(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 379 964**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05729545 .3**
(96) Fecha de presentación: **01.04.2005**
(97) Número de publicación de la solicitud: **1864522**
(97) Fecha de publicación de la solicitud: **12.12.2007**

(54) Título: **Método para inciar comunicaciones basadas en IMSI**

(45) Fecha de publicación de la mención BOPI:
07.05.2012

(45) Fecha de la publicación del folleto de la patente:
07.05.2012

(73) Titular/es:
TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)
PATENT UNIT
164 83 STOCKHOLM, SE

(72) Inventor/es:
TERRILL, Stephen y
PRZYBYSZ, Hubert

(74) Agente/Representante:
de Elzaburu Márquez, Alberto

DESCRIPCIÓN

Método para iniciar comunicaciones basadas en el IMSI

Campo de la invención

La presente invención se refiere a un método y un aparato para iniciar comunicaciones basadas en el Subsistema Multimedia IP (IMS) y, en particular, para iniciar comunicaciones para usuarios que no están registrados en el IMS.

Antecedentes de la invención

Los servicios Multimedia IP (IPMM) proporcionan una combinación dinámica de voz, vídeo, mensajería, datos, etcétera, dentro de la misma sesión. Con el aumento del número de aplicaciones básicas y los medios que es posible combinar, aumentará el número de servicios ofrecidos a los usuarios finales, y se enriquecerá la experiencia de la comunicación interpersonal. Esto conducirá a una nueva generación de servicios de comunicación multimedia enriquecidos, personalizados, incluyendo los servicios denominados “Multimedia IP combinatorios” que se consideran de forma más detallada posteriormente.

El Subsistema Multimedia IP (IMS) es la tecnología definida por el Proyecto de Asociación de Tercera Generación (3GPP) para proporcionar servicios Multimedia IP a través de redes de comunicaciones móviles (3GPP TS 22.228, TS 23.228, TS 24.229, TS 29.228, TS 29.229, TS 29.328 y TS 29.329 Versión 5 y Versión 6). El IMS proporciona características clave para enriquecer la experiencia de comunicación de persona-a-persona de los usuarios finales, a través de la integración y la interacción de servicios. El IMS permite nuevas comunicaciones enriquecidas de persona-a-persona (cliente-a-cliente) así como de persona-a-contenido (cliente-a-servidor) a través de una red basada en el IP. El IMS hace uso del Protocolo de Inicio de Sesión (SIP) para establecer y controlar llamadas o sesiones entre terminales de usuario (o terminales de usuario y servidores de aplicaciones). El Protocolo de Descripción de Sesión (SDP), transportado mediante señalización SIP, se usa para describir y negociar los componentes de los medios de la sesión. Aunque el SIP se creó como un protocolo de usuario-a-usuario, el IMS permite que los operadores y los proveedores de servicios controlen el acceso de los usuarios a servicios y que cobren, de forma correspondiente, a los usuarios.

La Figura 1 ilustra esquemáticamente cómo encaja el IMS en la arquitectura de una red móvil en el caso de una red de acceso GPRS/PS. Las Funciones de Control de Llamadas/Sesiones (CSCFs) funcionan como proxies SIP con el IMS. La arquitectura del 3GPP define tres tipos de CSCFs: el CSCF Proxy (P-CSCF), que es el primer punto de contacto dentro del IMS para un terminal SIP; la CSCF de Servicio (S-CSCF), que proporciona al usuario servicios a los que está abonado dicho usuario; y la CSCF de Interrogación (I-CSCF) cuyo papel es identificar la S-CSCF correcta y reenviar a esta S-CSCF una solicitud recibida desde un terminal SIP a través de una P-CSCF.

Un usuario se registra en el IMS usando el método especificado SIP REGISTER. Este es un mecanismo para incorporarse al IMS y para anunciar al IMS la dirección en la que se puede contactar con una identidad de usuario SIP. En el 3GPP, cuando un terminal SIP lleva a cabo un registro, el IMS autentica al usuario, y asigna a ese usuario una S-CSCF de entre el conjunto de S-CSCFs disponibles. Aunque los criterios para asignar S-CSCFs no están especificados por el 3GPP, los mismos pueden incluir requisitos de compartición de carga y servicios. Se observa que la asignación de una S-CSCF es clave para controlar (y cobrar por) el acceso de los usuarios a servicios basados en el IMS. Los operadores pueden proporcionar un mecanismo para evitar sesiones SIP directas de usuario-a-usuario que, de otro modo, eludirían la S-CSCF.

Durante el proceso de registro, es responsabilidad de la I-CSCF seleccionar una S-CSCF si es que no se ha seleccionado ya una S-CSCF. La I-CSCF recibe las capacidades requeridas S-CSCF desde el Servidor de Abonados Domésticos (HSS) de la red doméstica, y selecciona una S-CSCF apropiada sobre la base de las capacidades recibidas. [Se observa que la asignación de la S-CSCF es llevada también para un usuario por la I-CSCF en el caso de que al usuario le llame otro participante, y el usuario no tenga asignada en ese momento una S-CSCF]. Cuando posteriormente un usuario registrado envía una solicitud de sesión al IMS, la P-CSCF puede reenviar la solicitud a la S-CSCF seleccionada, sobre la base de información recibida desde la S-CSCF durante el proceso de registro.

Dentro de la red de servicio IMS, se proporcionan servidores de aplicaciones (ASs) para implementar una funcionalidad de servicio IMS. Aunque originalmente se concibió que los ASs funcionaran como “esclavos” con respecto a las CSCFs IMS, respondiendo a solicitudes delegadas por las S-CSCFs, esto no es necesario que sea así y, de hecho, en la actualidad se espera que los ASs puedan tener interfaces con redes externas (es decir, no del 3GPP), y que puedan recibir un estímulo interno para realizar una acción (por ejemplo, la expiración de un temporizador). La Figura 2 ilustra la interfaz de Control de Servicio IMS (ISC) entre un AS y una S-CSCF, así como otras interfaces dentro del IMS. Aunque el AS en la Figura 2 se muestra de manera que tiene solamente una única interfaz con una S-CSCF, se apreciará que, en la práctica, la interfaz de ISC discurrirá a través de una red de comunicaciones a la cual están conectados muchos (o la totalidad) de los servidores de CSCF de la red de un operador dado, permitiendo que un AS se comunique con todas estas CSCFs. [Otras entidades ilustradas en la Figura 1 serán bien conocidas para aquellos expertos en la materia].

Existe otra interfaz (Ut) entre el AS y el terminal de usuario (TS23.002) aunque la misma no se muestra en la Figura. La interfaz Ut permite que el usuario gestione información relacionada con sus servicios, por ejemplo, la creación y asignación de Identidades de Servicios Públicos, gestión de políticas de autorización que son usadas, por ejemplo, por servicios de "presencia", gestión de políticas de conferencias, etcétera.

La arquitectura IMS actual permite que un AS inicie una sesión IMS en respuesta a la recepción, por parte del AS, de una solicitud apropiada a través de una interfaz externa. Se podría concebir, por ejemplo, el envío de una solicitud de sesión IMS hacia el AS a través de una interfaz HTTP, donde un usuario da inicio al envío de una solicitud accediendo a una página web en Internet. En este caso, al producirse la recepción de la solicitud de sesión, el AS en primer lugar contactará con un Servidor de Abonados Domésticos (HSS) del usuario iniciador para determinar si el usuario ya está registrado o no en el IMS. El AS envía al HSS una identidad SIP generada para el usuario y que puede ser usada por el HSS para determinar si el usuario está o no registrado. En caso afirmativo, el HSS enviará al AS la identidad de la S-CSCF ya asignada al usuario. A continuación, el AS reenviará un SIP INVITE a la S-CSCF identificada, y el procedimiento de establecimiento de sesión continuará tal como se ilustra en la Figura 3. Un escenario ejemplificativo en el que podría surgir esta situación es el caso en el que un abonado móvil 3GPP está registrado en el IMS, y el abonado a continuación entra en una página web, a través de un PC doméstico, y solicita una sesión IMS a través de ese canal.

Si se da el caso de que el usuario no está registrado todavía en el IMS, y el HSS comunica esto al AS, la solicitud no se puede procesar. La TS.228 establece específicamente que "*Si el AS no pudiera adquirir una dirección de S-CSCF para la Identidad de Usuario Público, el AS no iniciará una sesión en nombre del usuario*".

Se apreciará que surge un problema similar cuando el estímulo para establecer una sesión IMS se genera internamente, dentro del AS. Por ejemplo, se puede concebir un escenario en el que se haya solicitado al AS que realice una actualización del estado de un usuario en un servidor de presencia en un tiempo solicitado. Como en el caso de un servicio que se origina externamente, las normas actuales permitirán que el AS inicie la sesión IMS requerida únicamente si el usuario en cuestión está registrado en el IMS.

Aunque la argumentación anterior se refiere a un usuario que se supone que es un usuario que posee una identidad de usuario público, el usuario puede ser una aplicación, es decir, que posea una identidad de servicio público.

Sumario de la invención

Se reconoce que los usuarios claramente pueden desear acceder a servicios IMS incluso cuando no estén registrados todavía en el IMS, y, en particular, cuando los medios que están usando para iniciar la solicitud de comunicación IMS no facilitan el registro IMS.

Según un primer aspecto de la presente invención, se proporciona un método de inicio de una comunicación del Subsistema Multimedia IP para un usuario que no está registrado *a priori* en el Subsistema Multimedia IP, comprendiendo el método:

recibir una solicitud de comunicación desde el usuario no registrado, en un Servidor de Aplicaciones del Protocolo de Inicio de Sesión a través de una interfaz con una red externa, o recibir un estímulo generado interna o externamente que requiere el establecimiento de una comunicación del Subsistema Multimedia IP;

asignar una Función de Control de Llamadas/Estados de Servicio al usuario no registrado;

enviar una solicitud de Protocolo de Inicio de Sesión desde el Servidor de Aplicaciones hacia la Función de Control de Llamadas/Estados de Servicio asignada; y

establecer la comunicación solicitada.

En una primera realización de la presente invención, la etapa de asignar una Función de Control de Llamadas/Estados de Servicio al usuario la lleva a cabo el Servidor de Aplicaciones. El Servidor de Aplicaciones obtiene capacidades de Función de Control de Llamadas/Estados de Servicio de un Servidor de Abonados Domésticos y asigna una Función de Control de Llamadas/Estados de Servicio basándose en estas capacidades. [El AS debe tener o poder obtener conocimiento de una S-CSCF disponible]. A continuación, el Servidor de Aplicaciones envía una solicitud de Protocolo de Inicio de Sesión a la Función de Control de Llamadas/Estados de Servicio asignada.

En una segunda realización de la presente invención, la etapa de asignar una Función de Control de Llamadas/Estados de Servicio al usuario la lleva a cabo una Función de Control de Llamadas/Estados de Interrogación. El Servidor de Aplicaciones envía una solicitud de Protocolo de Inicio de Sesión a la Función de Control de Llamadas/Estados de Interrogación, y, como respuesta, la Función de Control de Llamadas/Estados de Interrogación obtiene capacidades de Función de Control de Llamadas/Estados de Servicio de un Servidor de Abonados Domésticos y asigna una Función de Control de Llamadas/Estados de Servicio basándose en estas capacidades. A continuación, la Función de Control de Llamadas/Estados de Interrogación envía la solicitud de Protocolo de Inicio de Sesión a la Función de Control de Llamadas/Estados de Servicio asignada.

En una tercera realización de la invención, la etapa de asignar una Función de Control de Llamadas/Estados de Servicio al usuario la lleva a cabo una Función de Control de Llamadas/Estados de Servicio. El Servidor de Aplicaciones envía una solicitud de Protocolo de Inicio de Sesión a una Función de Control de Llamadas/Estados de Servicio, y, como respuesta, esa CSCF de Servicio obtiene capacidades de Función de Control de Llamadas/Estados de Servicio de un Servidor de Abonados Domésticos, y asigna una Función de Control de Llamadas/Estados de Servicio basándose en estas capacidades. A continuación, la Función de Control de Llamadas/Estados de Servicio envía una solicitud de Protocolo de Inicio de Sesión a la Función de Control de Llamadas/Estados de Servicio asignada en caso de que la Función de Control de Llamadas/Estados de Servicio no sea ella misma.

Se apreciará que el Servidor de Aplicaciones inicialmente puede no tener conocimiento de que el usuario no está registrado en el Subsistema Multimedia IP, y enviará una consulta al Servidor de Abonados Domésticos para determinar si el usuario está registrado o no. Con el fin de proporcionar una seguridad mejorada, la respuesta del Servidor de Abonados Domésticos informando al Servidor de Aplicaciones de que el usuario no está registrado puede venir acompañada por un “testigo” de seguridad. Este testigo de seguridad proporciona unos medios para autenticar el Servidor de Aplicaciones, y se incluye con la solicitud de Protocolo de Inicio de Sesión enviada por el Servidor de Aplicaciones. Una Función de Control de Llamadas/Estados de Servicio asignada puede autenticar la solicitud de Protocolo de Inicio de Sesión como originaria de un Servidor de Aplicaciones válido, por ejemplo, reenviando el testigo de seguridad al Servidor de Abonados Domésticos y confiando en que el Servidor de Abonados Domésticos devolverá capacidades de Función de Control de Llamadas/Estados de Servicio únicamente si el testigo es válido.

Se proporciona un método de funcionamiento de un Servidor de Aplicaciones para iniciar una comunicación del Subsistema Multimedia IP para un usuario que no está registrado *a priori* en el Subsistema Multimedia IP, comprendiendo el método:

recibir una solicitud de comunicación desde dicho usuario a través de una interfaz con una red externa, o recibir un estímulo generado interna o externamente que requiere el establecimiento de una comunicación del Subsistema Multimedia IP;

asignar una Función de Control de Llamadas/Estados de Servicio al usuario; y

reenviar una solicitud de Protocolo de Inicio de Sesión a la Función de Control de Llamadas/Estados de Servicio asignada.

Se proporciona un método de funcionamiento de una Función de Control de Llamadas/Estados de Interrogación con el fin de iniciar una comunicación del Subsistema Multimedia IP para un usuario que no está registrado *a priori* en el Subsistema Multimedia IP, comprendiendo el método:

recibir una solicitud de comunicación asociada a dicho usuario desde un Servidor de Aplicaciones;

asignar una Función de Control de Llamadas/Estados de Servicio al usuario; y

reenviar una solicitud de Protocolo de Inicio de Sesión a la Función de Control de Llamadas/Estados de Servicio.

Se proporciona un método de funcionamiento de una Función de Control de Llamadas/Estados de Servicio con el fin de iniciar una comunicación del Subsistema Multimedia IP para un usuario que no está registrado *a priori* en el Subsistema Multimedia IP, comprendiendo el método:

recibir una solicitud de comunicación asociada a dicho usuario desde un Servidor de Aplicaciones;

asignar una Función de Control de Llamadas/Estados de Servicio al usuario; y

si la Función de Control de Llamadas/Estados de Servicio asignada es una Función de Control de Llamadas/Estados de Servicio diferente a ella misma, reenviar una solicitud de Protocolo de Inicio de Sesión a la Función de Control de Llamadas/Estados de Servicio asignada.

Según las normas pertinentes, la Función de Control de Llamadas/Estados de Servicio asignada recibe del Servidor de Abonados Domésticos un perfil específico del identificador de usuario. Este perfil debería incluir soporte para llamadas de origen sin registro.

Se proporciona un método de protección de señalización enviada entre un servidor de Función de Control de Llamadas/Estados de un Subsistema Multimedia IP y un Servidor de Aplicaciones del Protocolo de Inicio de Sesión, estando asociada la señalización al establecimiento de una comunicación para un usuario, comprendiendo el método:

enviar un testigo de seguridad desde un Servidor de Abonados Domésticos del usuario al servidor de Función de Control de Llamadas/Estados o Servidor de Aplicaciones del Protocolo de Inicio de Sesión;

enviar el testigo de seguridad recibido, desde el servidor de Función de Control de Llamadas/Estados o el Servidor de Aplicaciones del Protocolo de Inicio de Sesión al otro de entre el Servidor de Aplicaciones del Protocolo de Inicio de Sesión o la Función de Control de Llamadas/Estados; y

en el servidor de Función de Control de Llamadas/Estados o Servidor de Aplicaciones del Protocolo de Inicio de Sesión de recepción, verificar la autenticidad del testigo de seguridad comunicándose con el Servidor de Abonados Domésticos.

El término "comunicación" tal como se usa en el presente documento abarca tanto procedimientos de establecimiento de sesión como procedimientos que no sean de establecimiento de sesión incluyendo, por ejemplo, simples intercambios de mensajes SIP.

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente la integración de un Subsistema Multimedia IP en un sistema de comunicaciones de móviles 3G;

la Figura 2 ilustra esquemáticamente ciertas entidades del Subsistema Multimedia IP, incluyendo un Servidor de Aplicaciones y una Función de Control de Llamadas/Estados de Servicio;

la Figura 3 es un diagrama de señalización que ilustra señalización asociada al inicio de una sesión del Subsistema Multimedia IP por un Servidor de Aplicaciones;

la Figura 4 es un diagrama de señalización que ilustra señalización asociada al inicio de una sesión del Subsistema Multimedia IP por un Servidor de Aplicaciones según una primera realización de la invención;

la Figura 5 es un diagrama de señalización que ilustra señalización asociada al inicio de una sesión del Subsistema Multimedia IP por un Servidor de Aplicaciones de acuerdo con una segunda realización de la invención; y

la Figura 6 es un diagrama de señalización que ilustra señalización asociada al inicio de una sesión del Subsistema Multimedia IP por un Servidor de Aplicaciones según una tercera realización de la invención.

Descripción detallada de ciertas realizaciones

El problema que afronta la presente invención es que, según el estado de la técnica, un Servidor de Aplicaciones (AS) del Protocolo de Inicio de Sesión (SIP) no puede iniciar una solicitud SIP en nombre de un usuario no registrado dentro del Subsistema Multimedia IP (IMS), y al mismo tiempo seguir permitiendo la introducción de una Función de Control de Llamadas/Estados de Servicio en la vía de señalización con el fin de proporcionar un análisis de servicios de origen. No obstante, esto puede resultar necesario en el caso de que el AS esté utilizando otro protocolo (no SIP) para comunicarse con el usuario (por ejemplo, HTTP, SMS, MMS, u otro protocolo multimedia [o surge un estímulo interno dentro del AS, por ejemplo, en relación con la actualización el estado de presencia en un tiempo especificado], y el usuario requiere que el AS inicie una solicitud SIP en su nombre.

El concepto básico utilizado en el presente documento es asignar una Función de Control de Llamadas/Estados de Servicio (S-CSCF) cuando el AS determina que todavía no se ha asignado una S-CSCF al usuario (por ejemplo, el usuario no está registrado en el IMS). Una vez que se ha asignado una S-CSCF, la S-CSCF informa al Servidor de Abonados Domésticos (HSS) de que en este momento está asignada como CSCF de Servicio aunque manteniendo el estado no registrado del usuario, y la S-CSCF descarga el perfil del usuario. La solicitud de sesión del AS entregada al IMS se trata como una solicitud en origen. A continuación se considerarán tres realizaciones alternativas, partiendo del punto en el que el AS ha recibido una solicitud de inicio de sesión IMS a través de una interfaz no SIP. [Otras posibilidades para iniciar el proceso incluyen la generación de un estímulo interno dentro del AS, por ejemplo, como consecuencia de la "programación" del AS, por parte del usuario, a través de la interfaz Ut, y la recepción de un estímulo externo desde una fuente que no sea el usuario].

Asignación de S-CSCF realizada por Servidor de Aplicaciones

En la Figura 4 se ilustra el flujo de señalización asociado a esta primera realización, donde las etapas del proceso son las siguientes:

1. El AS intenta recuperar la dirección de la S-CSCF para el usuario mediante entrada en contacto con el Servidor de Abonados Domésticos (HSS) a través de la interfaz Sh (Figura 1), enviando una identidad SIP del usuario, generada en nombre del usuario, al HSS. El AS determina que el usuario no está registrado y que no se ha asignado ninguna S-CSCF al usuario.

2. El AS solicita del HSS las capacidades de S-CSCF requeridas.

3. El HSS devuelve las capacidades de S-CSCF requeridas al AS a través de la interfaz Sh. Esta funcionalidad es nueva, ya que en la actualidad las capacidades de S-CSCF únicamente se pueden transferir a través de la interfaz Cx.

4. El AS realiza la selección de la S-CSCF según ciertos criterios predefinidos, cuyos detalles no son relevantes en el presente documento. (En la actualidad esta funcionalidad reside en la I-CSCF).

5. El AS genera una solicitud SIP (por ejemplo, una SIP INVITE), incluyendo una identidad de usuario (por ejemplo, sip:nombreusuario@operador.com). La solicitud SIP es enviada a la S-CSCF seleccionada, a través de la interfaz ISC. [La dirección IP del AS se identifica para la S-CSCF en el encabezamiento IP].

6. La S-CSCF recupera del HSS el perfil de usuario e informa al HSS que esta es ahora la S-CSCF asignada al usuario, aunque manteniendo el estado no registrado del usuario en el HSS. La S-CSCF registra el establecimiento de correspondencia entre la identidad SIP asignada y la dirección IP del AS.

7. El HSS devuelve el perfil de usuario a la S-CSCF. En este momento, el perfil de abonado puede incluir información de perfil de servicio no registrado de origen, así como información de perfil de servicio registrado de origen, registrado de destino, y no registrado de destino.

8. La S-CSCF realiza cualquier control de servicio sobre la base del perfil de usuario recibido (por ejemplo, enlazando con otro AS), y registra el establecimiento de correspondencia entre la identidad SIP asignada y la dirección IP del AS. El control del servicio puede conllevar, por ejemplo, la utilización de filtros de cribado para controlar el acceso de los usuarios a servicios IMS.

9. La solicitud SIP se reenvía al destino apropiado.

10. Se recibe una respuesta SIP del destino.

11. La respuesta SIP se reenvía al AS. Este establece la sesión SIP.

Asignación de S-CSCF realizada por la I-CSCF

En la Figura 5 se ilustra el flujo de señalización asociado a esta segunda realización, donde las etapas del proceso son las siguientes:

1. El AS intenta recuperar del HSS la dirección del S-CSCF para el usuario. El AS determina que el usuario no está registrado y que no se ha asignado ninguna S-CSCF al usuario, tal como se ha descrito anteriormente.

2. El AS solicita un testigo de seguridad del HSS. Esto es necesario para que la S-CSCF asignada (véase más abajo) confirme que la solicitud es válida. Sin este mecanismo de seguridad, existe un riesgo de que otra entidad SIP (por ejemplo, un usuario SIP registrado) pueda enviar una solicitud de inicio de sesión falsa a una S-CSCF, y de que la S-CSCF no pueda distinguir esta solicitud falsa de una solicitud válida enviada a ella misma por un AS. Aunque en la solicitud se incluya algún identificador para identificar la solicitud como originada en un AS, esta es una identidad que puede ser copiada y, por lo tanto, puede plantear una amenaza de seguridad.

3. El HSS responde al AS con un testigo de seguridad. El HSS debería autenticar el AS y debería autorizar al AS a actuar en nombre del usuario antes de generar el testigo de seguridad.

4. El AS envía una solicitud SIP, que incluye el testigo de seguridad (y la identidad de usuario y la dirección IP del AS), a una I-CSCF designada.

5. La I-CSCF ejecuta un intercambio *Cx-query* y *Cx-select-pull* con el HSS para obtener las capacidades de S-CSCF requeridas.

6. El HSS responde a la *Cx-query* y *Cx-select-pull*, proporcionando las capacidades de S-CSCF requeridas.

7. La I-CSCF realiza una selección de S-CSCF usando los criterios predefinidos.

8. La solicitud SIP se reenvía desde la I-CSCF a la S-CSCF seleccionada, nuevamente con el testigo de seguridad. La I-CSCF no debería Registrar la Ruta (*Record Rute*) de esta solicitud ya que no es necesario que permanezca en la vía de señalización SIP después del establecimiento de la sesión.

9. La S-CSCF recupera el perfil de usuario del HSS e informa al HSS de que ahora es la S-CSCF del usuario aunque manteniendo el estado no registrado del usuario. El testigo de seguridad se incluye en las solicitudes *Cx-put/Cx-pull*. Si el HSS confirma la validez del testigo, entonces la S-CSCF sabe que la solicitud SIP proviene de un AS válido. Nuevamente, este perfil puede incluir información de perfil sin registro de origen.

10. El HSS devuelve el perfil de usuario a la S-CSCF (suponiendo que el testigo es válido).

11. La S-CSCF ejecuta cualquier control de servicio requerido sobre la base del perfil de uso recibido.

12. La solicitud SIP se reenvía al destino.

13. Se recibe una respuesta SIP desde el destino.

14. La respuesta SIP se reenvía a la I-SCSF.

15. La respuesta SIP se reenvía al AS.

[El SIP especifica que la respuesta SIP debe atravesar los mismos nodos atravesados por la solicitud SIP. Por tanto, la S-CSCF no envía la respuesta directamente al AS].

Asignación de S-CSCF realizada por la S-CSCF

En la Figura 6 se ilustra el flujo de señalización asociado a esta tercera realización, en donde las etapas del proceso son las siguientes:

1. El AS intenta recuperar la dirección de la S-CSCF para el usuario. El AS determina que el usuario no está registrado y que no se ha asignado ninguna S-CSCF al usuario.

2. El AS solicita del HSS un testigo de seguridad. Esto es necesario para que la S-CSCF (véase más abajo) verifique que la solicitud proviene de un AS válido.

3. El HSS responde con un testigo de seguridad. El HSS debería autenticar el AS y debería autorizar al AS a actuar en nombre del usuario antes de generar el testigo de seguridad.

4. El AS envía la solicitud SIP, que incluye el testigo de seguridad, a una S-CSCF adecuada, por ejemplo, el AS puede realizar una conjetura fundamentada sobre la S-CSCF más probable basándose en datos históricos correspondientes al usuario en cuestión.

5. La S-CSCF ejecuta un intercambio de *Cx-query* y *Cx-select-pull* con el HSS para obtener las capacidades de S-CSCF requeridas.

6. El HSS responde a la *Cx-query* y *Cx-select-pull*, proporcionando las capacidades de S-CSCF requeridas a la S-CSCF. Esta es una funcionalidad nueva, ya que previamente las capacidades de S-CSCF requeridas se incluían solamente en los procedimientos Cx para la I-CSCF.

7. La S-CSCF realiza una selección de S-CSCF. Se puede seleccionar a sí misma en el caso de que disponga de las capacidades de S-CSCF requeridas.

8. La solicitud SIP se reenvía desde la S-CSCF asignadora a la S-CSCF asignada junto con el testigo de seguridad. [La S-CSCF seleccionadora no debería registrar la ruta (*record route*) de la solicitud].

9. La S-CSCF asignada recupera el perfil de usuario a partir del HSS e informa al HSS de que ahora es ella la S-CSCF para el usuario aunque manteniendo el estado no registrado del usuario. El testigo de seguridad se incluye en las solicitudes *Cx-put/Cx-pull*. Si el HSS valida el testigo para ese usuario, entonces la S-CSCF sabe que la solicitud SIP proviene de un AS válido.

10. El HSS devuelve el perfil de usuario a la S-CSCF asignada, suponiendo que el testigo es válido. Nuevamente, este perfil incluye información de perfil sin registro de origen.

11. La S-CSCF ejecuta cualquier control de servicio requerido basándose en el perfil de usuario recibido.

12. La solicitud SIP se reenvía al destino apropiado.

13. Se recibe una respuesta SIP desde el destino.

14. La respuesta SIP se reenvía a la primera S-CSCF.

15. La respuesta SIP se reenvía al AS.

Aunque los procedimientos antes detallados se refieren a un AS que inicia una sesión SIP con un usuario asociado a un Identificador de Usuario Público (PUI), los mismos son también aplicables a un AS que inicia una sesión SIP con un “usuario” asociado a un Identificador de Servicio Público (PSI). El PSI se describe en la 3GPP TS 23.228.

Los expertos en la materia apreciarán que en las realizaciones antes descritas se pueden realizar varias modificaciones sin desviarse con respecto al alcance de la presente invención. En una modificación ejemplificativa, el mecanismo de testigo de seguridad antes descrito en referencia a la segunda y la tercera realizaciones también se puede utilizar con la primera realización con el fin de permitir que el HSS (en nombre de la S-CSCF asignada) valide el AS desde el cual se ha recibido una solicitud SIP.

Los expertos en la materia apreciarán además que el uso de un testigo de seguridad emitido por el HSS se puede utilizar para proteger comunicaciones relacionadas con el IMS que no sean las correspondientes relacionadas con el

suministro de servicios IMS a usuarios no registrados. Por ejemplo, un testigo de seguridad emitido por el HSS se puede usar en general para proporcionar unos medios mejores de seguridad para la señalización enviada desde la S-CSCF a un AS (es decir, para proteger toda la señalización ISC). En particular, cuando la S-CSCF recibe un perfil de usuario desde el HSS (es decir, en el registro SIP del usuario), la misma recibe también un testigo de seguridad. Al producirse la recepción de este testigo por el AS, el HS debe verificar que el testigo de seguridad es válido (comunicándose con el HSS a través de la interfaz Sh). Probablemente, el testigo de seguridad tendrá un tiempo de vida limitado.

REIVINDICACIONES

1. Método de inicio de una comunicación del Subsistema Multimedia IP para un usuario que no está registrado *a priori* en el Subsistema Multimedia IP, comprendiendo el método:

recibir una solicitud de comunicación desde el usuario no registrado, en un Servidor de Aplicaciones del Protocolo de Inicio de Sesión a través de una interfaz con una red externa, o recibir un estímulo generado interna o externamente que requiere el establecimiento de una comunicación del Subsistema Multimedia IP;

asignar una Función de Control de Llamadas/Estados de Servicio al usuario no registrado;

enviar una solicitud de Protocolo de Inicio de Sesión desde el Servidor de Aplicaciones hacia la Función de Control de Llamadas/Estados de Servicio asignada; y

establecer la comunicación solicitada.

2. Método según la reivindicación 1, en el que dicha etapa de asignar una Función de Control de Llamadas/Estados de Servicio al usuario no registrado la lleva a cabo el Servidor de Aplicaciones.

3. Método según la reivindicación 2, en el que el Servidor de Aplicaciones obtiene capacidades de Función de Control de Llamadas/Estados de Servicio de un Servidor de Abonados Domésticos y asigna una Función de Control de Llamadas/Estados de Servicio basándose en estas capacidades, y a continuación, envía una solicitud de Protocolo de Inicio de Sesión a la CSCF de Servicio asignada.

4. Método según la reivindicación 1, en el que dicha etapa de asignar una Función de Control de Llamadas/Estados de Servicio al usuario no registrado la lleva a cabo una CSCF de Interrogación al producirse la recepción de una solicitud de Protocolo de Inicio de Sesión desde el Servidor de Aplicaciones.

5. Método según la reivindicación 4, en el que el Servidor de Aplicaciones envía la solicitud SIP a la CSCF de Interrogación, y, como respuesta, la CSCF de Interrogación obtiene capacidades de Función de Control de Llamadas/Estados de Servicio de un Servidor de Abonados Domésticos y asigna una Función de Control de Llamadas/Estados de Servicio basándose en estas capacidades, enviando a continuación, la CSCF de Interrogación, la solicitud de Protocolo de Inicio de Sesión a la CSCF de Servicio asignada.

6. Método según la reivindicación 1, en el que dicha etapa de asignar una Función de Control de Llamadas/Estados de Servicio al usuario no registrado la lleva a cabo una CSCF de Servicio.

7. Método según la reivindicación 6, en el que el Servidor de Aplicaciones envía la solicitud de Protocolo de Inicio de Sesión a una CSCF de Servicio, y, como respuesta, esa CSCF de Servicio obtiene capacidades de Función de Control de Llamadas/Estados de Servicio de un Servidor de Abonados Domésticos, y asigna una Función de Control de Llamadas/Estados de Servicio basándose en estas capacidades, enviando a continuación, la CSCF de Servicio, la solicitud de Protocolo de Inicio de Sesión a la CSCF de Servicio asignada en caso de que la CSCF de Servicio no sea ella misma.

8. Método según una cualquiera de las reivindicaciones anteriores, y que comprende enviar desde el Servidor de Abonados Domésticos al Servidor de Aplicaciones un testigo de seguridad, y enviar este testigo de seguridad desde el Servidor de aplicaciones junto con dicha solicitud de Protocolo de Inicio de Sesión como medios de validación de la solicitud.

9. Método según la reivindicación 8, y que comprende, al producirse la recepción de dicha solicitud en la Función de Control de Llamadas/Estados de Servicio asignada, reenviar dicho testigo de seguridad al Servidor de Abonados Domésticos, validando, el Servidor de Abonados Domésticos, el testigo en nombre de la Función de Control de Llamadas/Estados de Servicio.

10. Método según una cualquiera de las reivindicaciones anteriores, y que comprende transferir un perfil de servicio para el usuario no registrado desde el Servidor de Abonados Domésticos a la Función de Control de Llamadas/Estados de Servicio asignada, incluyendo este perfil de servicio información de perfil para solicitudes sin registro de origen.

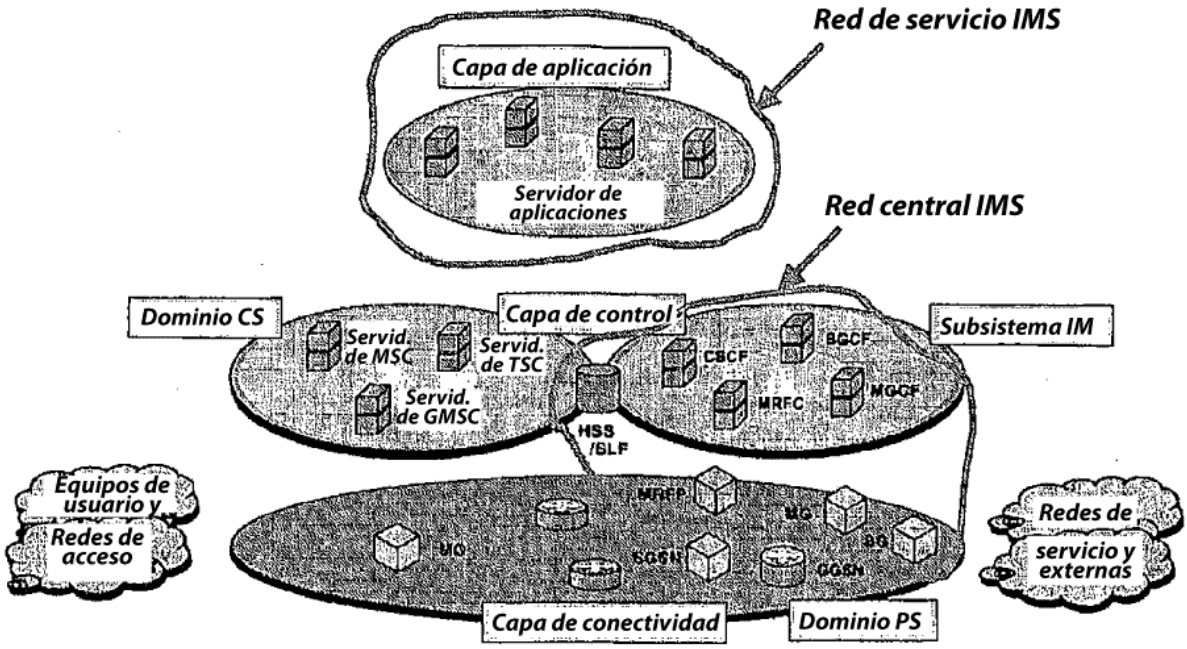

Figura 1

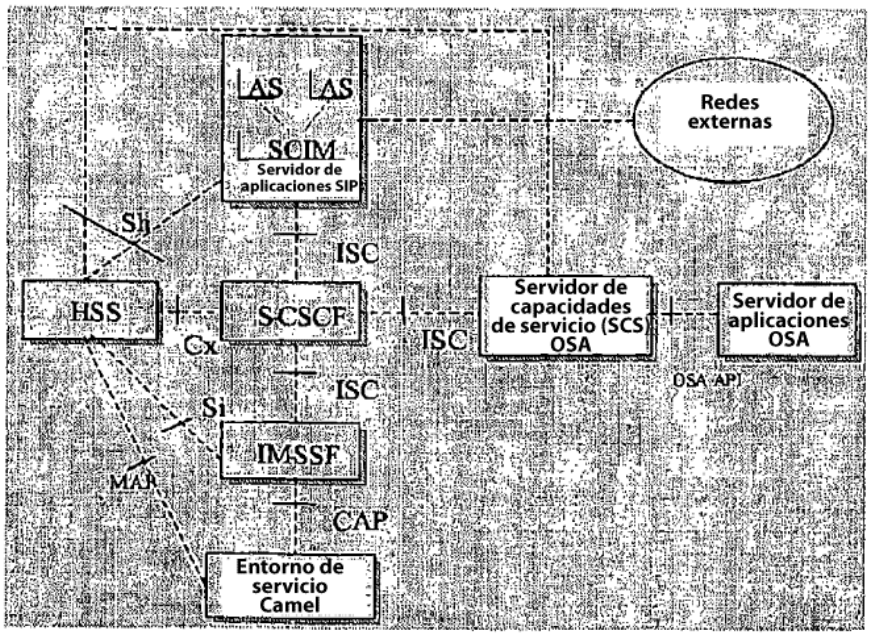

Figura 2

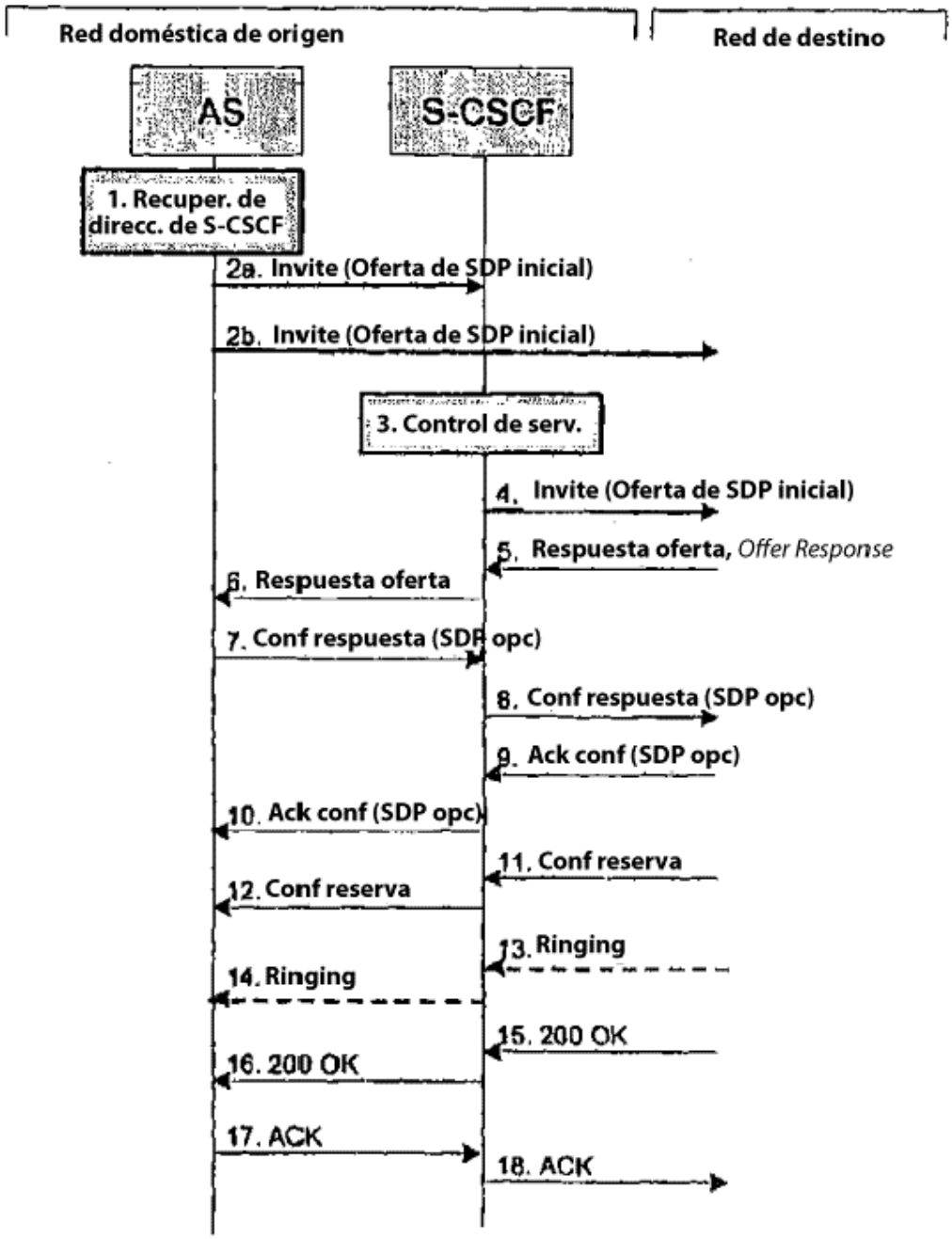
Red doméstica de origen
Red de destino
AS
S-CSCF
1. Recuper. de direcc. de S-CSCF
2a. Invite (Oferta de SDP inicial)
2b. Invite (Oferta de SDP inicial)
3. Control de serv.
4. Invite (Oferta de SDP inicial)
5. Respuesta oferta, Offer Response
6. Respuesta oferta
7. Conf respuesta (SDP opc)
8. Conf respuesta (SDP opc)
9. Ack conf (SDP opc)
10. Ack conf (SDP opc)
11. Conf reserva
12. Conf reserva
13. Ringing
14. Ringing
15. 200 OK
16. 200 OK
17. ACK
18. ACK

Figura 3

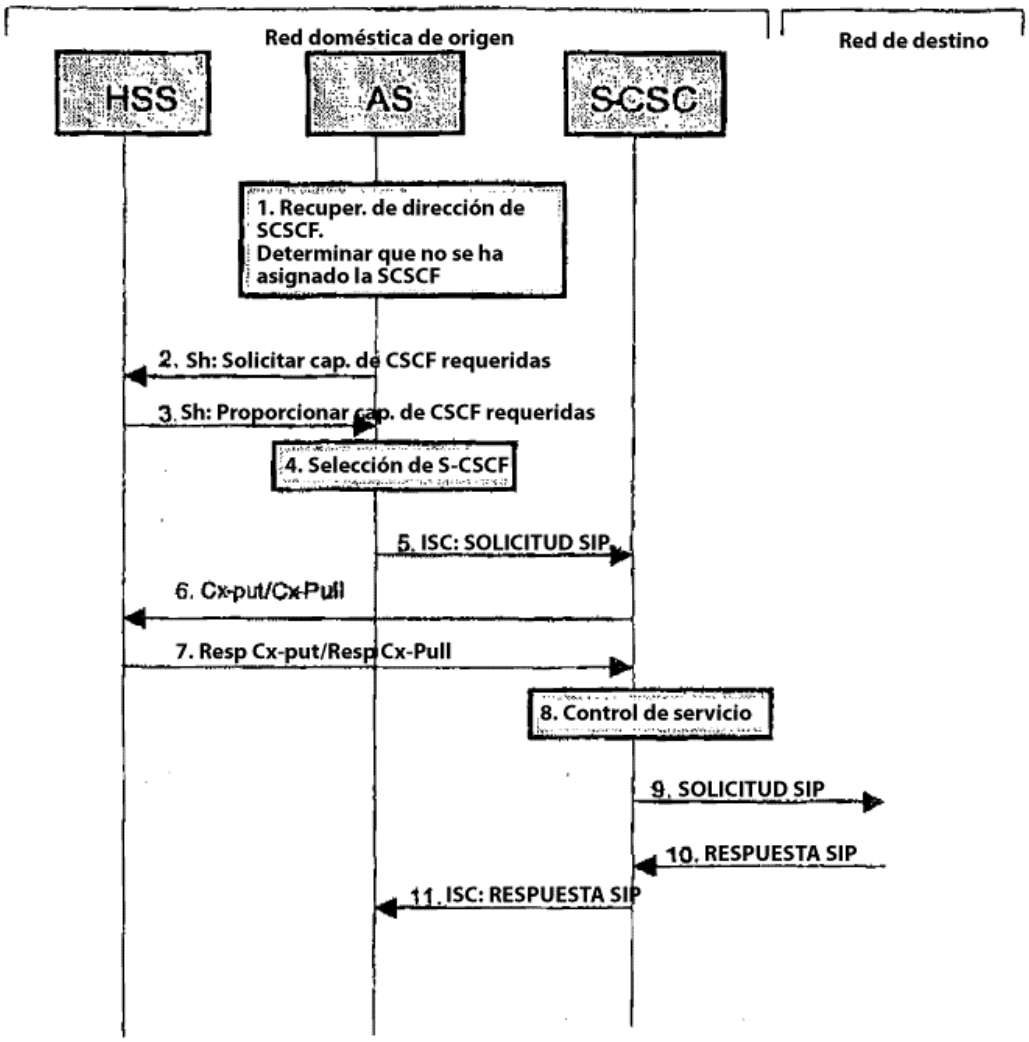
Red doméstica de origen
Red de destino
HSS
AS
S-CSC
1. Recuper. de dirección de SCSCF. Determinar que no se ha asignado la SCSCF
2. Sh: Solicitar cap. de CSCF requeridas
3. Sh: Proporcionar cap. de CSCF requeridas
4. Selección de S-CSCF
5. ISC: SOLICITUD SIP
6. Cx-put/Cx-Pull
7. Resp Cx-put/Resp Cx-Pull
8. Control de servicio
9. SOLICITUD SIP
10. RESPUESTA SIP
11. ISC: RESPUESTA SIP

Figura 4

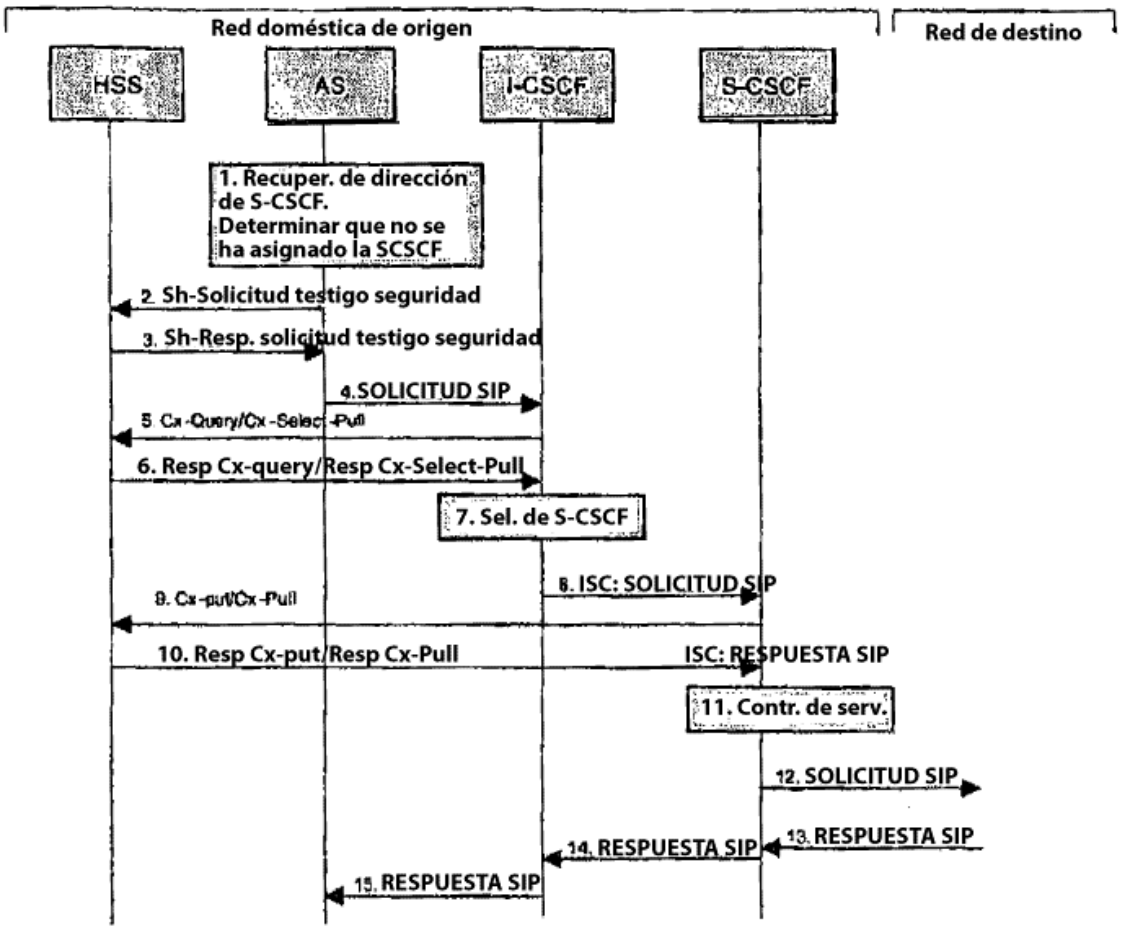
Red doméstica de origen
Red de destino
HSS
AS
I-CSCF
S-CSCF
1. Recuper. de dirección de S-CSCF. Determinar que no se ha asignado la SCSCF
2. Sh-Solicitud testigo seguridad
3. Sh-Resp. solicitud testigo seguridad
4.SOLICITUD SIP
5 Cx-Query/Cx-Select-Pull
6. Resp Cx-query/Resp Cx-Select-Pull
7. Sel. de S-CSCF
8. ISC: SOLICITUD SIP
9. Cx-put/Cx-Pull
10. Resp Cx-put/Resp Cx-Pull
ISC: RESPUESTA SIP
11. Contr. de serv.
12. SOLICITUD SIP
13. RESPUESTA SIP
14. RESPUESTA SIP
15. RESPUESTA SIP

Figura 5

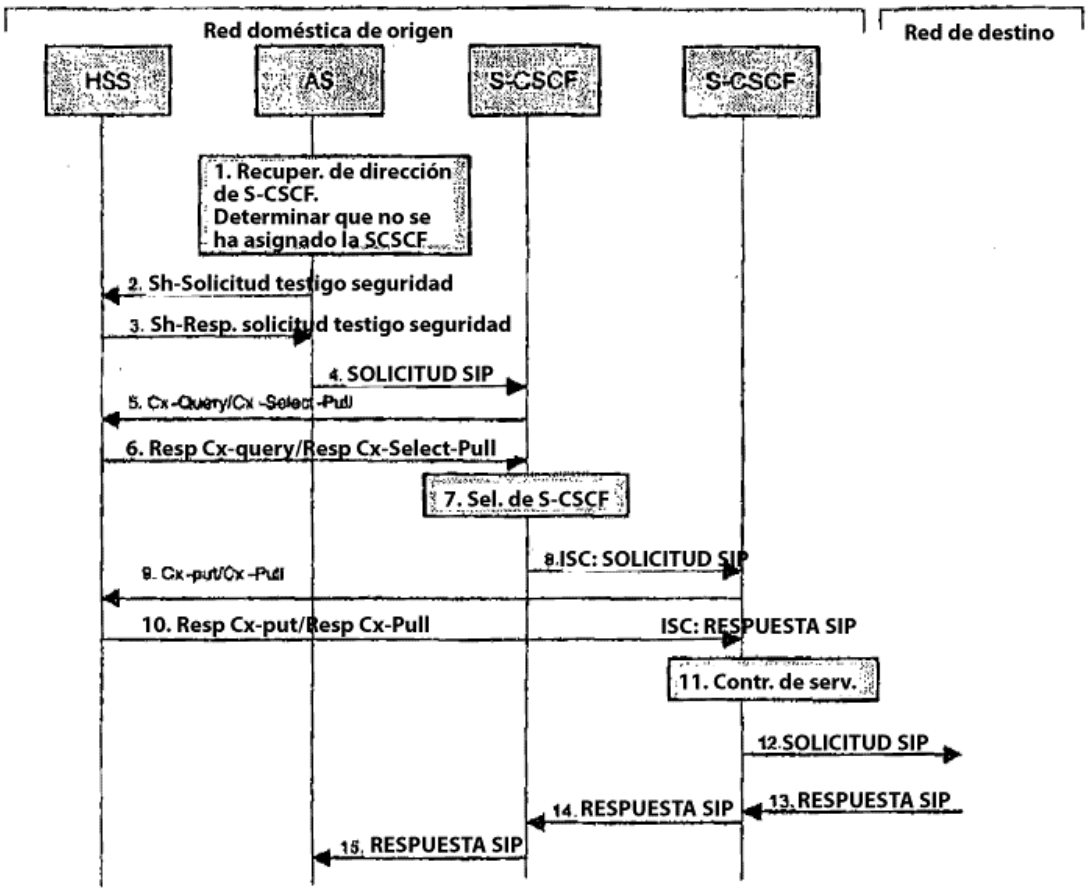
Red doméstica de origen
Red de destino
HSS
AS
S-CSCF
S-CSCF
1. Recuper. de dirección de S-CSCF. Determinar que no se ha asignado la SCSCF
2. Sh-Solicitud testigo seguridad
3. Sh-Resp. solicitud testigo seguridad
4. SOLICITUD SIP
5. Cx-Query/Cx-Select-Pull
6. Resp Cx-query/Resp Cx-Select-Pull
7. Sel. de S-CSCF
8.ISC: SOLICITUD SIP
9. Cx-put/Cx-Pull
10. Resp Cx-put/Resp Cx-Pull
ISC: RESPUESTA SIP
11. Contr. de serv.
12.SOLICITUD SIP
13.RESPUESTA SIP
14. RESPUESTA SIP
15. RESPUESTA SIP

Figura 6