(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 389 250**

(51) Int. CI.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06741743 .6**
(96) Fecha de presentación: **27.04.2006**
(97) Número de publicación de la solicitud: **1879324**
(97) Fecha de publicación de la solicitud: **16.01.2008**

(54) Título: **Un método para autenticar un terminal de usuario en un subsistema multimedia IP**

(30) Prioridad:
30.04.2005 CN 200510070351

(45) Fecha de publicación de la mención BOPI:
24.10.2012

(45) Fecha de la publicación del folleto de la patente:
24.10.2012

(73) Titular/es:
HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
HUAWEI ADMINISTRATION BUILDING, BANTIAN, LONGGANG DISTRICT, SHENZHEN GUANGDONG 518129, CN

(72) Inventor/es:
WEN, KAI y
GU, JIONGJIONG

(74) Agente/Representante:
LEHMANN NOVO, Isabel

DESCRIPCIÓN

Un método para autenticar un terminal de usuario en un subsistema multimedia IP

Campo de la invención

La presente invención está relacionada con tecnologías de seguridad en el campo de las comunicaciones de red y, en particular, con un método para autenticar un equipo de usuario en un subsistema multimedia IP (IMS).

Antecedentes de la invención

Un subsistema multimedia IP (IMS), que es una capa de control de la sesión principal de una red fija o móvil, se ha convertido en una cuestión tratada en la industria en la actualidad. En los sistemas de comunicaciones móviles de 3ª Generación (3G) y en los estándares TISPAN (Servicios Convergentes de Telecomunicaciones e Internet y Protocolos para Redes Avanzadas) se han definido numerosas especificaciones relacionadas con IMS, incluyendo varios aspectos como, por ejemplo, arquitecturas de red, interfaces, protocolos, etc. En particular, la seguridad es un aspecto importante tenido en cuenta en 3G y los TISPAN. De acuerdo con las especificaciones actuales, en términos de seguridad, una red IMS se divide en un dominio de acceso y un dominio de red, y las especificaciones de seguridad se definen, respectivamente, para el dominio de acceso y para el dominio de red. En la Fig. 1 se muestra un modelo de seguridad de la red IMS. Una entidad de Función de Control de Sesión de Llamada (CSCF) de la red IMS se adapta para llevar a cabo funciones tales como el control y el encaminamiento durante una llamada o sesión. Las P/S/I-CSCF se distinguen entre sí por sus distintas funciones. La Función de Control de Sesión de Llamada de Proxy (Agente) (P-CSCF, CSCF de Proxy) se adapta para un acceso de un equipo de usuario (UE), y cualquier UE podrá obtener un acceso a la red IMS a través de la P-CSCF. La Función de Control de Sesión de Llamada de Servicio (S-CSCF, CSCF de Servicio) proporciona funciones fundamentales tales como control de sesión y encaminamiento. La Función de Control de Sesión de Llamada de Consulta (I-CSCF, CSCF de consulta) se adapta para seleccionar la S-CSCF y la intercomunicación entre diferentes proveedores de servicio o diferentes redes de área, y se adapta para proporcionar funciones tales como enmascaramiento de red. Un Servidor Local de Abonados (HSS), que ha evolucionado a partir de un Registro de Localización de Usuarios (HLR) y un Centro de Autenticación (AUC), se adapta para almacenar datos de suscripción y datos de configuración de abonados y para soportar una función de Autenticación y Autorización (AAA) para los abonados.

Como se muestra en la Fig. 1, un mecanismo de seguridad para el dominio de acceso incluye dos interfaces asociados con un Equipo de Usuario (UE): Interfaz 1 e Interfaz 2, donde la Interfaz 1 es una interfaz de autenticación bidireccional entre el UE y una red IMS, y está adaptada para permitir una función de autenticación de abonados, y la Interfaz 2 se adapta para garantizar la seguridad de las comunicaciones entre el UE y la P-CSCF. La Interfaz 1 y la Interfaz 2 se implementan en el 3GPP mediante la utilización de un mecanismo AKA (Autenticación, Autenticación de claves) de IMS durante un proceso de registro del equipo de usuario. Las principales entidades de red involucradas durante el proceso de registro del equipo de usuario incluyen el equipo de usuario UE, la P-CSCF, la S-CSCF y el HSS.

Como se muestra en la Fig. 2, la utilización del mecanismo AKA de IMS durante el proceso de registro del equipo de usuario puede ser como sigue.

1. Se comparte un clave K inicial entre el UE y el HSS.

2. Un abonado inicia un mensaje de petición de registro SM1, y la S-CSCF solicita datos al HSS a través de un mensaje CM1. El HSS genera una quíntupla de autenticación basada en la clave K inicial y un número de secuencia SQN, y envía la quíntupla a la S-CSCF mediante un mensaje CM2. La quíntupla incluye datos aleatorios (RAND), un símbolo de autenticación (AUTN), una respuesta esperada (XRES), una clave de integridad (IK) y una clave de cifrado (CK).

3. La S-CSCF devuelve al abonado una respuesta 401 (Petición de autenticación) que incluye una cuádrupla de información excepto la XRES.

4. La P-CSCF almacena la información acerca de la IK y la CK y, en la respuesta 401, envía al UE información de RAND y AUTN.

5. El UE autentica la credibilidad del equipo de red en función de información como, por ejemplo, la clave K inicial y el SQN y el AUTN recibido enviada desde el equipo de red. Si la autenticación se realiza con éxito, el equipo de red es fiable y se genera información sobre una respuesta RES en función del RAND y la K. La RES se toma como una "contraseña" para el cálculo de una Respuesta por parte del UE. En un mensaje SM7 (Respuesta de Autenticación) se envía a la parte de red un resultado del cálculo. Al mismo tiempo, el UE calcula por sí mismo la IK y la CK.

6. La S-CSCF recibe, en un mensaje SM9, la información de Respuesta generada en función de la RES y compara la información con el resultado del cálculo a partir de la XRES. Si ambos son idénticos, se puede determinar que se

ha realizado con éxito la autenticación del abonado.

Como se puede observar a partir de lo anterior, el UE inicia el registro en la red IMS y, mediante el AKA del IMS, se lleva a cabo la autenticación bidireccional entre el UE y la red IMS. Además, se puede establecer una relación de seguridad entre el UE y la P-CSCF, y se pueden compartir tanto la clave CK de cifrado como la clave IK de integridad. Ambas claves se pueden utilizar para establecer un canal de comunicación seguro entre el UE y la P-CSCF.

Para más información sobre la "Seguridad en el Dominio de Acceso de IMS", se puede citar el Estándar Técnico TS33.203 del 3GPP, que ofrece descripciones detalladas sobre la seguridad del dominio de acceso de la red de IMS, y para más información sobre el mecanismo AKA de IMS, se puede citar el TS33.203, Sección 6.1 y la RFC3310 del IETF.

En el campo inalámbrico, existe un gran número de equipos de usuario en uso que son incompatibles con las especificaciones del protocolo del 3GPP y no pueden soportar el mecanismo de seguridad en el dominio de acceso como se requiere para el TS 33.203 del 3GPP como, por ejemplo, un equipo de usuario que utiliza una tarjeta SIM o un equipo de usuario 2G que utiliza una tarjeta USIM/ISIM. Para proporcionar un servicio de IMS para dicho cliente final, en el TR 33.878 se ha definido un mecanismo de seguridad en el dominio de acceso denominado como "Early IMS" (IMS temprano). El principio básico del dominio de acceso de seguridad del Early IMS consiste en que la seguridad de la capa de aplicación se puede habilitar sobre la seguridad de la capa de acceso. Después de que un acceso de un equipo se ha autenticado en la capa de acceso, la información autenticada se transfiere a la capa de aplicación que, a su vez, lleva a cabo una autenticación de seguridad de la capa de aplicación para la petición del abonado en función de dicha información. Como se muestra en la Fig. 3, el mecanismo de seguridad para el dominio de acceso del Early IMS se puede dividir en las siguientes partes.

1. Activación de PDP: un equipo de usuario obtiene un acceso a una red GPRS a través de un Nodo de Soporte de la Pasarela GPRS (GGSN). Durante un proceso de activación del Protocolo de Paquetes de Datos (PDP), el GGSN autentica las identidades IMSI y MSISDN de los abonados, y asigna al equipo de usuario una identidad de la capa de transporte de red (dirección IP). El GGSN transfiere al HSS correlaciones entre las identidades del abonado y la dirección IP del equipo a través de un mensaje "Accounting Request Start" (Inicio de Petición de Contabilidad), el cual, a su vez, almacena las correlaciones.

2. Autenticación de Petición de Registro: el equipo de usuario inicia una petición de registro REGISTER (registrar). Cuando la P-CSCF reenvía la petición a la S-CSCF, en la petición REGISTER se puede incluir una dirección IP de origen del equipo de usuario. En función de la identidad pública del abonado en la petición REGISTER, la S-CSCF comprueba si el equipo de usuario se ha registrado. Si no se ha registrado, el HSS obtiene la dirección IP del equipo correspondiente a la identidad pública del abonado utilizando un MAR/MAA (el HSS configura de forma estática la correlación entre la identidad pública del abonado y el MSISDN y, de este modo, se puede obtener la dirección IP correspondiente del equipo utilizando la identidad pública del abonado). La S-CSCF comprueba la dirección IP de origen del equipo a partir de la petición REGISTER recibida y, si es la misma que la obtenida desde el HSS, la autenticación se realiza con éxito.

3. Autenticación de Petición sin Registro: debido a que no se establece ningún canal de seguridad entre la P-CSCF y el UE, para asegurar que el nombre de usuario se corresponde con la dirección IP de origen, es necesario que la S-CSCF autentique todos los mensajes de petición iniciados por el equipo. Después de que el abonado se ha registrado, la S-CSCF almacena las correlaciones entre las identidades de los abonados y las direcciones IP. Al recibir cualquier mensaje de petición sin registro, se tiene que comparar la dirección IP de origen del equipo de usuario que inicia la petición con la dirección IP del abonado almacenada en la S-CSCF y, si son diferentes, la petición se puede rechazar.

Teniendo en cuenta lo anterior, la aplicación del Early IMS tiene la siguiente limitación.

La red de acceso de GPRS puede garantizar que la dirección IP del equipo de usuario no será imitada por ningún otro usuario y, de este modo, cada uno de los equipos puede enviar únicamente un mensaje con su propia dirección IP.

La comunicación entre el GPRS y la P-CSCF puede ser segura y no existe NAT entre el GPRS y la P-CSCF.

No se soportan los registros simultáneos de una única identidad pública de abonado de IMPU (Identidad Pública Multimedia IP) con respecto a una pluralidad de identidades de usuario privadas de IMPI (Identidad Privada Multimedia IP).

Por lo tanto, el mecanismo de seguridad para el dominio de acceso de Early IMS únicamente se puede dirigir a un entorno de acceso inalámbrico específico y, también impone un requisito especial en la red de acceso. Si se tiene que actualizar o adaptar un equipo de usuario relevante, no se puede garantizar la seguridad de acceso del abonado en cualquier otro entorno de acceso.

El documento WO 02/11469 A2 divulga una técnica para autenticar un usuario frente a un servidor utilizando mensajes SIP que incluye reenviar una petición SIP desde el agente de usuario al servidor. A continuación, el servidor reenvía una petición de autenticación al agente de usuario en respuesta a la petición de invitación, incluyendo la petición de autenticación información de que la autenticación se llevará a cabo utilizando un mecanismo AKA de UMTS. A continuación, el agente de usuario reenvía al servidor una respuesta de autenticación de acuerdo con el mecanismo AKA de UMTS y, después, el servidor realiza las acciones apropiadas para llevar a cabo un procedimiento SIP invocado en respuesta a la petición SIP. Sin embargo, el documento WO 02/11469 A no proporciona un método para llevar a cabo la autenticación en un equipo de usuario convencional que no soporte AKA de IMS.

El documento WO 02/091786 A1 divulga un método en un sistema de comunicación en donde se prepara un usuario para registrarse con una entidad de control comprendiendo el envío de un mensaje desde el sistema de comunicación al usuario solicitando que el usuario se vuelva a registrar en dicha red de comunicación. Como respuesta a dicho mensaje se obliga al usuario a volverse a registrar en dicha red. Este documento está relacionado con el registro de abonados en un sistema de comunicaciones móviles, pero no resuelve el problema de autenticar equipos convencionales de usuario en diferentes entornos de acceso.

Resumen de la invención

Teniendo en cuenta lo anterior, la presente invención proporciona métodos para autenticar un equipo de usuario en una red IMS, de modo que un equipo convencional de usuario que soporte una Autenticación Simplificada pueda obtener un acceso seguro en distintos entornos de acceso.

De acuerdo con un modo de realización, la presente invención proporciona un método para autenticar un equipo convencional de usuario que soporte una Autenticación Simplificada pero que no soporta un Acuerdo de Autenticación de Claves del subsistema multimedia IP, en un subsistema multimedia IP, incluyendo:

generar, por parte de una entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF), una petición de autenticación mediante un Algoritmo de Autenticación Simplificado como respuesta a una petición del abonado, y enviar a un equipo de usuario la petición de autenticación mediante una entidad de Función de Control de Sesión de Llamada de Proxy (P-CSCF);

generar, por parte del equipo de usuario, una respuesta de autenticación mediante el Algoritmo de Autenticación Simplificado de acuerdo con una clave de abonado así como parámetros asociados a la petición de autenticación y enviar, por parte de la entidad de P-CSCF, la respuesta de autenticación a la entidad de S-CSCF; y

verificar por parte de la entidad de S-CSCF la respuesta de autenticación mediante el Algoritmo de Autenticación Simplificado de acuerdo con la información HA1 obtenida a través de la interacción con el Servidor Local de Abonados (HSS) y un cálculo HASH que toma como una entrada la clave de abonado así como parámetros asociados y, si se pasa la verificación, determinar que se ha realizado con éxito la autenticación del equipo de usuario; en caso contrario, determinar que ha fallado la autenticación del equipo de usuario.

Opcionalmente, la petición del abonado es una petición de registro.

Opcionalmente, el Algoritmo de Autenticación Simplificado es un algoritmo MD5 Simplificado, y la entidad de S-CSCF puede obtener el HA1 mediante la interacción con el Servidor Local de Abonados (HSS) antes de la generación de la petición de autenticación o al recibir la respuesta de autenticación.

Opcionalmente, la obtención del HA1 incluye:

enviar al HSS, por parte de la entidad de S-CSCF, un mensaje de petición que incluya una identidad de abonado; y

generar, por parte del HSS, el HA1 de acuerdo con el nombre de dominio de un dominio correspondiente al abonado, la identidad del abonado y la clave del abonado, y devolver a la entidad de S-CSCF el HA1 en un mensaje de respuesta.

Opcionalmente, el Algoritmo de Autenticación Simplificado es un algoritmo MD5-Sess Simplificado.

Opcionalmente, la obtención del HA1 incluye:

enviar al HSS, por parte de la S-CSCF, un mensaje de petición que incluye una identidad de abonado, un parámetro “nonce” y un parámetro “cnonce” al recibir la respuesta de autenticación; y

generar, por parte del HSS, el HA1 de acuerdo con el nombre de dominio de un dominio correspondiente al abonado, la identidad del abonado, la clave del abonado, el parámetro “nonce” y el parámetro “cnonce”, y devolver a la entidad de S-CSCF el HA1 en un mensaje de respuesta.

Opcionalmente, la identidad de abonado es una identidad pública de usuario o una identidad privada de usuario.

Opcionalmente, después de que se ha realizado con éxito la autenticación del registro del equipo de usuario, se puede autenticar un mensaje de petición posterior de acuerdo con un método de autenticación para un mensaje de petición posterior configurado en el HSS.

Opcionalmente, el método de autenticación para un mensaje de petición posterior incluye uno entre los siguientes: autenticar únicamente un mensaje de petición de registro, autenticar únicamente una petición de registro y un mensaje de petición de sesión, y autenticar cada mensaje de petición.

Opcionalmente, en el caso de autenticación de cada mensaje de petición, se configura una sesión de autenticación para un mensaje de petición de abonado igual a un periodo de registro de abonado o un periodo de sesión de abonado.

De acuerdo con un modo de realización, la presente invención proporciona un método para autenticar un equipo convencional de usuario que soporta una Autenticación Simplificada pero no es capaz de soportar un Acuerdo de Autenticación de Clave del subsistema multimedia IP, en un subsistema multimedia IP, incluyendo:

generar, por parte de un Servidor Local de Abonados (HSS), los parámetros necesarios durante una Autenticación Simplificada para la generación de una petición de autenticación de acuerdo con una identidad de abonado en un mensaje de petición enviado por una entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF), y enviar los parámetros a la entidad de S-CSCF;

generar, por parte de la entidad de S-CSCF, una petición de autenticación de acuerdo con los parámetros, y enviar la petición de autenticación a un equipo de usuario a través de una entidad de Función de Control de Sesión de Llamada de Proxy (P-CSCF);

generar, por parte del equipo de usuario, una respuesta de autenticación mediante un Algoritmo de Autenticación Simplificado en función de una clave de abonado así como de los parámetros incluidos en la petición de autenticación y transferir la respuesta de autenticación al HSS a través de la entidad de P-CSCF y la entidad de S-CSCF; y

verificar, por parte del HSS, los contenidos incluidos en la respuesta de autenticación utilizando el Algoritmo de Autenticación Simplificado en función de la clave de abonado y los parámetros asociados y, si se ha pasado la verificación, informar a la entidad de S-CSCF que se ha realizado con éxito la autenticación del equipo de usuario; en caso contrario, informar a la entidad de S-CSCF que ha fallado la autenticación del equipo de usuario.

Opcionalmente, la identidad de abonado es una identidad pública de usuario o una identidad privada de usuario.

Opcionalmente, la petición del abonado es una petición de registro.

Opcionalmente, después de que se ha realizado con éxito la autenticación del registro del equipo de usuario, se autentica un mensaje de petición posterior de acuerdo con un método de autenticación para un mensaje de petición posterior configurado en el HSS.

Opcionalmente, el método de autenticación para un mensaje de petición posterior incluye uno de los siguientes: autenticar únicamente un mensaje de petición de registro, autenticar únicamente una petición de registro y un mensaje de petición de sesión, y autenticar cada mensaje de petición.

Opcionalmente, en el caso de autenticación de cada mensaje de petición, se configura una sesión de autenticación para un mensaje de abonado igual a un periodo de registro de abonado o un periodo de sesión de abonado.

En resumen, de acuerdo con la invención, en el dominio de acceso de IMS, se puede autenticar un equipo de usuario convencional que no soporte AKA de IMS utilizando un método de autenticación Simplificado soportado por el equipo sin ningún requisito especial en relación con el entorno de acceso. Por lo tanto, es posible permitir la compatibilidad con un equipo de usuario convencional, y también es aplicable en varios entornos de acceso como, por ejemplo, un entorno de acceso móvil o fijo, etc.

En la invención, se autentica cada mensaje de petición, incluyendo un mensaje de petición de establecimiento de sesión y, de este modo, se garantiza la seguridad de un canal de transmisión de señalización.

Además, se puede habilitar la autenticación de un equipo de usuario por parte de la entidad de S-CSCF o del HSS y, por lo tanto, se puede mejorar la flexibilidad de la red.

Breve descripción de los dibujos

La Fig. 1 muestra un modelo de seguridad para una red IMS en la técnica anterior;

la Fig. 2 muestra un diagrama de flujo del registro de un equipo de usuario en la técnica anterior;

la Fig. 3 muestra un diagrama de flujo esquemático de un mecanismo de seguridad en un dominio de acceso de Early IMS en la técnica anterior;

la Fig. 4a y la Fig. 4b son, respectivamente, diagramas de flujo de la autenticación del equipo de usuario a través de una entidad de S-CSCF con la utilización del MD5 Simplificado y el MD5-sess Simplificado de acuerdo con los modos de realización de la invención;

la Fig. 5 muestra un diagrama de flujo para la autenticación de equipos de usuario utilizando una entidad de S-CSCF con la utilización de MD5-sess Simplificado de acuerdo con un modo de realización de la invención;

la Fig. 6 muestra un diagrama de flujo para la autenticación de equipos de usuario utilizando un HSS con la utilización de un Algoritmo de Autenticación Simplificado de acuerdo con un modo de realización de la invención; y

la Fig. 7 muestra un diagrama de flujo para la Autenticación Simplificada en respuesta a un mensaje de petición posterior para el establecimiento de sesión de acuerdo con un modo de realización.

Descripción detallada de la invención

De acuerdo con la RFC3261, un número de equipos actuales del Protocolo de Inicio de Sesión (SIP) pueden soportar la Autenticación Simplificada, pero no pueden soportar el AKA de IMS requerido por el 3GPP. Por lo tanto, es necesario soportar la Autenticación Simplificada en una red IMS y, de este modo se puede servir a un equipo SIP que cumple la RFC3261. Específicamente, la Autenticación Simplificada de acuerdo con la invención incluye un algoritmo de autenticación MD5 o MD5-sess.

Se puede verificar la autenticidad de un abonado que inicia una petición basándose en el método de Autenticación Simplificado. Cuando se ha confirmado la autenticidad del abonado, la red puede determinar si proporciona el servicio correspondiente a la petición del abonado. La Autenticación Simplificada se puede llevar a cabo mediante un modo de “Petición Respuesta” básico, donde la “Información de Petición de Autenticación” se incluye en un campo de cabecera of WWW-Authenticate (Autenticación WWW), mientras que la información de “Respuesta de Autenticación” se incluye en un campo de cabecera de Authorization (Autorización). Para más información acerca de la Autenticación Simplificada, se puede citar la RFC3261, Capítulo 22, y la RFC2617 y la RFC2069.

(1) Los parámetros principales involucrados en el WWW-Authenticate incluyen:

realm=”biloxi.com”,

qop=”auth,auth-int”,

nonce=”dcd98b7102dd2f0e8b11d0f600bfb0c093”,

opaque=”5ccc069c403ebaf9f0171e9517f40e41”.

En particular:

El parámetro “realm” indica para un equipo de usuario el “dominio” desde el que se está llevando a cabo en ese momento una autenticación sobre el terminal del usuario.

Si el valor del parámetro “qop” (i.e., calidad de protección) es “auth”, indica que pretende ser únicamente para autenticación de abonados, o “auth-int” indica que pretende ser simultáneamente tanto para autenticación de abonados como para protección de integridad del cuerpo del mensaje.

El parámetro “nonce” se genera en la red, en correspondencia con la hora local de la misma. El equipo de usuario envía de vuelta, en un campo de cabecera de una respuesta de autenticación de Autorización devuelta, el contenido de “nonce”. A partir del contenido del parámetro “nonce”, la red obtiene la hora en la que se generó el parámetro “nonce” (i.e., el momento en el que se envió la petición de autenticación WWW-Authenticate). Si la diferencia entre el momento en el que se generó el parámetro “nonce” y el momento en el que se recibe realmente la Autorización es demasiado grande, se puede señalar que existe un “Ataque de Respuesta”.

(2) El campo de cabecera de Authorization generado por un equipo de usuario a partir de un número de cuenta y el contenido WWW-Authenticate recibido incluye, principalmente:

realm=”biloxi.com”,

nonce=”dcd98b7102dd2f0e8b11d0f600bfb0c093”,

uri=”sip:bob@biloxi.com”,

qop=auth,

nc=00000001,

cnonce=”0a4f113b”,

response=”6629fae49393a05397450978507c4ef1”,

opaque=”5ccc069c403ebaf9f0171e9517f40e41”.

En particular:

El parámetro “nc” indica el número de veces que se ha utilizado el mismo “nonce” para generar una respuesta de autenticación. La red puede mantener un contador y, cuando la red recibe el mismo valor de nc dos o más veces, indica que existe un Ataque de Respuesta.

El parámetro “cnonce” se utiliza para que un UE autentique la red, y este parámetro se genera en un equipo de usuario, y lo devuelve la red en el campo de cabecera de Authentication-Info (Información de Autenticación).

El parámetro “response” (respuesta) se utiliza para verificación de una identidad de abonado. El UE obtiene datos de este parámetro en función de un username (nombre de usuario), una password (contraseña) de usuario, valores de realm-value (valor de dominio), “nonce”, uri, etc. La red también puede obtener una cadena de datos mediante el mismo algoritmo en función de dichos datos de entrada. Si ambos datos son iguales, se prueba que la contraseña de usuario es correcta y, de este modo, se puede verificar la identidad del abonado. A continuación se describirá el algoritmo para la generación de un parámetro “response” (i.e., Request-Digest (Petición-Simplificada))(para detalles, se cita la RFC2617, secciones 3.2.2.1 – 3.2.2.3):

request-digest = <”> < KD (H (A1), unq(nonce-value)

“:” nc-value

“:” unq(cnonce-value)

“:” unq(qop-value)

“:” H(A2)

) <”>

En particular, los parámetros A1 y A2 se pueden calcular del siguiente modo:

A1 = unq(username-value) “:” unq(realm-value) “:” passwd

A2 = Method “:” digest-uri-value

(3) Además de los dos campos de cabecera básicos, “WWW-Authenticate” y “Authorization”, en la RFC2617 se ha definido otro campo de cabecera de Authentication-Info. Este campo de cabecera se puede enviar al UE en una respuesta positiva a una autenticación de equipo y, de este modo, se puede transmitir información adicional asociada con la autenticación; este campo de cabecera no existe en la RFC2069, pero es una extensión de las definiciones de la RFC2617. Los parámetros específicos son los siguientes:

Authentication-Info:

qop=auth,

rspauth=”6629fae49393a05397450978507c4ef1”,

cnonce=”0a4f113b”,

nc=00000001.

El parámetro “qop” indica un tipo de autenticación (si se necesita protección del cuerpo del mensaje), que se ha descrito más arriba.

El parámetro “rspauth” se utiliza para que la red indique al UE que conoce la contraseña del UE. Al recibir este parámetro, el UE lleva a cabo los cálculos para determinar si el resultado del cálculo es idéntico al valor del parámetro. Si son idénticos, el UE puede determinar que la red es fiable. Este parámetro se puede calcular del mismo modo que se calculó el parámetro “response” descrito más arriba.

El parámetro “cnonce” se utiliza para que la red devuelva al UE el contenido incluido en el campo de la cabecera Authorization sin modificar.

El parámetro “nc”, i.e. nonce-count (cuenta de nonce), indica el número de veces que se utiliza el mismo “nonce” para la generación de una respuesta de autenticación.

Además de los cuatro parámetros anteriores, en este campo de cabecera se puede incluir el parámetro “nextnonce” (nonce siguiente). El parámetro “nextnonce” contiene un parámetro “nonce” que utilizará el equipo de usuario para generar la próxima respuesta de autenticación tal y como espera la red. Con este parámetro, la red puede conseguir un parámetro “nonce” exclusivo o modificar el valor del mismo.

Para soportar la Autenticación Simplificada en la red IMS, el operador debería configurar en el HSS el mecanismo de autenticación Simplificada correspondiente soportado por un abonado en función de una identidad de abonado del abonado. El HSS determina la realización de la Autenticación Simplificada del equipo de usuario en función de la identidad del abonado y los datos correspondientes de configuración del abonado. La identidad del abonado puede ser una identidad privada de usuario, que es aplicable normalmente en el caso de un acceso de un abonado con una tarjeta de abonado (por ejemplo una tarjeta ISIM, etc.). En el caso de que el equipo de usuario no tenga una tarjeta de abonado semejante, se puede configurar un mecanismo de autenticación correspondiente para una identidad pública de abonado (para consistencia de los procesos internos, la identidad privada de usuario se puede considerar que es idéntica a la identidad pública de usuario).

En el dominio de acceso de IMS, como se muestra en la Fig. 4A, la entidad de S-CSCF puede llevar a cabo los siguientes pasos específicos para la autenticación MD5 Simplificada como respuesta a una petición de registro desde un equipo de usuario.

En el paso 1, el equipo de usuario UE envía a la entidad de P-CSCF un mensaje REGISTER de petición de registro.

En el paso 2, la entidad de P-CSCF reenvía a la entidad de S-CSCF el mensaje REGISTER de petición de registro.

En el paso 3, la entidad de S-CSCF envía al HSS un mensaje Multimedia-Auth-Request (MAR) (Petición de Autorización Multimedia) que incluye una identidad de abonado que se puede obtener a partir del mensaje REGISTER de petición de registro.

En el paso 4, el HSS recibe el mensaje MAR, y determina llevar a cabo la autenticación MD5 Simplificada para el abonado en función de los datos de configuración del abonado correspondientes a la identidad del abonado. El HSS calcula un H(A1) mediante una fórmula H(A1)=H(unq(username-value) “:” unq(realm-value) “:” passwd) en función del nombre de usuario “username-value”, el nombre del dominio correspondiente “realm-value” y la contraseña del abonado “passwd” de los datos de configuración del abonado, y devuelve a la S-CSCF un mensaje Multimedia-Auth-Answer (MAA) (Respuesta de Autorización Multimedia) que incluye el H(A1).

En el paso 5, la S-CSCF almacena el HA1 y también genera los parámetros respectivos para la Petición de la Autenticación como, por ejemplo, el parámetro “nonce”. El parámetro “realm”, i.e. un nombre de dominio de un dominio en el que se localiza el abonado, se puede obtener directamente a partir de la identidad del abonado. Por otra parte, el campo de cabecera de WWW-Authenticate se puede generar de acuerdo con los parámetros respectivos y, a continuación, se pueden enviar a la entidad de P-CSCF en una respuesta 401.

En el paso 6, la P-CSCF recibe la respuesta 401 desde la S-CSCF y comprueba el contenido del mensaje para determinar que el algoritmo de autenticación es para la Autenticación Simplificada. En este momento, la P-CSCF no modifica la respuesta 401, y transmite al equipo de usuario UE la respuesta 401 de forma transparente (en el caso del AKA de IMS, la P-CSCF debería almacenar la IK/CK para el establecimiento IPSec posterior).

En el paso 7, el equipo de usuario obtiene el WWW-Authenticate (Petición de autenticación) a partir de la respuesta 401 y, a continuación, calcula una “request-digest” junto con su clave. Además, el equipo de usuario incluye la “request-digest” en el parámetro “response” de la respuesta Authorization de autenticación, y envía a la entidad de P-CSCF la respuesta de autenticación en un mensaje REGISTER de petición de registro reiniciado.

En el paso 8, la entidad de P-CSCF transfiere a la entidad de S-CSCF el mensaje REGISTER de petición de registro.

En el paso 9, la entidad de S-CSCF recibe la respuesta de autenticación y, a continuación, calcula una “request-digest” junto con el HA1, y compara la “request-digest” con el contenido del parámetro “response” de la respuesta Authorization de autenticación. Si ambos son idénticos, la autenticación se realiza con éxito, enviándose una respuesta 200 al abonado; en caso contrario, la autenticación falla.

En el paso 10, la entidad de P-CSCF envía al equipo de usuario un mensaje de respuesta 200.

En lo anterior, la interacción MAR/MAA entre la S-CSCF y el HSS también se puede llevar a cabo después de que la

entidad de S-CSCF reciba la respuesta de autenticación, como se muestra en la Fig. 4B, donde se ha omitido la entidad de P-CSCF. En este caso, en teoría, la implementación es la misma que se muestra en la Fig. 4A, y no se describe aquí.

El HA1 se puede obtener mediante un cálculo HASH tomando como entrada la clave del abonado, sin involucrar ninguna clave de abonado en texto plano. Por lo tanto, este caso puede ser más seguro comparado con el caso en el que la clave en texto plano se transfiere entre la S-CSCF y el HSS. Sin embargo, si la comunicación entre la S-CSCF y el HSS no es segura, un atacante puede obtener el HA1. Para este método se recomienda un canal de seguridad entre la S-CSCF y el HSS como, por ejemplo, IPSec.

Para el algoritmo MD5-sess, en el cálculo del HA1 se pueden utilizar números aleatorios asociados con la autenticación de un solo uso como, por ejemplo, “nonce”, “cnonce” y similares y, de este modo, se pueden superar las desventajas del algoritmo MD5. Incluso si el atacante obtiene el HA1, él/ella no puede apropiarse del servicio siguiente. Por esta razón, puede no ser necesario el canal de seguridad entre la S-CSCF y el HSS. El cálculo del HA1 para el algoritmo MD5-sess Simplificado es como sigue:

H(A1) = H(H(unq(username-value) “:” unq(realm-value)

“:” passwd)

“:” unq(nonce-value) “:” unq(cnonce-value))

Haciendo referencia a la Fig. 5, en el dominio de acceso de IMS, la entidad de S-CSCF lleva a cabo los siguientes pasos específicos para la autenticación MD5-sess Simplificada como respuesta a una petición de registro desde un equipo de usuario, donde se ha omitido la parte de la entidad de P-CSCF.

En el paso 1, el equipo de usuario envía a la entidad de S-CSCF un mensaje REGISTER de petición de registro.

En el paso 2, como respuesta al mensaje de petición recibido, la S-CSCF genera los parámetros respectivos para una Petición de Autenticación como, por ejemplo, “nonce”, “qop”, “realm”, etc., y, a continuación, genera el campo de cabecera de WWW-Authenticate, y envía al equipo de usuario el campo de cabecera en una respuesta 401 (lo transmite al equipo de usuario de forma transparente a través de la entidad de P-CSCF).

En el paso 3, el equipo de usuario obtiene el WWW-Authenticate (Petición de Autenticación) a partir de la respuesta 401 y, a continuación, calcula una “request-digest” junto con su clave. Además, el equipo de usuario incluye la “request-digest” en el parámetro “response” de la respuesta Authorization de autenticación, y envía la respuesta de autenticación a la entidad de S-CSCF en un mensaje REGISTER de petición de registro reiniciado.

En el paso 4, la entidad de S-CSCF obtiene los parámetros “nonce” y “cnonce” del campo de cabecera Authorization, y transfiere al HSS los parámetros junto con la identidad del usuario en una petición MAR.

En el paso 5, con respecto a la identidad del abonado, el HSS calcula el HA1 mediante la fórmula de más arriba en función de los parámetros relevantes y envía a la entidad de S-CSCF el HA1 en una respuesta MAA.

En el paso 6, la entidad de S-CSCF calcula una “request-digest” en función del HA1 y los parámetros de autenticación relevantes. Si el resultado del cálculo es el mismo que el contenido incluido en el parámetro “response” de la respuesta de autenticación, la autenticación tiene éxito, devolviendo al UE una respuesta 200; en caso contrario, se devuelve una respuesta de fallo de autenticación.

En el Servidor Local de Abonados (HSS) de la red IMS, “MD5” o “MD5-sess” pueden ser algoritmos correspondientes configurados para un abonado y dicha información de configuración se puede utilizar para un proceso en el que la I-CSCF selecciona una S-CSCF para el abonado. Por ejemplo, un operador configura una S-CSCF para utilizar únicamente el algoritmo MD5 (existe un canal de seguridad entre la S-CSCF y el HSS) y otra S-CSCF para utilizar únicamente el algoritmo MD5-sess. Una petición de registro de un abonado para el que se ha configurado la autenticación MD5 debe asignarse a la primera S-CSCF.

En el caso en el que la S-CSCF soporte ambos algoritmos (MD5 y MD5-sess), la S-CSCF puede obtener del HSS un tipo de algoritmo de autenticación correspondiente al abonado y, a continuación, se puede enviar una petición de autenticación (si el tipo es MD5, el HA1 se enviará directamente de vuelta en un MAA). Alternativamente, la S-CSCF indica al equipo de usuario que soporta ambos algoritmos, y utiliza un algoritmo de autenticación elegido por el UE. Cuando la S-CSCF interactúa con el HSS, si el HSS determina que el algoritmo de autenticación seleccionado por el UE es inconsistente con uno preconfigurado, se devuelve al abonado un mensaje de fallo de autenticación.

Haciendo referencia a la Fig. 6, en el dominio de acceso de IMS, la entidad de HSS lleva a cabo autenticación Simplificada para un equipo de usuario como respuesta a una petición de registro del siguiente modo (donde se ha omitido la entidad de P-CSCF).

En el paso 1, el equipo de usuario envía a la entidad de S-CSCF un mensaje REGISTER de petición de registro.

En el paso 2, la entidad de S-CSCF envía al HSS una petición MAR que incluye una identidad de abonado.

En el paso 3, con respecto a la identidad de abonado, la HSS genera todos los parámetros necesarios para una petición de autenticación como, por ejemplo, “nonce”, etc.; y envía a la entidad de S-CSCF estos parámetros en un SIP-Authenticate AVP (Pareja de Valores de Atributo de Autenticación SIP) de un mensaje MRR devuelto desde la entidad de S-CSCF.

En el paso 4, la S-CSCF genera el campo de cabecera de WWW-Authenticate en función de estos parámetros generados por el HSS y envía al UE el campo de cabecera de WWW-Authenticate en una respuesta 401 (la transmite al equipo de usuario de forma transparente a través de la entidad de P-CSCF).

En el paso 5, el equipo de usuario obtiene el WWW-Authenticate (Petición de Autenticación) a partir de la respuesta 401 y, a continuación, calcula una “request-digest” junto con su clave. Además, el equipo de usuario incluye la “request-digest” en el parámetro “response” de la respuesta Authorization de autenticación y envía la respuesta de autenticación a la entidad de P-CSCF en un mensaje REGISTER de petición de registro reiniciado.

En el paso 6, la entidad de S-CSCF obtiene la información de parámetros asociados a la autenticación generados por el UE como, por ejemplo, “cnonce”, etc., a partir del parámetro “response” y, a continuación, incluye estas informaciones en una SIP-Authentication AVP que se incluye en una petición MAR, y transfiere al HSS la petición MAR.

En el paso 7, el HSS recibe la respuesta de autenticación y, después, calcula una “request-digest” mediante el Algoritmo de Autenticación Simplificado en función del HA1 y los parámetros de autenticación apropiados. Si esta “request-digest” es igual que el contenido incluido en el parámetro “response” de la respuesta de autenticación, la autenticación tiene éxito; en caso contrario, la autenticación falla. El resultado de la autenticación se envía a la S-CSCF en un mensaje MAA.

En el paso 8, si la S-CSCF recibe una indicación de éxito en la autenticación, se devolverá al UE una respuesta 200; en caso contrario, se devolverá una respuesta de fallo.

Además, si el equipo de usuario no está habilitado para establecer ningún canal de seguridad con la P-CSCF y la red IP subyacente no puede garantizar ninguna seguridad de comunicación entre el equipo de usuario y la P-CSCF, al acceder dicho abonado no se puede garantizar ninguna comunicación segura entre el UE y la P-CSCF. Para garantizar una comunicación segura, en los datos de configuración del abonado en el HSS se puede configurar un método de autenticación para un mensaje de petición posterior. De acuerdo con este método de autenticación, al realizar con éxito la autenticación del registro, se puede llevar a cabo la Autenticación Simplificada para el mensaje de petición posterior. Si el mensaje de petición posterior pasa la Autenticación Simplificada, se lleva a cabo el proceso siguiente; en caso contrario, se rechaza el mensaje de petición.

El método de autenticación para un mensaje de petición posterior puede incluir lo siguiente:

1. La Autenticación Simplificada se puede llevar a cabo únicamente para el mensaje REGISTER de la petición de registro.

2. Además de la petición de registro, la Autenticación Simplificada se puede llevar a cabo para cada mensaje INVITE (invitar) de petición de sesión.

3. Además de la petición de registro y la petición de sesión, la Autenticación Simplificada se puede llevar a cabo para cualquier otro mensaje de petición.

Dicha información de configuración se puede efectuar por parte de una entidad de autenticación de la red IMS, por ejemplo, la entidad de S-CSCF o el HSS tal y como se ha descrito más arriba.

Como se muestra en la Fig. 7, la entidad de S-CSCF autentica el mensaje INVITE de petición de sesión como sigue.

En el paso 1, la entidad de S-CSCF recibe un mensaje INVITE de petición de sesión iniciado por un equipo de usuario UE1 para un equipo de usuario UE2 y, a continuación, genera el campo de encabezado de la petición de autenticación WWW-Authenticate. Como se ha descrito más arriba, se debería necesitar la interacción con el HSS para la generación de la petición de autenticación.

En el paso 2, la entidad de S-CSCF envía al equipo de usuario UE1 un mensaje de respuesta 401 (WWW-Authenticate) a través de la entidad de P-CSCF (no se muestra).

En el paso 3, el equipo de usuario UE1 recibe la respuesta 401 y, a continuación, envía a la entidad de S-CSCF un mensaje ACK (confirmación) de respuesta.

En el paso 4, el equipo de usuario UE1 genera una respuesta de autenticación (para detalles, ver las descripciones asociadas de más arriba), y envía a la entidad de S-CSCF la respuesta de autenticación en un mensaje INVITE de petición de sesión (Authorization).

En el paso 5, la entidad de S-CSCF verifica el contenido en la respuesta de autenticación mediante el Algoritmo de Autenticación Simplificado en función de los parámetros relevantes. Si se pasa la verificación, la entidad de S-CSCF envía una respuesta 200 al equipo de usuario UE1; en caso contrario, se puede devolver una respuesta de fallo de autenticación.

En el paso 6, el equipo de usuario UE1 devuelve a la S-CSCF un ACK de respuesta.

Después de haber pasado la autenticación de registro del equipo de usuario, se puede entregar a la entidad de S-CSCF el método de autenticación configurado en el HSS para un mensaje de petición posterior, y a su vez la entidad de S-CSCF determina un método de autenticación para un mensaje de petición posterior de acuerdo con el método de autenticación. Si es necesaria una autenticación, el HSS todavía puede actuar como una entidad de autenticación, y se puede llevar a cabo la autenticación del mismo modo que se ha descrito más arriba.

Se aplica un concepto de “Sesión de Autenticación” cuando se utiliza el método de autenticación Simplificado para autenticación de una petición de abonado, el cual se ha descrito en la RFC2617. Se inicia una sesión de autenticación cuando la red envía al UE una petición de autenticación. Durante esta sesión, el UE puede incluir una respuesta de autenticación en un mensaje de petición posterior. El parámetro “nc” se incrementa en 1 cada vez que se incluye una respuesta de autenticación. Únicamente se puede terminar la sesión de autenticación actual después de enviar una nueva petición de autenticación desde la red como respuesta a una petición desde el UE, y puede comenzar una nueva sesión de autenticación.

Cuando se lleva a cabo la Autenticación Simplificada para cada mensaje del UE, el operador de la red IMS puede seleccionar una “sesión de autenticación” para el abonado de cualquiera de los siguientes modos.

1. Una “sesión de autenticación” para un mensaje de petición de abonado puede ser igual a un período de registro del abonado.

Después de registrase satisfactoriamente el abonado, la S-CSCF puede negociar con el abonado el período de registro. El UE puede reiniciar una petición REGISTER dentro del período de registro y, de este modo, el estado de registro se puede mantener indefinidamente. Se pueden generar nuevos parámetros como, por ejemplo, “nonce” y se pueden enviar nuevas peticiones de autenticación únicamente cuando la S-CSCF recibe una petición de registro o de repetición de registro. No se pueden generar o enviar nuevas peticiones de autenticación para otras peticiones, incluyendo la petición de sesión INVITE.

2. Una “sesión de autenticación” para un mensaje de petición de abonado puede ser igual a un período de sesión del abonado.

Además de la generación y envío de una nueva petición de autenticación para cada mensaje REGISTER de petición de registro desde el abonado, la S-CSCF puede generar y enviar una nueva petición de autenticación para cada petición de establecimiento de sesión (Dialog (diálogo)) SIP y una petición fuera de sesión. Sin embargo, no se generará ninguna nueva petición de autenticación para una petición SIP dentro de la sesión.

En el caso de que la entidad de autenticación de la red IMS sea la S-CSCF, debido a que los datos de configuración de un abonado relativos al “método de autenticación para una petición posterior” y la “sesión de autenticación” se han configurado en el HSS, la S-CSCF necesita obtener dicha información de configuración asociada al abonado. La S-CSCF puede obtener dicha información de configuración del abonado de modo que, después de realizar con éxito la autenticación del abonado, la S-CSCF puede interactuar con el HSS mediante un mensaje Diameter SAR/SAA, con el fin de descargar dicha información desde el HSS a la S-CSCF junto con la información de suscripción del abonado.

Mientras que los modos preferidos de la presente invención se han descrito más arriba, se observará que el alcance de la presente invención no se limitará a ellos y, obviamente, aquellos experimentados en la técnica pueden realizar diversas variaciones y modificaciones a los modos de realización sin apartarse del alcance de la presente invención. Por lo tanto, se pretende que todas dichas variaciones y modificaciones se incluyan dentro del alcance de la presente invención como se define completamente en las siguientes reivindicaciones.

REIVINDICACIONES

1. Un método para autenticar un equipo de usuario convencional que soporta una Autenticación Simplificada, pero no es capaz de soportar un Acuerdo de Clave de Autenticación del subsistema multimedia IP, en un subsistema multimedia IP, que comprende:

generar, por parte de una entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF), una petición de autenticación mediante un Algoritmo de Autenticación Simplificado como respuesta a una petición del abonado, y enviar la petición de autenticación a un equipo de usuario a través de una entidad de Función de Control de Sesión de Llamada de Proxy (Agente) (P-CSCF);

generar, por parte del equipo de usuario, una respuesta de autenticación mediante el Algoritmo de Autenticación Simplificado en función de una clave de abonado así como parámetros asociados en la petición de autenticación, y enviar la respuesta de autenticación a la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF) a través de la entidad de Función de Control de Sesión de Llamada de Proxy (P-CSCF); y

verificar, por parte de la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF), la respuesta de autenticación mediante el Algoritmo de Autenticación Simplificado de acuerdo con la información HA1 obtenida a través de la interacción con un Servidor Local de Abonados (HSS) y un cálculo HASH tomando como entrada la clave del abonado así como parámetros asociados y, si se ha pasado la verificación, determinar que se ha realizado con éxito la autenticación del equipo de usuario; en caso contrario, determinar que falla la autenticación del equipo de usuario.

2. El método de acuerdo con la reivindicación 1, en donde la petición del abonado es una petición de registro.

3. El método de acuerdo con la reivindicación 1, en donde el Algoritmo de Autenticación Simplificado es un algoritmo MD5 Simplificado, y la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF) obtiene el HA1 mediante la interacción con el Servidor Local de Abonados (HSS) antes de la generación de la petición de autenticación o al recibir la respuesta de autenticación.

4. El método de acuerdo con la reivindicación 3, en donde la obtención del HA1 comprende:

enviar al Servidor Local de Abonados (HSS), por parte de la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF), un mensaje de petición que incluye una identidad de abonado; y

generar, por parte del Servidor Local de Abonados (HSS), el HA1 en función de un nombre de dominio de un dominio correspondiente al abonado, la identidad del abonado y la clave del abonado, y devolver el HA1 a la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF) en un mensaje de respuesta.

5. El método de acuerdo con la reivindicación 1, en donde el Algoritmo de Autenticación Simplificado es un algoritmo MD5-Sess Simplificado.

6. El método de acuerdo con la reivindicación 5, en donde la obtención del HA1 comprende:

enviar a un Servidor Local de Abonados (HSS), por parte de la Función de Control de Sesión de Llamada de Servicio (S-CSCF), un mensaje de petición que incluye una identidad de abonado, un parámetro “nonce” y un parámetro “cnonce” al recibir la respuesta de autenticación; y

generar, por parte del Servidor Local de Abonados (HSS), el HA1 en función de un nombre de dominio de un dominio correspondiente al abonado, la identidad del abonado, la clave del abonado, el parámetro “nonce” y el parámetro “cnonce”, y devolver el HA1 a la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF) en un mensaje de respuesta.

7. El método de acuerdo con la reivindicación 4 ó 6, en donde la identidad del abonado es una identidad pública de usuario o una identidad privada de usuario.

8. El método de acuerdo con la reivindicación 2, en donde después de realizar con éxito la autenticación del registro del equipo de usuario, se autentica un mensaje de petición posterior de acuerdo con un método de autenticación para un mensaje de petición posterior configurado en un Servidor Local de Abonados (HSS).

9. El método de acuerdo con la reivindicación 8, en donde el método de autenticación para un mensaje de petición posterior comprende uno de los siguientes: autenticar únicamente un mensaje de petición de registro, autenticar únicamente un mensaje de petición de registro y de petición de sesión, y autenticar cada mensaje de petición.

10. El método de acuerdo con la reivindicación 9, en donde en el caso de autenticación de cada mensaje de petición, se configura una sesión de autenticación para un mensaje de petición del abonado para que sea igual a un

período de registro del abonado o un período de sesión del abonado.

11. Un método para autenticar un equipo de usuario convencional que soporta una Autenticación Simplificada pero no es capaz de soportar un Acuerdo de Clave de Autenticación del subsistema multimedia IP, en un subsistema multimedia IP, que comprende:

generar, por parte de un Servidor Local de Abonados (HSS), los parámetros necesarios durante una Autenticación Simplificada para la generación de una petición de autenticación en función de una identidad de abonado en un mensaje de petición enviado desde una entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF), y enviar los parámetros a la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF);

generar, por parte de la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF), una petición de autenticación en función de los parámetros, y enviar la petición de autenticación a un equipo de usuario a través de una entidad de Función de Control de Sesión de Llamada de Proxy (P-CSCF);

generar, por parte del equipo de usuario, una respuesta de autenticación mediante un Algoritmo de Autenticación Simplificado en función de una clave de abonado así como de parámetros asociados en la petición de autenticación, y transferir la respuesta de autenticación al Servidor Local de Abonados (HSS) a través de la entidad de Función de Control de Sesión de Llamada de Proxy (P-CSCF) y la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF); y

verificar, por parte del Servidor Local de Abonados (HSS), los contenidos asociados en la respuesta de autenticación mediante el Algoritmo de Autenticación Simplificado en función de la clave del abonado y de los parámetros relacionados, y si se pasa la verificación, informar a la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF) que se ha realizado con éxito la autenticación del equipo de usuario; en caso contrario, informar a la entidad de Función de Control de Sesión de Llamada de Servicio (S-CSCF) que la autenticación del equipo de usuario ha fallado.

12. El método de acuerdo con la reivindicación 11, en donde la identidad de abonado es una identidad pública de usuario o una identidad privada de usuario.

13. El método de acuerdo con la reivindicación 11 ó 12, en donde la petición de abonado es una petición de registro.

14. El método de acuerdo con la reivindicación 13, en donde después de realizar con éxito la autenticación del registro del equipo de usuario, se autentica un mensaje de petición posterior de acuerdo con un método de autenticación para un mensaje de petición posterior configurado en el Servidor Local de Abonados (HSS).

15. El método de acuerdo con la reivindicación 14, en donde el método de autenticación para un mensaje de petición posterior comprende uno de los siguientes: autenticar únicamente un mensaje de petición de registro, autenticar únicamente un mensaje de petición de registro y de petición de sesión, y autenticar cada mensaje de petición.

16. El método de acuerdo con la reivindicación 15, en donde en el caso de autenticación de cada mensaje de petición, se configura una sesión de autenticación para un mensaje del abonado para que sea igual a un período de registro del abonado o un período de sesión del abonado.

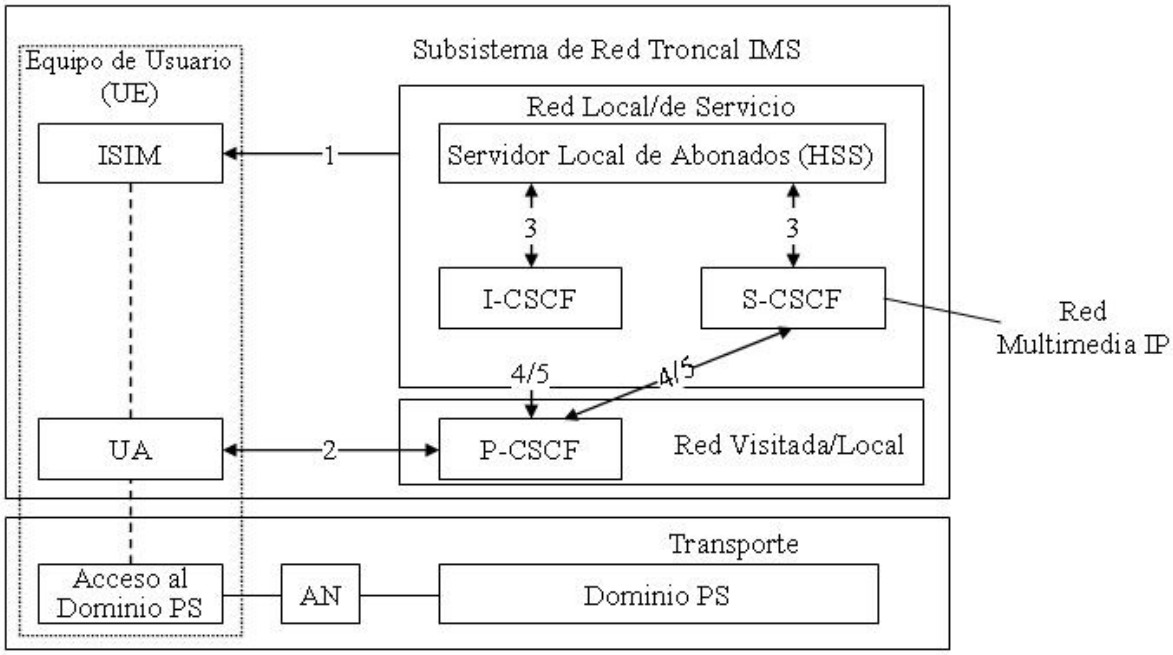
Subsistema de Red Troncal IMS
Equipo de Usuario (UE)
Red Local/de Servicio
ISIM
1
Servidor Local de Abonados (HSS)
3
3
I-CSCF
S-CSCF
Red Multimedia IP
4/5
4/5
UA
2
P-CSCF
Red Visitada/Local
Transporte
Acceso al Dominio PS
AN
Dominio PS

FIG.1

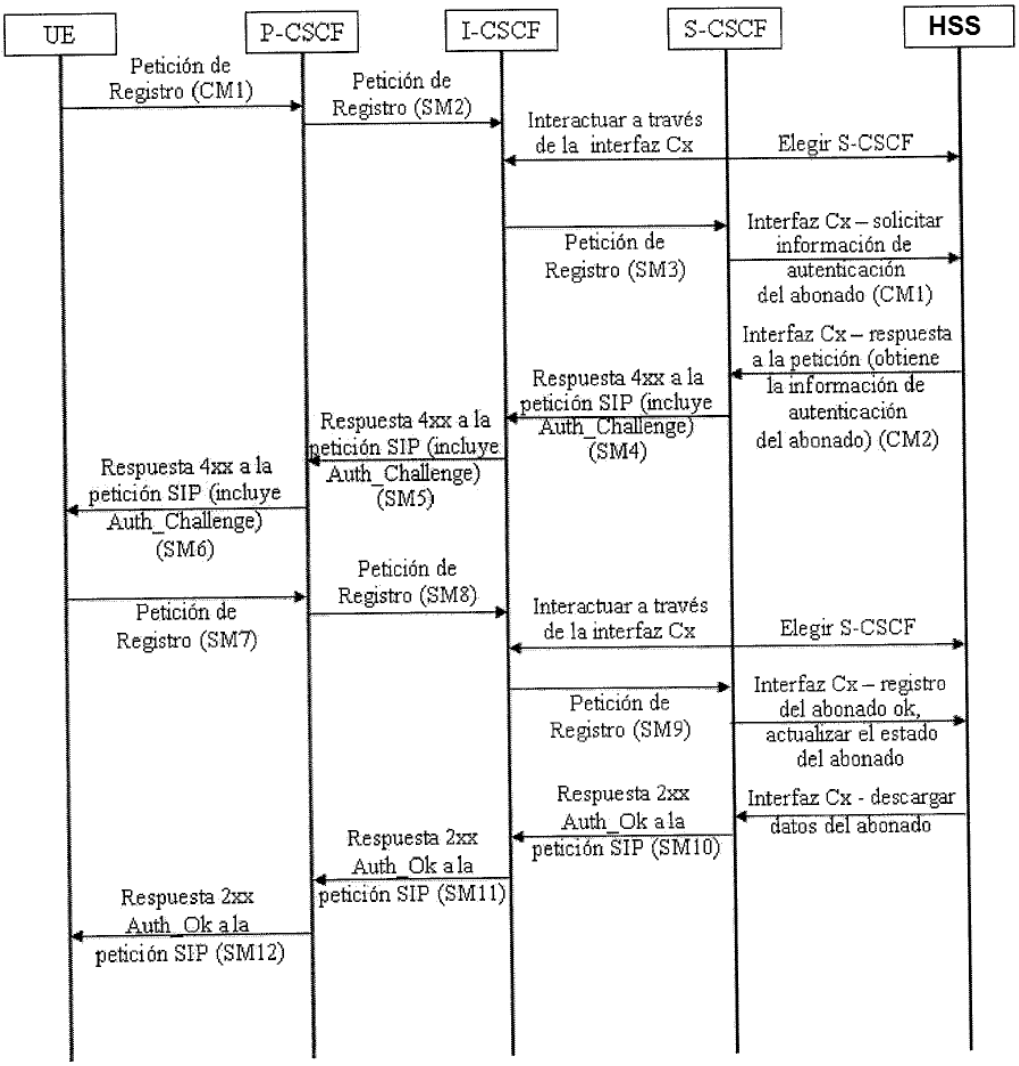
UE
P-CSCF
I-CSCF
S-CSCF
HSS
Petición de Registro (CM1)
Petición de Registro (SM2)
Interactuar a través de la interfaz Cx
Elegir S-CSCF
Petición de Registro (SM3)
Interfaz Cx – solicitar información de autenticación del abonado (CM1)
Interfaz Cx – respuesta a la petición (obtiene la información de autenticación del abonado) (CM2)
Respuesta 4xx a la petición SIP (incluye Auth_Challenge) (SM4)
Respuesta 4xx a la petición SIP (incluye Auth_Challenge) (SM5)
Respuesta 4xx a la petición SIP (incluye Auth_Challenge) (SM6)
Petición de Registro (SM7)
Petición de Registro (SM8)
Interactuar a través de la interfaz Cx
Elegir S-CSCF
Petición de Registro (SM9)
Interfaz Cx – registro del abonado ok, actualizar el estado del abonado
Respuesta 2xx Auth_Ok a la petición SIP (SM10)
Interfaz Cx - descargar datos del abonado
Respuesta 2xx Auth_Ok a la petición SIP (SM11)
Respuesta 2xx Auth_Ok a la petición SIP (SM12)

FIG.2

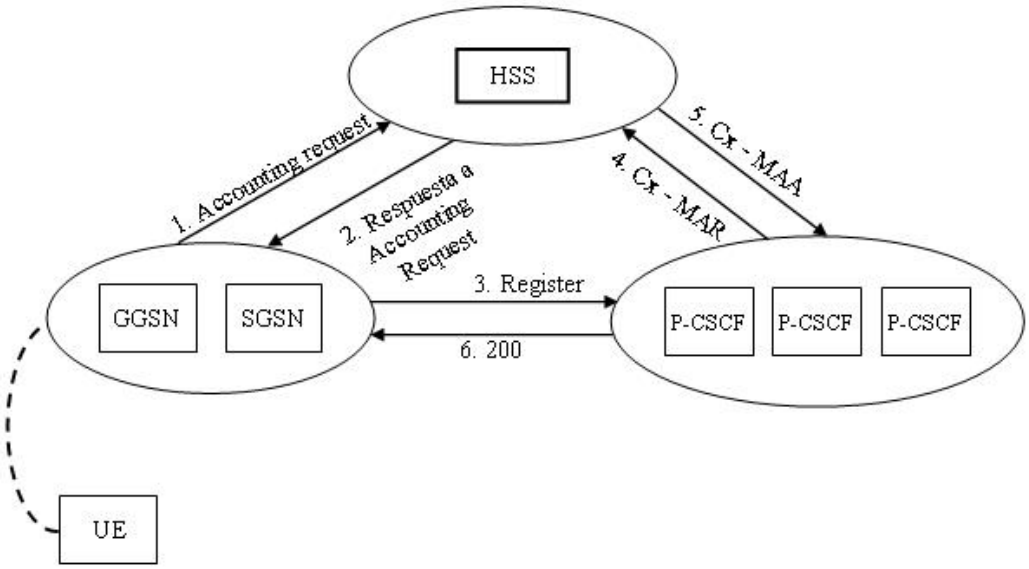
HSS
1. Accounting request
2. Respuesta a Accounting Request
3. Register
4. Cx - MAR
5. Cx - MAA
6. 200
GGSN
SGSN
P-CSCF
P-CSCF
P-CSCF
UE

FIG.3

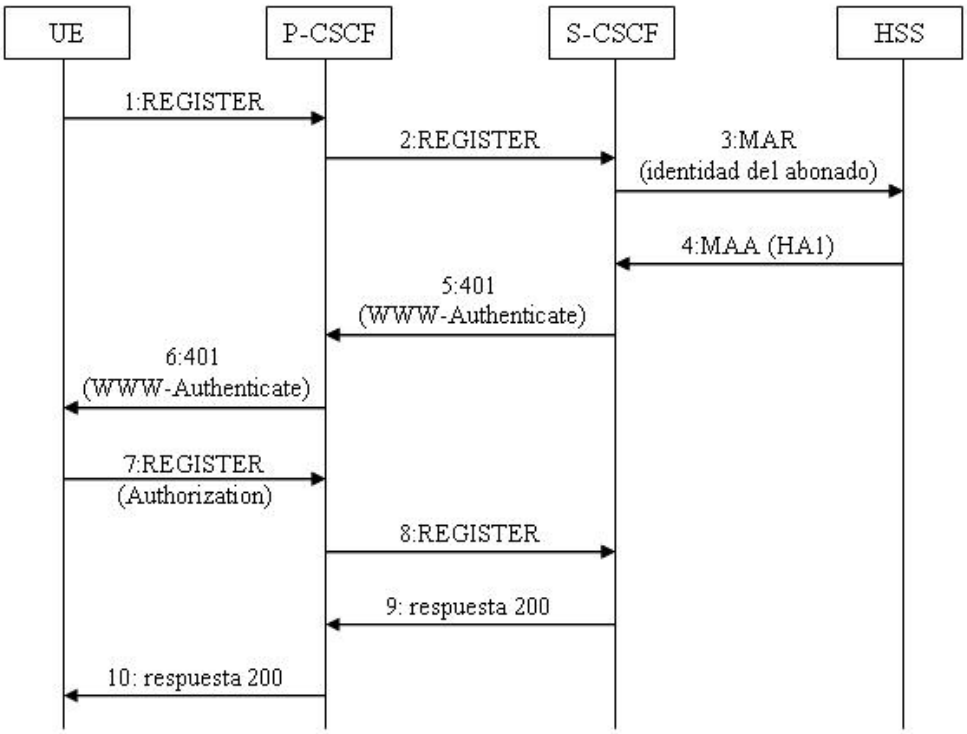
UE
P-CSCF
S-CSCF
HSS
1:REGISTER
2:REGISTER
3:MAR
(identidad del abonado)
4:MAA (HA1)
5:401
(WWW-Authenticate)
6:401
(WWW-Authenticate)
7:REGISTER
(Authorization)
8:REGISTER
9: respuesta 200
10: respuesta 200

FIG.4A

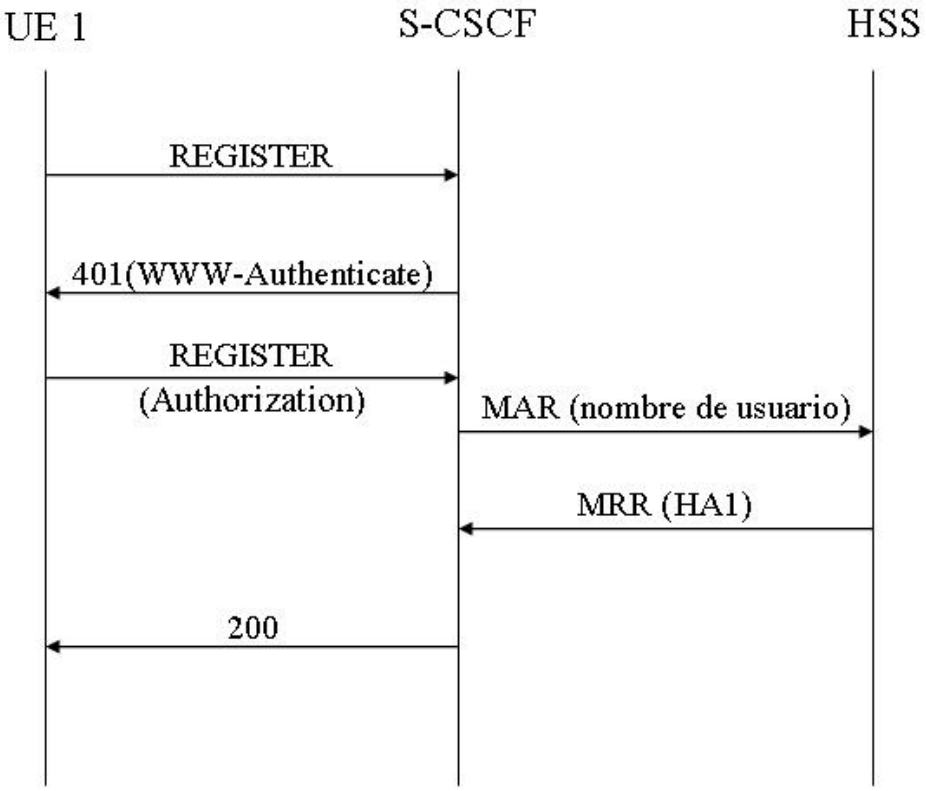
UE 1
S-CSCF
HSS
REGISTER
401(WWW-Authenticate)
REGISTER
(Authorization)
MAR (nombre de usuario)
MRR (HA1)
200

FIG.4B

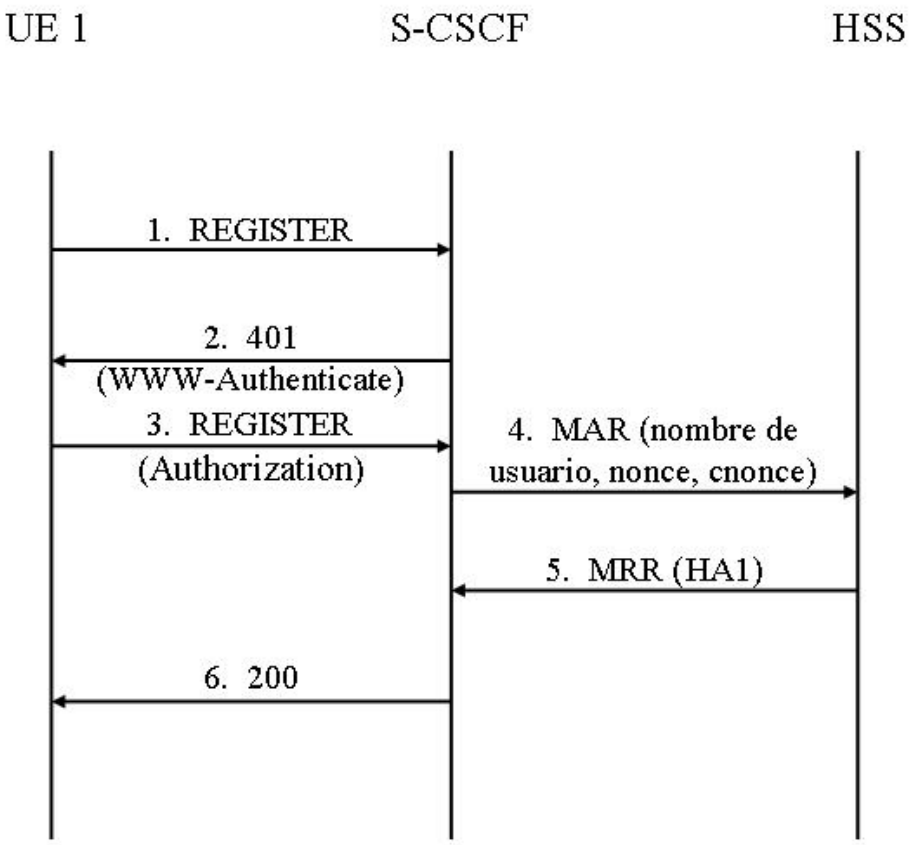
UE 1
S-CSCF
HSS
1. REGISTER
2. 401
(WWW-Authenticate)
3. REGISTER
(Authorization)
4. MAR (nombre de usuario, nonce, cnonce)
5. MRR (HA1)
6. 200

FIG.5

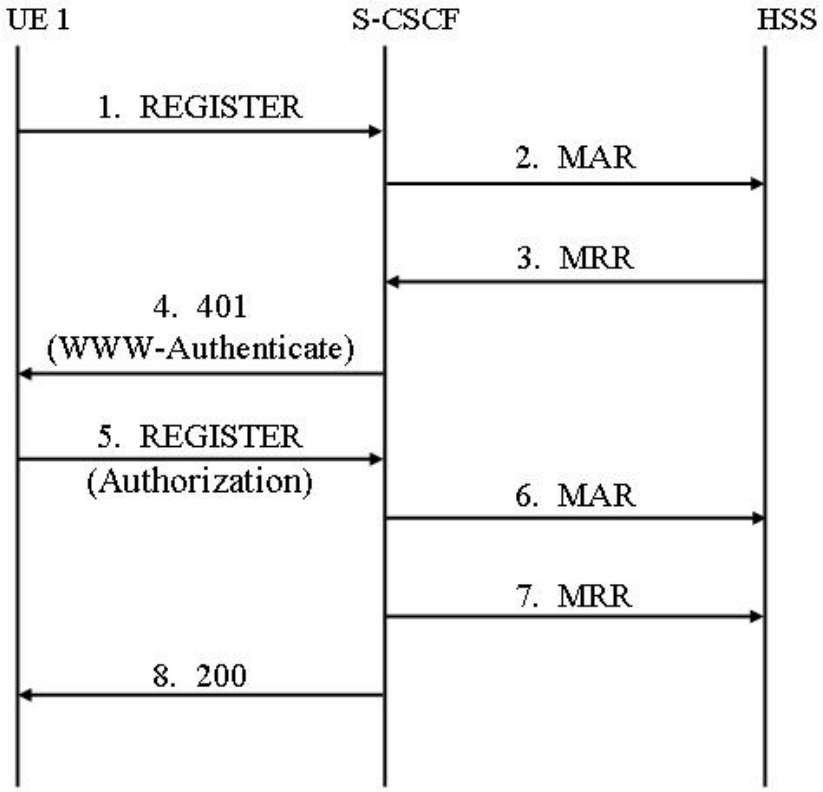
UE 1
S-CSCF
HSS
1. REGISTER
2. MAR
3. MRR
4. 401
(WWW-Authenticate)
5. REGISTER
(Authorization)
6. MAR
7. MRR
8. 200

FIG.6

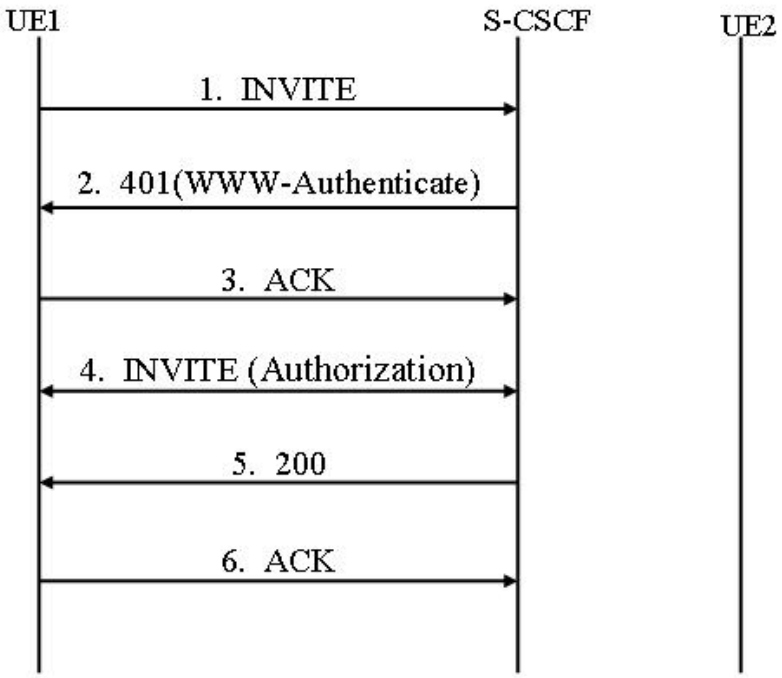
UE1
S-CSCF
UE2
1. INVITE
2. 401(WWW-Authenticate)
3. ACK
4. INVITE (Authorization)
5. 200
6. ACK

FIG.7