(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 424 474**

(51) Int. CI.:

H04L 29/08 (2006.01)
H04L 12/70 (2013.01)
H04L 29/06 (2006.01)
H04L 9/08 (2006.01)
H04W 12/04 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.10.2006 E 11184132 (6)**

(97) Fecha y número de publicación de la concesión europea: **22.05.2013 EP 2437469**

(54) Título: **Método y aparato para establecer una asociación de seguridad**

(30) Prioridad:

13.10.2005 US 248589
19.12.2005 US 305329

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.10.2013

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

BLOM, ROLF y
NORRMAN, KARL

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCION

Método y aparato para establecer una asociación de seguridad

Campo de la invención

La presente invención se refiere a un método y un aparato para establecer una asociación de seguridad entre un terminal de cliente y un nodo de servicio con el fin de entregar un servicio de ofrecimiento iniciado en el nodo de servicio y en particular, aunque no necesariamente, a dichos método y aparato que emplean una Arquitectura Genérica de Rutina de Arranque y Carga.

Antecedentes de la invención

Con el fin de facilitar la prestación de servicios a los terminales de usuario, una red móvil, tal como una red 3G, a menudo requerirá el establecimiento de un canal de comunicación seguro o "asociación de seguridad" entre los terminales de cliente (es decir, los terminales móviles) y los nodos de servicios basados en la red que proporciona los servicios. La Arquitectura Genérica de Rutina de Arranque y Carga (GBA) se describe en la Especificación Técnica 3GPP TS 33,220 y proporciona un mecanismo por el que un terminal de cliente (UE) puede ser autenticado para una Función de Autenticación de Red (el nodo de servicio) y las claves de sesión segura obtenidas para ser usadas entre el terminal del cliente y la Función de Autenticación de Red. El modelo simple de red para esta arquitectura se ilustra en la figura 1. Este mecanismo de rutina arranque y carga se basa en el conocido procedimiento [3GPP TS 33.102] Autenticación y Acuerdo de Clave (AKA) que permite que un terminal de cliente sea autenticado para una Función de Servidor de Rutina de Arranque y Carga (BSF) de la red doméstica del cliente basándose en una K secreta que está compartida entre el USIM del terminal del cliente y el Sistema de Abonado Doméstico (HSS) de la red doméstica del abonado. El procedimiento AKA establece además las claves de sesión a partir de las cuales se derivan las claves que se aplican después entre el terminal del cliente y una Función de Aplicación de Red (NAF). Cuando un terminal de cliente y NAF desean obtener las claves de sesión de la BSF, la NAF envía una identificación de la transacción a la BSF, identificación de la transacción que contiene un índice que la BSF utiliza para identificar al terminal del cliente y las claves adecuadas que él remite a la NAF.

De acuerdo con el mecanismo de GBA, un UE inicia el proceso de generación de claves mediante el envío de una petición que contiene una identificación de usuario a la BSF. La petición también contiene la identificación de la NAF. La BSF recupera un vector de autenticación del Sistema de Abonado Doméstico (HSS), consistiendo cada vector de autenticación en un número aleatorio RAND, una respuesta esperada XRES, una clave de cifrado CK, una clave de integridad IK y un símbolo de autenticación AUTN. La BSF genera el material de la clave KS mediante la concatenación de las claves CK e IK contenidas dentro del vector de autenticación. La BSF genera una identificación de clave B-TID en el formato de un NAI en base64 codificando el valor de RAND y combinando el valor codificado con el nombre del servidor BSF, por ejemplo como base64encode(RAND)@BSF_servers_domain_name.

La BSF retiene la clave KS en asociación con la identificación de la transacción B-TID y la identificación de la NAF. La B-TID y el AUTN son enviadas por la BSF al UE, el USIM del terminal del cliente verifica el valor AUTN usando la K secreta compartida y devolviendo un resumen de los resultados esperados XRES a la BSF. El USIM también genera el material de la clave KS utilizando la K secreta y el valor RAND (recuperado de la B-TID).

Tras la finalización de este procedimiento, el UE comunica a la NAF, la B-TID recibida. La NAF y la BSF se autentican entre sí, y la NAF envía a la BSF la B-TID recibida junto con su propia identificación. La BSF utiliza la B-TID y la identificación de la NAF para localizar la clave correcta KS, y utiliza la KS para generar una clave NAF. Otra información tal como la identificación de la NAF también se utiliza en la generación de la clave de la NAF. La clave NAF generada se devuelve a la NAF. El UE es igualmente capaz de generar la clave NAF utilizando la clave KS que ya ha generado.

Después de que el mecanismo de GBA ha sido ejecutado por primera vez, las peticiones posteriores para establecer una asociación de seguridad entre el UE y la misma o una diferente NAF pueden utilizar el material de la clave KS ya establecida, siempre que la clave no haya expirado. Sin embargo, esto aún requerirá que el UE inicie una petición para establecer una asociación de seguridad mediante el envío de su B-TID a la NAF.

Resumen de la invención

Hay ocasiones en las que es deseable permitir que la NAF inicie el establecimiento de una asociación de seguridad con el UE. Por ejemplo, se podría considerar un servicio del tipo de los que se inician en el nodo, que aporta información de noticias, deportes y financiera, etc., a los usuarios que se hayan registrado previamente para el servicio. Un procedimiento operativo típico para lograr esto podría ser que el proveedor de servicios envíe un mensaje SMS al UE en el que se le pide al usuario abrir una conexión segura. Sin embargo, hay muchas amenazas relacionadas con este modelo ya que un SMS podría ser manipulado, enviado por un tercero no autorizado, repetido, etc. Si existiera una asociación de seguridad, o que el nodo del servicio pudiera iniciar una, antes de que se enviaran los datos del servicio real, se podrían basar en esto los procedimientos de seguridad y la mayoría de los problemas podrían atenuarse.

De acuerdo con un primer aspecto de la presente invención, se proporciona un método de establecer una asociación de seguridad entre una Función de Aplicación de Red (NAF) y un equipo de usuario (UE) con el fin de pasar información de la NAF al UE, en el cual el UE y un Sistema de Abonado Doméstico (HSS) comparten una clave secreta. El método comprende:

- enviar una petición para la generación y provisión de una clave NAF desde la NAF a la Función de Servidor de Rutina de Arranque y Carga (BSF), conteniendo la petición las identificaciones de la NAF y del UE;
- generar una clave NAF en la BSF usando la identificación NAF, una identificación del UE, material derivado de la clave usando el secreto, y un valor aleatorio;
- enviar la clave NAF a la NAF junto con la información requerida por el UE con el fin de derivar la clave NAF, incluyendo la información la identificación NAF y el valor aleatorio y firmar la información utilizando lo derivado del material de la clave;
- en la NAF, iniciar la comunicación con el UE incluyendo la transmisión de la información firmada con el UE;
- en el UE, derivar el material de clave usando el secreto, verificar la información usando lo derivado del material de la clave, generar la clave NAF utilizando la información recibida, la identificación del UE y el material de la clave; y
- establecer una asociación de seguridad entre el UE y la NAF utilizando dicha clave NAF.

El método puede comprender además, en la BSF, la recuperación de un vector de autenticación para el UE desde el HSS, comprendiendo el vector de autenticación al menos el número aleatorio, una clave de cifrado, una clave de integridad y un valor de autenticación. La clave de cifrado y la clave de integridad pueden estar derivadas del secreto y del número aleatorio, y el material de la clave puede luego ser derivado de la clave de cifrado y de la clave de integridad.

La BSF puede enviar el valor de autenticación a la NAF. La NAF puede entonces enviar el valor de autenticación al UE, junto con la información requerida por el UE para generar la clave específica NAF, de tal manera que el UE puede utilizar el secreto y el valor de autenticación para autenticar la BSF.

El secreto puede almacenarse en un ISIM/USIM del UE, y la etapa de derivar el material de la clave, puede a continuación llevarse a cabo dentro del ISIM/USIM.

De acuerdo con un segundo aspecto de la presente invención, se proporciona una Función de Aplicación de Red (NAF) para la entrega de un servicio que se inicia en el nodo a un Equipo de Usuario (UE) a través de un enlace de comunicación seguro. La NAF comprende:

- medios para enviar una petición de generación y provisión de una clave NAF a una Función de Servidor de Rutina de Arranque y Carga (BSF) identificando en la petición el UE y la NAF;
- medios para recibir desde la BSF una clave NAF junto con la información requerida por el UE con el fin de derivar la clave NAF, incluyendo en la información la identificación NAF y el valor aleatorio, habiendo sido firmada la información por la BSF;
- medios para iniciar la comunicación con el UE incluyendo el reenvío de la información firmada al UE; y
- medios para cifrar y/o proteger la integridad de la información del servicio usando la clave NAF y para enviar la información cifrada/protegida al UE.

De acuerdo con un tercer aspecto de la presente invención se proporciona un Equipo de Usuario (UE) para recibir un servicio iniciado en el nodo entregado por una Función de Aplicación de Red, (NAF). El UE comprende:

- medios de memoria para almacenar un secreto que se comparte con un Sistema de Abonado Doméstico (HSS);
- medios para recibir de la NAF, información de generación de las claves iniciada por la NAF, incluyendo la información una identificación de la NAF y un valor aleatorio, estando firmada la información usando una derivada del secreto;
- medios para verificar la información de generación de claves utilizando la derivada del secreto;
- medios para generar una clave NAF utilizando el secreto y la información de generación de claves; y
- medios para usar la clave NAF para descifrar y/o verificar la integridad de las comunicaciones con la NAF.

El UE puede comprender además medios para derivar el material de la clave usando el secreto. Los medios para derivar el material de la clave usando el secreto puede ser configurados para usar el secreto y el valor aleatorio

recibido para derivar una clave de cifrado y una clave de integridad, y para derivar el material de la clave de la clave de cifrado y de la clave de integridad.

Los medios para verificar la información de generación de claves pueden ser configurados para usar una derivada del material de la clave para verificar la información firmada de generación de la clave.

Los medios para generar una clave NAF pueden ser configurados para generar la clave NAF utilizando la identificación NAF, el valor aleatorio recibido, la identificación del UE, y el material de la clave.

El UE puede comprender además medios para verificar una red proporcionando la información de generación de claves, estando configurados los medios para verificar la red para utilizar el secreto para verificar un valor de autenticación recibido con la información de generación de claves ofrecida por la NAF.

De acuerdo con un cuarto aspecto de la presente invención, se proporciona una Función de Servidor de Rutina de Arranque y Carga (BSF) para usarla en el establecimiento de una asociación de seguridad entre un Equipo de Usuario (UE) y una Función de Aplicación de la Red (NAF) con el fin de ofrecer la información de la NAF al UE, en la que el UE y un Sistema de Abonado Doméstico (HSS) comparten un secreto. La BSF comprende:

medios para recibir una petición de generación y provisión de una clave NAF desde la NAF, identificando en la petición el UE y la NAF;

medios para recuperar un vector de autenticación para el UE desde el HSS, comprendiendo el vector de autenticación al menos un número aleatorio, una clave de cifrado y una clave de integridad, habiéndose derivado la clave de cifrado y la clave de integridad del secreto y del número aleatorio;

medios para generar una clave NAF utilizando la identificación NAF, la identificación del UE, el material de la clave derivado usando la clave de cifrado y la clave de integridad y el valor aleatorio; y

medios para enviar la clave NAF a la NAF junto con la información requerida por el UE con el fin de derivar la clave NAF, incluyendo en la información la identificación NAF y el valor aleatorio y para firmar la información usando una derivada del material de la clave.

Los medios para enviar la clave NAF a la NAF pueden ser además configurados para reenviar un valor de autenticación a la NAF junto con la información requerida por el UE para generar la clave NAF, habiendo sido recuperado el valor de autenticación como parte del vector de autenticación.

Breve descripción de los dibujos

La figura 1 ilustra un modelo simple de red para la Arquitectura Genérica de Rutina de Arranque y Carga;

Las figuras 2-7 ilustran flujos de señalización asociados con los respectivos procedimientos para establecer una asociación de seguridad entre un cliente (UE) y la NAF, y

Las figuras 8 y 9 ilustran flujos de señalización asociados con los procedimientos respectivos para establecer una asociación de seguridad entre un par de clientes (UE_A y UE_B).

Descripción detallada de ciertas realizaciones

La Arquitectura Genérica de Rutina de Arranque y Carga (GBA) general para las redes 3G se ha descrito con referencia a la figura 1, que ilustra los interfaces (Ua, Ub, Zn y Zh) entre las diversas entidades. Hay que tener en cuenta que la descripción se hace en un nivel relativamente alto y las ejecuciones reales pueden "parecer" diferentes, aunque empleen la misma funcionalidad general. Por ejemplo, es posible que cuando una BSF reciba una petición de clave de servicio de una NAF (como se describirá más adelante), la BSF receptora deba realizar una etapa de resolución de dirección para identificar una BSF "servidora" para la NAF o para el cliente (UE) y, si la BSF receptora no es la BSF servidora, la petición se reenvía a la BSF servidora.

Esta descripción se refiere a la provisión de un servicio de ofrecer información a un cliente. Por lo general, el cliente se habrá registrado previamente con el proveedor del servicio, pero la iniciativa de ofrecer la información en particular la toma el proveedor del servicio. En tal situación, el proveedor del servicio y el cliente no tendrán ya una asociación de seguridad establecida entre sí (las asociaciones de seguridad suelen ser de corta duración), y se debe establecer una.

Una primera solución que se propone aquí plantea que la NAF pregunte a la BSF por una clave (o servicio) NAF. La BSF devuelve a la NAF la clave NAF junto con la identificación de la transacción del cliente (B-TID) y el valor correspondiente de autenticación de la red (AUTN). Como se ha indicado anteriormente, la B-TID contiene el valor codificado RAND (como el prefijo NAI), que puede ser utilizado por el cliente para derivar la clave de base (KS). La NAF ahora puede redactar un mensaje que contenga la B-TID, la AUTN y datos adicionales incluyendo la identificación NAF que el cliente requiere con el fin de derivar la clave NAF, y enviar este mensaje al cliente. Este mensaje puede ser un mensaje que sólo activa la configuración de un SA (es decir, intercambiar una clave de

servicio) o podría contener datos del servicio (es decir, datos útiles) cifrados con la clave del servicio. En ambos casos, los valores de B-TID, AUTN y otros datos requeridos por el cliente para generar KS se envían como texto sin formato, pero "firmados" con un Código de Autenticación de Mensajes. Téngase en cuenta que la clave (s) en el SA se deriva usando la clave compartida entre el HSS y el UE, y que la AUTN está incluida en el mensaje. Por lo tanto, no es posible "falsear" los mensajes incluso aunque la clave utilizada para proteger la integridad del mensaje sea derivada de la propia SA que pretende establecerla.

Cuando el cliente recibe el mensaje, recupera la parte RAND de la B-TID (invirtiendo la codificación) y la AUTN y las aplica al USIM/ISIM para derivar la clave base Ks. A continuación, utiliza los datos adicionales para derivar la clave NAF y verifica el mensaje recibido mediante MAC.

Los intercambios de señalización asociados con este procedimiento se ilustran en la figura 2.

Con el fin de evitar la manipulación de los datos adicionales (requeridos por el cliente) por la NAF, la BSF puede firmar esos datos utilizando una derivada de la KS. Esto puede ser importante, por ejemplo, para evitar a la NAF que se prorrogue la validez de una clave.

La solución presentada anteriormente permite que la NAF ofrezca al cliente la información necesaria para establecer una asociación de seguridad entre las dos partes. Así, el cliente no tiene que configurar una conexión con la BSF para realizar estas tareas. Esto representa una solución extremadamente eficiente en el tiempo. Sin embargo, se requiere que la NAF reenvíe toda la información relativa a la clave (duración de la clave, Add-info, etc) en forma protegida de la BSF al UE. La B-TID y los otros datos podrían entonces comprender eliminar una gran estructura de datos. Esto podría ser problemático en el caso del volumen de datos que puedan ser incorporados en la estructura del mensaje que se utilice entre el cliente y la NAF, por ejemplo, en el caso de que esta estructura fuera un SMS.

Con el fin de reducir el volumen de datos requerido intercambiado entre la NAF y el cliente para establecer la asociación de seguridad, la solución anterior puede ser modificada omitiendo el valor AUTN a partir de los datos enviados por la BSF a la NAF. La NAF ahora compone un mensaje que contiene la B-TID y otros datos necesarios (incluyendo la identificación NAF) que el terminal necesita para derivar la clave NAF y enviarla al cliente. De nuevo, este mensaje podría ser un mensaje que sólo activa la configuración de una asociación de seguridad, o podría contener datos útiles cifrados.

Cuando el cliente recibe el mensaje de la NAF, se conecta a la BSF transmitiéndoselo a la B-TID, él mismo lo autentica y solicita la información restante necesaria para derivar el material de la clave asociado con la B- TID, por ejemplo, la AUTN. Después de haber recibido esta información se deduce la clave (NAF) de servicio y verifica la integridad del mensaje. Ya que el cliente tiene que conectarse a la BSF, puede al mismo tiempo, obtener toda la información relacionada con el material de la clave, por ejemplo, Add-info, vida útil de la clave, etc., lo que reduce la cantidad de información "administrativa" que tiene que ser transmitida desde la NAF al cliente.

El intercambio de señalización asociada con este procedimiento, suponiendo el escenario de generación Ks (es decir, análogo al de la figura 2), se muestra en la figura 3.

Puede no ser deseable en algunas circunstancias revelar el valor RAND a la NAF. Esto se puede evitar mediante la formación de la B-TID utilizando una referencia al valor real RAND (o al RAND efectivo, RANDe), por lo que la NAF sólo ve el valor de referencia. El RAND efectivo (RANDE) entonces tendría que ser señalizado, junto con la AUTN desde la BSF al cliente. Este procedimiento modificado se ilustra en la Figura 4.

La principal ventaja de las soluciones descritas con referencia a las figuras 3 y 4 es que la BSF tendrá una oportunidad adicional para controlar la generación de claves en el cliente. El cliente necesita la AUTN para derivar la clave. Por otro lado, el cliente tendrá que conectarse a la BSF y autenticarse a sí mismo hacia la BSF necesitando una nueva variante del protocolo GBA sobre el interfaz Ub.

Una amenaza para las soluciones de las figuras 3 y 4 es que un atacante podría generar un lote de mensajes (dando a entender que contienen una B-TID válida) y enviarlos a diferentes clientes para lanzar un ataque de Denegación de Servicio (DoS). Ya que los clientes no tienen medios para autenticar los mensajes (por ejemplo, un AUTN), ellos se conectarán a la BSF en un intento de autenticar los mensajes recibidos. Tal ataque, si no es resistido, consumirá considerables recursos por parte de la BSF. Para hacer tal ataque DoS más difícil, sería deseable habilitar al cliente para que pueda comprobar de inmediato la MAC del mensaje ofrecido por la NAF con el fin de validar el mensaje sin tenerse que conectar a la BSF. Para lograr esto, el cliente tiene que ser capaz de derivar la clave que se utiliza para la MAC del mensaje. Ya que la AUTN no se envía al cliente en el mensaje ofrecido, esta derivación tiene que basarse únicamente en la RAND (o valor derivado, figura 4) en la B-TID.

Una solución es utilizar el RAND (o valor derivado) en la B-TID para derivar dos claves Ck' e Ik' en la BSF. La BSF a continuación, deriva una clave MAC utilizando estas claves, y envía la clave MAC a la NAF. Esta clave de integridad debe también depender preferiblemente de la identificación NAF. El uso de una huella distintiva de la otra información necesaria para derivar la clave NAF en la deducción de la clave de integridad sería una forma de conseguirla sin tener que enviar toda la información al UE. La NAF calcula un segunda (corta) MAC sobre al menos una parte de los datos a enviar al cliente, e incluye la MAC en el mensaje enviado al cliente. En el cliente, el

USIM/ISIM utiliza los algoritmos AKA para generar Ck' e Ik' y de ahí la segunda clave de MAC, y el cliente puede entonces verificar el mensaje. Alternativamente, la BSF puede proporcionar las claves de Ck' e Ik' a la NAF para hacer que la NAF genere la propia segunda clave MAC. Esto no impide la repetición del mensaje antiguo (aunque esto podría resolverse con el uso de marcas horarias), pero impide que los atacantes puedan generar mensajes aleatorios.

En una solución alternativa, ilustrada en el diagrama de señalización de la figura 5, la BSF no genera y envía la clave NAF ella misma a la NAF en respuesta a la petición de NAF de una clave PUSH para un usuario determinado. Más bien, la BSF envía un valor público Diffie-Hellman $g^{NAF\ Key}$ basándose en la clave NAF (o en algún otro valor basado en la Ks secreta asociada compartida) y en datos relacionados con la identificación de las partes involucradas y con el uso previsto de la clave. La NAF ahora puede elegir un valor secreto RAND de sí misma, y añadir el correspondiente valor Diffie-Hellman público g^{RAND} a ese valor secreto a la información enviada al UE. Ambas partes pueden entonces derivar una clave común compartida, S_Key = Clave $g^{RAND*NAF}$. La S_Key se utiliza para codificar la MAC. Obsérvese que los esquemas Diffie-Hellman se pueden llevar a cabo sobre diferentes tipos de grupos. Aquí se utiliza la notación normalizada cuando el grupo es Zp y la generación del elemento g utilizado se designa como g.

De acuerdo con aún otra solución alternativa adicional, que se ilustra en el diagrama de señalización de la figura 6, cuando la NAF solicita una clave PUSH para un usuario dado, la BSF no incluye una clave NAF normalizada, sino que más bien deriva una clave que confía adicionalmente tanto en la identificación del UE como en la identificación de la NAF (además de cualquier dato adicional). Tal clave se designa como "NAF_UE_Key" en la figura. A fin de garantizar la entrega al entregar la clave a la NAF desde la BSF, la BSF incluye en el mensaje a la BSF un MAC calculado utilizando la Clave NAF_UE.

La descripción anterior ha considerado la aplicación de la invención a la provisión de claves relacionadas con el servicio a los usuarios y a los nodos de servicio. Otra aplicación de la presente invención se refiere a la provisión de claves a terminales de cliente para permitir que un terminal de cliente ofrezca mensajes a un terminal de cliente similar de una manera segura, es decir, gestión de claves similar-a-similar (p2p).

De acuerdo con una solución, un UE que empieza, por ejemplo, UE_A, emplea el método ilustrado en general en la figura 7. Este planteamiento se basa en una relación de confianza explícita entre BSF_A y BSF_B.

El interlocutor que empieza primero realiza un procedimiento normalizado GBA con la BSF_A de su red doméstica con el fin de obtener una clave de base, Ks_A. El UE_A entonces utiliza la clave de base para derivar una RAND unida a la otra parte UE_B a la que UE_A desea ofrecer un mensaje. Esto se puede hacer en la misma forma en que se derivan las claves NAF. La segunda acción realizada por el UE_A es solicitar la información de la clave para el UE_B. Esta petición, que contiene la identificación de ambos clientes, se envía a la BSF_A, que reenvía la petición a la BSF dentro de la red doméstica de UE_B, es decir, BSF_B.

La BSF_B devuelve al UE_A, a través de BSF_A, un valor público Diffie-Hellman para el UE_B, es decir $g^{NAF\ Key}$. También devuelve la B-TID (que contiene el valor RAND' que se utiliza para generar la clave NAF), la AUTN y datos necesarios adicionales. El interlocutor que empieza UE_A forma entonces un mensaje que contiene su valor público Diffie-Hellman, g^{RAND}, y la información que necesita el receptor para derivar la KS_B, la referida NAF_Key, y por tanto la clave de sesión $g^{RAND*NAF\text{-}Key}$. El UE_A por supuesto puede derivar la misma clave de sesión.

Una solución alternativa de gestión de claves p2p se ilustra en la figura 8 y requiere que la BSF_B genere la clave que va a ser compartida por los usuarios similares. La primera acción del interlocutor que empieza UE_A es solicitar una clave para el otro interlocutor UE_B. Esta petición se envía a la BSF_A del interlocutor iniciador, el cual reenvía la petición a la BSF_B del interlocutor receptor. El interlocutor iniciador incluye su identificación, así como la del interlocutor receptor en la petición, y la BSF_B deriva la clave para ser compartida, es decir la clave NAF_UE. La clave derivada junto con la B-TID, la AUTN, etc., se envía entonces al UE_A.

Con este esquema, el interlocutor receptor recibe una verificación implícita de la identificación reclamada del remitente tal como esta identificación se utiliza en la derivación de la clave NAF_UE.

El interlocutor receptor podría obtener también una autenticación explícita si la BSF_B incluyera una MAC basada en una "NAF_Key" que cubriera todos los datos, como se describió anteriormente.

Se apreciará por los expertos en la técnica que pueden hacerse diversas modificaciones a las realizaciones descritas anteriormente sin apartarse del alcance de la presente invención. Por ejemplo, mientras que las soluciones presentadas anteriormente conciernen a la GBA, la invención tiene aplicabilidad general a las arquitecturas en las que la información tiene que ser ofrecida desde un proveedor de servicios y en las que el prestador de servicios y el cliente no comparten un secreto común. En otra modificación, en la que se efectúan múltiples soluciones en paralelo, la petición de autenticación enviada a la BSF contiene una selección que indica qué solución NAF/UE tiene que emplear.

REIVINDICACIONES

1. Un método de establecer una asociación de seguridad entre una Función de Aplicación de Red, NAF, y un equipo de usuario, UE, con el fin de ofrecer información de la NAF al UE, donde el UE y un Sistema de Abonado Doméstico, HSS, comparten un secreto, comprendiendo dicho método:

- enviar una petición para la generación y la provisión de una clave NAF desde la NAF a una Función de Servidor de Rutina de Arranque y Carga, BSF, conteniendo la petición las identificaciones de la NAF y del UE;
- generar una clave de NAF en la BSF usando la identificación NAF, una identificación del UE, material de la clave derivado utilizando el secreto y un valor aleatorio;
- enviar la clave NAF a la NAF junto con la información requerida por el UE con el fin de derivar la clave NAF, incluyendo la información la identificación NAF y el valor aleatorio, y firmar la información usando una derivada del material de la clave;
- en la NAF, iniciar la comunicación con el UE incluyendo reenviar la información firmada al UE;
- en el UE, derivar el material de la clave usando el secreto, verificar lainformación utilizando la derivada del material de la clave, generar la clave NAF utilizando la información recibida, la identificación del UE y el material de la clave; y
- establecer una asociación de seguridad entre el UE y la NAF utilizando dicha clave NAF

2. Un método de acuerdo con la reivindicación 1 y que comprende además:

en la BSF, recuperar un vector de autenticación para el UE desde el HSS, comprendiendo el vector de autenticación al menos el número aleatorio, una clave de cifrado, una clave de integridad y un valor de autenticación.

3. Un método de acuerdo con la reivindicación 2, en el que la clave de cifrado y la clave de integridad se derivan del secreto y del número aleatorio y el material de la clave se deriva de la clave de cifrado y de la clave de integridad.

4. Un método de acuerdo con cualquiera de las reivindicaciones precedentes, en el que el secreto se almacena en un ISIM/USIM del UE y la etapa de derivar el material de la clave se realiza dentro del ISIM/USIM.

5. Un método de acuerdo con la reivindicación 2, en el que la BSF envía el valor de autenticación a la NAF y la NAF reenvía el valor de autenticación al UE junto con la información requerida por el UE para generar la clave específica NAF, y en el que el UE utiliza el secreto y el valor de autenticación para autenticar la BSF.

6. Una Función de Aplicación de Red, NAF, para entregar un servicio de ofrecido por un nodo de servicio para un Equipo de Usuario, UE, a través de un enlace de comunicación seguro, comprendiendo dicha NAF:

- medios para enviar una petición para la generación y la provisión de una clave NAF a una función de Servidor de Rutina de Arranque y Carga, BSF, identificando en dicha petición al UE y a la NAF;
- medios para recibir desde la BSF una clave NAF junto con la información requerida por el UE con el fin de derivar la clave NAF, incluyendo en dicha información la identificación NAF y el valor aleatorio, habiendo sido firmada la información por la BSF;
- medios para iniciar la comunicación con el UE incluyendo reenviar la información firmada al UE; y
- medios para cifrar y/o proteger la integridad de la información del servicio usando la clave NAF y para enviar la información cifrada/protegida al UE.

7. Un equipo de usuario, UE, para recibir un servicio ofrecido entregado por una Función de Aplicación de Red, NAF, comprendiendo dicho UE:

- medios de memoria para almacenar un secreto que es compartido con un Sistema de Abonado Doméstico, HSS;
- medios para recibir desde la NAF, información de generación de la clave ofrecida por la NAF, incluyendo dicha información una identificación de la NAF y un valor aleatorio, estando firmada la información usando una derivada del secreto;
- medios para verificar la información de generación de la clave utilizando la derivada del secreto;
- medios para generar una clave NAF utilizando el secreto y la información de generación de la clave, y
- medios para usar la clave NAF para descifrar y/o verificar la integridad de las comunicaciones con la NAF.

8. Un equipo de usuario según la reivindicación 7, y que comprende además medios para derivar el material de la clave utilizando el secreto.

9. Un equipo de usuario según la reivindicación 8, en el que los medios para derivar el material de la clave utilizando el secreto están configurados para utilizar el secreto y el valor aleatorio recibido para derivar una clave de cifrado y una clave de integridad, y para derivar el material de la clave de la clave de cifrado y de la clave de integridad.

10. Un equipo de usuario de acuerdo con cualquiera de las reivindicaciones 8 o 9, en el que los medios para verificar la información de generación de la clave están configurados para utilizar una derivada del material de la clave para verificar la información firmada de generación de la clave.

11. Un equipo de usuario de acuerdo con cualquiera de las reivindicaciones 8 a 10, en el que los medios para generar una clave NAF están configurados para generar la clave NAF utilizando la identificación NAF, el valor aleatorio recibido, la identificación del UE y el material de la clave.

12. Un Equipo de Usuario de acuerdo con cualquiera de las reivindicaciones 8 a 11, y que comprende además medios para verificar una red que proporciona la información de generación de la clave que están configurados para utilizar el secreto para verificar un valor de autenticación recibido con la información de generación de la clave ofrecida por la NAF.

13. Una Función de Servidor de Rutina de Arranque y Carga, BSF, para usarla en el establecimiento de una asociación de seguridad entre un Equipo de Usuario, UE, y una Función de Aplicación de Red, NAF, con el fin de ofrecer la información de la NAF al UE, en la que el UE y un Sistema de Abonado Doméstico, HSS, comparten un secreto, comprendiendo dicha BSF:

medios para recibir una petición para la generación y la provisión de una clave NAF a desde la NAF,

identificando en la petición al UE y a la NAF;

medios para recuperar un vector de autenticación para el UEdesde el HSS comprendiendo dicho vector de autenticación al menos un número aleatorio, una clave de cifrado y una clave de integridad, habiendo sido derivadas la clave de cifrado y la clave de integridad del secreto y del número aleatorio; medios para generar una clave NAF utilizando la identificación NAF, la identificación del UE,el material de la clave derivada usando la clave de cifrado y el clave de la integridad y el valor aleatorio, y medios para enviar la clave NAF a la NAF junto con la información requerida por el UE con el fin de derivar la clave NAF, incluyendo en dicha información, la identificación NAF y el valor aleatorio, y utilizar una derivada del material de la clave para firmar la información.

14. Una Función de Servidor de Rutina de Arranque y Carga según la reivindicación 13, en la que los medios para enviar la clave NAF a la NAF están configurados además para reenviar un valor de autenticación a la NAF junto con la información requerida por el UE para generar la clave NAF, habiendo sido recuperado el valor de autenticación como parte del vector de autenticación.

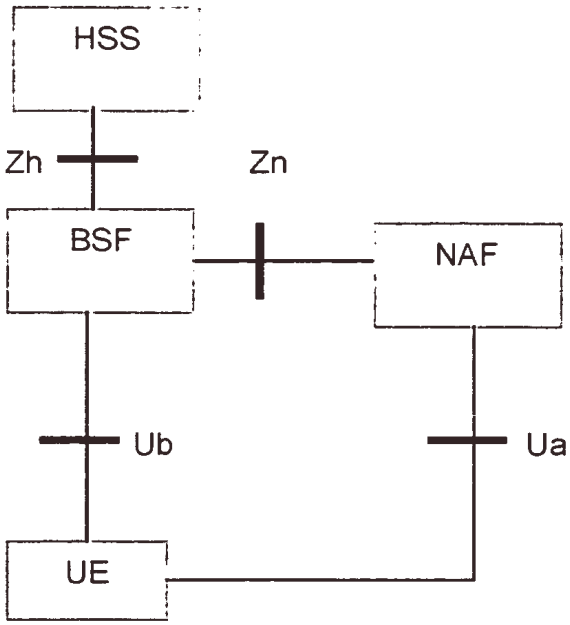

Figura 1

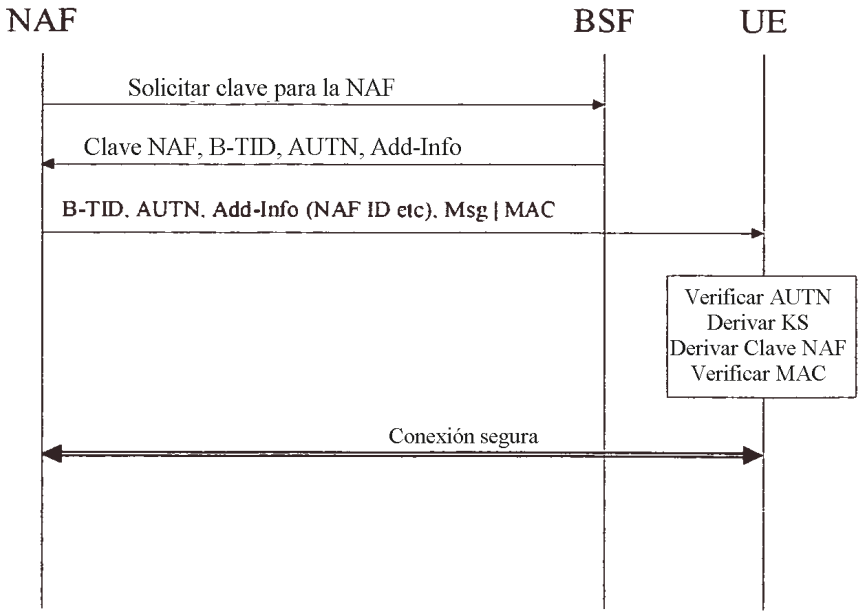

Figura 2

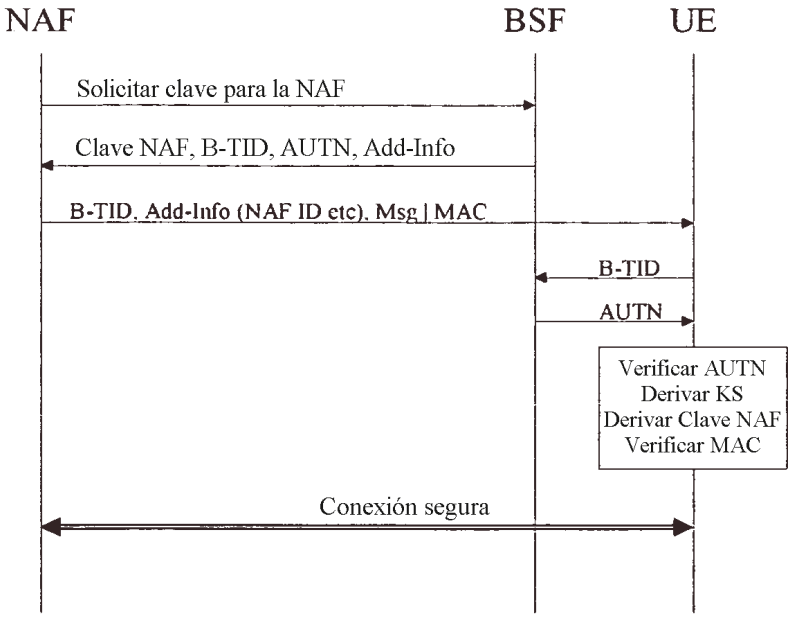

Figura 3

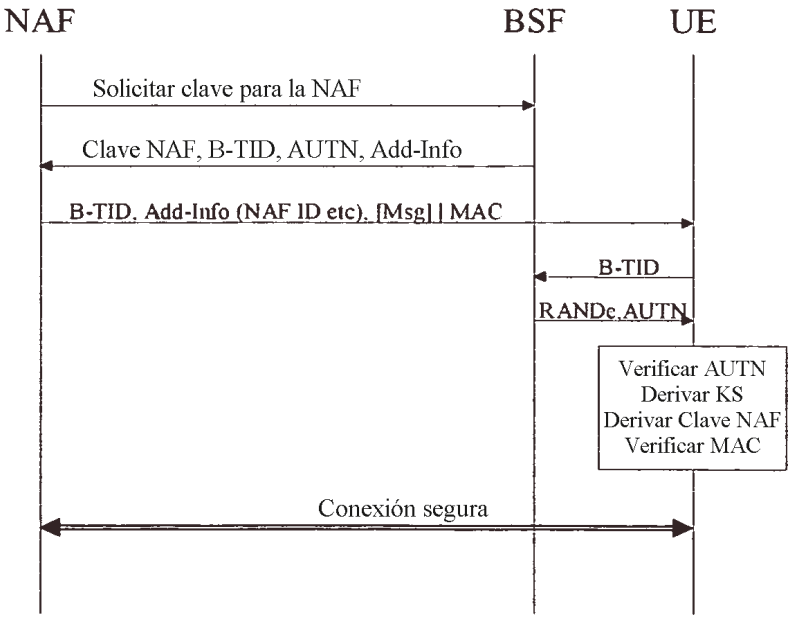

Figura 4

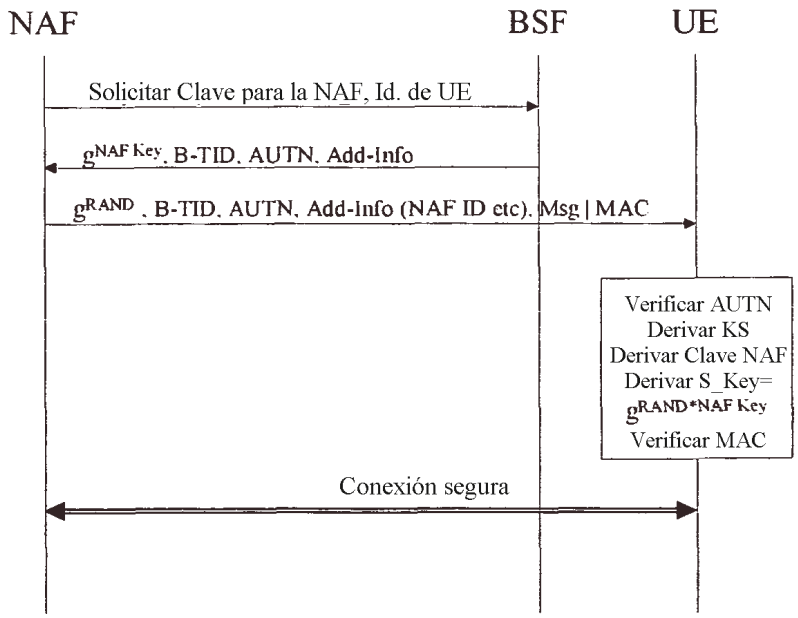

Figura 5

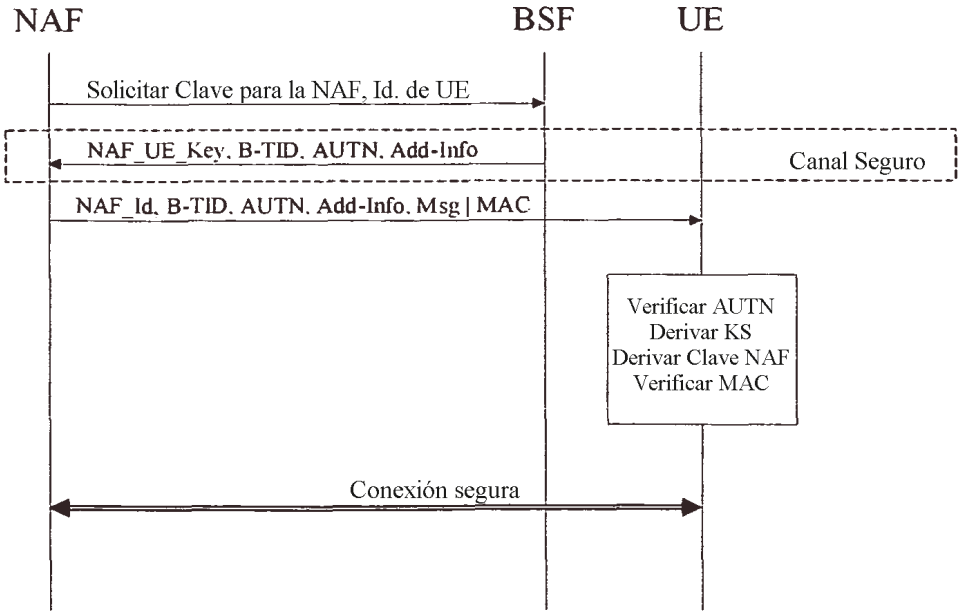

Figura 6

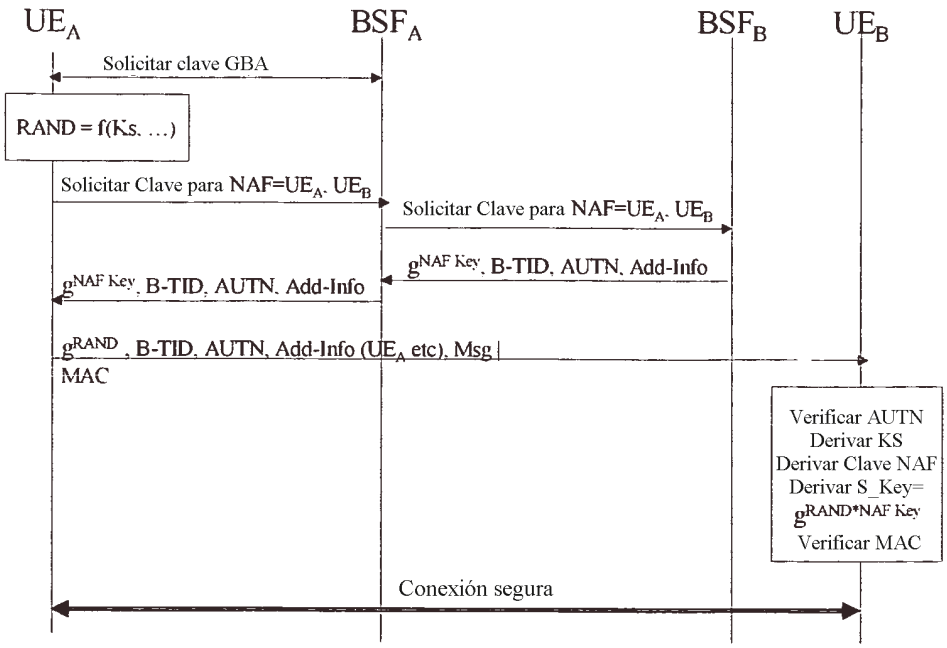

Figura 7

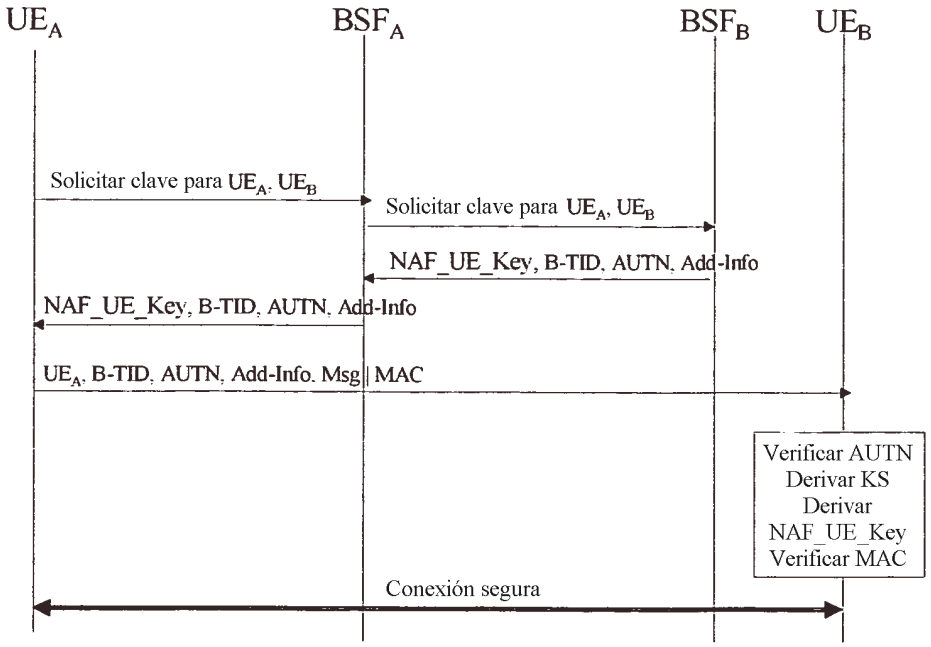

Figura 8