las redes centrales es gestionado por los llamados proveedores, que proporcionan acceso a las redes centrales para dispositivos móviles de abonados utilizando un conjunto de datos de abonado llamado identidad de abonado SI. La SI comprende datos de identidad de abonado para acceder a una red central, para un respectivo abonado al proveedor.

En general, dichos dispositivos de comunicación inalámbrica local están equipados para la comunicación inalámbrica de acuerdo con un protocolo de comunicación local, como Wi-Fi, y no tienen una unidad transceptora para la comunicación inalámbrica con una red central. Por ejemplo, en el llamado Internet de las Cosas, varios tipos de dispositivos de comunicación inalámbrica local pueden conectarse a Internet a través de Wi-Fi, por ejemplo, los dispositivos sin cabeza, que no tienen una interfaz de usuario, o los dispositivos con interfaz de usuario (UI), que cuentan con una pantalla táctil, un visualizador y/o botones. Entonces, al menos inicialmente, dichos dispositivos no tienen ningún dato de identidad de abonado o credenciales que se requieran para acceder a una red central. En este documento, se denominan dispositivos de comunicación inalámbrica local sin SI a dichos dispositivos.

La integración de dispositivos sin SI en las redes centrales se está discutiendo actualmente entre varias partes llamadas 3GPP, que definen nuevas generaciones y extensiones de las redes centrales existentes. El Proyecto de Asociación de Tercera Generación (3GPP) es una colaboración entre grupos de asociaciones de estándares de telecomunicaciones, conocidos como los Socios Organizativos. 3GPP propone varios mecanismos para permitir que un dispositivo móvil, en términos de 3GPP llamado UE o Equipo de Usuario, acceda a la red celular central utilizando una red de acceso no 3GPP, como Wi-Fi, por ejemplo, para descargar el tráfico celular en otras redes de acceso. El acceso no 3GPP a una red central 4G, llamada Núcleo de paquete evolucionado o EPC, se especifica, entre otros, en las especificaciones 3GPP: [TS 23.402] (última versión 15.3.0), [TS 24.302] (última versión 15.3.0) y [TS 33.402] (última versión 15.1.0). El acceso no 3GPP a la red central 5G se especifica, entre otros, en las especificaciones de 3GPP: [TS 23.501] (última versión 15.2.0) sección 4.2.8, [TS 23.502] (última versión 15.2.0) sección 4.12 y [TS 24.502] (última versión 15.0.0). Actualmente, el trabajo se centra en el soporte de dispositivos no 3GPP detrás de una puerta de enlace residencial (RG), pero esto podría extenderse a un soporte más genérico de dispositivos no 3GPP, dada la demanda de los operadores celulares 5G de incorporar Wi-Fi como parte de su oferta de red 5G y utilizar sus servicios (como voz por Wi-Fi con medición, servicios de vídeo en vivo, etc.).

Comúnmente, los dispositivos móviles como los teléfonos inteligentes están equipados con un transceptor dedicado para la comunicación con una red central y además cuentan con una identidad de abonado, SI. La SI representa la identidad de un abonado y los datos adicionales necesarios para acceder a la red principal, mientras que el uso de la red principal se factura al abonado correspondiente por parte del proveedor, por ejemplo, a través de un denominado paquete de voz y datos. Por ejemplo, la SI puede comprender un código de identidad de abonado como IMSI (Identidad Internacional de Abonado Móvil). Estos dispositivos generalmente se suministran con la SI al insertar un módulo físico de semiconductores llamado SIM en el dispositivo móvil. Una tarjeta SIM es un circuito integrado incrustado en una tarjeta de plástico que tiene como objetivo almacenar de forma segura el número de identidad internacional del abonado móvil (IMSI) y sus claves relacionadas, las cuales se utilizan para identificar y autenticar a los abonados en dispositivos de telefonía móvil (como teléfonos móviles y ordenadores). Se conocen varios tipos de módulos o tarjetas, por ejemplo, USIM que se refiere al Módulo de Identidad del Abonado Universal y funciona en el Sistema Universal de Telecomunicaciones Móviles (UMTS), que es un estándar de red central de 3G. La tarjeta física relacionada también se conoce como UICC (Tarjeta de Circuito Integrado Universal) y USIM es una aplicación que se ejecuta sobre UICC. Un tipo adicional de SIM se llama e-SIM o eSIM (SIM incorporada) o tarjeta de circuito integrado universal incorporada (eUICC). Es un chip incorporado no reemplazable que se suelda directamente en una placa de circuito. Por ahora, cualquier tipo de dispositivo que esté equipado para la comunicación inalámbrica con una red central y esté provisto de una SI original, ya sea a través de una tarjeta SIM o de otra manera, se denomina dispositivo SIM en este documento.

Además, los datos de SI también pueden estar disponibles en otros lugares como un sistema de gestión del proveedor de la red principal, por ejemplo, en una base de datos de abonados en un servidor que gestiona los datos de identidad de abonado, mientras que las credenciales del abonado pueden ser autenticadas y autorizadas utilizando un servidor de autorización, generalmente llamado una autoridad de certificación, CA. Por ejemplo, los datos de la SI también pueden ser accedidos por el abonado al iniciar sesión en una cuenta de usuario en un servidor de aplicaciones, AS, a través de internet utilizando credenciales de usuario como un nombre de usuario y

contraseña o utilizando una autorización de dos factores. El AS puede estar acoplado a, o puede comprender, la base de datos de abonados y la CA.

En este documento, un dispositivo SI, también conocido como dispositivo local, tiene acceso a la SI, ya sea que comprenda la SI o esté acoplado a al menos un servidor proveedor de la red central, el cual está diseñado para gestionar los datos del SI. El dispositivo SI está configurado para comunicarse con el dispositivo sin SI y tiene acceso a la CA. Un primer ejemplo de un dispositivo SI es un dispositivo SIM dispuesto para comunicarse a través de la red central con uno o más servidores que almacenan una base de datos de abonados y la CA, al mismo tiempo que también está dispuesto para comunicarse con el dispositivo sin SI. Un ejemplo adicional del dispositivo SI es un dispositivo de interfaz de usuario, UI, para comunicarse con el dispositivo sin SI, el cual está además diseñado para acceder a los datos SI y a la CA en servidores a través de la red central, y donde el propietario de la suscripción debe iniciar sesión para obtener acceso a los datos SI. Otro ejemplo es un dispositivo de interfaz de usuario (UI) dispuesto para comunicarse a través de la red local con el dispositivo sin SI, mientras que el dispositivo de interfaz de usuario se dispone además para acceder a los datos SI y a la CA en servidores a través de una conexión a internet. Un sistema SI puede incluir un sistema de gestión basado en servidor acoplado a un punto de acceso local para comunicación inalámbrica en una red local, y también el dispositivo SIM definido anteriormente o el dispositivo de interfaz de usuario acoplado adecuadamente a los servidores de datos respectivos de la red central.

Antecedentes de la invención

Un posible sistema y procedimiento para permitir que dispositivos no 3GPP se conecten a una red central 4G/5G es mediante el uso de Hotspot 2.0 (también conocido como Wi-Fi Certified Passpoint) según se define en la Especificación Técnica de Hotspot 2.0 [HOTSPOT], permitiendo a un operador equipar dispositivos con, por ejemplo, certificados X.509. Sin embargo, muchos dispositivos pueden no ser controlados por el operador, y no está claro cómo otros dispositivos básicos de solo Wi-Fi en los hogares de las personas pueden tener acceso a la red central 4G/5G.

El documento US9648019B2 describe la integración de Wi-Fi para dispositivos sin tarjeta SIM. El sistema propuesto permite que los dispositivos no 3GPP se conecten a una red central 4G/5G. Un Servidor de Aplicaciones (AS) puede ser utilizado para permitir que un dispositivo sin módulo de identidad de abonado (sin-SIM) acceda a una primera red (por ejemplo, una red móvil o 3GPP) a través de una segunda red (por ejemplo, Wi-Fi), donde el dispositivo sin SIM está asociado con un dispositivo SIM y donde el AS recibe, del dispositivo SIM, información sobre el dispositivo SIM y su dispositivo sin SIM asociado. La asociación entre el dispositivo SIM y el dispositivo sin SIM es creada por el AS en base a la información recibida del dispositivo SIM. La asociación entre un dispositivo sin SIM y un dispositivo con SIM se guarda en una base de datos de s.

Posteriormente, para acceder a la primera red a través de la segunda red, en base a una solicitud de autorización a la primera red desde el dispositivo sin SIM, el sistema obtiene la identidad asociada con el dispositivo sin SIM y transmite una solicitud de perfil de usuario asociado con un usuario del dispositivo sin SIM a la base de datos de s, la cual solicitud comprende la identidad obtenida para el dispositivo sin SIM. Entonces, el sistema recibe, desde la base de datos del Abonado, el perfil de usuario solicitado para el dispositivo sin SIM, estando el perfil de usuario solicitado para el dispositivo sin SIM asociado con un dispositivo SIM. Basado en el perfil de usuario recibido, el sistema autoriza al dispositivo sin SIM a acceder a la primera red a través de la segunda red. Entonces, después de que se haya establecido y almacenado la asociación entre el dispositivo sin SIM y el dispositivo con SIM en la base de datos del abonado, el dispositivo sin SIM puede obtener autorización para acceder a la primera red cuando desee acceder a ella.

En el documento US9648019B2, la descripción de la Figura 1b puede corresponder al documento [TS 23.402] de 3GPP, especialmente para el caso de no itinerancia de acuerdo con la Figura 4.2.2-1 y la Figura 4.2.2-2, así como la descripción de los nodos y enlaces mostrados en estas figuras y cómo utilizar estos nodos y enlaces en, por ejemplo, la Cláusula 7 de [TS 23.402]. La Figura 4.2.3-1 hasta la Figura 4.2.3-5 de [TS 23.402] muestra el caso de itinerancia. El dispositivo sin SIM puede acceder a la primera red a través del nodo "Acceso IP No-3GPP Confiable" o el nodo "Acceso IP No-3GPP No Confiable".

Resumen de la invención

En el documento US9648019B2 no se explica cómo el dispositivo SIM obtiene de manera confiable la identidad del dispositivo sin SIM o cómo el dispositivo SIM puede obtener confianza en una identidad obtenida. La falta de confianza puede abrir el camino para que los atacantes obtengan acceso a sus dispositivos en la red móvil o 3GPP al [mal]usar el dispositivo SIM. Además, después de que se haya establecido la asociación entre el dispositivo sin SIM y el dispositivo SIM, el dispositivo sin SIM puede operar de forma independiente al dispositivo SIM. Dado que el dispositivo sin tarjeta SIM puede ser más vulnerable a los ataques informáticos, las credenciales que permiten al dispositivo sin tarjeta SIM conectarse a la red celular central podrían ser robadas, después de lo cual un hacker podría utilizar esta información para acceder a la red central y cargar la suscripción del usuario del dispositivo con tarjeta SIM.

Es un objetivo de la invención proporcionar un sistema para establecer de manera confiable el acceso inalámbrico a una red central para un dispositivo sin SI.

Con este propósito, se proporcionan dispositivos y procedimientos tal como se definen en las reivindicaciones adjuntas. De acuerdo con un aspecto de la invención, se proporciona un dispositivo sin SI como se define en la reivindicación 1. De acuerdo con otro aspecto de la invención, se proporciona un dispositivo SI según se define en la reivindicación 9. De acuerdo con otro aspecto de la invención, se proporcionan procedimientos según se definen en las reivindicaciones 14 y 15. De acuerdo con otro aspecto de la invención, se proporciona un producto de programa informático descargable desde una red y/o almacenado en un medio legible por ordenador y/o medio ejecutable por microprocesador, el producto comprende instrucciones de código de programa para implementar el procedimiento anterior cuando se ejecuta en un ordenador.

El dispositivo sin SI anterior está configurado para la comunicación inalámbrica en una red local de acuerdo con un protocolo de comunicación local. El protocolo de comunicación local define mensajes de protocolo y transmisión-recepción inalámbrica en un área limitada. Una identidad de abonado, SI, comprende datos de identidad de abonado de un abonado para acceder a una red central, la cual proporciona comunicación inalámbrica para dispositivos móviles a través de al menos un área regional. El dispositivo no perteneciente a la SI no comprende la SI y está dispuesto para cooperar con un dispositivo SI que tiene acceso a la SI. El dispositivo sin SI comprende un transceptor dispuesto para la transmisión-recepción local de acuerdo con el protocolo de comunicación local y un procesador dispuesto para ejecutar una secuencia de asociación para establecer una asociación con la SI. La secuencia de asociación comprende almacenar una clave privada sin SI que constituye un par con una clave pública sin SI, proporcionar la clave pública sin SI al dispositivo SI a través de un primer canal de comunicación y compartir un código de verificación con el dispositivo SI a través de un segundo canal de comunicación para verificar que el dispositivo SI ha obtenido la clave pública sin SI. El primer y segundo canal de comunicación son diferentes y comprenden, como un solo canal, un canal fuera de banda, OOB. La secuencia de asociación además comprende proporcionar prueba de posesión de la clave privada sin SI al dispositivo SI a través del primer o segundo canal de comunicación, y posteriormente recibir, del dispositivo SI, datos de seguridad.

Los datos de seguridad comprenden datos relacionados con la SI, comúnmente llamados credenciales. Los datos de seguridad son generados en nombre del proveedor utilizando la clave pública sin SI. En este contexto, los datos de seguridad constituyen una prueba validada de que el propietario de los datos de seguridad tiene derechos para utilizar la red central en base a credenciales relacionadas con la SI.

Los datos de seguridad pueden, por ejemplo, incluir una firma tradicional sobre al menos parte de la clave pública sin SI, generada por la CA, e incluye credenciales relacionadas con la SI que pueden, al menos en parte, estar cifradas utilizando la clave pública sin SI. Por ejemplo, las credenciales pueden ser una combinación de nombre de usuario/contraseña o solo una contraseña, mientras que al menos la contraseña está cifrada y el nombre de usuario puede permanecer sin cifrar. El dispositivo sin SI puede verificar los datos de seguridad, por ejemplo, verificando que la firma proviene de la CA o descifrando credenciales cifradas con la clave privada sin SI.

Las credenciales pueden haber sido generadas anteriormente a través de un servidor de aplicaciones, la CA y/o una base de datos de s, y pueden ser almacenadas, por ejemplo, en la base de datos de s. Para constituir los datos de seguridad, las credenciales pueden ser recuperadas por la CA y al menos parcialmente cifradas con la clave pública sin SI antes de ser enviadas al dispositivo SI. Las credenciales permiten que el dispositivo sin SI acceda a la red principal a través de la red local y una puerta de enlace entre la red local y la red principal. Las credenciales cifradas constituyen datos de seguridad y proporcionan seguridad, ya que el dispositivo sin SI es el único dispositivo que conoce la clave privada sin SI. Entonces, el dispositivo sin SI es el único dispositivo que puede utilizar los datos de seguridad y descifrar las credenciales para acceder a la red principal. Además, el cifrado de al menos algunas credenciales con la clave pública sin SI no excluye el uso de otras claves para cifrar credenciales.

Después de verificar los datos de seguridad, las credenciales, después de descifrar las partes cifradas, permiten que el dispositivo sin SI acceda a la red central a través de la red local y una puerta de enlace entre la red local y la red central.

La secuencia de asociación anterior también puede implementarse en un procedimiento para su uso en un dispositivo sin SI, por ejemplo, en software en una aplicación llamada app.

El dispositivo SI anterior está configurado para la comunicación inalámbrica con el dispositivo sin SI anterior. El dispositivo SI tiene acceso a los datos de identidad de abonado, por ejemplo, porque el dispositivo contiene o puede acoplarse a una tarjeta SIM, o está dispuesto para acceder, a través de una red, a un servidor que contiene la SI. El dispositivo SI comprende un transceptor dispuesto para la comunicación inalámbrica con el dispositivo sin SI, y un procesador dispuesto para ejecutar una secuencia de asociación para establecer una asociación con la SI. La secuencia de asociación en el dispositivo SI comprende recibir una clave pública sin SI del dispositivo sin SI a través del primer canal de comunicación, y compartir un código de verificación con el dispositivo sin SI a través del segundo canal de comunicación. La secuencia de asociación en el dispositivo SI además comprende recibir, a través del primer o segundo canal de comunicación, una prueba de posesión de una clave privada sin SI que constituye un par

con la clave pública sin SI del dispositivo sin SI. Tras una exitosa evaluación de la prueba recibida, la secuencia de asociación continúa obteniendo los datos de seguridad mencionados anteriormente y transmitiéndolos al dispositivo sin SI. Esta secuencia de asociación también puede ser implementada en un procedimiento para su uso en un dispositivo SI.

Las características anteriores tienen los siguientes efectos. En el dispositivo sin SI, la clave privada sin SI debe estar disponible para su uso durante la ejecución de la secuencia de asociación en base a la clave pública sin SI emparejada. Entonces, el procesador puede acceder a una memoria donde la clave ya está almacenada, o puede generar primero u obtener de otra manera un par de claves, mientras que la clave privada sin SI se almacena posteriormente para su uso durante la secuencia de asociación.

La clave pública sin SI se transfiere al dispositivo SI a través de un primer canal de comunicación, mientras que el código de verificación se comparte con el dispositivo SI a través de un segundo canal de comunicación diferente para verificar que el dispositivo SI ha obtenido la clave pública sin SI. Entonces, el dispositivo sin SI está dispuesto para establecer dichos primer y segundo canales de comunicación con el dispositivo SI, los cuales incluyen un canal OOB y se configuran de forma independiente. En este contexto, un canal de comunicación es una conexión de datos a través de un mecanismo físico como la transmisión de radio o información visual que se muestra y escanea o códigos leídos y comparados por un usuario, o un código leído e ingresado manualmente por un usuario, o códigos ingresados manualmente en ambos dispositivos. Cada canal transfiere datos entre los puntos finales del canal, en este caso el dispositivo sin SI y el sistema SI. Un canal puede ser, por ejemplo, un canal inalámbrico creado a través de la red de comunicación local mediante el intercambio de mensajes de protocolo entre el dispositivo sin SI y el dispositivo SI. Otro ejemplo es un canal inalámbrico que no utiliza la red de comunicación local, sino algún otro protocolo de comunicación inalámbrica como Bluetooth o una red Wi-Fi separada. El otro canal es un canal fuera de banda, OOB, con respecto al mencionado canal inalámbrico que utiliza una banda de frecuencia para la transmisión de radio. Entonces, el canal OOB está utilizando un mecanismo físico diferente al de dicho canal inalámbrico, por ejemplo, visual o ingresando datos manualmente por parte del usuario. Al menos uno de los canales se crea mediante un mecanismo físico que tiene un rango limitado para permitir al usuario verificar que el dispositivo sin SI destinado a ser integrado se encuentra dentro de ese rango limitado desde el dispositivo SI que constituye el punto final físico del respectivo canal. Se proporcionan varios ejemplos más adelante.

Aplicar dos canales de comunicación diferentes, siendo uno de los canales un canal OOB, tiene la ventaja de asegurar de manera confiable que el dispositivo sin SI se encuentre dentro de un rango limitado, es decir, dentro del rango de comunicación de ambos los primeros y segundos canales de comunicación. Utilizar ventajosamente el canal OOB evita que una parte intermedia malintencionada detecte toda la comunicación inalámbrica y la manipule para obtener o cambiar los derechos de acceso y/o el tráfico de datos del usuario, lo que se conoce como ataque de intermediario. Además, el canal OOB puede requerir interacción del usuario que involucra al dispositivo sin SI, lo cual proporciona ventajas al confirmar al usuario que el dispositivo sin SI previsto está realmente acoplado a la identidad de abonado del usuario, SI, por ejemplo, para utilizar el crédito o paquete de voz/datos del abonado.

El código de verificación permite al dispositivo sin SI verificar que el dispositivo SI ha obtenido la clave pública sin SI, tal como se pretendía. Efectivamente, el código de verificación representa la prueba de que el remitente está efectivamente acoplado o en comunicación con el dispositivo sin SI previsto de acuerdo con un protocolo predefinido. Hay muchas variantes para compartir dicho código a través de un canal de comunicación que opera de acuerdo a dicho protocolo. La palabra "compartir" utilizada en este contexto abarca cualquier forma de transferir el código de verificación a través de un canal de comunicación entre el dispositivo sin SI y el dispositivo SI. Por ejemplo, la clave pública sin SI se envía a través de un canal inalámbrico que es un canal OOB, como Bluetooth o NFC, que en este contexto es OOB porque utiliza una banda de transmisión diferente al otro canal de comunicación. El código de verificación se envía de vuelta a través del segundo canal inalámbrico, por ejemplo, a través de Wi-Fi. Alternativamente, la clave pública sin SI puede ser transferida a través de un canal inalámbrico y el código de verificación generado por el dispositivo sin SI se transfiere a través de un canal OOB que involucra al usuario. Por ejemplo, el código de verificación se comunica al usuario, por ejemplo, a través de una pantalla o una señal de audio, mientras que el usuario debe ingresar el mismo código al dispositivo SI, por ejemplo, a través de un teclado. O, viceversa, un código puede ser mostrado en el dispositivo SI para ingresarse en el dispositivo sin SI. Además, el código de verificación puede ser mostrado tanto por el dispositivo sin SI como por el dispositivo SI, mientras que una confirmación debe ser ingresada en uno o ambos lados, por ejemplo, presionando un botón o haciendo clic en un ícono. Además, el código de verificación puede ser un código que el usuario conoce o debe generar, el cual posteriormente debe ingresarse en ambos lados.

El código de verificación puede ser un hash de la clave pública sin SI obtenida por el dispositivo SI. El código de verificación también puede ser, o incluir, la propia clave pública sin SI. También puede ser cualquier código numérico, contraseña o frase de acceso generada por uno de los dispositivos o el usuario. Un primer ejemplo define la prueba de que el remitente ha obtenido la clave pública sin SI correcta de acuerdo con el protocolo. Por ejemplo, la clave pública sin SI puede ser obtenida por el dispositivo SI escaneando un código QR. Dicha exploración constituye un canal OOB (en este caso, un canal de comunicación unidireccional) y el dispositivo SI envía, como código de verificación, la propia clave pública sin SI y/o un hash de la misma, al dispositivo sin SI a través de Wi-Fi (el otro canal de comunicación). Entonces, el dispositivo sin SI sabe que el dispositivo que se comunica con él a

través de Wi-Fi acaba de escanear su clave pública sin SI. Alternativamente, la clave pública sin SI puede ser transferida a través de Wi-Fi, mientras que el código de verificación es transferido de vuelta desde el dispositivo SI al dispositivo sin SI utilizando el canal OOB (por ejemplo, ingresando manualmente el código), lo cual brinda la misma garantía al dispositivo sin SI a través de este canal de comunicación unidireccional.

La prueba de posesión de la clave privada sin SI se transfiere al dispositivo SI, por ejemplo, a través de la red de comunicación local, el primer o segundo canal de comunicación, o una red adicional. La prueba de posesión de una clave privada por parte de una entidad se puede realizar mediante el cifrado de datos de esa entidad con la clave privada. La otra parte puede verificar el resultado mediante la descifrado de los datos cifrados con la clave pública correspondiente y comprobando si el resultado es igual a los datos proporcionados. La otra parte también puede cifrar algo con la clave pública del dispositivo que debe demostrar la posesión de la clave privada, enviar el resultado cifrado y pedir al dispositivo que demuestre la posesión de la clave privada descifrando el resultado y devolviendo el resultado. La prueba de posesión de una clave privada también se realiza cuando los dispositivos establecen un canal seguro intercambiando una o más claves públicas, como se hace, por ejemplo, en los protocolos SSL, TLS y de autenticación DPP. De esta manera, el dispositivo sin SI y el dispositivo SI pueden establecer un canal seguro a través de redes como Wi-Fi, Bluetooth o la red local, en base a la clave pública sin SI. La prueba de posesión asegura de manera confiable al dispositivo SI que el dispositivo sin SI es realmente el propietario del par de claves sin SI.

Los datos de seguridad representan al menos parte de las credenciales requeridas para utilizar la red central e identificar al usuario ante el proveedor de la red central. En las redes centrales gestionadas de acuerdo con el 3GPP, las credenciales pueden ser llamadas credenciales 3GPP. Los datos de seguridad son emitidos en nombre del proveedor, por ejemplo, generados en un servidor del proveedor o en un servidor de aplicación, y comprenden al menos algunas credenciales relacionadas con la SI que están cifradas utilizando la clave pública sin SI. Opcionalmente, la autoridad de certificación CA puede generar una firma que represente su autorización, en este contexto autorizando los derechos para utilizar la red central mientras está asociado a la SI de un abonado conocido en la red central. Por ejemplo, los datos de seguridad pueden comprender una firma generada por la CA sobre al menos parte de la clave pública sin SI y/o sobre parte de las credenciales cifradas y no cifradas. Los datos de seguridad pueden contener datos adicionales de la red central, como un código de identidad central, un código de dispositivo como IMEI (Identidad Internacional de Equipo Móvil) o un código de identidad de abonado como IMSI (Identidad Internacional de Abonado Móvil). Además, los datos de seguridad pueden contener otra información, como el nombre del abonado, el propietario de la clave pública y privada asociada, su dirección, etc. Los datos de seguridad pueden ser transferidos al dispositivo sin SI utilizando el canal seguro ya establecido a través de la red local.

Al recibir los datos de seguridad, el dispositivo sin SI puede verificar los datos de seguridad. Por ejemplo, puede verificar la firma en los datos de seguridad utilizando una clave de verificación pública de la AC, al mismo tiempo que utiliza al menos una parte de la clave pública sin SI en los datos de seguridad y/o su propia copia de la clave pública sin SI. Las credenciales, o los datos adicionales de la red central, pueden estar, al menos en parte, cifrados, por ejemplo, utilizando la clave pública sin SI, mientras que el dispositivo sin SI puede verificar los datos de seguridad descifrando utilizando la clave privada sin SI.

Los datos de seguridad, tras descifrar cualquier parte cifrada, permiten que el dispositivo sin SI acceda a la red central a través de la red local y una puerta de enlace entre la red local y la red central. En la práctica, el dispositivo sin SI puede utilizar diferentes puertas de enlaces en diferentes ubicaciones para comunicarse a través de la red central. La puerta de enlace traduce el protocolo y los mensajes en el lado de la red local, por ejemplo, Wi-Fi, a mensajes correspondientes en el lado de la red central de acuerdo con el protocolo de comunicación central.

Cuando un dispositivo utiliza los datos de seguridad para obtener autorización de acceso, la red principal puede intentar autenticar el dispositivo en varios aspectos. Por ejemplo, la red central puede verificar la firma de los datos de seguridad para determinar si está firmada correctamente, y al verificar que los datos de seguridad estén firmados por la CA. Además, la red central puede requerir que el dispositivo demuestre que posee la clave privada sin SI correspondiente a la clave pública sin SI. Si la firma es correcta, o al recibir y verificar exitosamente dicha prueba, la red central utilizará los datos de identidad proporcionados por el dispositivo sin SI, como la clave pública sin SI o parte de los datos adicionales de la red central, para buscar en una base de datos de abonados y determinar si esta identidad tiene derecho a acceder a la red. Por ejemplo, cuando se haya pagado una suscripción para la SI, debido a la asociación entre el dispositivo sin SI y la SI, el uso de la red central por parte del dispositivo sin SI puede ser facturado al abonado. Los datos de asociación que definen la conexión entre el dispositivo sin SI y el abonado se almacenan en una base de datos de la red central.

Cuando un dispositivo utiliza credenciales, por ejemplo, una combinación de nombre de usuario/contraseña o una identidad y una clave secreta, para obtener autorización de acceso, la red principal intenta autenticar el dispositivo verificando si la combinación suministrada de nombre de usuario/contraseña es conocida por la red y es correcta. La contraseña puede ser enviada en claro a la red para este propósito, pero también se puede enviar un hash sobre la contraseña concatenada antes de hacer el hash con otra información, como un nonce suministrado por la red. En caso de que las credenciales comprendan una identidad y una clave secreta, la red solicita al dispositivo que

proporcione su identidad y realice un cálculo con la clave secreta y envíe el resultado a la red, el cual puede ser verificado por la red para comprobar su corrección. Si la autenticación se realizó correctamente, la red central utilizará el nombre de usuario o los datos de identidad proporcionados por el dispositivo sin SI para buscar en una base de datos de abonados y verificar si esta identidad tiene derecho a acceder a la red.

5 En una realización, la secuencia de asociación comprende proporcionar un canal seguro como el otro canal del primer y segundo canal de comunicación mediante la conexión.

- 10 - una capa de socket seguro, SSL [RFC 6101], o un protocolo de seguridad de capa de transporte, TLS [RFC 5246], con el dispositivo sin SI que actúa como servidor, donde el dispositivo sin SI proporciona la clave pública sin SI en un certificado autofirmado y utiliza este certificado como certificado de servidor en un mensaje de certificado de servidor; o
- 15 - un protocolo SSL o TLS con el dispositivo sin SI que actúa como cliente, donde el dispositivo sin SI proporciona la clave pública sin SI en un certificado autofirmado en un establecimiento de comunicación autenticado por el cliente; o
- 20 - un túnel de seguridad del protocolo de Internet, IPsec [RFC 4301], establecido mediante cifrado de clave pública en el que se utiliza la clave pública sin SI o la clave privada sin SI; o
- un protocolo de aprovisionamiento de dispositivos, DPP [DPP], protocolo de autenticación, donde el dispositivo sin SI proporciona la clave pública sin SI o una clave pública sin SI adicional como clave de inicio de DPP o como clave de protocolo DPP. Efectivamente, se proporciona un canal seguro entre el dispositivo sin SI y el dispositivo SI, mientras que el otro canal entre ambos dispositivos es un canal OOB. Ventajosamente, los diferentes canales independientes brindan seguridad al usuario de que el dispositivo sin SI es el dispositivo destinado a ser asociado. Al establecer el canal seguro de las formas mencionadas anteriormente o utilizando otros protocolos, el dispositivo sin SI también ha demostrado poseer la clave privada sin SI al dispositivo SI.

25 En una realización, dicho recibimiento de los datos de seguridad comprende recibir los datos de seguridad a través del canal seguro. Ventajosamente, los datos de seguridad, incluyendo cualquier credencial, se entregan de manera controlada y segura al dispositivo sin SI, que es el dispositivo destinado a ser asociado.

30 En una realización, el canal OOB se proporciona a través de uno de los grupos.

- un protocolo de comunicación de radio de corto alcance como NFC o Bluetooth,
- un canal visual que utiliza un código visual como un código de barras o un código QR en el lado del dispositivo sin SI y un escáner o cámara en el lado del dispositivo SI,
- 35 - un canal de usuario donde se muestra un código en el lado del dispositivo SI y debe ingresarse en el lado del sistema sin SI,
- un canal de usuario donde se muestra un código en el lado del dispositivo sin SI y debe ingresarse en el lado del sistema SI, o debe compararse con código adicional en el lado del dispositivo SI, y
- 40 - un canal de usuario donde debe ingresarse un código en el dispositivo sin SI y debe ingresarse un código relacionado en el dispositivo SI. Las diversas opciones para el canal OOB son efectivamente diferentes e independientes del canal seguro mencionado anteriormente a través de una red local.

En una realización, los datos de seguridad comprenden credenciales relacionadas con la SI, al menos parte de las credenciales se cifran utilizando la clave pública sin SI.

45 En una realización, la clave pública sin SI comprende una primera clave pública sin SI y una segunda clave pública sin SI, correspondientes respectivamente a una primera clave privada sin SI y una segunda clave privada sin SI,

- 50 - la primera clave pública sin SI se proporciona inicialmente al dispositivo SI a través del canal OOB, y la segunda clave pública sin SI se utiliza posteriormente para generar los datos de seguridad. Ventajosamente, la segunda clave pública sin SI es única para ser utilizada como identidad y/o clave de cifrado en los datos de seguridad, mientras que la primera clave pública sin SI puede ser distribuida libremente o puede ser fija, ya que está impresa, por ejemplo, en la carcasa o manual del dispositivo.

55 En una realización, el procesador en el dispositivo sin SI se dispone además para

- recibir mensajes de latido cardíaco del dispositivo SI, el dispositivo SI que transfiere los mensajes de latido cardíaco al recibir los mensajes de latidos cardíacos de la red central, y transfiriendo los mensajes de latido cardíaco a la red central a través de la puerta de enlace; o
- 60 - recibir mensajes de latido del corazón desde la red central a través de la puerta de enlace y transferir los mensajes de latido del corazón al dispositivo SI, el dispositivo SI que transfiere los mensajes de latido del corazón a la red central;

65 para permitir que la red central deshabilite el acceso del dispositivo sin SI a la red central al no recibir, durante un intervalo predeterminado, los mensajes de latido del dispositivo sin SI. Ventajosamente, los mensajes de latidos del corazón proporcionan evidencia de que el dispositivo SI consiente en el uso de la SI por parte del dispositivo sin SI.

En una realización, el procesador en el dispositivo sin SI se configura además para gestionar una multitud de cuentas de usuario, y para

- 5 - selectivamente para las cuentas de usuario respectivas, ejecutar la secuencia de asociación para establecer múltiples instancias respectivas de datos de seguridad, y
- selectivamente para una cuenta de usuario respectiva, permitir que el dispositivo sin SI acceda a la red central en base a la instancia respectiva de datos de seguridad. Ventajosamente, se pueden proporcionar múltiples asociaciones para las respectivas cuentas de usuario.

10 Los procedimientos de acuerdo con la invención pueden ser implementados en un ordenador como un procedimiento implementado por ordenador, o en hardware dedicado, o en una combinación de ambos. El código ejecutable para un procedimiento de acuerdo con la invención puede ser almacenado en un producto de programa informático. Ejemplos de productos de programas informáticos incluyen dispositivos de memoria como una memoria USB, dispositivos de almacenamiento óptico como un disco óptico, circuitos integrados, servidores, software en línea, etc.

El producto de programa informático en una forma no transitoria puede comprender medios de código de programa no transitorio almacenados en un medio legible por ordenador para llevar a cabo un procedimiento de acuerdo con la invención cuando dicho producto de programa se ejecuta en un ordenador. En una realización, el programa informático comprende medios de código de programa informático adaptados para realizar todos los pasos o etapas de un procedimiento de acuerdo con la invención cuando el programa informático se ejecuta en un ordenador. Preferiblemente, el programa informático está contenido en un medio legible por ordenador. También se proporciona un producto de programa informático en forma transitoria descargable desde una red y/o almacenado en una memoria volátil legible por ordenador y/o medio ejecutable por microprocesador, el producto comprende instrucciones de código de programa para implementar un procedimiento como se describe anteriormente cuando se ejecuta en un ordenador.

Otro aspecto de la invención proporciona un procedimiento para hacer que el programa informático en una forma transitoria esté disponible para su descarga. Este aspecto se utiliza cuando el programa informático se carga en, por ejemplo, la App Store de Apple, la Play Store de Google o la Windows Store de Microsoft, y cuando el programa informático está disponible para descargar desde dicha tienda.

Se dan a continuación otras realizaciones preferentes de los dispositivos y procedimientos de acuerdo con la invención en las reivindicaciones adjuntas, cuya descripción se incorpora en la presente memoria como referencia.

Breve descripción de las figuras

Estos y otros aspectos de la invención serán evidentes y se explicarán más a fondo con referencia a las realizaciones descritas a modo de ejemplo en la siguiente descripción y con referencia a las figuras adjuntas, en las cuales

La Figura 1 muestra un dispositivo sin SI y un dispositivo SI para comunicación inalámbrica y establecimiento de un canal de comunicación OOB,

La Figura 2 muestra un dispositivo sin SI y un dispositivo SI para comunicación inalámbrica,

La Figura 3 muestra un dispositivo sin SI y un dispositivo UI para comunicación inalámbrica,

La Figura 4 muestra otro ejemplo de un dispositivo sin SI y un dispositivo de interfaz de usuario (UI) para comunicación inalámbrica,

La Figura 5 muestra un procedimiento para su uso en un dispositivo sin SI dispuesto para la comunicación inalámbrica con un dispositivo SI,

La Figura 6 muestra un procedimiento para su uso en un dispositivo SI dispuesto para la comunicación inalámbrica con un dispositivo sin SI,

La Figura 7a muestra un medio legible por ordenador, y

La Figura 7b muestra en una representación esquemática de un sistema de procesador.

Las figuras son puramente diagramáticas y no están dibujadas a escala. En las Figuras, los elementos que corresponden a elementos ya descritos pueden tener los mismos números de referencia.

Descripción detallada de las realizaciones

La Figura 1 muestra un dispositivo sin SI y un dispositivo SI para comunicación inalámbrica y establecimiento de un canal de comunicación OOB. En un sistema de comunicación 100, un dispositivo sin identidad de abonado 120, sin SI, está configurado para la comunicación inalámbrica en una red local de acuerdo con un protocolo de comunicación local. El protocolo de comunicación local, por ejemplo, Wi-Fi, define mensajes de protocolo y transmisión-recepción inalámbrica en un área limitada, siendo esta área limitada al alcance de transmisión de radio de los transceptores Wi-Fi.

En dicho sistema de comunicación, también conocido como sistema SI, una identidad de abonado, SI, comprende datos de identidad de abonado para acceder a una red central, la cual proporciona comunicación inalámbrica para dispositivos móviles a través de al menos un área regional. Como se explica en la introducción, la red central puede ser una red central celular 3G, LTE, 4G o 5G con extensiones propuestas por 3GPP para permitir que un dispositivo sin SI acceda a la red celular central utilizando una red local, como Wi-Fi, para acceder, por ejemplo, a una red central 4G llamada Núcleo de paquete evolucionado o EPC.

La Figura 1 muestra esquemáticamente una comunicación inalámbrica 130 para proporcionar un canal de comunicación entre el dispositivo sin SI 120 y el dispositivo SI 110. Un sistema SI de este tipo tiene al menos una red de comunicación local inalámbrica para la comunicación en un área limitada y al menos una red central de comunicación inalámbrica para dispositivos móviles a través de al menos un área regional. La red central es gestionada por al menos un proveedor, por ejemplo, para gestionar una base de datos de abonados y facturación. El sistema SI puede incluir cualquier combinación de los siguientes elementos:

- al menos un módulo de identidad de abonado, SIM, que comprende los datos de identidad de abonado; o
- al menos un dispositivo SIM que comprende una tarjeta SIM y un transceptor dispuesto para comunicarse con la red central.
- un servidor de aplicaciones, AS, dispuesto para permitir la secuencia de asociación en el lado del proveedor; o
- una base de datos de abonados para almacenar, en el lado del proveedor, datos de abonados relacionados con el uso de la red central; o
- una autoridad de certificación, CA, encargada de autorizar las credenciales del abonado; o
- un servidor de usuario dispuesto para, en base a las credenciales del usuario, acceder y proporcionar los datos de identidad de abonado y las credenciales del abonado a través de internet, etc.

El dispositivo sin SI 120 inicialmente no tiene la SI y está dispuesto para cooperar con un dispositivo SI 110 que tiene acceso a la SI. El dispositivo sin SI tiene un transceptor 121 dispuesto para la transmisión-recepción local de acuerdo con el protocolo de comunicación local, y un procesador 122 dispuesto para ejecutar una secuencia de asociación para establecer una asociación con la SI.

El procesador 122 está configurado para proporcionar un canal inalámbrico al dispositivo SI, por ejemplo, a través de la red local. Sin embargo, el canal inalámbrico también puede ser proporcionado a través de un sistema de comunicación diferente, por ejemplo, otra conexión Wi-Fi o un sistema Bluetooth adicional.

El procesador 122 está configurado para proporcionar, como un canal de comunicación adicional, un canal fuera de banda, OOB 140 al dispositivo SI, como se indica por la flecha discontinua. Como se explica en la introducción, el canal OOB está fuera de banda con respecto al canal inalámbrico mencionado anteriormente, utilizando una banda de frecuencia para la transmisión de radio. Entonces, el canal OOB está utilizando un mecanismo físico diferente al de dicho canal inalámbrico, por ejemplo, visual o ingresando datos manualmente por parte del usuario. Al menos uno de los canales se crea mediante un mecanismo físico que tiene un rango limitado para permitir al usuario verificar que el dispositivo sin SI destinado a ser asociado se encuentra dentro de ese rango limitado desde el dispositivo SI que constituye el punto final físico del respectivo canal.

El dispositivo SI 110 está configurado para la comunicación inalámbrica con el dispositivo sin SI mencionado anteriormente. El dispositivo SI tiene un transceptor 111 dispuesto para la comunicación inalámbrica con el dispositivo sin SI, y un procesador 112 dispuesto para ejecutar una secuencia de asociación para establecer una asociación con la SI. El dispositivo SI puede estar provisto de un módulo de identidad de abonado, SIM, 116. El dispositivo SI también puede estar provisto de una interfaz de usuario 113, por ejemplo, que incluya una pantalla y uno o más elementos de entrada de usuario 115. Por ejemplo, los elementos de entrada del usuario pueden comprender uno o más de una pantalla táctil, varios botones, un ratón o un panel táctil, etc. Los botones pueden ser botones físicos tradicionales, sensores táctiles o botones virtuales, por ejemplo, en una pantalla táctil o iconos que se activan mediante un ratón. La interfaz de usuario también puede ser una interfaz de usuario remota.

El procesador 112 está configurado para proporcionar un canal inalámbrico al dispositivo sin SI, por ejemplo, a través de la red local. Sin embargo, el canal inalámbrico también puede ser proporcionado a través de un sistema de comunicación diferente, por ejemplo, otra conexión Wi-Fi o un sistema Bluetooth adicional. El procesador está configurado para proporcionar, como un canal de comunicación adicional, un canal fuera de banda, OOB 140 al dispositivo SI, como indica la flecha discontinua. Entonces, la primera y segunda comunicación son diferentes e incluyen como un canal el canal OOB. El dispositivo sin SI comprende una clave privada sin SI, por ejemplo, almacenada en una memoria. La clave privada sin SI constituye un par de claves con una clave pública sin SI.

En el dispositivo sin SI, la secuencia de asociación incluye proporcionar la clave pública sin SI al dispositivo SI a través de un primer canal de comunicación. A continuación, se comparte un código de verificación con el dispositivo SI a través de un segundo canal de comunicación. Entonces, se proporciona una prueba de posesión de la clave privada sin SI al dispositivo SI a través del primer o segundo canal de comunicación. A continuación, se recibirá desde el dispositivo SI datos de seguridad que se relacionan con la SI. Los datos de seguridad incluyen credenciales y pueden tener alguna firma generada por una autoridad de certificación utilizando la clave pública sin SI, como se

ha explicado anteriormente. Las credenciales, después de descifrar cualquier parte cifrada, permiten que el dispositivo sin SI acceda a la red central a través de la red local y una puerta de enlace (mostrado en la Figura 2) entre la red local y la red central.

En el dispositivo SI, el procesador 112 está configurado para ejecutar la secuencia de asociación que incluye recibir una clave pública sin SI del dispositivo sin SI a través del primer canal de comunicación. A continuación, se comparte un código de verificación con el dispositivo sin SI a través del segundo canal de comunicación. Luego, a través del primer o segundo canal de comunicación, se recibe una prueba de posesión de una clave privada sin SI que constituye un par con la clave pública sin SI del dispositivo sin SI. Tras una exitosa evaluación de la prueba recibida, se obtienen los datos de seguridad que se relacionan con la SI, tal como se ha explicado anteriormente. Finalmente, los datos de seguridad se transmiten al dispositivo sin SI.

En relación al uso de claves públicas y privadas, por ejemplo, utilizando un canal OOB, se observa lo siguiente. Cuando dos dispositivos inalámbricos necesitan asegurar su comunicación, generalmente cifran su comunicación. Sin embargo, esto requiere que ambos dispositivos inalámbricos conozcan la misma clave.

Diffie-Hellman, ver documento de referencia [DH], es una técnica bien conocida para establecer una clave secreta entre dos partes, donde la comunicación entre las partes para establecer la clave secreta no revela ninguna información a terceros sobre la clave secreta establecida. Las dos partes utilizan cada una su propio par de claves pública/privada e intercambian la clave pública entre sí. Cada parte es capaz de calcular la clave secreta utilizando su propia clave privada y la clave pública de la otra parte, y posiblemente alguna otra información, por ejemplo, un nonce (número aleatorio) de cada parte. Cada parte puede generar un par de claves nuevo cada vez que realice Diffie-Hellman o reutilizar un par de claves antiguo.

El Protocolo de Aprovisionamiento de Dispositivos (DPP) de la Wi-Fi Alliance, ver documento de referencia [DPP], utiliza Diffie-Hellman para establecer una clave secreta entre dos dispositivos, un DPP Enrollee que desea ser configurado y un DPP Configurator que puede configurar DPP Enrollees, para que estos puedan acceder a una red habilitada para DPP, ver también el documento de referencia [802.11].

Al realizar Diffie-Hellman a través de una red, un dispositivo que recibe una clave pública para realizar Diffie-Hellman no sabe de qué dispositivo proviene esta clave pública. Esto puede ser aprovechado por un atacante en lo que se conoce como un ataque de hombre en el medio. Un atacante E podría hacerse pasar por el dispositivo real B con el que el dispositivo A desea conectarse. El atacante E realiza Diffie-Hellman con el dispositivo A y establece una clave secreta con el dispositivo A. De manera similar, el atacante se hace pasar por el dispositivo A ante el dispositivo B y establece una clave secreta con el dispositivo B. Cuando llega un mensaje de uno de los dispositivos A o B, el atacante descifra el mensaje con una de las claves secretas, lo cifra con la otra y lo reenvía al otro dispositivo. De esta manera, los dispositivos A y B no perciben nada extraño en su comunicación, excepto por cierto retraso adicional. Cuando verifiquen su comunicación enviando la misma información utilizando otra forma de comunicación y comparando los resultados, no notarán ninguna manipulación en su comunicación. Pero el atacante tiene un conocimiento completo sobre lo que comunican.

Para prevenir ataques de hombres en el medio, se propone utilizar un protocolo de comunicación de corto alcance adicional, el canal fuera de banda (OOB), para intercambiar las claves públicas o códigos de verificación como los hashes de las claves públicas. Por ejemplo, el usuario de un dispositivo sabe que la clave pública recibida OOB proviene de un dispositivo dentro del rango de operación del protocolo de comunicación de corto alcance. En caso de que el hash de las claves públicas se intercambie fuera de banda (OOB), el dispositivo puede verificar si la clave pública recibida a través del primer canal de comunicación, por ejemplo, Wi-Fi, que necesita ser cifrada, lleva al mismo hash que el hash recibido OOB. Tenga en cuenta que el uso del término protocolo de comunicación en este documento abarca múltiples capas del modelo ISO-OSI, incluyendo la capa física para la transmisión y recepción.

En [DPP], se describen varios procedimientos de OOB, uno de los cuales es Comunicación de campo cercano (NFC). NFC es una técnica de comunicación de forma inalámbrica a una distancia relativamente corta, digamos 10-20 cm. NFC puede, por ejemplo, ser utilizado como comunicación OOB para intercambiar claves públicas. Cuando se utiliza NFC, el usuario sabe que la clave pública recibida a través de NFC proviene de un dispositivo situado a una distancia de 10-20 cm de su propio dispositivo, es decir, del dispositivo con el que realizó un "toque" NFC. Cuando se utiliza NFC en modo entre iguales, el otro dispositivo también puede estar seguro de que recibió una clave pública del dispositivo del usuario.

La Figura 2 muestra un dispositivo sin SI y un dispositivo SI para comunicación inalámbrica a través de una red central. En un sistema de comunicación 200, un dispositivo sin SI 220 se encuentra dispuesto para la comunicación inalámbrica en una red local 236 de acuerdo con un protocolo de comunicación local, por ejemplo, Wi-Fi.

En el sistema de comunicación, la red central CORE_N 230 proporciona comunicación inalámbrica 232, 233 para dispositivos móviles o estacionarios a través de al menos un área regional. Como se explica en la introducción, la red central puede ser un Núcleo de Paquetes Evolucionado o EPC de 3GPP. El sistema de comunicación puede incluir además una puerta de enlace GW 234 entre la red local 236 y la red central. Además, la red central puede

estar acoplada a un servidor de aplicaciones AS 252, una base de datos de abonados Sub_DB 250 y una autoridad de certificación CA 254. Los datos SI pueden estar disponibles en ubicaciones como un sistema de gestión del proveedor de la red central, por ejemplo, en la base de datos de abonados 250 en un servidor que gestiona los datos de identidad de abonado. Las credenciales del abonado pueden ser autenticadas y autorizadas utilizando el servidor de autorización o la autoridad de certificación 254. Por ejemplo, los datos de la SI también pueden ser accedidos por el abonado al iniciar sesión en una cuenta de usuario en el servidor de aplicaciones 252, a través de internet utilizando credenciales de usuario como un nombre de usuario y contraseña, o utilizando una autorización de dos factores. El AS puede estar acoplado a, o puede comprender, la base de datos de abonados y la CA. El AS puede controlar el proceso de asociar un dispositivo sin SI a una SI.

El dispositivo SI puede ser un dispositivo SIM dispuesto para comunicarse 233 a través de la red central con uno o más servidores que almacenan una base de datos de abonados y la CA, al mismo tiempo que está dispuesto para comunicarse a través de un canal inalámbrico 242 con el dispositivo sin SI, en particular un canal seguro.

En una realización, la secuencia de asociación comprende proporcionar un canal seguro como el otro canal de comunicación de primer y segundo canal mediante la utilización de un protocolo de capa de sockets seguros, SSL [RFC 6101], o un protocolo de seguridad de capa de transporte, TLS [RFC 5246], con el dispositivo sin SI que actúa como servidor, donde el dispositivo sin SI proporciona la clave pública sin SI en un certificado autofirmado y utiliza este certificado como certificado de servidor en un mensaje de certificado de servidor. Alternativamente, el canal seguro puede ser proporcionado mediante la utilización de un protocolo SSL o TLS, al igual que con el dispositivo sin SI que actúa como cliente, donde el dispositivo sin SI proporciona la clave pública sin SI en un certificado autofirmado en un establecimiento de comunicación autenticado por el cliente. Alternativamente, el canal seguro puede ser proporcionado mediante la utilización de un túnel de seguridad de protocolo de internet, IPsec [RFC 4301], establecido mediante cifrado de clave pública en el cual se utiliza la clave pública o clave privada sin SI. Alternativamente, el canal seguro puede ser proporcionado mediante la utilización de un protocolo de aprovisionamiento de dispositivos, DPP [DPP], protocolo de autenticación, donde el dispositivo sin SI proporciona la clave pública sin SI o una clave pública sin SI adicional como clave de inicio de DPP o como clave de protocolo DPP. Opcionalmente, en la secuencia de asociación, después de proporcionar uno de los canales seguros mencionados anteriormente, los datos de seguridad también se transfieren a través del canal seguro.

Cuando solo se utiliza el SSL, TLS o IPsec mencionados anteriormente, el dispositivo SI no tiene ninguna prueba de que está comunicándose con el dispositivo sin SI al demostrar la posesión de la clave privada. Al obtener la clave de arranque del dispositivo sin SI de manera fuera de banda (OOB), el dispositivo SI tiene la prueba de que está comunicándose con el dispositivo sin SI cuando este último demuestra poseer la clave privada correspondiente, especialmente cuando el par de claves de arranque se ha generado justo antes de utilizar la comunicación OOB y se utiliza una tecnología de comunicación de corto alcance para la comunicación OOB. La clave de arranque del dispositivo sin SI se puede utilizar como la primera clave pública mencionada anteriormente, o se puede utilizar otra clave pública, la clave de protocolo, como la primera clave pública. La especificación de DPP proporciona ejemplos de cómo un dispositivo puede transferir la clave del protocolo a través de una red inalámbrica y cómo ese dispositivo demuestra la posesión de la clave privada que corresponde con la clave del protocolo.

Asimismo, se puede utilizar un canal OOB entre el dispositivo sin SI y el dispositivo SI antes de que se involucren en una sesión de protocolo SSL, TTL o IPsec, donde la primera clave pública, un certificado que contiene la primera clave pública o un hash de la clave pública o certificado se comunica OOB al dispositivo SI. El dispositivo SI debe verificar si la información sobre la primera clave pública que obtuvo OOB corresponde con la primera clave pública que obtuvo del dispositivo sin SI a través del canal seguro. El dispositivo SI, como opción, también puede hacer que la clave pública que utiliza para establecer el canal seguro, un certificado que contiene su clave pública o un hash de su clave pública o certificado, esté disponible para el dispositivo sin SI a través del protocolo OOB. Los protocolos de comunicación de corto alcance como NFC, la visualización y escaneo de códigos QR, Bluetooth, etc. son protocolos OOB adecuados. Un ejemplo de un procedimiento OOB que involucra al usuario es cuando el dispositivo sin SI muestra un hash (acortado) de su clave pública o certificado, que el usuario debe comparar con el hash (acortado) de la clave pública o certificado recibido a través de la tercera red y mostrado por el dispositivo SI.

Otro ejemplo de un procedimiento OOB que involucra al usuario es cuando el usuario ingresa un código numérico (por ejemplo, un código PIN), contraseña o frase de acceso en ambos dispositivos antes de que se inicie la sesión del protocolo SSL, TTL o IPsec, y donde los dispositivos deben verificar que se utilice la misma verificación. Otro ejemplo de un procedimiento OOB que involucra al usuario es cuando el usuario ingresa un código numérico (por ejemplo, un código PIN), contraseña o frase de contraseña como el 'código' de PKEX (Intercambio de Clave Pública) en ambos dispositivos antes de que participen en la sesión del protocolo de autenticación DPP, donde PKEX se utiliza para el arranque de la seguridad del protocolo de autenticación DPP, ver [DPP] para PKEX y el 'código' de PKEX (sección 5.6) y el protocolo de autenticación DPP (sección 6.2).

Además, como canal seguro de corto alcance OOB, si el dispositivo SI y el dispositivo sin SI están conectados de forma segura al mismo Punto de Acceso Wi-Fi o Puerta de enlace Residencial, la conexión de infraestructura Wi-Fi puede ser utilizada como canal OOB a través del cual el dispositivo sin SI demuestra la posesión de la clave privada.

En otra realización, el dispositivo SI puede ser un Punto de Acceso Wi-Fi y Puerta de Enlace Residencial (por ejemplo, 5G-RG en [TR 23.716]), conectado a la red central 5G y compatible con los protocolos de red 5G), equipado con una tarjeta SIM y capaz de comunicarse con el dispositivo sin SI a través del canal OOB, en el cual el dispositivo sin SI proporciona una identidad que posteriormente se utiliza en un intercambio de Diffie-Hellman para establecer un canal seguro entre el dispositivo sin SI y SI. Esta identidad u otra clave pública o certificado utilizados en el establecimiento del canal seguro pueden ser utilizados como la identidad del dispositivo sin SI para asociar el dispositivo sin SI a una red celular central. Además, alguna parte de la identidad o certificado puede ser utilizada como una clave pública para cifrar credenciales adicionales que están asociadas con la SI, las cuales pueden ser posteriormente utilizadas por el dispositivo sin SI para obtener autorización para acceder a la red principal. El dispositivo SI puede ser operado a través de una interfaz de usuario remota en, por ejemplo, un teléfono inteligente. El canal seguro puede ser cualquiera de las cuatro opciones descritas anteriormente o cualquier otro canal seguro.

En otra realización, el dispositivo SI es un dispositivo móvil que actúa como configurador DPP, ver [DPP], para un 5G-RG, donde el dispositivo SI tiene una interfaz de usuario que permite al usuario elegir si desea asociar el dispositivo sin SI con el dispositivo SI o el 5G-RG o ambos. El dispositivo puede mostrar información de la base de datos del abonado relacionada con el dispositivo SI y el dispositivo 5G-RG, en el perfil del usuario o en la información de precios/cobros relacionada con las diferentes opciones. En caso de que el dispositivo sin SI vaya a ser asociado con el dispositivo SI para acceder a la red central, la clave del protocolo DPP o la clave de arranque DPP del dispositivo sin SI pueden ser utilizadas como la identidad del dispositivo sin SI.

En las opciones anteriores, se puede solicitar al usuario/propietario del dispositivo SI que acepte la asociación del dispositivo sin SI con el dispositivo SI, ya que esto puede implicar un costo adicional para el usuario/propietario.

En la práctica, la secuencia de asociación puede involucrar lo siguiente. Después de que el dispositivo SI haya obtenido con éxito la prueba de la identidad del dispositivo sin SI, el dispositivo SI utiliza la primera clave pública o un certificado generado por el dispositivo sin SI que contiene la primera clave pública como identidad del dispositivo sin SI y lo envía a un servidor AS, por ejemplo, a través de la red central 3GPP, ya sea directamente o a través de un punto de acceso Wi-Fi/portal residencial, que puede o no estar habilitado para 5G. El servidor AS crea un perfil de usuario para el dispositivo sin SI y una asociación entre la SI del dispositivo SI y el (perfil de usuario del) dispositivo sin SI utilizando la primera clave pública como identidad del dispositivo sin SI. El AS envía este perfil de usuario del dispositivo sin SI a una base de datos de abonados que almacena este perfil de usuario. El AS puede solicitar datos de seguridad utilizando una primera clave pública de una autoridad de certificación o servidor de autoridad de certificación (CA) y puede enviar los datos de seguridad al dispositivo SI, que posteriormente envía estos datos de seguridad al dispositivo sin SI, preferiblemente a través de un canal seguro como la conexión SSL, TLS, túnel IPsec o utilizando la clave simétrica establecida durante la autenticación DPP, por ejemplo, como parte de un mensaje de protocolo de configuración DPP en el objeto de configuración DPP o incluso en un conector DPP. Además de la primera clave pública, la solicitud de datos de seguridad a la CA puede incluir otra información a ser incluida, como información sobre el perfil del usuario, el IMEI (si corresponde) a ser utilizado por el dispositivo sin SI, el IMSI (si corresponde) a ser utilizado por el dispositivo SI, etc. Se proporcionan más ejemplos de los conceptos del servidor AS, CA y Sub_DB, y cómo dichos servidores pueden ayudar a crear una asociación entre la tarjeta SIM y el dispositivo sin SIM, en el documento US9648019B2, utilizando ahora la clave pública sin SIM como identidad y el canal seguro entre la tarjeta SIM y el dispositivo sin SIM. El AS también puede solicitar credenciales de una CA, un servidor proveedor o una base de datos, las cuales permiten que el dispositivo sin SI sea autorizado para acceder a la red principal. Estas credenciales son almacenadas por el proveedor, por ejemplo, en la base de datos del abonado. El AS cifra al menos parte de las credenciales con la primera clave pública y envía datos de seguridad que incluyen las credenciales cifradas al dispositivo SI, el cual reenvía los datos de seguridad al dispositivo sin SI para su procesamiento como se describe anteriormente.

La Figura 3 muestra un dispositivo sin SI y un dispositivo UI para comunicación inalámbrica a través de una red central. En un sistema de comunicación 300, se dispone un dispositivo sin SI 320 para la comunicación inalámbrica con el dispositivo UI 310, por ejemplo, a través de Wi-Fi. Varios elementos del sistema de comunicación 300 corresponden a elementos similares en el sistema de comunicación 200 descrito con referencia a la Figura 2. Tales elementos tienen los mismos números de referencia y no se describen nuevamente. El dispositivo de interfaz de usuario (UI) 310 tiene una interfaz de usuario y un transceptor para comunicarse a través de la red central para acceder a la SI. Para ello, el dispositivo de IU está diseñado para conectarse al AS 252 y obtener la SI de la base de datos de abonados Sub-DB 250 y los datos de seguridad, por ejemplo, de la CA 254.

En una realización, las credenciales para acceder a una red central 3GPP pueden estar vinculadas a una persona; un escenario podría ser el siguiente. El propietario de una tarjeta (U-)SIM también tiene una cuenta en el sitio web de su proveedor. Al iniciar sesión en el sitio web de su proveedor, utilizando cualquier dispositivo de interfaz de usuario con una conexión 3GPP a un transceptor 3GPP, un usuario puede solicitar credenciales basadas en la persona. Iniciar sesión en el sitio web del proveedor puede requerir cualquier procedimiento de autenticación, por ejemplo, nombre de usuario/contraseña, un certificado, etc. El dispositivo de interfaz de usuario puede tener que suministrar la clave pública que se utilizará para generar los datos de seguridad. También puede ser que las credenciales entregadas por el sitio web incluyan una clave privada correspondiente. El sitio web puede almacenar las credenciales, y posiblemente la clave privada correspondiente, en un lugar adecuado en el dispositivo de interfaz

de usuario (UI) y después de eso, el dispositivo de interfaz de usuario puede utilizar el certificado para autenticarse en una red 3GPP a través de un punto de acceso (AP) o una puerta de enlace residencial que está conectada a una red 3GPP. El propietario de la tarjeta (U-)SIM es facturado por el uso 3GPP del dispositivo sin SI. En el certificado, el dispositivo UI también puede solicitar y recibir credenciales que están cifradas con la clave pública, como se explicó anteriormente.

Lo anterior puede implementarse en un dispositivo que tenga una interfaz de usuario (UI) o que pueda ejecutar dicha aplicación. Para un dispositivo sin cabeza, es decir, un dispositivo sin interfaz de usuario, como el dispositivo sin SI 320, se propone instalar unas credenciales 3GPP. Una serie de pasos sería como se describe en la Figura 2, mientras que el dispositivo UI tiene el papel del dispositivo SI mencionado anteriormente, pero donde el dispositivo UI obtiene los datos de seguridad como se describe anteriormente para el dispositivo UI. El dispositivo de interfaz de usuario puede ser un dispositivo SIM que utiliza la SIM para conectarse a la red 3GPP y al Servidor de Aplicaciones.

La Figura 4 muestra otro ejemplo de un dispositivo sin SI y un dispositivo de interfaz de usuario (UI) para comunicación inalámbrica a través de una red central. En un sistema de comunicación 400, se dispone un dispositivo sin SI 420 para la comunicación inalámbrica con el dispositivo UI 410, por ejemplo, a través de Wi-Fi. Varios elementos del sistema de comunicación 400 corresponden a elementos similares en el sistema de comunicación 200 descrito con referencia a la Figura 2. Tales elementos tienen los mismos números de referencia y no se describen nuevamente. El dispositivo de interfaz de usuario 410 tiene una interfaz de usuario y está dispuesto para la comunicación a través de internet IN 433. Por ejemplo, el dispositivo de interfaz de usuario (UI) 410 puede conectarse al servidor de aplicaciones AS 252 a través de Internet para obtener los datos de seguridad, de manera similar a obtener los datos de seguridad mediante una conexión a la red central como se describe arriba con la Figura 3.

En una realización, el proveedor puede proporcionar una aplicación que los usuarios pueden descargar y ejecutar en un dispositivo que no tiene un transceptor 3GPP. El usuario debe ingresar su nombre de usuario y contraseña en la aplicación y luego la aplicación solicita los datos de seguridad a través de una conexión a Internet que no involucra la red celular 3GPP. La aplicación puede utilizar luego los datos de seguridad para autenticar el dispositivo sin SI en una red 3GPP a través de un AP o Puerta de enlace Residencial que está conectado a una red 3GPP. En la práctica, el dispositivo de interfaz de usuario puede ser un dispositivo con conexión a Internet, por ejemplo, a través de una línea terrestre, donde se establece un canal confiable hacia el Servidor de Aplicaciones donde el usuario debe proporcionar su nombre de usuario y contraseña, o un certificado, etc.

En una realización, el dispositivo sin SI es un dispositivo sin cabeza que muestra su clave de arranque público en una etiqueta o en su manual en forma de un código legible por máquina, por ejemplo, un código QR o un código de barras. Dispositivos sin cabeza con una pantalla lo suficientemente buena pueden mostrar una nueva clave de arranque público generada en su pantalla. A continuación, el dispositivo de interfaz de usuario escanea la clave de arranque pública del dispositivo sin cabeza. A continuación, el dispositivo de interfaz de usuario envía la información del dispositivo sin cabeza a través de Wi-Fi, con la cual el dispositivo sin cabeza puede saber que el dispositivo de interfaz de usuario ha leído su clave de inicio pública, por ejemplo, enviando un hash de la clave pública.

Posteriormente, para establecer un canal seguro, el dispositivo de interfaz de usuario realiza un intercambio de Diffie-Hellman a través de Wi-Fi con el dispositivo sin cabeza, donde espera que el dispositivo sin cabeza utilice la clave de arranque de clave pública que ha escaneado y establece una conexión segura con el dispositivo sin cabeza de esta manera. Opcionalmente, el dispositivo sin cabeza crea un segundo par de claves pública/privada sin SI, envía la segunda clave pública sin SI al dispositivo de interfaz de usuario y demuestra la posesión de la clave privada. Este paso puede integrarse con la configuración del canal seguro.

A continuación, el dispositivo de interfaz de usuario utiliza la clave de inicio público, o la segunda clave pública sin SI, como clave pública para solicitar datos de seguridad al proveedor de la red celular. Esta comunicación puede realizarse a través de un canal adicional seguro con un servidor del proveedor de red celular que se configura utilizando las credenciales del usuario, por ejemplo, nombre de usuario y contraseña, para acceder a la cuenta del usuario en el proveedor de red celular.

El dispositivo de interfaz de usuario ahora recibe datos de seguridad, incluyendo credenciales, del proveedor de la red celular, y transfiere los datos de seguridad al dispositivo sin SI utilizando dicho canal seguro. El dispositivo sin SI ahora puede utilizar la segunda red (236) para autenticarse en la red 3GPP (232, 230) y utilizar la red 3GPP.

Alternativamente a los datos de seguridad anteriores en base a la clave pública sin SI, el dispositivo de interfaz de usuario puede recibir datos de seguridad alternativos en base a una clave pública generada por el proveedor y también la clave privada generada por el proveedor que la acompaña, y transferir ambas al dispositivo sin SI. El dispositivo sin SI ahora puede utilizar los datos de seguridad alternativos en base a la clave pública generada por el proveedor y la clave privada generada por el proveedor para utilizar la red 3GPP.

En una realización, un operador o usuario puede desear limitar el área en la cual el dispositivo sin SI, mientras está asociado a la SI, puede operar para obtener acceso a la red central, por ejemplo, para mayor seguridad adicional.

Se proporcionan varias opciones para determinar si el dispositivo sin SI se encuentra dentro del rango operativo previsto, por ejemplo, asegurándose de que los dos dispositivos permanezcan cerca uno del otro.

En una realización, la red central envía mensajes de latido al dispositivo SI a través de la primera red, por ejemplo, mensajes de paginación. Los mensajes de latidos del corazón pueden tener un componente aleatorio, de manera que sean difíciles de predecir por el dispositivo sin SI. El dispositivo SI está configurado para enviar los mensajes de latidos del corazón al dispositivo sin SI, por ejemplo, utilizando el canal seguro establecido para el procedimiento de asociación entre el dispositivo sin SI y el dispositivo SI. El dispositivo sin SI luego envía los latidos cardíacos recibidos a la red central a través de la segunda red. La red central desactiva el acceso del dispositivo sin SI a la red central cuando la red central no ha recibido las señales de latido correctas durante algún tiempo. La red central puede permitir el acceso nuevamente después de haber recibido nuevamente las señales de latido cardíaco correctas.

Opcionalmente, los latidos del corazón también pueden ser utilizados por el dispositivo SI para limitar el acceso del dispositivo sin SI a la red central en tiempo o uso, ya que este acceso puede implicar costos adicionales para el abonado. Cuando el dispositivo SI desea limitar el acceso, deja de reenviar las señales de latido cardíaco. Cuando el dispositivo SI permite el acceso nuevamente, comienza a reenviar las señales de latido cardíaco nuevamente. Otra forma de detener el acceso a la red central del dispositivo sin SI es mediante el dispositivo SI revocando la asociación de la primera clave pública como identidad para un dispositivo sin SI asociado en el servidor AS.

En otra realización, el dispositivo SI comunica regularmente información sobre la distancia entre el dispositivo SI y el dispositivo sin SI al AS utilizando una corriente de mensajes firmados por el dispositivo SI. Una distancia puede, por ejemplo, determinarse utilizando el mecanismo de medición de tiempo (TM) o la medición de tiempo precisa (FTM) como se describe en [802.11]. Alternativamente, cuando el dispositivo SI está conectado al mismo punto de acceso Wi-Fi / Puerta de enlace residencial que el dispositivo sin SI, puede enviar información sobre dichas conexiones al AS utilizando una secuencia de mensajes firmados por el dispositivo SI. El AS puede ser configurado para verificar esta información y comprobar que esta información está debidamente firmada por el dispositivo SI. Si la distancia supera un umbral configurado determinado, o si no ha recibido recientemente dicha información de conexión, se deniega el acceso a la red principal al dispositivo sin SI.

En otra realización, el dispositivo SI actúa como relé para una cierta parte del tráfico hacia y/o desde el dispositivo sin SI. Además, el dispositivo SI está configurado para cifrar parte de los mensajes utilizando las credenciales propias del dispositivo SI. El AS puede utilizar la parte cifrada para detectar que el dispositivo SI está directamente involucrado en la comunicación con el dispositivo sin SI y que la red central no está siendo accedida desde un dispositivo sin SI hackeado en algún otro lugar conectado a la red central.

En otra realización adicional, el dispositivo SI y/o el AP/RG al que está conectado el dispositivo sin SI pueden llevar un seguimiento continuo y enviar información sobre los servicios/contenido que son solicitados por el dispositivo sin SI al AS. El AS ahora puede verificar si los servicios y contenido cumplen con el derecho de acceso asignado al dispositivo sin SI. Si no es así, un dispositivo pirateado puede estar utilizando las credenciales del dispositivo sin SI que intenta acceder a un conjunto diferente de servicios/contenido solicitado por el dispositivo sin SI. El AS puede revocar el acceso o los servicios al dispositivo sin SI.

En otra realización, el dispositivo sin SI puede configurarse con más de una cuenta de usuario. Normalmente hay al menos una cuenta de usuario principal con la cual se pueden crear otras cuentas secundarias. Las cuentas de usuario pueden ser diferentes de las cuentas de usuario del dispositivo SIM, mientras que los usuarios pueden tener diferentes derechos para acceder a contenido/servicios en Internet o en la red celular (por ejemplo, padre versus hijo). Cada cuenta puede, por ejemplo, estar conectada con una cuenta de Google, Apple ID o Microsoft diferente. Cada cuenta secundaria puede o no haber recibido permiso para utilizar el sistema Wi-Fi o 3GPP del dispositivo. Además, cada cuenta puede necesitar ser configurada con diferentes tipos de restricciones de acceso para el contenido/servicios ofrecidos por la red celular (por ejemplo, para el control parental de cuentas de niños menores de edad). Opcionalmente, en un dispositivo sin SI multiusuario, solo se permitirá asociar cuentas de usuarios específicas con un dispositivo SI. La asociación podría ser al mismo SI para cada una de las cuentas de usuario permitidas, en cuyo caso la asociación con el dispositivo SI solo necesita hacerse una vez. Alternativamente, se pueden asociar múltiples SI diferentes a las respectivas cuentas de usuario, en cuyo caso la asociación debe realizarse con cada uno de los SI diferentes por separado.

En una realización, un nombre de cuenta de usuario, o múltiples nombres de cuenta de usuario que están asociados con una SI, pueden tener el nombre de cuenta o ID de cuenta listado en las credenciales que el dispositivo SI asociado solicita al servidor CA. Con este fin, el dispositivo sin SI debe proporcionar el nombre de la cuenta de usuario(s) al dispositivo SI utilizando el canal seguro establecido con el dispositivo sin SI, durante el cual el dispositivo sin SI demostró poseer la clave privada perteneciente a la clave pública del dispositivo sin SI. Opcionalmente, el nombre de la cuenta o cuentas se mencionan en un certificado que contiene una primera clave pública y está firmado con la clave privada correspondiente a la primera clave pública (por ejemplo, en los certificados SSL o TLS autofirmados generados por el dispositivo sin SI). En lugar de solo la primera clave, el dispositivo SI envía este certificado al servidor AS y los datos de seguridad que se generarán por el servidor CA

pueden contener el nombre de la cuenta(s). La ventaja para el usuario del dispositivo SI es que puede ver desde el certificado qué usuarios del dispositivo sin SI están habilitados. La ventaja del dispositivo SI, AS y CA es que pueden verificar que ha sido el dispositivo sin SI el que ha nombrado las cuentas de usuario.

En otra realización, cuando se ha concedido el acceso del dispositivo sin SI a la red central, la información sobre las cuentas de usuario del dispositivo sin SI y las posibles restricciones de acceso para las cuales se ha concedido acceso, se envía a través del mismo canal seguro por el cual el dispositivo sin SI demostró poseer la clave privada perteneciente a la clave pública del dispositivo sin SI. Al recibir esta información, el dispositivo sin SI aplica estas restricciones de acceso para las respectivas cuentas de usuario diferentes del dispositivo sin SI.

La Figura 5 muestra un procedimiento para su uso en un dispositivo sin SI dispuesto para la comunicación inalámbrica con un dispositivo SI. Los dispositivos han sido descritos anteriormente. El procedimiento puede ser ejecutado, por ejemplo, mediante circuitos y software en un procesador en un dispositivo informático estacionario o móvil. La comunicación inalámbrica en una red local, una red central o de otra manera, y varias opciones para un canal OOB, se han descrito anteriormente. Se observa que la Figura 5 muestra un procedimiento para un dispositivo sin SI, que puede estar cooperando con el dispositivo SI. En el dispositivo sin SI se almacena una clave privada sin SI que constituye un par con una clave pública sin SI. El par de claves puede ser almacenado de forma permanente o temporal, o puede ser generado primero para establecer una nueva asociación.

En el procedimiento, se ejecuta una secuencia de asociación que comienza en el nodo START 501. En una primera etapa PR-NPK 503, la clave pública sin SI se proporciona al dispositivo SI a través de un primer canal de comunicación. Para ello, se establece el primer canal de comunicación, por ejemplo, a través de una red inalámbrica como Wi-Fi. El primer canal también puede ser un canal OOB como se ha explicado anteriormente, por ejemplo, la clave pública sin SI puede ser proporcionada al dispositivo SI en forma impresa, mientras que la clave privada correspondiente debe ser almacenada internamente en el dispositivo sin SI.

En una etapa siguiente SH-VER 504, se comparte un código de verificación con el dispositivo SI a través de un segundo canal de comunicación. Para ello, se establece el segundo canal de comunicación, por ejemplo, a través de una comunicación inalámbrica diferente al primer canal de comunicación, como Bluetooth. El primer y segundo canal de comunicación son diferentes, mientras que uno de los primeros y segundos canales de comunicación es un canal OOB. Por ejemplo, el código de verificación puede ser compartido a través de un canal OOB mostrando el código en el dispositivo SI, mientras que el usuario debe ingresar el código manualmente en el dispositivo sin SI. En una etapa siguiente, PR-PRO 505, se proporciona una prueba de posesión, utilizando cualquiera de los protocolos mencionados anteriormente, de la clave privada sin SI al dispositivo SI a través del primer o segundo canal de comunicación.

Si la evaluación de la prueba no tiene éxito, el procedimiento termina según indica la flecha 510 al no recibir datos de seguridad, por ejemplo, después de un período de tiempo de espera predeterminado o al recibir un mensaje que indica que no hay datos de seguridad disponibles. Si la prueba ha sido evaluada con éxito, el dispositivo SI puede obtener los datos de seguridad, incluyendo las credenciales, y enviar los datos de seguridad al dispositivo sin SI. En una etapa siguiente, se recibe desde el dispositivo SI los datos de seguridad REC-SEC 506, los cuales están relacionados con la SI y pueden incluir una firma, por ejemplo, una firma generada por una autoridad de certificación sobre al menos parte de la clave pública sin SI, e incluye credenciales relacionadas con la SI, al menos parte de las cuales están cifradas utilizando la clave pública sin SI.

Finalmente, en una etapa AC-CORE 507, los datos de seguridad, después de descifrar las partes cifradas, permiten que el dispositivo sin SI acceda a la red central a través de la red local y una puerta de enlace entre la red local y la red central. La secuencia de asociación se termina en el nodo END 508.

La Figura 6 muestra un procedimiento para su uso en un dispositivo SI dispuesto para la comunicación inalámbrica con un dispositivo sin SI. Los dispositivos han sido descritos anteriormente. El procedimiento puede ser ejecutado, por ejemplo, mediante circuitos y software en un procesador en un dispositivo informático estacionario o móvil.

En el procedimiento, se ejecuta una secuencia de asociación que comienza en el nodo START 601. En una primera etapa, OB-NPK 602, se obtiene la clave pública sin SI del dispositivo sin SI a través de un primer canal de comunicación. Para ello, se establece el primer canal de comunicación, por ejemplo, a través de una red inalámbrica como Wi-Fi. El primer canal también puede ser un canal OOB como se ha explicado anteriormente, por ejemplo, la clave pública sin SI puede ser obtenida por el dispositivo SI escaneando un código QR impreso.

En una etapa siguiente SH-VER 603, se comparte un código de verificación con el dispositivo SI a través de un segundo canal de comunicación. Para ello, se establece un segundo canal de comunicación, por ejemplo, a través de una comunicación inalámbrica diferente al primer canal de comunicación. El primer y segundo canal de comunicación son diferentes, mientras que uno de los primeros y segundos canales de comunicación es un canal OOB. Por ejemplo, el código de verificación puede ser compartido a través de un canal OOB mostrando el código en el dispositivo SI, mientras que el usuario debe ingresar el código manualmente en el dispositivo sin SI. En una etapa siguiente, se recibe el RC-PRO 604, prueba de posesión de la clave privada sin SI, utilizando cualquiera de los

protocolos mencionados anteriormente a través del primer o segundo canal de comunicación, la cual clave privada sin SI constituye un par con la clave pública sin SI del dispositivo sin SI.

En una etapa siguiente EV-PRO 605, se evalúa la prueba recibida, y si la evaluación de la prueba no tiene éxito, el procedimiento termina como se indica por la flecha 610 hacia el nodo FIN 608. No se obtienen datos de seguridad, por ejemplo, después de un período de tiempo de espera predeterminado. Además, se puede enviar un mensaje de aborto indicando que no hay datos de seguridad disponibles. Si la prueba ha sido evaluada con éxito, el dispositivo SI puede obtener los datos de seguridad como se describe anteriormente y enviar los datos de seguridad al dispositivo sin SI en una siguiente etapa TR-SEC 606.

Finalmente, en una etapa opcional MN-NSI 607, mientras los datos de seguridad permiten que el dispositivo sin SI acceda a la red central a través de la red local y una puerta de enlace entre la red local y la red central, el acceso y/o uso de la red central por parte del dispositivo sin SI puede ser monitoreado, por ejemplo, monitoreando la ubicación del dispositivo sin SI, o el acceso, servicios y/o tráfico del dispositivo sin SI. La secuencia de asociación se termina en el nodo END 608.

Existen muchas formas diferentes de implementar los procedimientos, como será evidente para un experto en la técnica. Por ejemplo, el orden de las etapas o pasos puede variar o algunas etapas pueden ejecutarse en paralelo. Además, entre los pasos, se pueden insertar otros pasos del procedimiento. Los pasos insertados pueden representar mejoras del procedimiento tal como se describe en la presente memoria o pueden no estar relacionados con el procedimiento.

Se proporcionan productos de programas informáticos, descargables desde una red y/o almacenados en un medio legible por ordenador y/o medio ejecutable por microprocesador, que comprenden instrucciones de código de programa para implementar el procedimiento anterior, la secuencia de conexión, el proceso de seguridad y otras operaciones adicionales cuando se ejecutan en un dispositivo informático. Entonces, el procedimiento de acuerdo con la invención puede ser ejecutado utilizando software, que comprende instrucciones para hacer que un sistema de procesador realice el respectivo procedimiento.

Normalmente, el dispositivo sin SI y el dispositivo SI que interactúan para ejecutar la secuencia de asociación, cada uno comprende un procesador acoplado a una memoria que contiene un código de software apropiado almacenado en los dispositivos; por ejemplo, ese software puede haber sido descargado y/o almacenado en una memoria correspondiente, por ejemplo, una memoria volátil como RAM o una memoria no volátil como Flash (no mostrado). Los dispositivos pueden estar equipados, por ejemplo, con microprocesadores y memorias (no mostrados). Alternativamente, los dispositivos pueden, en su totalidad o en parte, implementarse en lógica programable, por ejemplo, como una matriz de puertas programables en campo (FPGA). Los dispositivos y el servidor pueden implementarse, total o parcialmente, como un circuito integrado específico de aplicación (ASIC), es decir, un circuito integrado (IC) personalizado para su uso particular. Por ejemplo, los circuitos pueden ser implementados en CMOS, por ejemplo, utilizando un lenguaje de descripción de hardware como Verilog, VHDL, etc.

El software solo puede incluir aquellos pasos tomados por una subentidad particular del sistema. El software puede ser almacenado en un medio de almacenamiento adecuado, como un disco duro, un disquete, una memoria, etc. El software puede ser enviado como una señal a lo largo de un cable, de forma inalámbrica o utilizando una red de datos, por ejemplo, Internet. El software puede estar disponible para descargar y/o para su uso remoto en un servidor. Un procedimiento de acuerdo con la invención puede ser ejecutado utilizando una secuencia de bits dispuesta para configurar una lógica programable, por ejemplo, una matriz de puertas programables en campo (FPGA), para llevar a cabo el procedimiento. Se apreciará que el software puede estar en forma de código fuente, código objeto, un código intermedio de código fuente y objeto, como una forma parcialmente compilada, o en cualquier otra forma adecuada para su uso en la implementación del procedimiento de acuerdo con la invención. Una realización relacionada con un producto de programa informático comprende instrucciones ejecutables por ordenador correspondientes a cada uno de los pasos de procesamiento de al menos uno de los procedimientos expuestos. Estas instrucciones pueden subdividirse en subrutinas y/o almacenarse en uno o más archivos que pueden estar enlazados estática o dinámicamente. Otra realización relacionada con un producto de programa informático comprende instrucciones ejecutables por ordenador correspondientes a cada uno de los medios de al menos uno de los sistemas y/o productos mencionados.

La Figura 7a muestra un medio legible por ordenador 1000 que tiene una parte escribible 1010 que comprende un programa informático 1020, el programa informático 1020 que comprende instrucciones para hacer que un sistema de procesador realice uno o más de los procedimientos y procesos anteriores en el sistema como se describe con referencia a las Figuras 1-6. El programa informático 1020 puede incorporarse en el medio legible por ordenador 1000 como marcas físicas o mediante la magnetización del medio legible por ordenador 1000. Sin embargo, también es concebible cualquier otra realización adecuada. Además, se apreciará que, aunque el medio legible por ordenador 1000 se muestra aquí como un disco óptico, el medio legible por ordenador 1000 puede ser cualquier medio legible por ordenador adecuado, como un disco duro, memoria de estado sólido, memoria flash, etc., y puede ser no grabable o grabable. El programa informático 1020 comprende instrucciones para hacer que un sistema de procesador realice dichos procedimientos.

La Figura 7b muestra en una representación esquemática de un sistema de procesador 1100 de acuerdo con una realización de los dispositivos o procedimientos descritos con referencia a las Figuras 1-6. El sistema del procesador puede comprender un circuito 1110, por ejemplo, uno o más circuitos integrados. La arquitectura del circuito 1110 se muestra esquemáticamente en la Figura. El circuito 1110 comprende una unidad de procesamiento 1120, por ejemplo, una CPU, para ejecutar componentes de programas informáticos y llevar a cabo un procedimiento de acuerdo con una realización y/o implementar sus módulos o unidades. El circuito 1110 comprende una memoria 1122 para almacenar código de programación, datos, etc. Parte de la memoria 1122 puede ser de solo lectura. El circuito 1110 puede comprender un elemento de comunicación 1126, por ejemplo, una antena, un transceptor, conectores o ambos, y similares. El circuito 1110 puede comprender un circuito integrado dedicado 1124 para realizar parte o todo el procesamiento definida en el procedimiento. El procesador 1120, la memoria 1122, el circuito integrado dedicado 1124 y el elemento de comunicación 1126 pueden estar conectados entre sí a través de una interconexión 1130, como por ejemplo un bus. El sistema de procesador 1110 puede estar configurado para comunicación por cable y/o inalámbrica, utilizando conectores y/o antenas, respectivamente.

Se apreciará que, para mayor claridad, la descripción anterior describe realizaciones de la invención con referencia a diferentes unidades funcionales y procesadores. Sin embargo, será evidente que cualquier distribución adecuada de funcionalidad entre diferentes unidades funcionales o procesadores puede ser utilizada sin desviarse de la invención. Por ejemplo, la funcionalidad ilustrada para ser realizada por unidades, procesadores o controladores separados puede ser realizada por el mismo procesador o controladores. Por lo tanto, las referencias a unidades funcionales específicas solo deben considerarse como referencias a medios adecuados para proporcionar la funcionalidad descrita, en lugar de indicar una estructura u organización lógica o física estricta. La invención puede ser implementada en cualquier forma adecuada, incluyendo hardware, software, firmware o cualquier combinación de estos.

Se observa que en este documento el verbo 'comprender' no excluye la presencia de elementos o pasos distintos a los mencionados, y la palabra 'un' o 'una' que precede a un elemento no excluye la presencia de una pluralidad de dichos elementos. Expresiones como "al menos uno de" cuando preceden a una lista de elementos representan una selección de todos o de cualquier subconjunto de elementos de la lista. Por ejemplo, la expresión "al menos uno de A, B y C" debe entenderse como incluyendo solo A, solo B, solo C, tanto A como B, tanto A como C, tanto B como C, o todos A, B y C. Cualquier signo de referencia no limita el alcance de las reivindicaciones. La invención puede ser implementada mediante hardware y software. Varios 'medios' o 'unidades' pueden estar representados por el mismo elemento de hardware o software, y un procesador puede cumplir la función de una o más unidades, posiblemente en cooperación con elementos de hardware. Además, la invención no se limita a las realizaciones descritas, y la invención radica en cada característica novedosa o combinación de características descritas anteriormente o mencionadas en reivindicaciones dependientes mutuamente diferentes.

En resumen, se dispone de un dispositivo sin SI para comunicación inalámbrica que coopera con un dispositivo SI que tiene acceso a la identidad de abonado. El dispositivo sin SI tiene un transceptor para comunicarse en una red local y un procesador para establecer una asociación con la SI. Se proporciona una clave pública sin SI al dispositivo SI a través de un primer canal de comunicación. Se comparte un código de verificación con el dispositivo SI a través de un segundo canal de comunicación. Los canales son diferentes e incluyen un canal fuera de banda, OOB. Se proporciona una prueba de posesión de una clave privada sin SI al dispositivo SI a través del primer o segundo canal de comunicación. Desde el dispositivo SI, se recibe datos de seguridad que están relacionados con la SI y se calculan utilizando la clave pública sin SI. Los datos de seguridad permiten de manera confiable que el dispositivo sin SI acceda a la red central a través de la red local y una puerta de enlace entre la red local y la red central.

Documentos de referencia:

IEEE Computer Society, "IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," (IEEE Std. 802.11-2016), December 2016

[DH]Diffie, W.; Hellman, M. (1976), "New directions in cryptography", IEEE Transactions on Information Theory, 22 (6): 644-654

[DPP]Device Provisioning Protocol - Technical Specification - Version 1.0, Wi-Fi Alliance, 2018

[HOTSPOT]Hotspot 2.0 (Release 2) Technical Specification Package (see <https://www.wi-fi.org/discover-wi-fi/passpoint>)

[RFC 4301]"Security Architecture for the Internet Protocol", December 2005, <https://datatracker.ietf.org/doc/rfc4301/>

[RFC 5246]"The Transport Layer Security (TLS) Protocol, Version 1.2", August 2008, <https://datatracker.ietf.org/doc/rfc5246/>

[RFC 6101]"The Secure Sockets Layer (SSL) Protocol Version 3.0", August 2011,
<https://datatracker.ietf.org/doc/rfc6101/>

5 [TS 23.402]3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;
Architecture enhancements for non-3GPP accesses (Release 15); 3GPP TS 23.402 V15.3.0 (2018-03)
http://www.3gpp.org/ftp//Specs/archive/23_series/23.402/23402-f30.zip

10 [TS 24.302]3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals;
Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 (Release 15); 3GPP
TS 24.302 V15.3.0 (2018-06)

15 [TS 33.402]3rd Generation Partnership Project; Technical Specification Group Services and System Aspects;
3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses (Release 15); 3GPP TS
33.402 V15.1.0 (2018-06)

REIVINDICACIONES

1. Dispositivo sin identidad de abonado, sin SI, dispuesto para la comunicación inalámbrica (130) en una red local (236) de acuerdo con un protocolo de comunicación local,
 - el protocolo de comunicación local que define mensajes de protocolo y la transmisión-recepción inalámbrica en un área limitada,
 - el dispositivo sin SI (120) que no comprende una SI y está dispuesto para cooperar con un dispositivo SI que tiene acceso a la SI,
 - la SI que comprende datos de identidad de abonado de un abonado a un proveedor para acceder a una red central (230), la red central proporciona comunicación inalámbrica para dispositivos móviles a través de al menos un área regional,
 - el dispositivo sin SI que comprende
 - una clave privada sin SI que constituye un par con una clave pública sin SI;
 - un transceptor (121) dispuesto para la transmisión-recepción local de acuerdo con el protocolo de comunicación local;
 - un procesador (122) dispuesto para ejecutar una secuencia de asociación para establecer una asociación con la SI, comprendiendo la secuencia de asociación
 - proporcionar la clave pública sin SI al dispositivo SI a través de un primer canal de comunicación,
 - compartir un código de verificación con el dispositivo SI a través de un segundo canal de comunicación para verificar que el dispositivo SI ha obtenido la clave pública sin SI,
 - el primer y segundo canal de comunicación son diferentes y uno de los canales es un canal fuera de banda, OOB, (140),
 - proporcionar prueba de posesión de la clave privada sin SI al dispositivo SI a través del primer o segundo canal de comunicación,
 - recibir, tras una evaluación exitosa de la prueba proporcionada, desde el dispositivo SI, datos de seguridad generados en nombre del proveedor utilizando la clave pública sin SI,

los datos de seguridad que permiten al dispositivo sin SI acceder a la red central a través de la red local y una puerta de enlace entre la red local y la red central.
2. Dispositivo como se reivindicó en la reivindicación 1, en el que la secuencia de asociación comprende proporcionar un canal seguro como el otro canal del primer y segundo canal de comunicación mediante la conexión
 - un protocolo de capa de sockets seguros, SSL [RFC 6101], o un protocolo de seguridad de capa de transporte, TLS [RFC 5246], con el dispositivo sin SI que actúa como servidor, donde el dispositivo sin SI proporciona la clave pública sin SI en un certificado autofirmado y utiliza este certificado como certificado de servidor en un mensaje de certificado de servidor; o
 - un protocolo SSL o TLS como con el dispositivo sin SI que actúa como cliente, donde el dispositivo sin SI proporciona la clave pública sin SI en un certificado autofirmado en un establecimiento de comunicación autenticado por el cliente; o
 - un túnel de seguridad del protocolo de Internet, IPsec [RFC 4301], establecido mediante cifrado de clave pública en el que se utiliza la clave pública sin SI o la clave privada sin SI; o
 - un protocolo de aprovisionamiento de dispositivos, DPP [DPP], protocolo de autenticación, donde el dispositivo sin SI proporciona la clave pública sin SI o una clave pública sin SI adicional como clave de inicio de DPP o como clave de protocolo DPP.
3. Dispositivo como se reivindicó en la reivindicación 2, en el que dicha recepción de los datos de seguridad comprende recibir los datos de seguridad a través del canal seguro.
4. Dispositivo como se reivindicó en cualquiera de las reivindicaciones 1 a 3, en el que el canal OOB se proporciona a través de uno del grupo
 - un protocolo de comunicación de radio de corto alcance como NFC o Bluetooth,
 - un canal visual que utiliza un código visual como un código de barras o un código QR en el lado del dispositivo sin SI y un escáner o cámara en el lado del dispositivo SI,
 - un canal de usuario donde se muestra un código en el lado del dispositivo SI y debe ingresarse en el lado del sistema sin SI,
 - un canal de usuario donde se muestra un código en el lado del dispositivo sin SI y debe ingresarse en el lado del sistema SI, o debe compararse con código adicional en el lado del dispositivo SI, y
 - un canal de usuario donde debe ingresarse un código en el dispositivo sin SI y debe ingresarse un código relacionado en el dispositivo SI.

5. Dispositivo como se reivindicó en cualquiera de las reivindicaciones 1 a 4, en el que los datos de seguridad comprenden credenciales relacionadas con la SI, cifrándose al menos parte de las credenciales utilizando la clave pública sin SI.
- 5 6. Dispositivo como se reivindicó en cualquiera de las reivindicaciones 1 a 5, en el que la clave pública sin SI comprende una primera clave pública sin SI y una segunda clave pública sin SI, correspondientes respectivamente a una primera clave privada sin SI y una segunda clave privada sin SI,
 - 10 - la primera clave pública sin SI se proporciona inicialmente al dispositivo SI a través del canal OOB, y la segunda clave pública sin SI se utiliza posteriormente para generar los datos de seguridad.
7. Dispositivo como se reivindicó en cualquiera de las reivindicaciones 1 a 6, en el que el procesador se dispone además para
 - 15 - recibir mensajes de latidos cardíacos del dispositivo SI, transfiriendo el dispositivo SI los mensajes de latidos cardíacos al recibir los mensajes de latidos cardíacos de la red central, y transferir los mensajes de latidos cardíacos a la red central a través de la puerta de enlace; o
 - recibir mensajes de latido del corazón desde la red central a través de la puerta de enlace y transferir los mensajes de latido del corazón al dispositivo SI, transfiriendo el dispositivo SI los mensajes de latido del corazón a la red central;
- 20 para permitir que la red central deshabilite el acceso del dispositivo sin SI a la red central al no recibir, durante un intervalo predeterminado, los mensajes de latido del dispositivo sin SI.
- 25 8. Dispositivo como se reivindicó en cualquiera de las reivindicaciones 1 a 7, en el que el procesador se configura además para gestionar una multitud de cuentas de usuario, y para
 - selectivamente para las cuentas de usuario respectivas, ejecutar la secuencia de asociación para establecer múltiples instancias respectivas de datos de seguridad, y
 - 30 - selectivamente para una cuenta de usuario respectiva, permitir que el dispositivo sin SI acceda a la red central en base a la instancia respectiva de datos de seguridad.
9. Dispositivo de identidad de abonado, SI, (110) dispuesto para la comunicación inalámbrica (130) con un dispositivo sin SI (120), teniendo el dispositivo SI acceso a una SI,
 - 35 - la SI que comprende datos de identidad de abonado de un abonado a un proveedor para acceder a una red central (230), proporcionando la red central comunicación inalámbrica para dispositivos móviles a través de al menos un área regional, el dispositivo SI que comprende
 - 40 - un transceptor (111) dispuesto para la comunicación inalámbrica con el dispositivo sin SI,
 - un procesador (112) dispuesto para ejecutar una secuencia de asociación para establecer una asociación con la SI, comprendiendo la secuencia de asociación
 - obtener una clave pública sin SI del dispositivo sin SI a través de un primer canal de comunicación,
 - 45 - compartir un código de verificación con el dispositivo sin SI a través de un segundo canal de comunicación para verificar que el dispositivo SI ha obtenido la clave pública sin SI,
 - el primer y segundo canal de comunicación son diferentes y uno de los canales es un canal fuera de banda, OOB, (140),
 - recibir, a través del primer o segundo canal de comunicación, una prueba de posesión de una clave privada sin SI que constituye un par con la clave pública sin SI del dispositivo sin SI,
 - 50 - tras una evaluación exitosa de la prueba recibida, obtener datos de seguridad generados en nombre del proveedor utilizando la clave pública sin SI, y
 - transmitir los datos de seguridad al dispositivo sin SI,
- los datos de seguridad que permiten al dispositivo sin SI acceder a la red central a través de la red local y una puerta de enlace entre la red local y la red central.
- 55 10. Dispositivo SI como se reivindicó en la reivindicación 9, que comprende
 - un módulo de identidad de abonado, SIM, (116) que comprende los datos de identidad de abonado;
 - 60 - un transceptor adicional dispuesto para la comunicación inalámbrica con la red central.
11. Dispositivo SI como se reivindicó en la reivindicación 9 o 10, en el que el procesador está dispuesto para
 - 65 - recibir mensajes de latidos del corazón desde la red central y transferir los mensajes de latidos del corazón al dispositivo sin SI, o

- recibir mensajes de latidos del corazón del dispositivo sin SI y transferir los mensajes de latidos a la red central

para permitir que la red central deshabilite el acceso del dispositivo sin SI a la red central al no recibir, durante un intervalo predeterminado, los mensajes de latidos del corazón del dispositivo sin SI.

12. Dispositivo SI como se reivindicó en la reivindicación 9, 10 o 11, en el que el procesador está dispuesto para

- recibir y transmitir una cierta parte de la comunicación de datos entre el dispositivo sin SI y la red central, mientras se cifra parte de los datos transmitidos utilizando una clave relacionada con la SI,

para determinar que la comunicación de datos del dispositivo sin SI está habilitada a través del dispositivo SI.

13. Dispositivo SI como se reivindicó en cualquiera de las reivindicaciones 9 a 12, en el que el procesador está dispuesto

- para determinar si la ubicación del dispositivo sin SI se encuentra dentro de un rango permitido, o
- para medir si la distancia entre el dispositivo SI y el dispositivo sin SI está dentro del rango permitido,

para permitir que la red central deshabilite el acceso del dispositivo sin SI a la red central al encontrar que el dispositivo sin SI no se encuentra dentro del rango permitido.

14. Procedimiento para su uso en un dispositivo sin identidad de abonado, sin SI, dispuesto para la comunicación inalámbrica con un dispositivo SI, teniendo el dispositivo SI acceso a una SI,

-la SI que comprende datos de identidad de abonado de un abonado a un proveedor para acceder a una red central (230), proporcionando la red central comunicación inalámbrica para dispositivos móviles a través de al menos un área regional,

el dispositivo sin SI que comprende una clave privada sin SI que constituye un par con una clave pública sin SI,
el procedimiento que comprende

- proporcionar la clave pública sin SI al dispositivo SI a través de un primer canal de comunicación,
- compartir un código de verificación con el dispositivo SI a través de un segundo canal de comunicación para verificar que el dispositivo SI ha obtenido la clave pública sin SI,
- el primer y segundo canal de comunicación son diferentes y uno de los canales es un canal fuera de banda, OOB,
- proporcionar prueba de posesión de la clave privada sin SI al dispositivo SI a través del primer o segundo canal de comunicación,
- recibir, tras una evaluación exitosa de la prueba proporcionada, desde el dispositivo SI, datos de seguridad generados en nombre del proveedor utilizando la clave pública sin SI,

los datos de seguridad que permiten al dispositivo sin SI acceder a la red central a través de la red local y una puerta de enlace entre la red local y la red central.

15. Procedimiento para su uso en un dispositivo de identidad de abonado, SI, dispuesto para la comunicación inalámbrica con un dispositivo sin SI, teniendo el dispositivo SI acceso a una SI,

- la SI que comprende datos de identidad de abonado de un abonado a un proveedor para acceder a una red central (230), proporcionando la red central comunicación inalámbrica para dispositivos móviles a través de al menos un área regional,
el procedimiento que comprende

- obtener una clave pública sin SI del dispositivo sin SI a través de un primer canal de comunicación,
- compartir un código de verificación con el dispositivo sin SI a través de un segundo canal de comunicación para verificar que el dispositivo SI ha obtenido la clave pública sin SI,
- el primer y segundo canal de comunicación son diferentes y uno de los canales es un canal fuera de banda, OOB,
- recibir, a través del primer o segundo canal de comunicación, una prueba de posesión de una clave privada sin SI que constituye un par con la clave pública sin SI del dispositivo sin SI,
- tras una evaluación exitosa de la prueba recibida, obtener datos de seguridad generados en nombre del proveedor utilizando la clave pública sin SI, y
- transmitir los datos de seguridad al dispositivo sin SI,

los datos de seguridad que permiten al dispositivo sin SI acceder a la red central a través de la red local y una puerta de enlace entre la red local y la red central.

16. Producto de programa informático descargable desde una red y/o almacenado en un medio legible por ordenador y/o medio ejecutable por microprocesador, comprendiendo el producto instrucciones de código de programa para implementar un procedimiento de acuerdo con las reivindicaciones 14 o 15 cuando se ejecuta en un dispositivo informático.

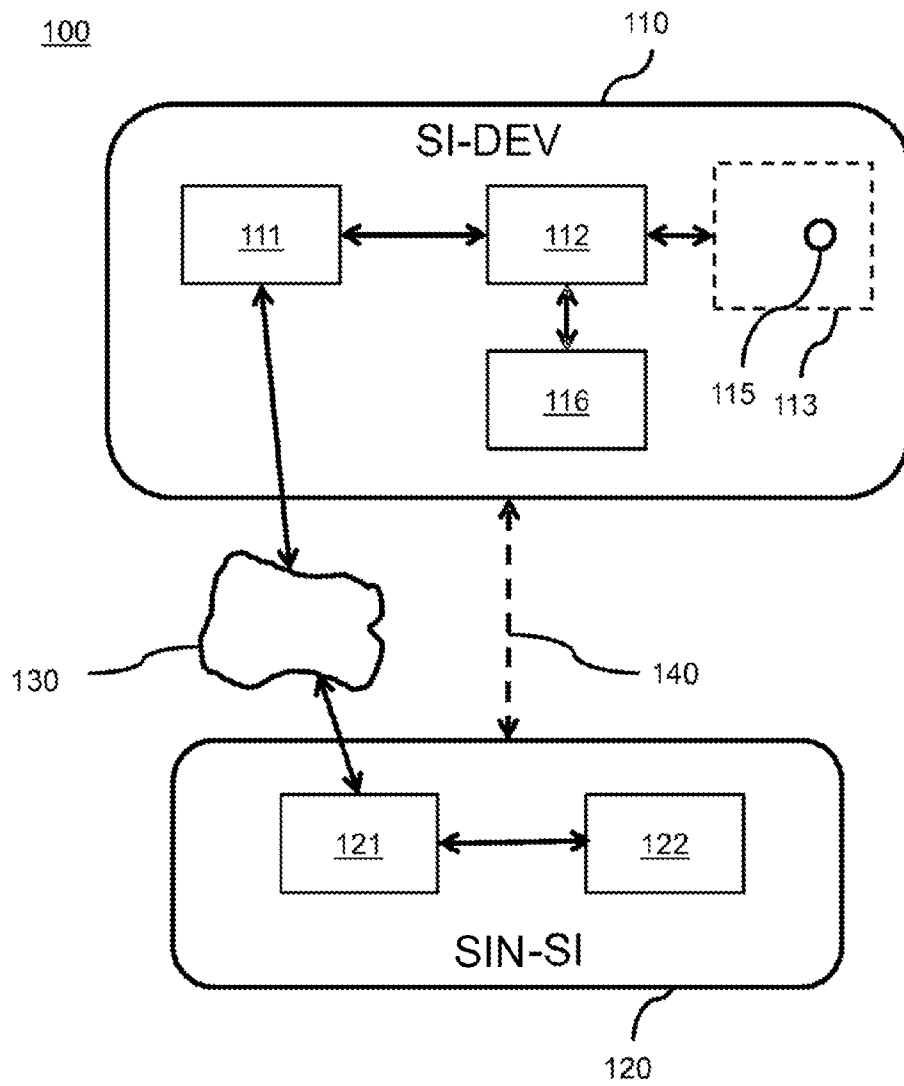


Figura 1

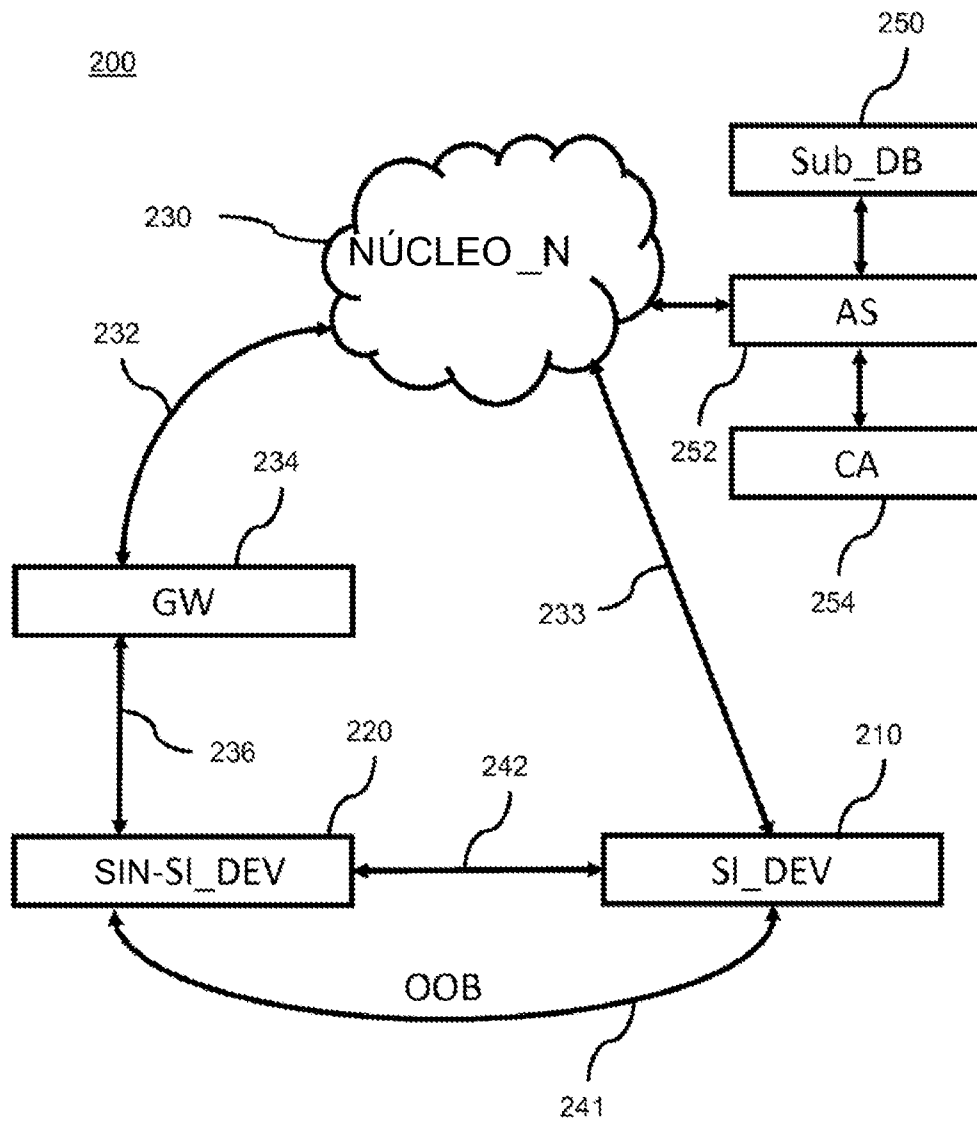


Figura 2

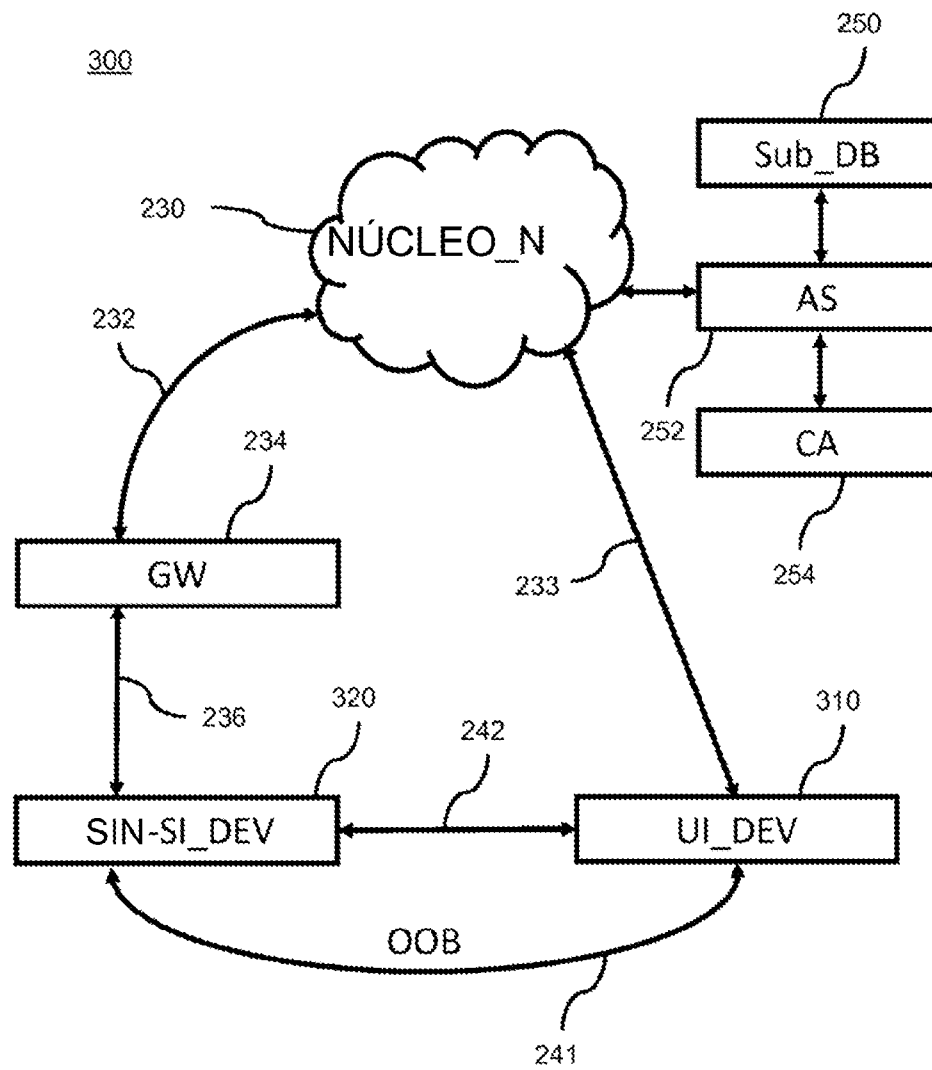


Figura 3

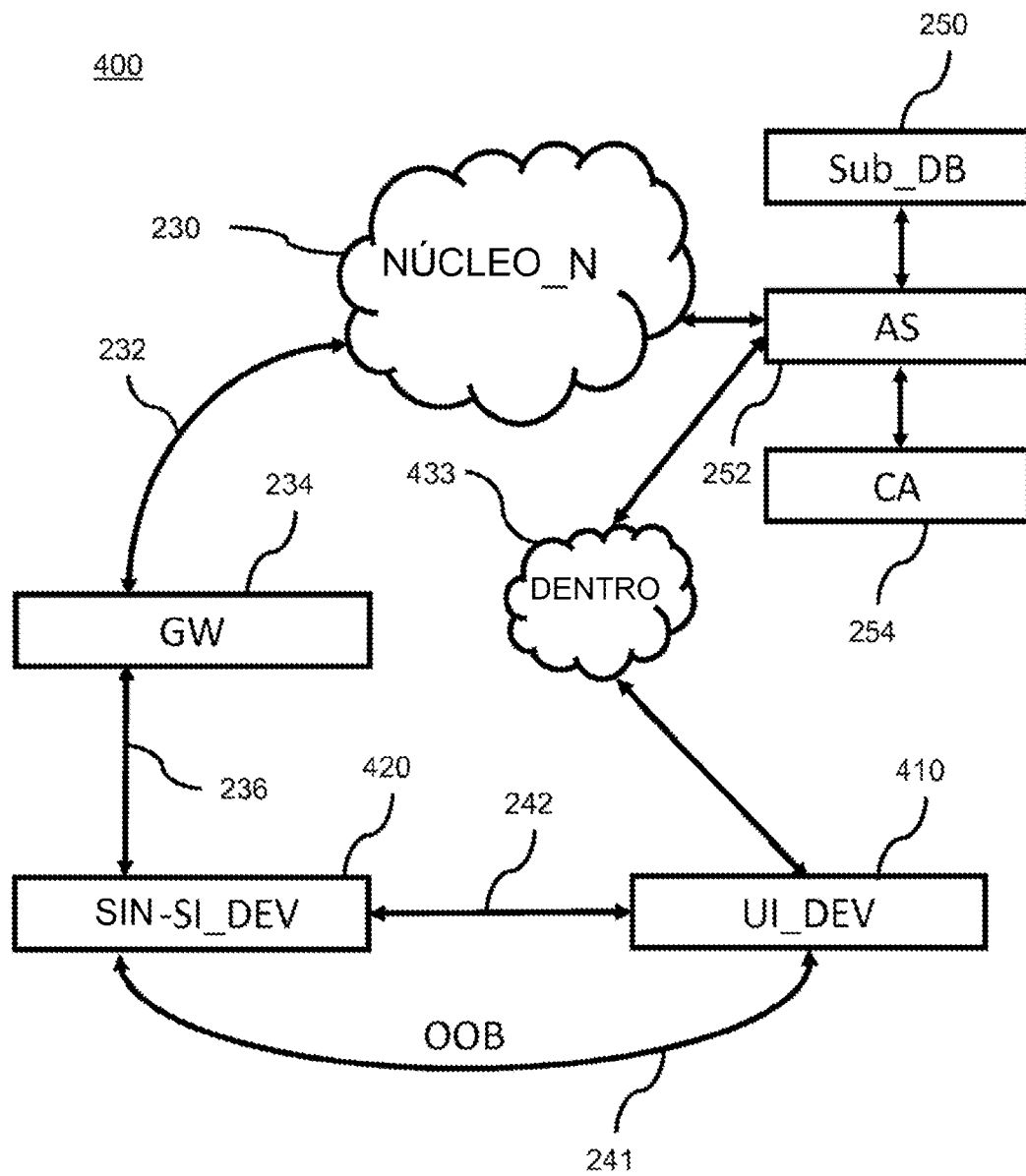


Figura 4

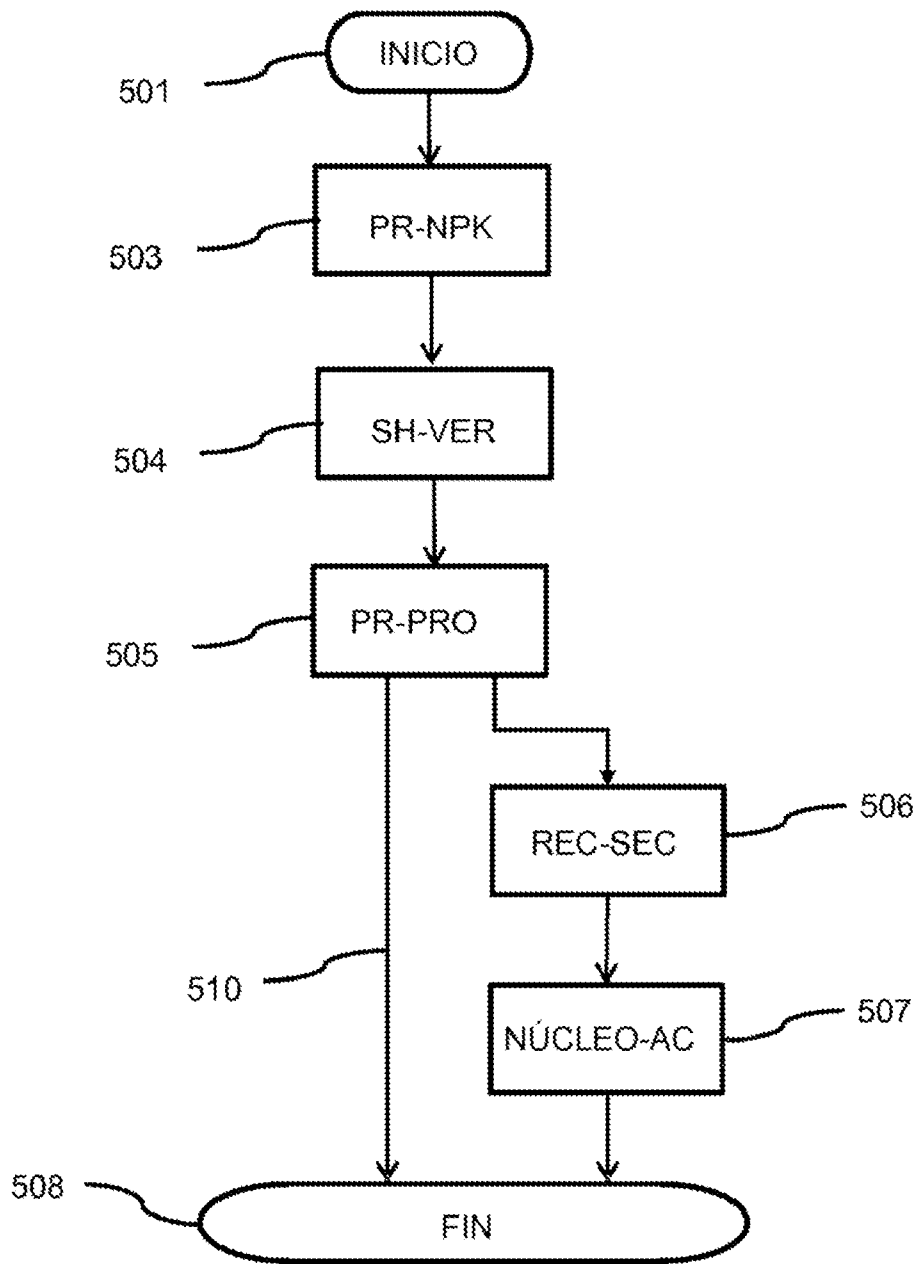


Figura 5

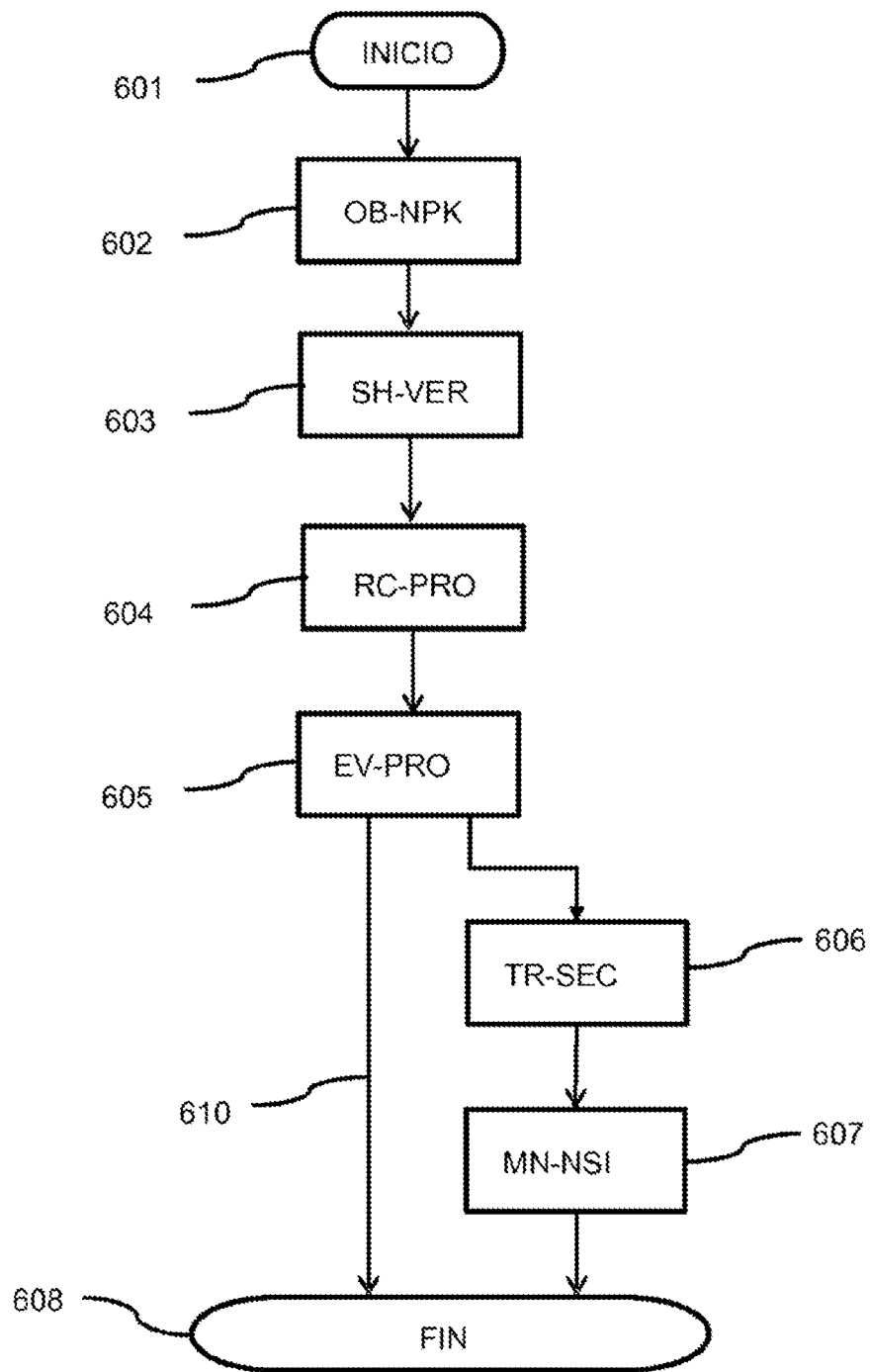


Figura 6

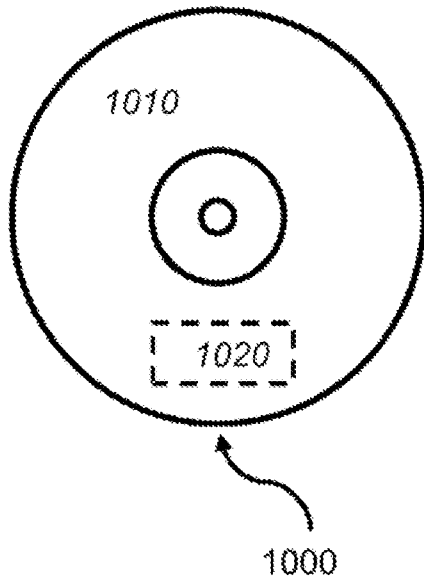


Figura 7a

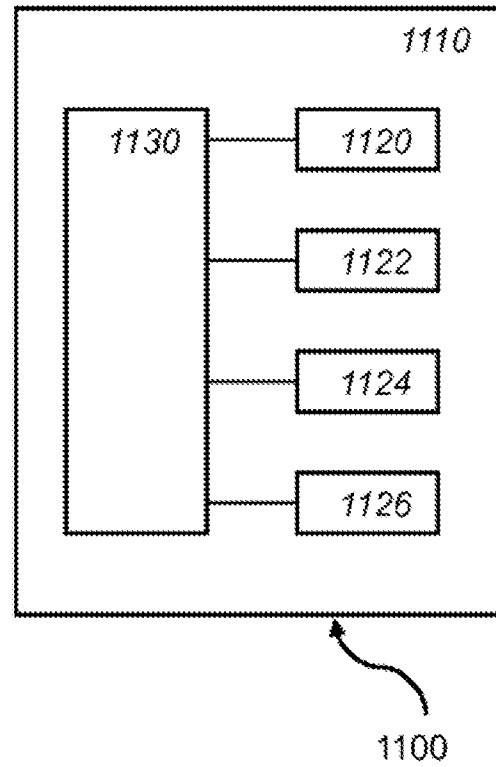


Figura 7b