(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 077**

(51) Int. Cl.:
H04W 12/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06710685 .6**
(96) Fecha de presentación : **17.01.2006**
(97) Número de publicación de la solicitud: **1844595**
(97) Fecha de publicación de la solicitud: **17.10.2007**

(54) Título: **Autenticación usando funcionalidad GAA para conexiones de red unidireccionales.**

(30) Prioridad: **03.02.2005 EP 05002300**
19.04.2005 US 108848

(45) Fecha de publicación de la mención BOPI:
18.05.2011

(45) Fecha de la publicación del folleto de la patente:
18.05.2011

(73) Titular/es: **NOKIA CORPORATION**
Keilalahdentie 4
02150 Espoo, FI

(72) Inventor/es: **Laitinen, Pekka**

(74) Agente: **López Bravo, Joaquín Ramón**

DESCRIPCIÓN

Autenticación usando funcionalidad GAA para conexiones de red unidireccionales

Campo de la invención

La presente invención se refiere a procedimientos, entidades de red, un sistema y un producto de programa de ordenador para la autenticación entre una entidad cliente y una red, en donde la entidad cliente no es capaz de comunicarse con la red de manera bidireccional. En particular, la presente invención se refiere a la autenticación usando funcionalidades de acuerdo a una arquitectura genérica de autenticación, GAA, p. ej., en escenarios de difusión.

Antecedentes de la invención

En años recientes, se han desarrollado diversas clases de sistemas de comunicación, en particular, sistemas de comunicación móvil y / o basada en IP (IP: Protocolo de Internet), así como una multitud de servicios ofrecidos en estos sistemas.

En tales sistemas de comunicación avanzada, tales como, p. ej., las redes de comunicación móvil de Tercera Generación actualmente en desarrollo por parte del Programa de Asociación de Tercera Generación (3GPP), los aspectos relacionados con la seguridad y la fiabilidad están jugando un papel cada vez más importante.

A partir del concepto de certificados de abonado, que dan soporte a los servicios que proporcionan los operadores móviles, y cuya provisión asiste a los operadores móviles, y en consideración de una necesidad de capacidades de seguridad más genéricas, el trabajo de estandarización del 3GPP se ha concentrado recientemente en la evolución de una arquitectura de autenticación genérica (GAA). Como puede colegirse a partir de la Figura 1, que muestra una visión general de un entorno de arquitectura de autenticación genérica en interrelación con un sistema HSS 14 de abonado doméstico, un equipo UE 12 de usuario y una entidad NE 13 de red, la GAA 11 consiste básicamente en tres subaspectos. Esto es, una arquitectura genérica de arranque (GBA) 11b, certificados 11a de abonado y un agente (AP) 11c de autenticación, en base, p. ej., al HTTPS (Protocolo Seguro de Transporte de Hipertexto). Por ello, la arquitectura genérica de arranque (GBA) también construye una base también para los otros subaspectos en los que la GBA ofrece una capacidad genérica de autenticación para diversas aplicaciones en base a un secreto compartido. Usualmente, la funcionalidad de la GBA es arrancar la autenticación y la concordancia de claves para la seguridad de la aplicación, y se basa en el mecanismo de Autenticación y Concordancia de Claves (AKA) Resumido del HTTP, de acuerdo al documento IETF RFC 3310.

En la Figura 2, se ilustra un modelo de red para el arranque genérico. Una función BSF 13a servidora de arranque y el equipo UE12 de usuario, que están conectados mediante un enlace bidireccional Ub, se autentican mutuamente usando el protocolo AKA, y concuerdan acerca de las claves de sesión. Estas claves han de usarse después para una sesión de arranque y han de usarse entre el equipo 12 de usuario y una función NAF 13b de aplicación de red, controlada por el operador, que también está conectada con el equipo 12 de usuario por medio de un enlace bidireccional Ua. Después del procedimiento de arranque, que se describe en detalle más adelante, el equipo 12 de usuario y la función 13b de aplicación de red pueden ejecutar algún protocolo específico para la aplicación, donde la autenticación de mensajes se basará en aquellas claves de sesión generadas durante la autenticación mutua. En consecuencia, la GAA / GBA puede considerarse, en general, como un escenario de autenticación de 3 partes, en el cual la función 13a servidora de arranque está adicionalmente conectada con un sistema HSS 14 de abonado doméstico que mantiene, p. ej., las configuraciones de seguridad del usuario (USS).

Los puntos (interfaces) de referencia entre las entidades individuales en la Figura 2 se indican con Ub, Ua, Zn y Zh. Las interfaces Zn y Zh se basan en Diameter (según el Protocolo Básico Diameter, que está especificado en el documento IETF RFC 3588), la interfaz Ub se basa en una reutilización de los mensajes de la AKA Resumida del HTTP, y el protocolo usado en la interfaz Ua depende de la aplicación a ejecutar.

La utilización de la arquitectura genérica de arranque se divide en dos fases. La primera fase, es decir, el procedimiento de arranque (genérico) como tal, se ilustra en la Figura 3 y la segunda fase, es decir, el procedimiento genérico de uso del arranque, se ilustra en la Figura 4.

En el procedimiento de arranque según la Figura 3, el equipo UE 12 de usuario envía una solicitud del HTTP hacia la función BSF 13a servidora de arranque (etapa S31). En la etapa S32, la BSF 13a extrae el perfil del usuario y un reto, es decir, un vector (VA) de autenticación, por la interfaz Za, proveniente del sistema HSS 14 de abonado doméstico. Luego, en la etapa S33, la BSF 13a remite los parámetros RAND y AUTN de autenticación al UE 12 a fin de solicitar al UE 12 que se autentique a sí mismo. El UE 12 calcula un código de autenticación de mensaje (MAC), a fin de verificar el reto proveniente de la red autenticada, así como también calcula las claves CK, IK y RES de sesión. Así, las claves CK, IK y RES de sesión están disponibles tanto en la BSF 13a como en el UE 12. En la etapa S35, el UE 12 envía nuevamente una solicitud a la BSF 13a, y la BSF 13a comprueba, en la etapa S36, si el parámetro recibido está

calculado usando RES y es igual al parámetro que se calcula de manera similar usando XRES, que ha sido obtenido antes como parte del vector de autenticación proveniente del HSS 14. Si estos parámetros son iguales, el UE 12 está autenticado, y la BSF 13a genera una clave ("clave maestra") Ks concatenando las claves CK e IK de sesión (etapa S37). La clave Ks se usa entonces para asegurar la interfaz Ua. En la etapa S38, la BSF 13a envía un mensaje de validación que incluye un identificador B-TID de transacción y otros datos posibles (tales como, por ejemplo, una vida útil de la clave Ks) al UE 12, por medio del cual se indica el éxito de la autenticación. Concatenando las claves CK e IK de sesión, la clave Ks para asegurar la interfaz Ua también se genera luego en el UE 12 (etapa S39). Con ello, se ha iniciado con éxito una sesión de arranque entre el equipo de usuario (cliente) y la función servidora de arranque.

En la Figura 4, se ilustra un ejemplo de procedimiento que usa una asociación de seguridad arrancada. Después de haber iniciado una sesión de arranque (S40a), el UE 12 puede comenzar a comunicarse con la función NAF 13b de aplicación de red. Por ello, la clave maestra Ks generada durante el procedimiento de arranque en el UE 12 y en la BSF 13a se usa para obtener la clave Ks_NAF específica de la NAF (etapa S40b). Una solicitud de aplicación (etapa S41) incluye el identificador de transacción B-TID obtenido durante el arranque, un conjunto de datos específicos de la aplicación, indicado por msje, y con todas las credenciales indicadas por MAC. En la etapa S42, la NAF 13b solicita una o más claves y, posiblemente, datos del perfil de usuario correspondientes a la información proporcionada por el UE 12 por la interfaz Zn desde la BSF 13a. Tal solicitud, p. ej., puede basarse en el identificador de transacción. Entre las etapas S42 y S43, la clave Ks_NAF específica de la NAF es generada en la entidad 13a de la BSF. En la etapa S43, la BSF 13a responde proporcionando la clave o claves solicitadas (incluyendo Ks_NAF y una parte específica de la aplicación del perfil de usuario, indicado por Perf) a la NAF 13b, que la NAF 13b usa directamente, o con las cuales la NAF 13b obtiene claves adicionales requeridas para proteger el protocolo usado sobre la interfaz Ua hacia el UE 12, que es una funcionalidad específica de la aplicación y que no se menciona en las especificaciones de la GAA. Tal deducción se lleva a cabo de la misma manera en que lo hizo el UE 12 de antemano.

Luego, la entidad NAF 13b almacena (etapa S44) al menos los parámetros Ks_NAF, Perf y la vida útil de la clave. Después, la NAF 13b continúa con el protocolo usado sobre la interfaz Ua enviando una respuesta de aplicación al UE 12 (etapa S45).

Para mayores detalles sobre la arquitectura genérica de arranque, se hace referencia a la especificación técnica 3GPP TS 33.220 (versión 6.3.0) de diciembre de 2004.

A la vista de la arquitectura genérica convencional de autenticación y de la arquitectura genérica de arranque descrita anteriormente, surge el siguiente problema.

En resumen, el comportamiento normal convencional de la GAA del 3GPP es que un cliente, es decir, un equipo de usuario, arranque con la entidad BSF usando un vector de autenticación AKA. Como resultado, se obtienen las llamadas credenciales de la GAA, que consisten en una clave compartida Ks y un identificador de transacción de arranque (B-TID). Estas credenciales de la GAA se usan adicionalmente para obtener una clave específica del servidor (Ks_NAF). Las claves específicas de la NAF (es decir, B-TID y Ks_NAF) pueden usarse luego entre el cliente UE y la NAF servidora, tal como, p. ej., el nombre de usuario y la contraseña en los protocolos existentes, caso este que se indica con el término "genérico".

El procedimiento convencional de arranque requiere que el cliente tenga una conexión bidireccional con la entidad de la BSF, y el uso subsiguiente de las credenciales específicas de la NAF entre el UE y la NAF también requiere esto habitualmente. Así, el problema consiste en que los mecanismos convencionales de la GAA y / o la GBA no funcionan, es decir, no pueden usarse para la autenticación, en caso de que no haya ningún canal de retorno desde el equipo del usuario a la red. Un ejemplo para tal escenario son las redes de difusión, p. ej., siendo el equipo de usuario un aparato de sobremesa (STB; o digibox) para la difusión de vídeo digital. En tal escenario, la GAA y / o la GBA, según la técnica anterior, no pueden usarse, ya que el UE no puede ni arrancar con la BSF ni comunicarse con la NAF de manera bidireccional, según se requiere.

En una contribución al consorcio de DVB-H (Difusión de Vídeo Digital para equipos de mano) y el ETSI (Instituto Europeo de Estándares de Telecomunicación), Vodafone presentó una propuesta para una interfaz para un elemento basado en tarjeta del USIM (Módulo de Identidad de Abonado Universal), usado para obtener claves para la protección del servicio. Sin embargo, esta propuesta no es adecuada para superar el problema anteriormente descrito y los inconvenientes relacionados.

Así, se necesita una solución para el problema y los inconvenientes anteriores, a fin de brindar seguridad en tales escenarios, que están haciéndose cada vez más importantes para el uso futuro.

Resumen de la invención

En consecuencia, es un objeto de la presente invención eliminar los inconvenientes anteriores, inherentes a la técnica anterior, y proporcionar, por consiguiente, procedimientos, entidades de red, un sistema y un producto de programa de

ordenador mejorados.

El anterior objeto se logra mediante procedimientos, aparatos y productos de programa de ordenador, según lo definido en las reivindicaciones adjuntas.

Según un primer aspecto de la presente invención, este objeto, por ejemplo, es logrado por un procedimiento que comprende realizar la autenticación entre una entidad cliente (UE) y una red que comprende al menos una entidad de la función servidora de arranque (BSF) y una entidad de la función de aplicación de red (NAF), en el cual la entidad cliente (UE) tiene una conexión unidireccional de red que carece de un canal de retorno a la entidad de la función servidora de arranque de red (BSF) y / o a la entidad de la función de aplicación de red (NAF), comprendiendo la autenticación: transmitir (S62) una solicitud de información de autenticación desde la entidad de la función de aplicación de red a la entidad de la función servidora de arranque, comprendiendo dicha solicitud una identidad privada de la entidad cliente, cuando la entidad de la función de aplicación de red necesita transmitir datos con seguridad a la entidad cliente; procesar (S63) la solicitud y extraer la información de autenticación en la entidad de la función servidora de arranque, en donde dicha extracción comprende crear datos de sesión de arranque para la entidad cliente; transmitir (S64) una respuesta que incluye la información de autenticación, que comprende los datos de la sesión de arranque para la entidad cliente, desde la entidad de la función servidora de arranque a la entidad de la función de aplicación de red; transmitir (S66) la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente y los datos a transmitir, desde la entidad de la función de aplicación de red a la entidad cliente; y autenticar (S67) la red usando la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente, en la entidad cliente, en donde dicha autenticación comprende realizar una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

Según un segundo aspecto de la presente invención, este objeto es logrado, por ejemplo, por un programa de ordenador realizado en un medio legible por ordenador, estando el programa de ordenador configurado para cargarse en una memoria de un medio de procesamiento digital y para controlar dicho medio de procesamiento digital a fin de llevar a cabo el procedimiento según el primer aspecto.

Según un tercer aspecto de la presente invención, este objeto es logrado, por ejemplo, por un aparato, siendo dicho aparato operable como una entidad cliente para su uso dentro de una arquitectura de autenticación, a fin de realizar la autenticación entre la entidad cliente (UE) y una red, comprendiendo la red al menos una entidad de función servidora de arranque (BSF) y una entidad de función de aplicación de red (NAF), en donde la entidad cliente (UE) es operable para tener una conexión unidireccional de red que carece de un canal de retorno desde la entidad cliente a la entidad de la función servidora de arranque (BSF) y / o a la entidad de la función de aplicación de red (NAF), comprendiendo dicho aparato: un medio (87) de recepción para recibir, desde la entidad de la función de aplicación de red, información de autenticación de la entidad de la función servidora de arranque y datos a transmitir desde la entidad de la función de aplicación de red a la entidad cliente, comprendiendo dicha información de autenticación datos de sesión de arranque para la entidad cliente, y un medio (81) de autenticación para autenticar la red usando la información de autenticación recibida, que comprende los datos de sesión de arranque para la entidad cliente, en donde dicha autenticación comprende realizar una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

Según un cuarto aspecto de la presente invención, este objeto es logrado, por ejemplo, por un procedimiento, que comprende realizar la autenticación entre una entidad cliente (UE) y una red que comprende al menos una entidad de la función servidora de arranque (BSF) y una entidad de la función de aplicación de red (NAF), en donde la entidad cliente (UE) tiene una conexión unidireccional de red que carece de un canal de retorno desde la entidad cliente a la entidad de la función servidora de arranque (BSF) y / o a la entidad de la función de aplicación de red (NAF), comprendiendo la autenticación recibir (S66), desde la entidad de la función de aplicación de red, información de autenticación de la función servidora de arranque y datos a transmitir desde la entidad de la función de aplicación de red, comprendiendo dicha información de autenticación datos de sesión de arranque para la entidad cliente, y autenticar (S67) la red usando la información de autenticación recibida, que comprende los datos de sesión de arranque para la entidad cliente, en donde dicha autenticación comprende realizar una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

Según un quinto aspecto de la presente invención, este objeto es logrado, por ejemplo, por un programa de ordenador realizado en un medio legible por ordenador, estando el programa de ordenador configurado para cargarse en una memoria de un medio de procesamiento digital y para controlar dicho medio de procesamiento digital para realizar el procedimiento según el cuarto aspecto.

Según un sexto aspecto de la presente invención, este objeto es logrado, por ejemplo, por un aparato, siendo dicho aparato operable como una entidad de la función de aplicación de red, para su uso dentro de una arquitectura de autenticación a fin de llevar a cabo la autenticación entre una entidad cliente (UE) y una red, comprendiendo la red al menos el aparato que funciona como una entidad de la función de aplicación de red (NAF) y una entidad de la función servidora de arranque (BSF), donde la entidad cliente (UE) es operable para tener una conexión unidireccional de red

que carece de un canal de retorno desde la entidad cliente a la entidad de la función servidora de arranque (BSF) y / o a la entidad de la función de aplicación de red (NAF), comprendiendo el aparato:

un medio (91) transceptor para enviar a la entidad cliente, y para enviar y recibir desde la entidad de la función servidora de arranque, en donde el medio transceptor está adaptado para transmitir una solicitud de información de autenticación a la entidad de la función servidora de arranque, comprendiendo dicha solicitud una identidad privada de la entidad cliente, cuando la entidad de la función de aplicación de red necesita transmitir datos con seguridad a la entidad cliente, recibir una respuesta que incluye la información de autenticación, que comprende datos de sesión de arranque para la entidad cliente desde la entidad de la función servidora de arranque, y transmitir la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente y los datos a transmitir, a la entidad cliente,

en el cual dicha información de autenticación está adaptada para una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

Según un séptimo aspecto de la presente invención, este objeto es logrado, por ejemplo, por un procedimiento, que comprende realizar la autenticación entre una entidad cliente (UE) y una red que comprende al menos una entidad de la función servidora de arranque (BSF) y una entidad de la función de aplicación de red (NAF), en donde la entidad cliente (UE) tiene una conexión unidireccional de red que carece de un canal de retorno desde la entidad cliente a la entidad de la función servidora de arranque (BSF), y / o a la entidad de la función de aplicación de red (NAF), comprendiendo la autenticación transmitir (S62) una solicitud de información de autenticación a la entidad de la función servidora de arranque, comprendiendo dicha solicitud una identidad privada de la entidad cliente, cuando la entidad de la función de aplicación de red necesita transmitir datos con seguridad a la entidad cliente, recibir (S64) una respuesta que incluye la información de autenticación, que comprende datos de sesión de arranque para la entidad cliente, desde la entidad de la función servidora de arranque, y transmitir (S66) la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente y los datos a transmitir, a la entidad cliente,

en donde dicha información de autenticación está adaptada para una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

Según un octavo aspecto de la presente invención, este objeto es logrado, por ejemplo, por un programa de ordenador realizado en un medio legible por ordenador, estando el programa de ordenador configurado para cargarse en una memoria de un medio de procesamiento digital y para controlar dicho medio de procesamiento digital para realizar el procedimiento según el séptimo aspecto.

Según un noveno aspecto de la presente invención, este objeto es logrado, por ejemplo, por un aparato, siendo dicho aparato operable como una entidad de la función servidora de arranque, para su uso dentro de una arquitectura de autenticación, a fin de realizar la autenticación entre una entidad cliente (UE) y una red, comprendiendo la red al menos el aparato que funciona como una entidad de la función servidora de arranque (BSF) y una entidad de la función de aplicación de red (NAF), en donde la entidad cliente (UE) es operable para tener una conexión unidireccional de red que carece de un canal de retorno desde la entidad cliente a la entidad de la función servidora de arranque (BSF) y / o a la entidad de la función de aplicación de red (NAF), comprendiendo el aparato: un medio transceptor (101) para enviar a, y recibir desde, la entidad de la función de aplicación de red, y un medio (102) de procesamiento y extracción para procesar una solicitud recibida desde la entidad de la función de aplicación de red, comprendiendo dicha solicitud una identidad privada de la entidad cliente, y para extraer información de autenticación, comprendiendo adicionalmente dicho medio de procesamiento y extracción un medio (104) de creación, para crear datos de sesión de arranque para la entidad cliente, en donde el medio transceptor (101) está configurado para recibir la solicitud desde la entidad de la función de aplicación de red y para transmitir la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente, a la entidad de la función de aplicación de red, en donde dicha información de autenticación está adaptada para una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

Según un décimo aspecto de la presente invención, este objeto es logrado, por ejemplo, por un procedimiento, que comprende realizar la autenticación entre una entidad cliente (UE) y una red, que comprende al menos una entidad de la función servidora de arranque (BSF) y una entidad de la función de aplicación de red (NAF), en donde la entidad cliente (UE) tiene una conexión unidireccional de red que carece de un canal de retorno desde la entidad cliente a la entidad de la función servidora de arranque (BSF) y / o a la entidad de la función de aplicación de red (NAF), comprendiendo la autenticación recibir (S62) una solicitud de información de autenticación desde la entidad de la función de aplicación de red, comprendiendo dicha solicitud una identidad privada de la entidad cliente, procesar (S63) la solicitud recibida desde la entidad de la función de aplicación de red y extraer información de autenticación, que comprende adicionalmente crear datos de sesión de arranque para la entidad cliente, transmitir (S64) una respuesta, que incluye la información de autenticación que comprende los datos de sesión de arranque para la entidad cliente, a la entidad de la función de aplicación de red,

en donde dicha información de autenticación está adaptada para una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

Según un undécimo aspecto de la presente invención, este objeto es logrado, por ejemplo, por un programa de ordenador realizado en un medio legible por ordenador, estando el programa de ordenador configurado para cargarse en una memoria de un medio de procesamiento digital, y para controlar dicho medio de procesamiento digital, a fin de llevar a cabo el procedimiento según el décimo aspecto.

Desarrollos y / o modificaciones ventajosos adicionales de cualquiera de los aspectos anteriores se definen en las respectivas reivindicaciones adjuntas. Por ejemplo, puede valer al menos uno entre los siguientes:

- la transmisión de la solicitud es activada por un medio distinto a la entidad cliente;

- la solicitud comprende adicionalmente una identidad de la entidad de la función de aplicación de red;

- la extracción de información de autenticación comprende capturar la información de autenticación desde un sistema de abonado doméstico;

- la información de autenticación comprende adicionalmente al menos un parámetro de reto aleatorio o un parámetro de autenticación de red;

- la respuesta comprende adicionalmente una clave de la entidad de la función de aplicación de red;

- la transmisión de la información de autenticación comprende adicionalmente la transmisión de una identidad de la entidad de la función de aplicación de red;

- la autenticación de la red comprende adicionalmente generar una clave de la entidad de la función de aplicación de red en la entidad cliente;

- la autenticación de la red comprende adicionalmente establecer una sesión de arranque entre la entidad cliente y la entidad de la función servidora de arranque;

- el establecimiento de una sesión de arranque se basa en la información de autenticación de la entidad de la función de aplicación de red;

- la autenticación de la red comprende adicionalmente almacenar los datos de sesión de arranque en la entidad cliente;

- existe una sesión de arranque válida entre la entidad cliente y la entidad de la función servidora de arranque;

- existe permanentemente una sesión válida de arranque;

- el procesamiento de la solicitud comprende adicionalmente activar la entidad cliente para establecer una sesión válida de arranque;

- la información de autenticación comprende al menos datos de sesión de arranque;

- la respuesta comprende adicionalmente una clave de la entidad de la función de aplicación de red;

- la autenticación de la red comprende adicionalmente generar una clave de la entidad de la función de aplicación de red en la entidad cliente;

- el procedimiento comprende adicionalmente entrar inicialmente en contacto con la entidad de la función de aplicación de red y enviar su identidad privada, por parte de la entidad cliente;

- el procedimiento comprende adicionalmente activar, por parte de la entidad de la función de aplicación de red, la entidad cliente para establecer una sesión válida de arranque;

- el procedimiento comprende adicionalmente activar, por parte de la entidad de la función de aplicación de red, la entidad de la función servidora de arranque, a fin de activar un procedimiento de arranque no solicitado con la entidad cliente;

- el procedimiento comprende adicionalmente cifrar los datos a transmitir en la entidad de la función de aplicación de red, usando su clave;

- el procedimiento comprende adicionalmente descifrar los datos cifrados en la entidad cliente, usando la clave de la entidad de la función de aplicación de red;

- la red comprende una red de difusión;

- un aparato comprende al menos un equipo de usuario y es conectable con un módulo de identidad de abonado universal;

- la entidad cliente comprende un aparato descodificador;

- la información de identidad de usuario disponible en el aparato es accesible;

- la información de identidad de usuario se almacena en una tarjeta inteligente conectable con la entidad cliente; y / o

- un aparato está configurado para difundir transmisiones.

Es una ventaja de la presente invención que se proporciona una solución en cuanto a cómo puede usarse el concepto de la GAA del 3GPP en escenarios donde el cliente no tiene un canal de retorno a la red.

Con las realizaciones de la presente invención, la fase de arranque entre el cliente y la función servidora de arranque se elimina prácticamente. Además, es ventajoso que esta fase de arranque se combina parcialmente con el meta-protocolo (o los mensajes individuales) entre la función de aplicación de red y el cliente.

Es otra ventaja de la presente invención que el arranque de la autenticación y la concordancia de claves se habilita para el escenario que carece de un canal de retorno, es decir, que carece de una conexión bidireccional con la red.

Por medio de la presente invención, el concepto de GAA / GBA se amplía así en su área de aplicación.

Breve descripción de los dibujos

En lo que sigue, la presente invención se describirá en mayor detalle por medio de realizaciones de la misma, así como ejemplos comparativos con referencia a los dibujos adjuntos, en los cuales

la Figura 1 ilustra una vista general de un entorno de la arquitectura genérica de autenticación,

la Figura 2 ilustra un modelo de red para el arranque genérico,

la Figura 3 ilustra un procedimiento de arranque genérico según la técnica anterior,

la Figura 4 ilustra un procedimiento de uso genérico de arranque según la técnica anterior,

la Figura 5 ilustra un diagrama de señalización de un procedimiento según un primer ejemplo comparativo,

la Figura 6 ilustra un diagrama de señalización de un procedimiento según una realización de la presente invención,

la Figura 7 ilustra un diagrama de señalización de un procedimiento según un segundo ejemplo comparativo,

la Figura 8 ilustra un diagrama en bloques de una entidad cliente según una realización de la presente invención,

la Figura 9 ilustra un diagrama en bloques de una entidad de la función de aplicación de red, según una realización de la presente invención, y

la Figura 10 ilustra un diagrama en bloques de una entidad de la función servidora de arranque, según una realización de la presente invención.

Descripción detallada de las realizaciones de la presente invención

La presente invención se describe en el presente documento por medio de realizaciones de la misma, así como ejemplos comparativos, con referencia a escenarios ejemplares específicos no limitadores. Una persona experta en la técnica apreciará que la invención no se limita a estos ejemplos, y que puede aplicarse más extensamente.

La presente invención y sus realizaciones se orientan ejemplarmente a casos de entornos de GAA y / o GBA, donde un cliente, o equipo de usuario, no tiene un canal de retorno a la red. Comprendiendo la red al menos una entidad de la función de aplicación de red y una entidad de la función servidora de arranque, esto significa que un equipo de usuario (entidad cliente) no es capaz de comunicarse con ambas entidades de red de manera bidireccional. Dicho en otras palabras, esto significa que el equipo de usuario (entidad cliente) carece de una conexión bidireccional, es decir, un canal de retorno, a la entidad de la función de aplicación de red, o a la entidad de la función servidora de arranque, o a ambas entidades.

La Figura 5 ilustra un diagrama de señalización de un procedimiento según un primer ejemplo comparativo. La Figura 5 ilustra un escenario donde la entidad cliente, o el equipo UE 12 de usuario, no tiene ningún canal de retorno a la red, es decir, la entidad cliente no es capaz de comunicarse ni con la entidad 13b de la función de aplicación de red (NAF) ni con la entidad 13a de la función servidora de arranque (BSF) de manera bidireccional. Así, la entidad cliente no puede

realizar un procedimiento de arranque con la entidad BSF. Un ejemplo para tal escenario puede ser un equipo de sobremesa (STB; o digibox) que esté equipado con un lector de tarjeta UICC (Tarjeta Universal de Circuitos Integrados).

Se describe más adelante un procedimiento para realizar la autenticación entre la entidad cliente y la red, a fin de utilizar las funcionalidades de la GAA.

En la etapa S51, la entidad NAF 13b necesita entregar algunos datos (p. ej., claves de difusión) al cliente UE 12. La entidad NAF 13b conoce la identidad privada del abonado, es decir, la IMPI (identidad privada del subsistema de red central de Multimedios de IP) del abonado, y los datos que deben entregarse al UE 12. En la etapa S52, la entidad NAF 13b envía una solicitud, que incluye la IMPI del abonado, su propia identidad NAF_ID (es decir, el nombre del anfitrión de la NAF) y, optativamente, uno o más GSID (identificadores de servicio de GAA para solicitar configuraciones de seguridad de usuario específicas de la NAF), por el punto Zn de referencia, a la entidad 13a de la función servidora de arranque (BSF).

Ha de observarse que la transmisión de la solicitud (de la etapa 2) puede activarse por un medio distinto a la entidad cliente. Por ejemplo, en el caso de DVB-H, el procedimiento de autenticación (arranque), o la necesidad del mismo, puede ser activado en la red (por ejemplo, en la misma entidad de la NAF) por una necesidad de actualizar las claves de difusión en la entidad terminal.

Al recibir la solicitud desde la entidad NAF 13b, la entidad BSF 13a comprueba, en la etapa S53, si la entidad NAF 13b está autorizada para solicitar información de autenticación, p. ej., un elemento de autenticación de red (AUTN) y un reto aleatorio (RAND). Si es así, la entidad BSF 13a extrae vectores de autenticación de un sistema HSS 14 de abonado doméstico, calcula la clave Ks_NAF de la entidad NAF, en base a la identidad NAF_ID de la entidad NAF, y otros parámetros de obtención de claves. También extrae las configuraciones de seguridad del usuario, USS, solicitadas (si las hubiera) de las configuraciones de seguridad del usuario de la GBA (GUSS).

En una cuarta etapa S54, la entidad BSF 13a envía luego los parámetros AUTN, RAND, Ks_NAF y vida útil de KS_NAF, y las USS solicitadas (si las hubiera), a la entidad NAF 13b. La NAF 13b usa la clave Ks_NAF para cifrar (o asegurar de otro modo) los datos a transmitir a la entidad cliente 12 (etapa S55). Optativamente, en el caso de la GBA habilitada para UICC (es decir, GBA_U), cada una de las claves Ks_int_NAF y Ks_ext_NAF puede usarse para este fin. Sin embargo, la funcionalidad del cifrado (así como el descifrado más adelante) es optativa.

En la etapa S56, la entidad NAF 13b usa el canal de difusión entre sí misma y el UE 12 para enviar los parámetros AUTN, RAND, NAF_ID y los datos cifrados al UE 12. AUTN, RAND, NAF_ID y los mismos datos cifrados pueden protegerse adicionalmente con otros medios conocidos (p. ej., usando una clave pública del certificado del dispositivo del UE). Cuando el UE 12 recibe los datos desde la NAF 13b, usa primero los parámetros AUTN y el RAND para autenticar la red. Si esto tiene éxito, obtendrá la clave (Ks) de arranque de las claves CK e IK de sesión, y continuará para obtener la clave Ks_NAF específica de la NAF, usando Ks, NAF_ID y otros parámetros de obtención de claves. Puede luego descifrar los datos usando la clave Ks_NAF, y poner los datos (p. ej., las claves de difusión) en uso en el UE 12.

En consecuencia, el punto de referencia Ub no se usa en absoluto en el presente procedimiento.

La Figura 6 ilustra un diagrama de señalización de un procedimiento según una realización de la presente invención. Hay nuevamente ilustrado un escenario donde la entidad cliente UE 12 no tiene ningún canal de retorno a la red, y por ello no puede llevar a cabo un procedimiento de arranque directamente con la entidad BSF 13a. En cambio, el arranque tiene lugar con la asistencia de una entidad NAF. Por ello, tal procedimiento puede denominarse un *arranque inverso*.

Un procedimiento de arranque inverso, según la presente realización, tiene lugar entre la entidad cliente UE 12 y la entidad BSF 13a de la función servidora de arranque, mediante una entidad NAF 13b de la función de aplicación de red. El procedimiento se describe más adelante.

En la etapa S61, la entidad NAF 13b necesita entregar algunos datos (p. ej., claves de difusión) al cliente UE 12. La entidad NAF 13b conoce la identidad del abonado, es decir, la IMPI del abonado (véase anteriormente), y los datos que deben entregarse al UE 12. Según los procedimientos convencionales, el UE 12 tiene siempre una conexión con la entidad NAF 13b, y entrega un identificador B-TID de transacción de arranque antes de que la entidad NAF 13b pueda solicitar las correspondientes claves de GBA a la entidad BSF 13a.

En el procedimiento según la presente realización, la entidad NAF 13b es activada para capturar los datos de GBA por algún otro medio.

La entidad NAF 13b en la etapa S62 envía la IMPI del abonado, su propio NAF_ID (es decir, el nombre de anfitrión de la NAF) y, optativamente, uno o más GSID (identificadores de servicio de GAA para solicitar configuraciones de

seguridad de usuario específicas de la NAF) por el punto Zn de referencia, a la entidad BSF 13a. Según los procedimientos convencionales, el identificador B-TID se usa para capturar las claves de GBA de la BSF 13a. En contraste con ello, la entidad NAF 13b aquí usa la IMPI del abonado para capturar los datos de GBA de la BSF 13a.

Al recibir la solicitud de la entidad NAF 13b, la BSF 13a comprueba, en la etapa S63, si la entidad NAF 13b está autorizada para solicitar información de autorización, tal como parámetros como AUTN y RAND, y para participar en un procedimiento de arranque inverso según la presente realización. Si es así, la entidad BSF 13a captura vectores de autenticación de un sistema HSS 14 de abonado doméstico y calcula la clave Ks_NAF en base a la identidad NAF_ID y otros parámetros de obtención de claves. También extrae las configuraciones USS de seguridad de usuario solicitadas (si las hubiera) de las GUSS del abonado. Luego, aún en la etapa S63, la entidad BSF 13a crea datos de sesión de arranque para el abonado, que también pueden usarse más tarde con otras NAF 13b.

Según los procedimientos de la técnica anterior, la entidad BSF 13a debería contener los datos existentes de sesión de arranque (identificados por el identificador B-TID de transacción de arranque), y calcular la clave Ks_NAF según lo indicado también anteriormente. En contraste con ello, la entidad BSF 13a, según esta realización, crea datos de sesión de arranque sin comunicarse con la entidad cliente UE 12, que han de usarse para el cálculo de Ks_NAF, y una selección de las USS. En la etapa S64, la entidad BSF 13a envía los parámetros AUTN, RAND, B-TID, Ks_NAF, la vida útil de la Ks_NAF y las USS solicitadas (si las hubiera), a la NAF. Además, AUTN, RAND y B-TID son devueltos a la NAF. La NAF, entonces (en la etapa 5), usa optativamente la clave Ks_NAF para cifrar (o asegurar de otro modo) los datos a transmitir. Según las especificaciones actuales, esta es una funcionalidad específica de la NAF. (Obsérvese que las especificaciones de la GBA están muy abiertas en cuanto a lo que ocurre en la NAF 13b y cómo usa la NAF 13b las claves de GBA). Como se ha mencionado anteriormente, la funcionalidad del cifrado (y descifrado) de los datos a transmitir es meramente optativa en el marco de la realización de la autenticación.

En la etapa S66, la entidad NAF usa el canal de difusión (unidireccional) entre sí misma y el UE 12 para enviar los parámetros AUTN, RAND, B-TID, NAF_ID y los datos cifrados al UE 12. AUTN, RAND, NAF_ID y los mismos datos cifrados pueden protegerse adicionalmente con otros medios (p. ej., el Modelo de Referencia de Datos (DRM) 2.0[2] de la Arquitectura de Gestión de Objetos (OMA), y usando una clave pública del certificado de dispositivo del UE 12).

Según los estándares actuales de la técnica anterior, el identificador B-TID se transfiere desde el UE 12 a la NAF 13b. Esto habría tenido lugar ya antes de la etapa S61 en un procedimiento normal de la GBA. Según la presente realización, el identificador B-TID, así como los parámetros AUTN y RAND, se envían desde la entidad NAF 13b al cliente UE 12.

Cuando el UE recibe los datos desde la NAF 13b (etapa S67), usa primero los parámetros AUTN y RAND para autenticar la red. Si esto tiene éxito, obtendrá la clave (Ks) de arranque de las claves CK e IK de sesión, y continuará para obtener la clave Ks_NAF específica de la NAF usando Ks, NAF_ID y otros parámetros de obtención de claves. Puede luego descifrar los datos usando la clave Ks_NAF y poner los datos (p. ej., las claves de difusión) en uso en el UE 12. El UE 12 puede también configurarse para almacenar los datos de sesión de arranque que puedan usarse más tarde con otra NAF 13b. El UE 12 establece entonces una sesión de arranque por medio de los parámetros B-TID, AUTN y RAND recibidos. Además, en la presente realización, la obtención de claves se gestiona en esta etapa del procedimiento (al hacerse válida la sesión de arranque). El UE 12 también puede usar una sesión de arranque recientemente creada con otras NAF 13b, mientras la sesión sea válida o se cree una sesión de arranque.

También aquí, el punto Ub de referencia no se usa en absoluto en el procedimiento presentado.

La Figura 7 ilustra un diagrama de señalización de un procedimiento adicional según un segundo ejemplo comparativo. Hay ilustrado un escenario en donde el cliente UE 12 no tiene ningún canal de retorno a la entidad NAF 13b, pero tiene tal conexión bidireccional con otros elementos de red tales como la BSF 13a. Es decir, de manera similar a los escenarios anteriores, la entidad cliente UE 12 no es capaz de comunicarse con ambos elementos relevantes de red NAF 13b y BSF 13a de manera bidireccional. Sin embargo, en el caso actual, el cliente puede llevar a cabo un procedimiento de arranque con la entidad BSF 13a. Un ejemplo de tal escenario puede ser un terminal móvil que tiene funcionalidades 3G, p. ej., conectividad de IP, pero que también está equipado con una utilidad para recibir, por ejemplo, la difusión de vídeo digital para terminales de mano, es decir, está habilitado para DVB-H.

Este escenario supone que el UE 12 tiene bien una sesión válida de arranque con la BSF 13a todo el tiempo (esto podría ser una opción de configuración en el UE 12), o bien que la BSF 13a es capaz de activar el UE 12 para ejecutar un establecimiento de sesión de arranque (p. ej., usando el Protocolo de Iniciación de Sesión (SIP)). El procedimiento actual utiliza las funcionalidades de la GAA según se describe más adelante.

En la etapa S71, la entidad NAF 13b necesita entregar algunos datos (p. ej., claves de difusión) a la entidad cliente UE 12. Conoce la identidad del abonado, es decir, su IMPI, y los datos que deben entregarse al UE 12. La entidad NAF 13b envía entonces la IMPI del abonado, su NAF_ID (es decir, el nombre del anfitrión de la NAF) y, optativamente, uno o más GSID (identificadores de servicio de GAA para solicitar configuraciones de seguridad de usuario específicas de

la NAF) por el punto Zn de referencia (etapa S72). Hasta este punto, el procedimiento es bastante similar al de la realización anteriormente descrita.

Al recibir la solicitud desde la entidad NAF 13b, la entidad BSF 13a comprueba, en la etapa S73, si el abonado tiene una sesión válida de arranque, y si puede hallarse en sus bases de datos. Si no está presente, la entidad BSF 13a puede bien indicar un error a la entidad NAF 13b o bien activar la entidad cliente UE 12 para ejecutar un procedimiento de establecimiento de arranque. La entidad BSF 13a calcula entonces la clave Ks_NAF en base a la identidad NAF_ID y otros parámetros de obtención de claves. También extrae las configuraciones USS de seguridad de usuario solicitadas (si las hubiera) de las GUSS del abonado. La entidad BSF 13a envía los parámetros B-TID, Ks_NAF, vida útil de Ks_NAF y las USS solicitadas (si las hubiera), a la entidad NAF 13b. Así, la entidad NAF 13b aprende el identificador B-TID válido de transacción de arranque cuando recibe esto de la entidad BSF 13a. En la quinta etapa, la entidad NAF 13b puede, optativamente, usar su clave Ks_NAF para cifrar (o asegurar de otro modo) los datos a transmitir. La entidad NAF 13b usa el canal de difusión entre sí misma y el UE 12 para enviar los parámetros B-TID, NAF_ID y los datos cifrados a la entidad cliente UE. Los parámetros B-TID, NAF_ID y los mismos datos cifrados pueden ser protegidos adicionalmente con otros medios (p. ej., por el Modelo de Referencia de Datos (DRM) 2.0[2] de la Arquitectura de Gestión de Objetos (OMA), y usando una clave pública del certificado de dispositivo del UE 12).

Cuando el UE 12 en la etapa S77 recibe los datos de la entidad NAF 13b, usa B-TID y NAF_ID para obtener la clave Ks_NAF específica de la NAF, usando Ks (identificado por B-TID), NAF_ID y otros parámetros de obtención de claves. Luego puede, si están cifrados, descifrar los datos usando la Ks_NAF y poner los datos (p. ej., las claves de difusión) en uso en el UE 12. La funcionalidad relacionada con el uso de la clave de GBA en el UE 12 (como en la NAF 13b, véase la etapa S75) es específica de la NAF. La obtención de claves se gestiona en esta etapa del procedimiento.

Las extensiones / modificaciones al implementar los procedimientos según cualquiera de las realizaciones de la presente invención, así como los ejemplos comparativos en una arquitectura GBA según la técnica anterior, son los siguientes:

- la NAF 13b es capaz de solicitar AUTN y RAND (pero no RES, CK, IK) y la clave de GBA obtenida de CK e IK (es decir, Ks_NAF, por ejemplo) usando la identidad privada del abonado (p. ej., IMPI o IMSI) en lugar de B-TID;

- la BSF 13a es capaz de crear datos de una sesión de arranque para un abonado, en base a una solicitud de la NAF de AUTN y RAND;

- además de los datos normales devueltos desde la BSF 13a, también se devuelven AUTN y RAND (pero no RES, CK, IK);

- el UE 12 es capaz de crear datos de una sesión de arranque en base a AUTN, RAND, B-TID y la vida útil de la clave recibidos desde la NAF 13b; y

- la NAF 13b es capaz de solicitar datos de sesión de arranque (B-TID, específicos de NAF, etc.) usando la IMPI del abonado.

Como una realización adicional de la presente invención, es concebible un caso donde la entidad cliente 12 no puede llegar a la BSF 13a, pero tiene un canal bidireccional a la NAF 13b. Por ejemplo, este es el caso cuando el UE 12 usa la GBA para la autenticación de acceso. El protocolo inverso básico de GBA no puede usarse, porque la NAF 13b no conoce la IMPI del abonado del UE 12. Tal escenario también podría estar presente, por ejemplo, en el caso de una WLAN (Red de Área Local Inalámbrica), donde la entidad cliente 12 necesita autenticar, pero sólo tiene una conexión, por ejemplo, con un servidor del EAP (Protocolo de Autenticación Extensible), que podría funcionar como la entidad NAF 13b en tal caso. En consecuencia, la entidad cliente UE 12 realiza un procedimiento de arranque (con la entidad BSF 13a) mediante la entidad NAF 13b. La señalización es similar a los procedimientos anteriormente descritos, excepto en que, antes de la primera etapa, el UE 12 toma contacto con la entidad NAF 13b y envía su identidad privada IMPI.

Una realización adicional más consiste en un caso donde la entidad NAF 13b tiene sólo un canal unidireccional con el UE 12, pero la BSF 13a tiene un canal bidireccional con el UE 12.

En esta realización, es posible que

(1) la entidad NAF 13b active el UE 12 para establecer una sesión de arranque válida; o

(2) la entidad NAF 13b active la entidad BSF 13a a fin de activar un procedimiento de arranque no solicitado con la entidad cliente UE 12.

Según realizaciones adicionales de la presente invención, se presentan una entidad cliente, una entidad de función de aplicación de red, una entidad de función servidora de arranque y un sistema para realizar la autenticación entre la

entidad cliente y la red de acuerdo a cualquiera de los procedimientos de la presente invención.

La Figura 8 ilustra un diagrama en bloques de una entidad cliente según una realización de la presente invención.

Una entidad cliente 12 según una realización comprende medios receptores 87 para recibir transmisiones desde la entidad 13b de la función de aplicación de red, NAF, y medios 81 de autenticación para autenticar la red usando la información de autenticación recibida.

Según realizaciones adicionales, la entidad cliente UE 12, optativamente, comprende adicionalmente uno o más de los siguientes (como puede colegirse de la Figura 8):

- un medio 82 de generación de claves para generar una clave de la entidad de la función de aplicación de red (p. ej., Ks_NAF);

- un medio 84 de establecimiento para establecer una sesión de arranque entre la entidad cliente 12 y la entidad 13 a de la función servidora de arranque;

- un medio 85 de almacenamiento para almacenar datos de sesiones de arranque; y / o

- un medio 83 de descifrado para descifrar datos cifrados recibidos de la entidad 13b de la función de aplicación de red, usando una clave de la entidad 13b de la función de aplicación de red, que se proporciona a partir del medio 82 de generación de claves.

La entidad cliente 12 según la realización mostrada en la Figura 8 comprende adicionalmente el medio 86 de procesamiento y control, que está configurado para procesar datos y señalización, y para controlar la entidad cliente 12 como un todo, así como sus constituyentes, tales como, p. ej., el medio 84 de establecimiento. Con este fin, el medio 86 de procesamiento y control tiene conexiones bidireccionales de datos y / o control con cualquiera de los medios constituyentes mostrados.

La entidad cliente según la presente realización comprende adicionalmente al menos un equipo de usuario y / o es conectable con un módulo de identidad universal de abonado, de acuerdo, p. ej., a los estándares del 3GPP.

Además, la entidad cliente según otra realización más de la presente invención es un aparato de sobremesa (o digibox). Si es así, la entidad de cliente, siendo tal aparato de sobremesa, está configurada para ser operada según cualquier técnica conocida adecuada, tal como, por ejemplo, según los estándares de DVB-H.

En la realización anterior, el medio 81 de autenticación de la entidad cliente está configurado para acceder a la información de identidad de usuario disponible en la entidad cliente. Tal información de identidad de usuario se usa, por ejemplo, además de la información de autenticación recibida, con fines de autenticación. Esta información de identidad de usuario, por ejemplo, se almacena en una tarjeta inteligente conectable con la entidad cliente, tal como, p. ej., una UICC, un módulo de identidad universal de abonado (USIM), o una tarjeta inteligente habilitada para su uso según los estándares de DVB-H.

La Figura 9 ilustra un diagrama en bloques de una entidad de la función de aplicación de red según una realización de la presente invención.

Una entidad de red, en particular, una entidad 13b de la función de aplicación de red, según una realización, comprende el medio transceptor 91, que está configurado para enviar transmisiones a una entidad cliente 12, y para enviar a, y recibir de, una entidad 13a de la función servidora de arranque. El medio transceptor 91, p. ej., está configurado para transmitir una solicitud de información de autenticación a la entidad 13a de la función servidora de arranque cuando la entidad 13b de la función de aplicación de red necesita transmitir datos con seguridad a la entidad cliente 12, para recibir una respuesta que incluye la información de autenticación de la entidad 13a de la función servidora de arranque, y para transmitir la información de autenticación y los datos a transmitir a la entidad cliente 12.

Según realizaciones adicionales, la entidad 13b de la función de aplicación de red, NAF, optativamente, comprende adicionalmente el medio 92 de cifrado para cifrar los datos a transmitir a la entidad cliente 12, usando la clave de la misma entidad 13b de la función de aplicación de red. Según la Figura 9, los datos a transmitir están representados por un símbolo de la base de datos etiquetado como DATOS 93.

Además, el medio transceptor 91 podría configurarse para transmitir una identidad de la entidad 13b de la función de aplicación de red a la entidad cliente 12. Tal identidad también puede almacenarse en la misma base de datos DATOS 93 que los datos a transmitir.

La entidad de red, según una realización adicional de la presente invención, está configurada para difundir transmisiones, p. ej., a la entidad cliente UE.

La Figura 10 ilustra un diagrama en bloques de una entidad de la función servidora de arranque, según una realización de la presente invención.

Una entidad de red, en particular, una entidad 13a de la función servidora de arranque, BSF, según una realización, comprende el medio transceptor 101 para enviar a, y recibir de, una entidad 13b de la función de aplicación de red, y un medio 102 de procesamiento y extracción para procesar una solicitud recibida de la entidad 13b de la función de aplicación de red, y para extraer información de autenticación. En la presente realización, el medio transceptor 101 está específicamente configurado para recibir la solicitud desde la entidad 13b de la función de aplicación de red y para transmitir la información de autenticación a la entidad 13b de la función de aplicación de red.

Según realizaciones adicionales, la entidad BSF 13a de la función servidora de arranque, optativamente, comprende adicionalmente uno más de los siguientes (como puede colegirse de la Figura 10):

- medio 105 de extracción para extraer la información de autenticación desde un sistema HSS 14 de abonado doméstico;

- medio 104 de creación para crear datos de sesión de arranque; y / o

- medio 103 de activación para activar la entidad cliente 12 a fin de establecer una sesión válida de arranque.

Un sistema según la presente invención comprende al menos una entidad cliente 12 (que puede, optativamente, ser un aparato de sobremesa), al menos una entidad 13b de la función de aplicación de red, y al menos una entidad 13a de la función servidora de arranque, según las Figuras 8 a 10.

Debe observarse que en las Figuras 8 a 10 sólo se ilustran aquellos medios y elementos funcionales que están asociados a la presente invención. Para mayor simplicidad, se omiten otros medios y elementos funcionales, que son conocidos por un experto como integrantes de cualquiera de los aparatos ilustrados en sus estructuras convencionales.

En general, ha de observarse que los elementos funcionales mencionados, es decir, el UE, la BSF y la NAF, según la presente invención, y sus constituyentes, pueden implementarse por cualquier medio conocido, bien en hardware y / o software, respectivamente, mientras estén configurados para llevar a cabo las funciones descritas de las partes respectivas. Por ejemplo, el medio de autenticación de la entidad cliente puede implementarse por cualquier unidad de procesamiento de datos, p. ej., un microprocesador, configurado para autenticar la red usando la información de autenticación recibida, según el procedimiento de la presente invención. Las partes mencionadas también pueden realizarse en bloques funcionales individuales, o por medios individuales, o bien una o más de las partes mencionadas pueden realizarse en un único bloque funcional, o por un único medio. En consecuencia, la ilustración anterior de las Figuras 8 a 10 es sólo con fines ilustrativos y no restringe una implementación de la presente invención en modo alguno.

En resumen, se han revelado procedimientos, una entidad cliente, entidades de red, un sistema y un producto de programa de ordenador para llevar a cabo la autenticación entre una entidad cliente y una red, comprendiendo la red al menos una entidad de la función servidora de arranque y una entidad de la función de aplicación de red, y en donde la entidad cliente no es capaz de comunicarse con ambas entidades de red de manera bidireccional, en donde el punto Ub de referencia estándar entre la entidad cliente y la entidad de la función servidora de arranque no se utiliza con fines de autenticación. En breve, la presente invención revela la autenticación usando la funcionalidad de la GAA para conexiones de red unidireccionales.

Según un aspecto ventajoso de la presente invención, la red es una red de difusión.

Incluso aunque la invención se describe en lo anterior con referencia a los ejemplos según los dibujos adjuntos, es claro que la invención no se restringe a los mismos. En cambio, es evidente para los expertos en la técnica que la presente invención puede modificarse de muchas maneras sin apartarse del ámbito de la idea inventiva, según lo revelado en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento que comprende

realizar la autenticación entre una entidad cliente (UE) y una red que comprende al menos una entidad (BSF) de la función servidora de arranque y una entidad (NAF) de la función de aplicación de red, en el cual la entidad cliente (UE) tiene una conexión de red unidireccional que carece de un canal de retorno desde la entidad cliente a la entidad (BSF) de la función servidora de arranque y / o a la entidad (NAF) de la función de aplicación de red, comprendiendo la autenticación:

transmitir (S62) una solicitud de información de autenticación desde la entidad de la función de aplicación de red a la entidad de la función servidora de arranque, comprendiendo dicha solicitud una identidad privada de la entidad cliente, cuando la entidad de la función de aplicación de red necesita transmitir datos con seguridad a la entidad cliente;

procesar (S63) la solicitud y extraer la información de autenticación en la entidad de la función servidora de arranque, en donde dicha extracción comprende crear datos de sesión de arranque para la entidad cliente;

transmitir (S64) una respuesta, que incluye la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente, desde la entidad de la función servidora de arranque a la entidad de la función de aplicación de red;

transmitir (S66) la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente y los datos a transmitir, desde la entidad de la función de aplicación de red a la entidad cliente; y

autenticar (S67) la red usando la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente, en la entidad cliente, en donde dicha autenticación comprende realizar una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

2. El procedimiento según la reivindicación 1, en el cual la transmisión de la solicitud es activada por un medio distinto a la entidad cliente.

3. El procedimiento según la reivindicación 1, en el cual la solicitud comprende adicionalmente una identidad de la entidad de la función de aplicación de red.

4. El procedimiento según la reivindicación 1, en el cual el procesamiento de la solicitud y la extracción de la información de autenticación comprende capturar la información de autenticación desde un sistema de abonado doméstico (HSS).

5. El procedimiento según la reivindicación 1, en el cual la información de autenticación comprende adicionalmente al menos un parámetro de reto aleatorio o un parámetro de autenticación de red.

6. El procedimiento según la reivindicación 5, en el cual la respuesta comprende adicionalmente una clave de la entidad de la función de aplicación de red.

7. El procedimiento según la reivindicación 1, en el cual la transmisión de la información de autenticación comprende adicionalmente transmitir una identidad de la entidad de la función de aplicación de red.

8. El procedimiento según la reivindicación 1, en el cual la autenticación de la red comprende adicionalmente generar una clave de la entidad de la función de aplicación de red en la entidad cliente.

9. El procedimiento según la reivindicación 1, en el cual la autenticación de la red comprende adicionalmente establecer una sesión de arranque entre la entidad cliente y la entidad de la función servidora de arranque.

10. El procedimiento según la reivindicación 9, en el cual el establecimiento de una sesión de arranque se basa en la información de autenticación proveniente de la entidad de la función de aplicación de red.

11. El procedimiento según la reivindicación 1, en el cual la autenticación de la red comprende adicionalmente almacenar los datos de sesión de arranque en la entidad cliente.

12. El procedimiento según la reivindicación 1, que comprende adicionalmente determinar que existe una sesión de arranque válida entre la entidad cliente y la entidad de la función servidora de arranque.

13. El procedimiento según la reivindicación 12, en el cual la sesión de arranque válida existe permanentemente.

14. El procedimiento según la reivindicación 12, en el cual el procesamiento de la solicitud comprende adicionalmente activar la entidad cliente para establecer la sesión de arranque válida.

15. El procedimiento según la reivindicación 12, en el cual la respuesta comprende adicionalmente una clave de la entidad de la función de aplicación de red.

16. El procedimiento según la reivindicación 12, en el cual la autenticación de la red comprende adicionalmente generar una clave de la entidad de la función de aplicación de red en la entidad cliente.

17. El procedimiento según la reivindicación 1, que comprende adicionalmente entrar en contacto con la entidad de la función de aplicación de red y enviar una identidad privada de la entidad cliente, por parte de la entidad cliente.

18. El procedimiento según la reivindicación 1, que comprende adicionalmente activar, por parte de la entidad de la función de aplicación de red, la entidad cliente para establecer una sesión de arranque válida.

19. El procedimiento según la reivindicación 1, que comprende adicionalmente activar, por parte de la entidad de la función de aplicación de red, la entidad de la función servidora de arranque, a fin de activar un procedimiento de arranque no solicitado con la entidad cliente.

20. El procedimiento según la reivindicación 1, que comprende adicionalmente cifrar los datos a transmitir en la entidad de la función de aplicación de red, usando una clave de la función de aplicación de red.

21. El procedimiento según la reivindicación 20, que comprende adicionalmente descifrar los datos en la entidad cliente usando la clave de la entidad de la función de aplicación de red.

22. Un procedimiento según la reivindicación 1, en el cual la red comprende una red de difusión.

23. Un programa de ordenador implementado en un medio legible por ordenador, estando el programa de ordenador configurado para cargarse en una memoria de un medio de procesamiento digital y para controlar dicho medio de procesamiento digital a fin de realizar el procedimiento según cualquiera de las reivindicaciones 1 a 22.

24. Un aparato,

siendo operable dicho aparato como una entidad cliente, para su uso dentro de una arquitectura de autenticación, a fin de realizar la autenticación entre la entidad cliente (UE) y una red, comprendiendo la red al menos una entidad (BSF) de la función servidora de arranque y una entidad (NAF) de la función de aplicación de red, en el cual la entidad cliente (UE) es operable para tener una conexión de red unidireccional que carece de un canal de retorno desde la entidad cliente a la entidad (BSF) de la función servidora de arranque y / o a la entidad (NAF) de la función de aplicación de red, comprendiendo dicho aparato:

un medio receptor (87) para recibir, desde la entidad de la función de aplicación de red, información de autenticación proveniente de la entidad de la función servidora de arranque, y datos a transmitir desde la entidad de la función de aplicación de red a la entidad cliente, comprendiendo dicha información de autenticación datos de sesión de arranque para la entidad cliente, y

un medio (81) de autenticación para autenticar la red, usando la información de autenticación recibida, que comprende los datos de sesión de arranque para la entidad cliente, en el cual dicha autenticación comprende realizar una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

25. El aparato según la reivindicación 24, que comprende adicionalmente un medio (82) de generación de claves para generar una clave de la entidad de la función de aplicación de red.

26. El aparato según la reivindicación 24, que comprende adicionalmente un medio (84) de establecimiento para establecer una sesión de arranque entre el aparato y la entidad de la función servidora de arranque.

27. El aparato según la reivindicación 24, que comprende adicionalmente un medio (85) de almacenamiento para almacenar los datos de sesión de arranque.

28. El aparato según la reivindicación 24, que comprende adicionalmente medios (83) de descifrado para descifrar datos cifrados recibidos desde la entidad de la función de aplicación de red, usando una clave de la entidad de la función de aplicación de red.

29. El aparato según la reivindicación 24, que comprende adicionalmente un medio (86) de procesamiento y control para procesar datos y señalización, y para controlar el aparato y sus medios constituyentes.

30. El aparato según la reivindicación 25, en el cual el aparato comprende al menos un equipo de usuario y es conectable con un módulo de identidad universal de abonado.

31. El aparato según la reivindicación 24, en el cual la entidad cliente comprende un aparato descodificador.

32. El aparato según la reivindicación 31, en el cual el medio de autenticación está configurado para acceder a la información de identidad de usuario disponible en el aparato.

33. El aparato según la reivindicación 32, en el cual la información de identidad de usuario está almacenada en una tarjeta inteligente conectable con la entidad cliente.

34. Un procedimiento, que comprende

realizar la autenticación entre una entidad cliente (UE) y una red que comprende al menos una entidad (BSF) de la función servidora de arranque y una entidad (NAF) de la función de aplicación de red, en el cual la entidad cliente (UE) tiene una conexión de red unidireccional que carece de un canal de retorno desde la entidad cliente a la entidad (BSF) de la función servidora de arranque y / o a la entidad (NAF) de la función de aplicación de red, comprendiendo la autenticación

recibir (S66), desde la entidad de la función de aplicación de red, información de autenticación proveniente de la función servidora de arranque y datos a transmitir desde la entidad de la función de aplicación de red, comprendiendo dicha información de autenticación datos de sesión de arranque para la entidad cliente, y

autenticar (S67) la red usando la información de autenticación recibida, que comprende los datos de sesión de arranque para la entidad cliente, en donde dicha autenticación comprende realizar una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

35. El procedimiento según la reivindicación 34, que comprende adicionalmente generar una clave de la entidad de la función de aplicación de red.

36. El procedimiento según la reivindicación 34, que comprende adicionalmente establecer una sesión de arranque entre la entidad cliente y la entidad de la función servidora de arranque.

37. El procedimiento según la reivindicación 34, que comprende adicionalmente almacenar los datos de sesión de arranque.

38. El procedimiento según la reivindicación 34, que comprende adicionalmente descifrar los datos cifrados recibidos desde la entidad de la función de aplicación de red, usando una clave de la entidad de la función de aplicación de red.

39. El procedimiento según la reivindicación 34, que comprende adicionalmente procesar datos y señalización, y para controlar la entidad cliente y sus medios constituyentes.

40. Un programa de ordenador implementado en un medio legible por ordenador, estando el programa de ordenador configurado para cargarse en una memoria de un medio de procesamiento digital y para controlar dicho medio de procesamiento digital a fin de llevar a cabo el procedimiento según cualquiera de las reivindicaciones 34 a 39.

41. Un aparato,

siendo dicho aparato operable como una entidad de la función de aplicación de red, para su uso dentro de una arquitectura de autenticación, a fin de llevar a cabo la autenticación entre una entidad cliente (UE) y una red, comprendiendo la red al menos el aparato que funciona como una entidad (NAF) de la función de aplicación de red y una entidad (BSF) de la función servidora de arranque, en el cual la entidad cliente (UE) es operable para tener una conexión de red unidireccional que carece de un canal de retorno desde la entidad cliente a la entidad (BSF) de la función servidora de arranque y / o a la entidad (NAF) de la función de aplicación de red, comprendiendo el aparato:

un medio transceptor (91) para enviar a la entidad cliente, y para enviar a, y recibir desde, la entidad de la función servidora de arranque,

en el cual el medio transceptor está adaptado para transmitir una solicitud de información de autenticación a la entidad de la función servidora de arranque, comprendiendo dicha solicitud una identidad privada de la entidad cliente, cuando la entidad de la función de aplicación de red necesita transmitir datos con seguridad a la entidad cliente,

recibir una respuesta, que incluye la información de autenticación que comprende los datos de sesión de arranque para la entidad cliente, desde la entidad de la función servidora de arranque, y

transmitir la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente y los datos a transmitir, a la entidad cliente,

en donde dicha información de autenticación está adaptada para una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

42. El aparato según la reivindicación 1, en el cual el medio transceptor (91) está configurado para transmitir una identidad de la entidad de la función de aplicación de red a la entidad cliente.

43. El aparato según la reivindicación 41, que comprende adicionalmente medios (92) de cifrado para cifrar los datos a transmitir a la entidad cliente, usando una clave de la entidad de la función de aplicación de red.

44. Un aparato según la reivindicación 41, en el cual el aparato está configurado para difundir transmisiones.

45. Un procedimiento, que comprende

efectuar la autenticación entre una entidad cliente (UE) y una red que comprende al menos una entidad (BSF) de la función servidora de arranque y una entidad (NAF) de la función de aplicación de red, en el cual la entidad cliente (UE) tiene una conexión de red unidireccional que carece de un canal de retorno desde la entidad cliente a la entidad (BSF) de la función servidora de arranque y / o a la entidad (NAF) de la función de aplicación de red, comprendiendo la autenticación

transmitir (S62) una solicitud de información de autenticación a la entidad de la función servidora de arranque, comprendiendo dicha solicitud una identidad privada de la entidad cliente, cuando la entidad de la función de aplicación de red necesita transmitir datos con seguridad a la entidad cliente,

recibir (S64) una respuesta, que incluye la información de autenticación que comprende datos de sesión de arranque para la entidad cliente, desde la entidad de la función servidora de arranque, y

transmitir (S66) la información de autenticación, que comprende los datos de sesión de arranque para la entidad cliente y los datos a transmitir, a la entidad cliente,

en el que dicha información de autenticación está adaptada para una autenticación que incluye una autenticación genérica, de acuerdo a una arquitectura genérica de autenticación.

46. El procedimiento según la reivindicación 45, que comprende adicionalmente transmitir una identidad de la entidad de la función de aplicación de red a la entidad cliente.

47. El aparato según la reivindicación 45, que comprende adicionalmente cifrar los datos a transmitir a la entidad cliente, usando una clave de la entidad de la función de aplicación de red.

48. Un programa de ordenador implementado en un medio legible por ordenador, estando el programa de ordenador configurado para cargarse en una memoria de un medio de procesamiento digital y para controlar dicho medio de procesamiento digital, a fin de llevar a cabo el procedimiento según cualquiera de las reivindicaciones 45 a 47.

49. Un aparato,

siendo dicho aparato operable como una entidad de la función servidora de arranque, para su uso dentro de una arquitectura de autenticación, a fin de llevar a cabo la autenticación entre una entidad cliente (UE) y una red, comprendiendo la red al menos el aparato que funciona como una entidad (BSF) de la función servidora de arranque y una entidad (NAF) de la función de aplicación de red, en el cual la entidad cliente (UE) es operable para tener una conexión de red unidireccional que carece de un canal de retorno desde la entidad cliente a la entidad (BSF) de la función servidora de arranque, y / o a la entidad (NAF) de la función de aplicación de red, comprendiendo el aparato:

un medio transceptor (101) para enviar a, y recibir de, la entidad de la función de aplicación de red, y

un medio (102) de procesamiento y extracción para procesar una solicitud recibida desde la entidad de la función de aplicación de red, comprendiendo dicha solicitud una identidad privada de la entidad cliente, y para extraer información de autenticación, comprendiendo adicionalmente dicho medio de procesamiento y extracción un medio (104) de creación para crear datos de sesión de arranque para la entidad cliente,

en el cual el medio transceptor (101) está configurado para recibir la solicitud desde la entidad de la función de aplicación de red y para transmitir la información de autenticación, que comprende los datos creados de sesión de arranque para la entidad cliente, a la entidad de la función de aplicación de red,

en el cual dicha información de autenticación está adaptada para una autenticación que incluye una autenticación genérica de acuerdo a una arquitectura genérica de autenticación.

50. El aparato según la reivindicación 49, que comprende adicionalmente un medio (105) de extracción para extraer información de autenticación desde un sistema de abonado doméstico (HSS).

51. El aparato según la reivindicación 49, que comprende adicionalmente un medio (103) de activación, para activar la

entidad cliente a fin de establecer una sesión de arranque válida.

52. El aparato según la reivindicación 49, en el cual la red comprende una red de difusión.

53. Un procedimiento, que comprende

efectuar la autenticación entre una entidad cliente (UE) y una red que comprende al menos una entidad (BSF) de la función servidora de arranque y una entidad (NAF) de la función de aplicación de red, en el cual la entidad cliente (UE) tiene una conexión de red unidireccional que carece de un canal de retorno desde la entidad cliente a la entidad (BSF) de la función servidora de arranque y / o a la entidad (NAF) de la función de aplicación de red, comprendiendo la autenticación

recibir (S62) una solicitud de información de autenticación desde la entidad de la función de aplicación de red, comprendiendo dicha solicitud una identidad privada de la entidad cliente,

procesar (S63) la solicitud recibida desde la entidad de la función de aplicación de red y extraer información de autenticación, que comprende adicionalmente crear datos de sesión de arranque para la entidad cliente,

transmitir (S64) una respuesta, que incluye la información de autenticación, que comprende los datos creados de sesión de arranque para la entidad cliente, a la entidad de la función de aplicación de red,

en el que dicha información de autenticación está adaptada para una autenticación que incluye una autenticación genérica, de acuerdo a una arquitectura genérica de autenticación.

54. El procedimiento según la reivindicación 53, que comprende adicionalmente extraer la información de autenticación desde un sistema de abonado doméstico (HSS).

55. El procedimiento según la reivindicación 53, que comprende adicionalmente activar la entidad cliente a fin de establecer una sesión válida de arranque.

56. Un programa de ordenador implementado en un medio legible por ordenador, estando el programa de ordenador configurado para cargarse en una memoria de un medio de procesamiento digital y para controlar dicho medio de procesamiento digital, a fin de llevar a cabo el procedimiento según cualquiera de las reivindicaciones 53 a 55.

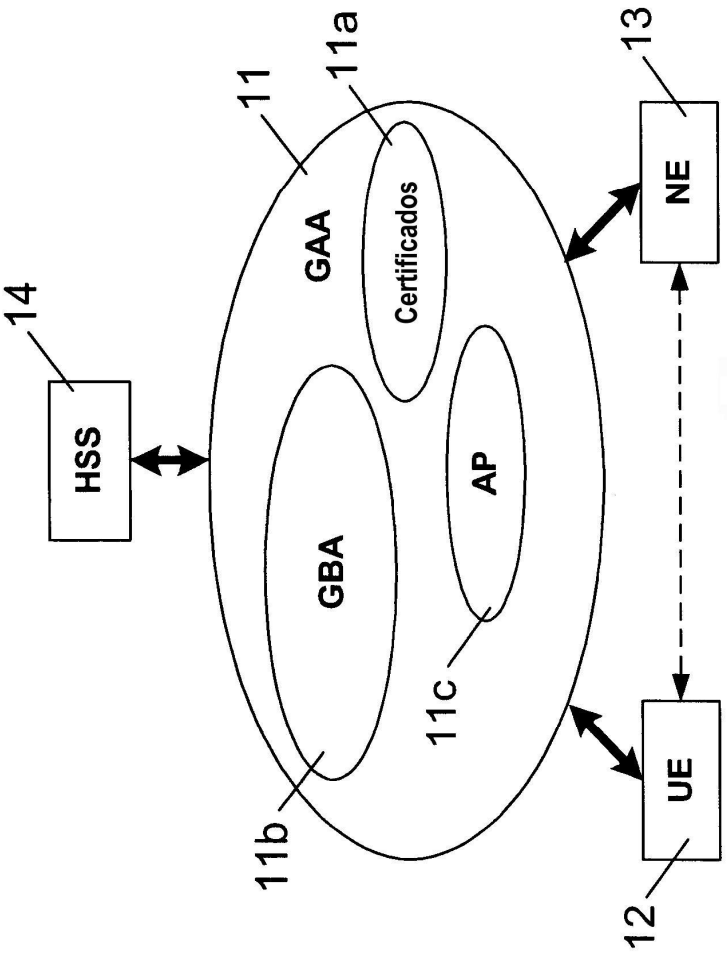

Figura 1

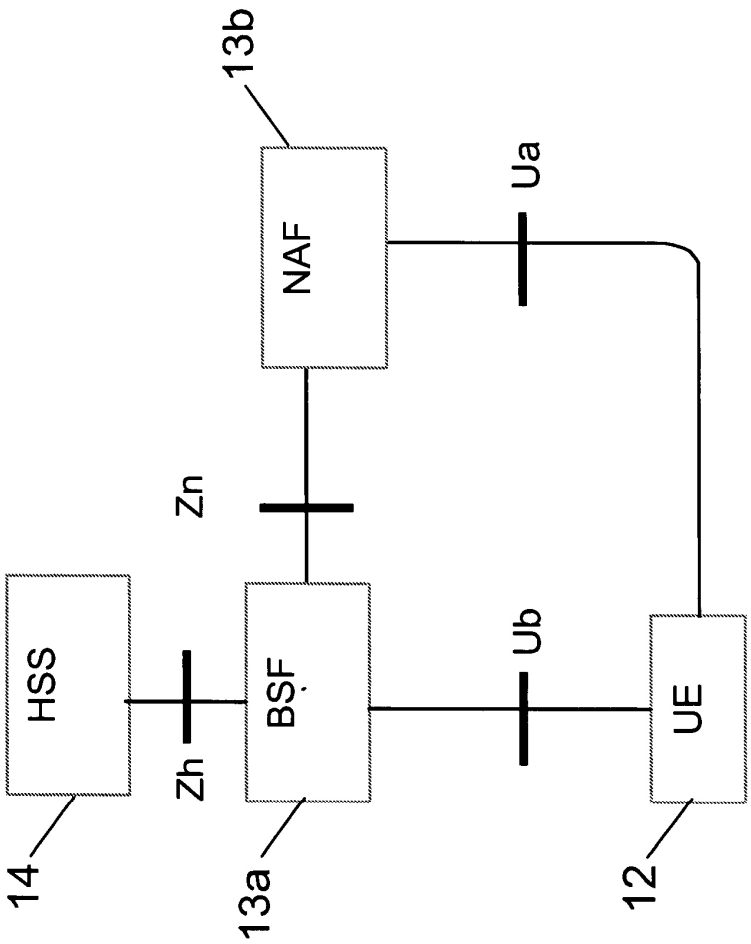

Figura 2

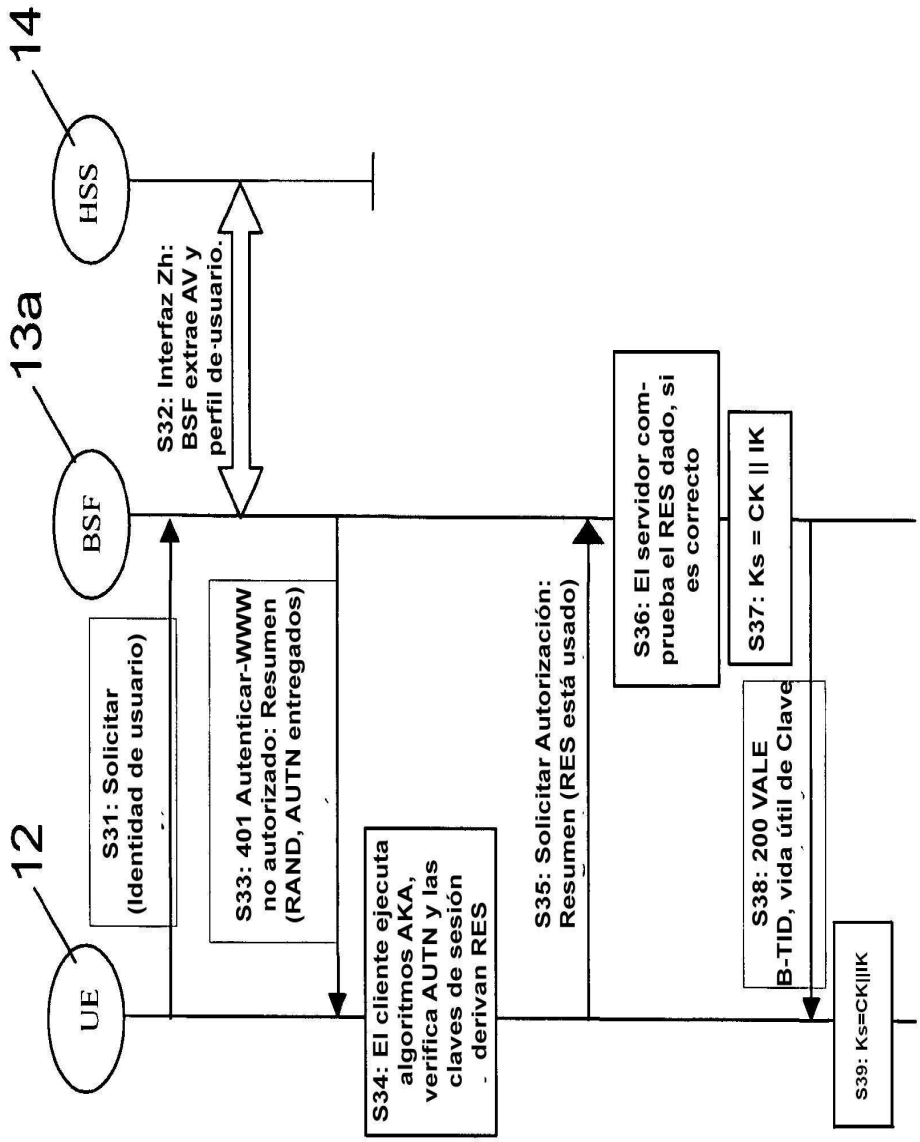
14
HSS
13a
BSF
12
UE
S32: Interfaz Zh: BSF extrae AV y perfil de-usuario.
S31: Solicitar (Identidad de usuario)
S33: 401 Autenticar-WWW no autorizado: Resumen (RAND, AUTN entregados)
S34: El cliente ejecuta algoritmos AKA, verifica AUTN y las claves de sesión derivan RES
S35: Solicitar Autorización: Resumen (RES está usado)
S36: El servidor comprueba el RES dado, si es correcto
S37: Ks = CK || IK
S38: 200 VALE B-TID, vida útil de Clave
S39: Ks=CK||IK

Figura 3

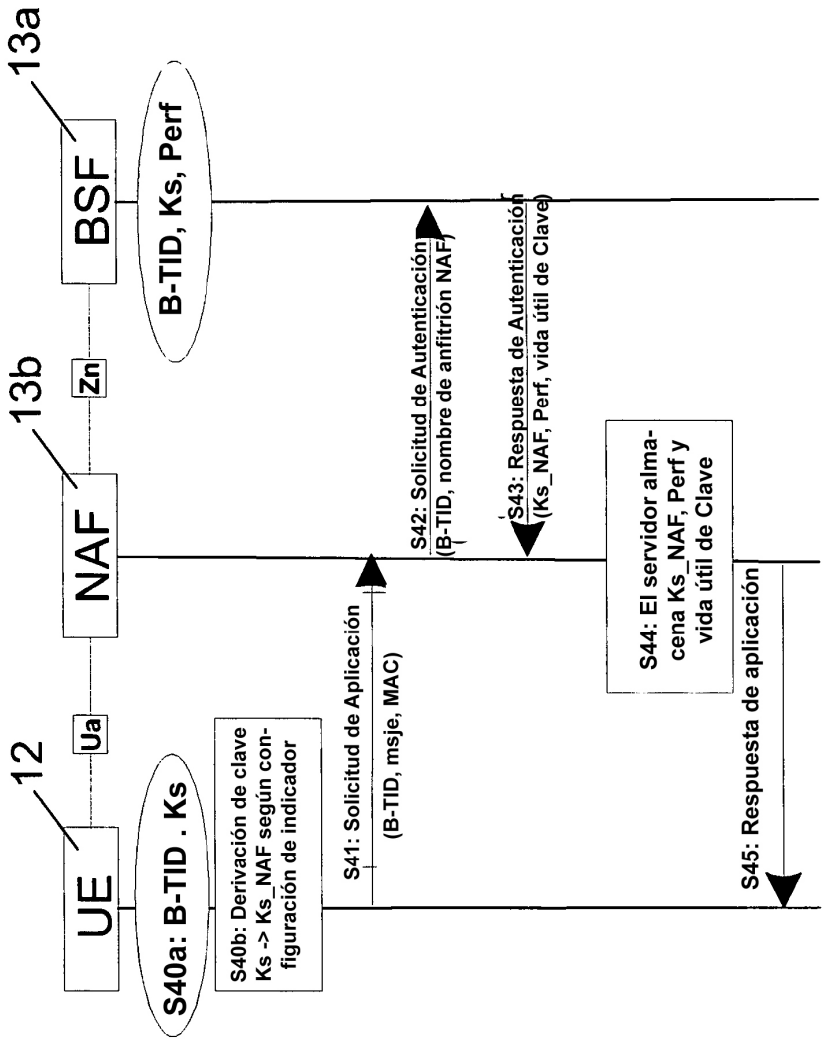
13a
BSF
B-TID, Ks, Perf
13b
Zn
NAF
12
Ua
UE
S40a: B-TID . Ks
S40b: Derivación de clave Ks -> Ks_NAF según configuración de indicador
S41: Solicitud de Aplicación (B-TID, msje, MAC)
S42: Solicitud de Autenticación (B-TID, nombre de anfitrión NAF)
S43: Respuesta de Autenticación (Ks_NAF, Perf, vida útil de Clave)
S44: El servidor almacena Ks_NAF, Perf y vida útil de Clave
S45: Respuesta de aplicación

Figura 4

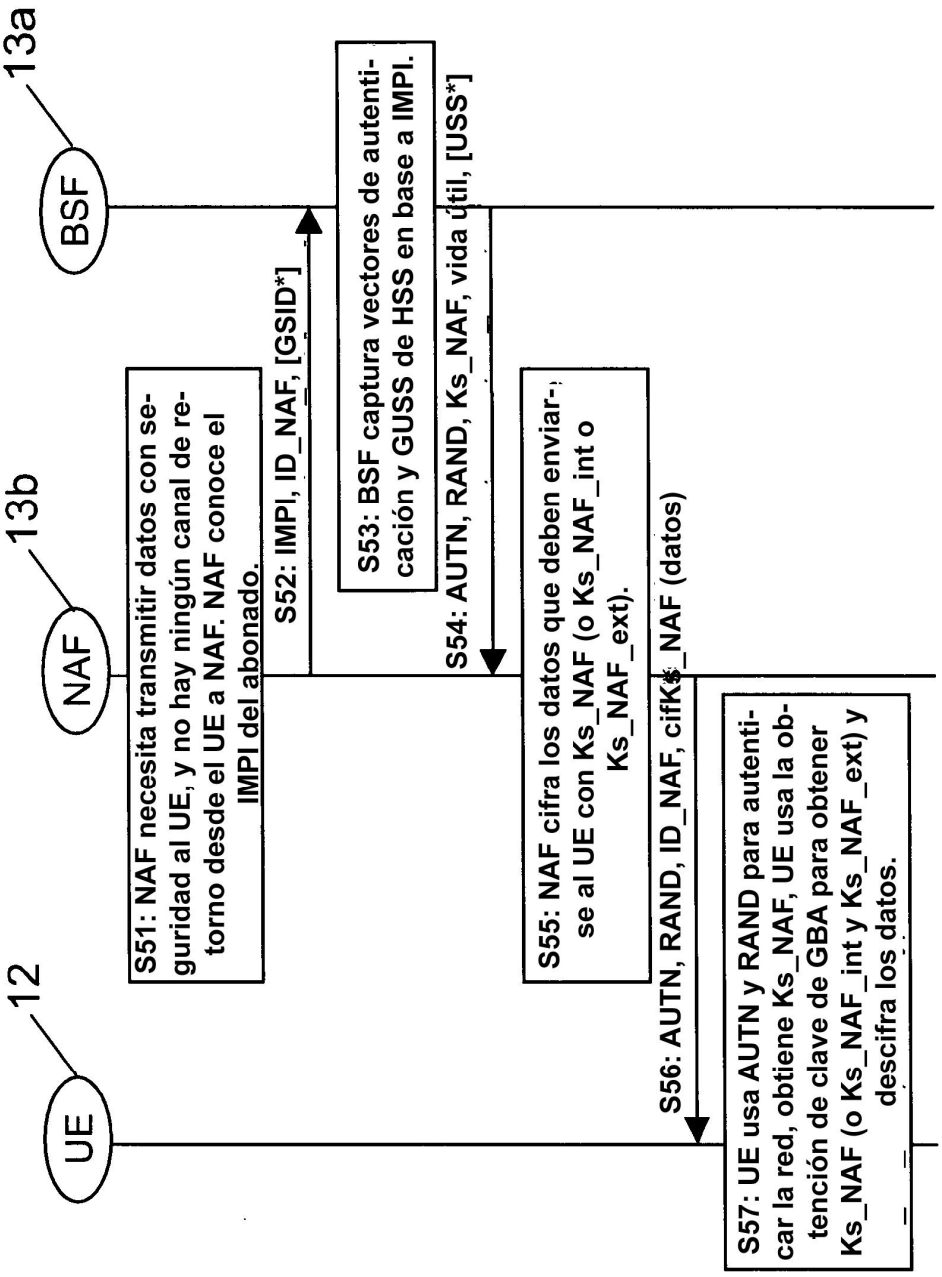
12
UE
13b
NAF
13a
BSF
S51: NAF necesita transmitir datos con seguridad al UE, y no hay ningún canal de retorno desde el UE a NAF. NAF conoce el IMPI del abonado.
S52: IMPI, ID_NAF, [GSID*]
S53: BSF captura vectores de autenticación y GUSS de HSS en base a IMPI.
S54: AUTN, RAND, Ks_NAF, vida útil, [USS*]
S55: NAF cifra los datos que deben enviarse al UE con Ks_NAF (o Ks_NAF_int o Ks_NAF_ext).
S56: AUTN, RAND, ID_NAF, cifKs_NAF (datos)
S57: UE usa AUTN y RAND para autenticar la red, obtiene Ks_NAF, UE usa la obtención de clave de GBA para obtener Ks_NAF (o Ks_NAF_int y Ks_NAF_ext) y descifra los datos.

Figura 5

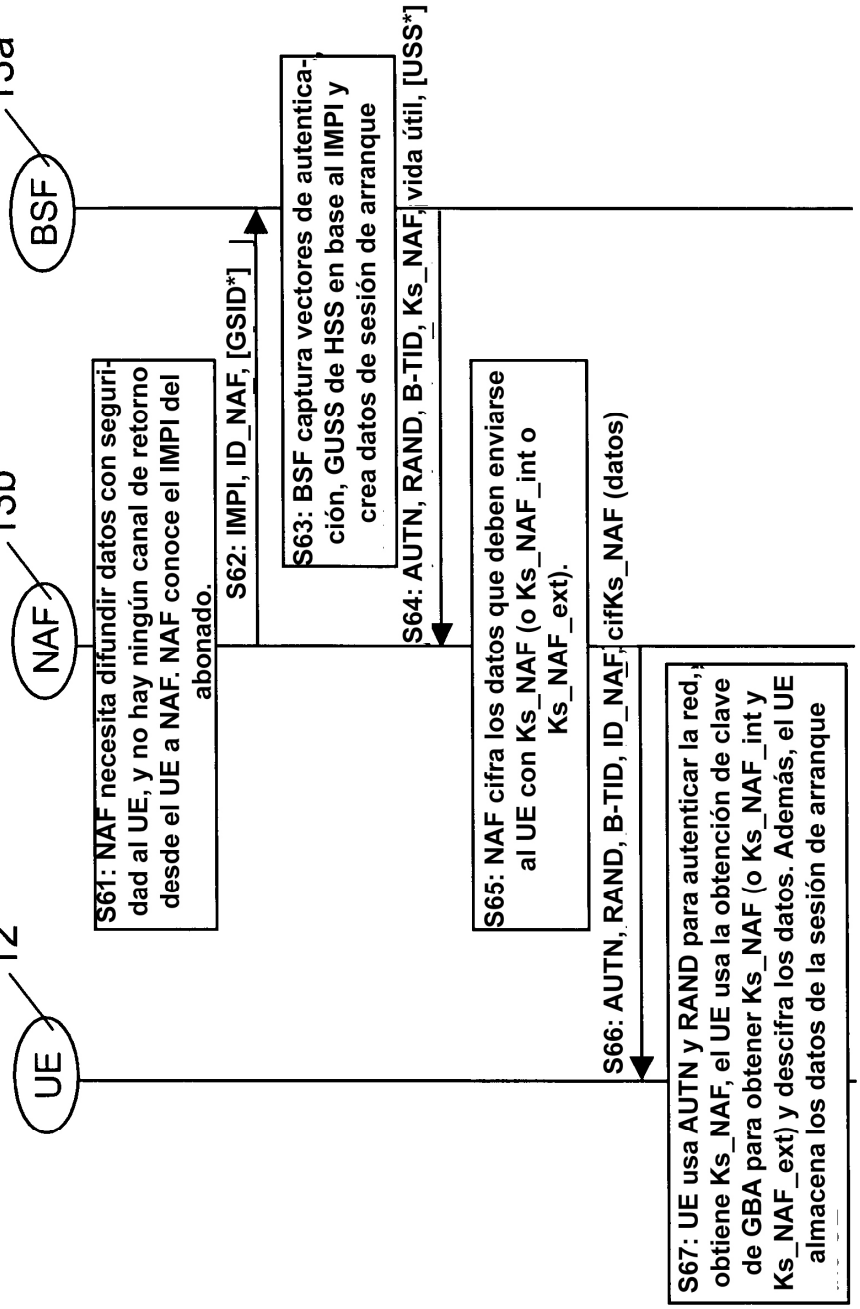
12
UE
13b
NAF
13a
BSF
S61: NAF necesita difundir datos con seguridad al UE, y no hay ningún canal de retorno desde el UE a NAF. NAF conoce el IMPI del abonado.
S62: IMPI, ID_NAF, [GSID*]
S63: BSF captura vectores de autenticación, GUSS de HSS en base al IMPI y crea datos de sesión de arranque
S64: AUTN, RAND, B-TID, Ks_NAF, vida útil, [USS*]
S65: NAF cifra los datos que deben enviarse al UE con Ks_NAF (o Ks_NAF_int o Ks_NAF_ext).
S66: AUTN, RAND, B-TID, ID_NAF, cifKs_NAF (datos)
S67: UE usa AUTN y RAND para autenticar la red, obtiene Ks_NAF, el UE usa la obtención de clave de GBA para obtener Ks_NAF (o Ks_NAF_int y Ks_NAF_ext) y descifra los datos. Además, el UE almacena los datos de la sesión de arranque

Figura 6

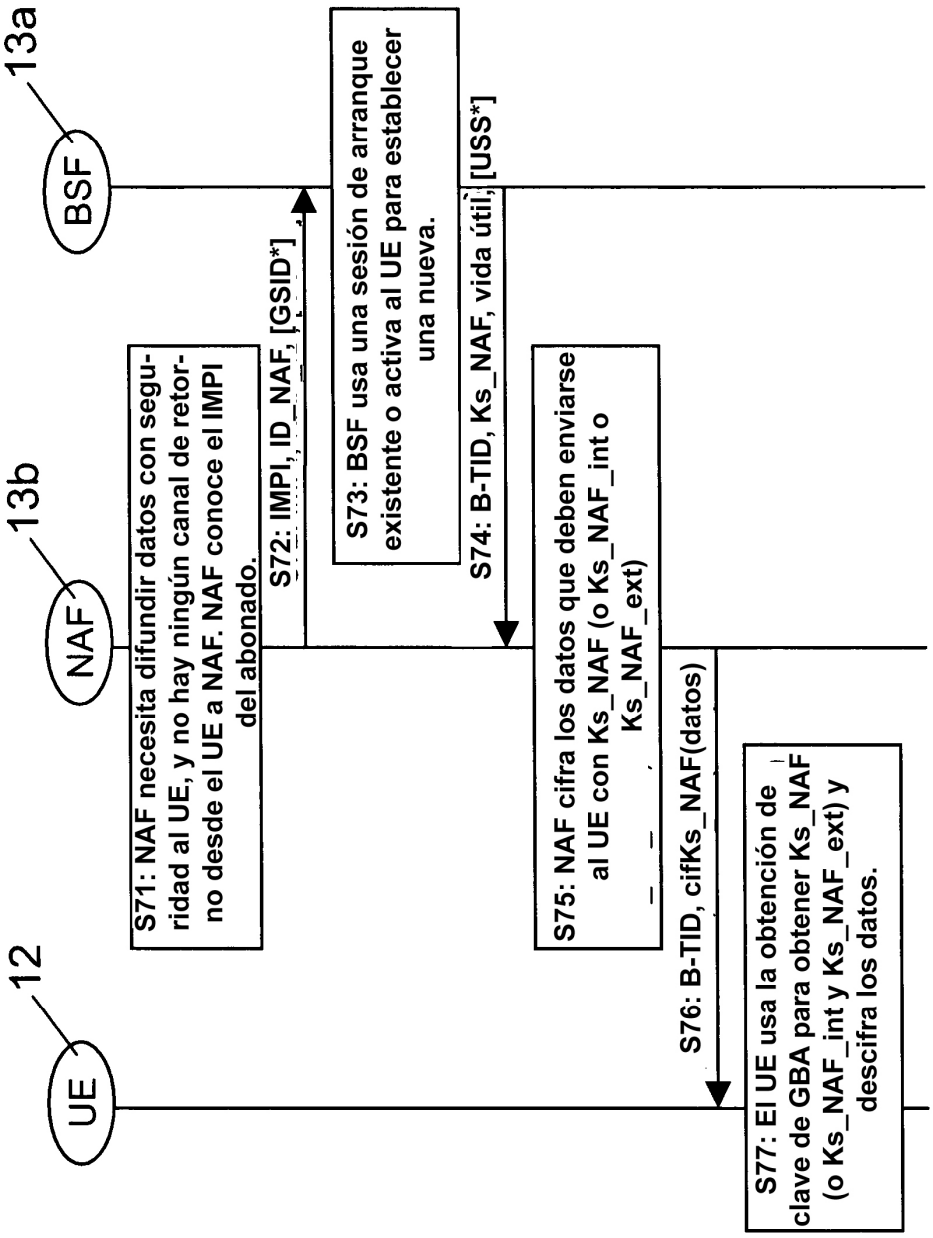
12
UE
13b
NAF
13a
BSF
S71: NAF necesita difundir datos con seguridad al UE, y no hay ningún canal de retorno desde el UE a NAF. NAF conoce el IMPI del abonado.
S72: IMPI, ID_NAF, [GSID*]
S73: BSF usa una sesión de arranque existente o activa al UE para establecer una nueva.
S74: B-TID, Ks_NAF, vida útil, [USS*]
S75: NAF cifra los datos que deben enviarse al UE con Ks_NAF (o Ks_NAF_int o Ks_NAF_ext)
S76: B-TID, cifKs_NAF(datos)
S77: El UE usa la obtención de clave de GBA para obtener Ks_NAF (o Ks_NAF_int y Ks_NAF_ext) y descifra los datos.

Figura 7

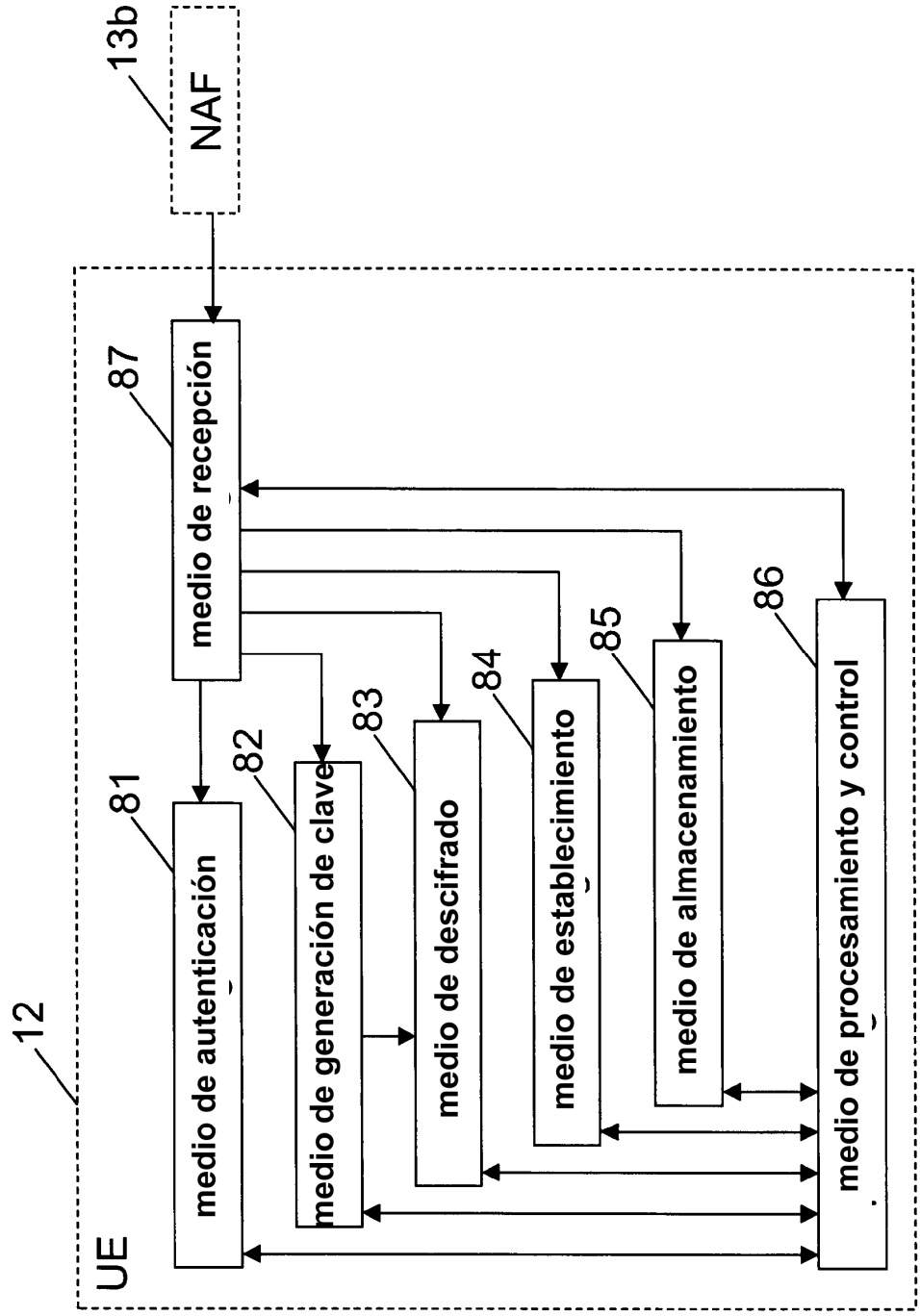
13b
NAF
87
medio de recepción
81
medio de autenticación
82
medio de generación de clave
83
medio de descifrado
84
medio de establecimiento
85
medio de almacenamiento
86
medio de procesamiento y control
12
UE

Figura 8

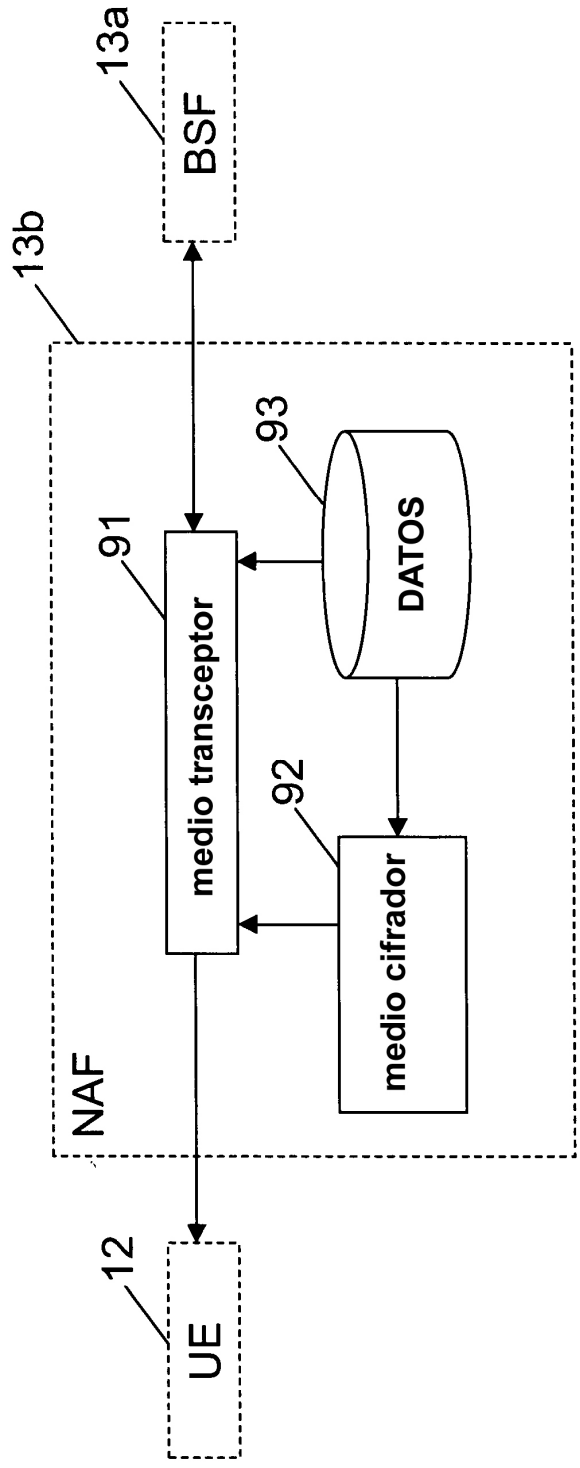
13a
BSF
13b
93
DATOS
91
medio transceptor
92
medio cifrador
NAF
12
UE

Figura 9

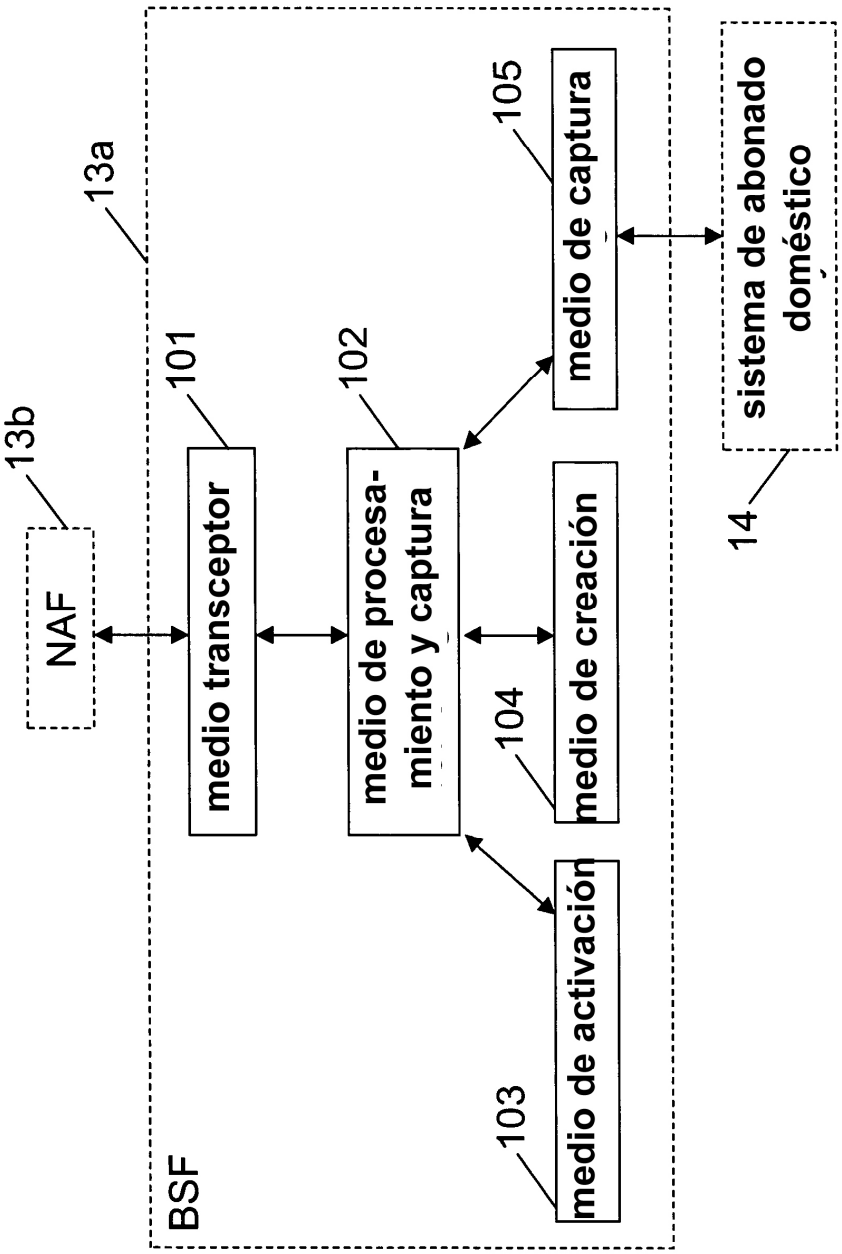
13a
13b
NAF
101
medio transceptor
102
medio de procesa-
miento y captura
104
medio de creación
103
medio de activación
105
medio de captura
BSF
14
sistema de abonado
doméstico

Figura 10