(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 988**

(51) Int. CI.:
H04L 29/08 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08707868 .9**
(96) Fecha de presentación: **11.01.2008**
(97) Número de publicación de la solicitud: **2253121**
(97) Fecha de publicación de la solicitud: **24.11.2010**

(54) Título: **Gestión de mensajes en un subsistema multimedia IP**

(45) Fecha de publicación de la mención BOPI:
20.11.2012

(45) Fecha de la publicación del folleto de la patente:
20.11.2012

(73) Titular/es:
TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) (100.0%)
164 83 Stockholm , SE

(72) Inventor/es:
VAN ELBURG, JOHANNES

(74) Agente/Representante:
DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Gestión de mensajes en un subsistema multimedia IP.

CAMPO TÉCNICO

La presente invención se refiere a la gestión de mensajes del Protocolo de Inicio de Sesión en una red de comunicaciones.

ANTECEDENTES

El Subsistema Multimedia IP (IMS, en sus siglas en inglés) es la tecnología definida por el Proyecto de la Asociación de Tercera Generación (3GPP, en sus siglas en inglés) para proporcionar servicios multimedia IP a través de redes de comunicaciones móviles (3GPP TS 22.228). El IMS proporciona características clave para enriquecer la experiencia de la comunicación de persona a persona al usuario final a través de la integración e interacción de los servicios. El IMS permite nuevas comunicaciones mejoradas de persona a persona (de cliente a cliente), así como de persona a contenidos (de cliente a servidor) sobre una red basada en IP.

El IMS hace uso del Protocolo de Inicio de Sesión (SIP, en sus siglas en inglés) para establecer y controlar llamadas o sesiones entre terminales de usuario (UE, en sus siglas en inglés), o entre UE y servidores de aplicaciones (AS, en sus siglas en inglés). El Protocolo de Descripción de Sesión (SDP, en sus siglas en inglés), llevado por la señalización del SIP, se utiliza para describir y negociar los componentes de los medios de la sesión. Mientras el SIP fue creado como un protocolo de usuario a usuario, el IMS permite a los operadores y a los proveedores de servicios controlar el acceso de usuarios a los servicios y cobrar a los usuarios en consecuencia.

Dentro de una red del IMS, las Funciones de Control de Llamada / Sesión (CSCF, en sus siglas en inglés) operan como entidades del SIP dentro del IMS. La arquitectura del 3GPP define tres tipos de CSCF: la CSCF de Proximidad (P-CSCF, en sus siglas en inglés), que es el primer punto de contacto dentro del IMS para un terminal del SIP; la CSCF de Servicio (S-CSCF, en sus siglas en inglés), que presta al usuario servicios a los cuales está suscrito el usuario; y la CSCF de Interrogación (I-CSCF), cuya función es identificar la S-CSCF correcta y transmitir a la S-CSCF una solicitud recibida desde un terminal del SIP a través de una P-CSCF.

La funcionalidad de servicio del IMS es ejecutada en la práctica utilizando servidores de aplicaciones (AS, en sus siglas en inglés). Para cualquier UE dado, uno o más AS pueden estar asociados con ese terminal. Los AS comunican con una S-CSCF a través de la interfaz de Control de Servicio del IMS (ISC, en sus siglas en inglés) y se vinculan en una ruta de mensajería del SIP según se solicite (por ejemplo, como resultado de la activación de los iFC descargados en la S-CSCF para un UE determinado).

Un usuario se registra en el IMS utilizando el método del SIP REGISTER especificado. Este es un mecanismo para unirse al IMS y dar a conocer al IMS la dirección que da la ubicación a la que puede ser alcanzada una identidad de usuario del SIP. En 3GPP, cuando un terminal del SIP lleva a cabo un registro, el IMS autentifica al usuario utilizando información de suscripción almacenada en un Servidor Doméstico de Abonado (HSS, en sus siglas en inglés), y asigna una S-CSCF a ese usuario del conjunto de S-CSCF disponibles. Aunque los criterios para la asignación de la S-CSCF no están especificados por el 3GPP, estos pueden incluir el intercambio de carga y requisitos de servicio. Cabe señalar que la asignación de una S-CSCF es clave para controlar, y para cobrar, por el acceso del usuario a servicios basados en IMS. Los operadores pueden proporcionar un mecanismo para impedir sesiones del SIP directas de usuario a usuario que de otro modo evitarían la S-CSCF.

Durante el proceso de registro, es responsabilidad de la I-CSCF seleccionar una S-CSCF, si no se ha seleccionado ya una S-CSCF. La I-CSCF recibe las capacidades de S-CSCF requeridas desde el HSS, y selecciona una S-CSCF apropiada basada en las capacidades recibidas. Cabe señalar que la asignación de S-CSCF también es llevada para un usuario por la I-CSCF en el caso de que el usuario sea llamado por otra parte, y el usuario no esté asignado actualmente a una S-CSCF. Cuando un usuario registrado envía posteriormente una solicitud de sesión al IMS, la P-CSCF es capaz de enviar la solicitud a la S-CSCF seleccionada sobre la base de la información recibida desde la S-CSCF durante el proceso de registro.

Todos los usuarios del IMS poseen una o más Identidades Privadas de Usuario. Una Identidad Privada de Usuario es asignada por el operador de red doméstica y es utilizado por el IMS, por ejemplo para fines de registro, autorización, administración y contabilidad. Esta identidad toma la forma de un Identificador de Acceso a la Red (NAI, en sus siglas en inglés) tal como se define en el IETF RFC 2486. Es posible para una representación de la Identidad Internacional del Abonado Móvil (IMSI, en sus siglas en inglés) estar contenida dentro del NAI para la identidad privada. 3GPP TS 23.228 especifica las siguientes propiedades de la Identidad Privada del Usuario:

- La Identidad Privada del Usuario no se utiliza para el enrutamiento de mensajes del SIP.
- La Identidad Privada del Usuario está contenida en todas las solicitudes de Registro, (incluyendo las solicitudes de Repetición de registro y de Anulación de registro) pasadas desde el UE a la red doméstica.
- Una aplicación de Módulo de Identidad de Servicios multimedia IP (ISIM, en sus siglas en inglés) almacena

de forma segura una Identidad Privada de Usuario. No es posible que el UE modifique la información de la Identidad Privada de Usuario almacenada en la aplicación del ISIM.
- La Identidad Privada del Usuario es una identidad única global definida por el Operador de Red Doméstica, lo que puede ser utilizado dentro de la red doméstica para identificar la suscripción del usuario (por ejemplo, la capacidad de servicio de IM) a partir de una perspectiva de red. La Identidad Privada del Usuario identifica la suscripción, no el usuario.
- La Identidad Privada del Usuario está asignada permanentemente a una suscripción de usuario (no es una identidad dinámica), y es válida para la duración de la suscripción del usuario con la red doméstica.
- La Identidad Privada del Usuario se utiliza para identificar la información del usuario (por ejemplo, información de autentificación) almacenados en el HSS (para su uso, por ejemplo, durante el Registro).
- La Identidad Privada del Usuario puede estar presente en la carga de registros basada en las políticas del operador.
- La Identidad Privada del Usuario es autentificada sólo durante el registro del usuario, (incluyendo el nuevo registro y la anulación del registro).
- La S-CSCF necesita, para obtener y almacenar la Identidad Privada del Usuario, tras el registro y la terminación no registrada.

Además de una Identidad Privada de Usuario, todos los usuarios del IMS tienen una o más Identidades Públicas de Usuario del IMS (PUI, en sus siglas en inglés). Las PUI son utilizadas por cualquier usuario para solicitar comunicaciones a otros usuarios. Un usuario podría incluir, por ejemplo, una PUI (pero no una Identidad Privada de Usuario) en una tarjeta de visita. 3GPP TS 23.228 especifica las siguientes propiedades de la PUI:

- Los esquemas tanto de numeración de las telecomunicaciones como de nombres de Internet se pueden utilizar para dirigirse a los usuarios en función de las PUI que tienen los usuarios.
- La o las PUI toman la forma de un SIP URI (como se define en los documentos RFC 3261 y RFC 2396 o el formato de “tel:”-URI definido en el documento RFC 3966).
- La solicitud de ISIM almacena de forma segura por lo menos una PUI (no será posible para el UE modificar la PUI), pero no es necesario que todas las PUI adicionales se almacenen en la solicitud de ISIM.
- Una PUI está registrada ya sea explícita o implícitamente, antes de que la identidad pueda ser utilizada para originar sesiones del IMS y procedimientos no relacionados de sesión del IMS.
- Una PUI está registrada ya sea explícita o implícitamente, antes de que las sesiones de terminación del IMS y los procedimientos no relacionados de sesiones de terminación del IMS puedan ser entregados al UE del usuario al que pertenece la PUI.
- Es posible registrar globalmente (es decir, a través de una única petición de UE) a un usuario que tiene más de una PUI a través de un mecanismo dentro de la IMS (por ejemplo, mediante el uso de un Conjunto de Registro Implícito). Esto no impide que el usuario se registre de forma individual algunas de sus PUI si es necesario.
- Las PUI no son autentificadas por la red durante el registro.
- Las PUI se pueden utilizar para identificar la información del usuario dentro del HSS (por ejemplo, durante la configuración de la sesión terminada del móvil).
- Las PUI pueden ser utilizadas por los AS dentro del IMS para identificar los datos de configuración del servicio que se aplicarán a un usuario.

Otra técnica anterior relevante está representada por el documento WO 2007/060074.

La figura 1 ilustra esquemáticamente relaciones ilustrativas entre una suscripción (IMS) de usuario y las Identidades Públicas y Privadas de Usuario. En el ejemplo mostrado, un abonado tiene dos identidades de usuario privadas, estando ambas asociadas con dos Identidades Públicas de Usuario (una de las Identidades Públicas de Usuario, 2 Identidades Públicas de Usuario, estando asociadas con ambas Identidades Privadas de Usuario). Un Perfil de Servicio está asociado con cada Identidad Pública de Usuario, especificando este perfil datos de servicio para las Identidades Públicas de Usuario asociadas. Un Perfil de Servicio es creado o modificado cuando hay previsto un servidor de aplicaciones para un usuario en el Servidor Doméstico de Abonados. Cada Perfil de Servicio comprende uno o más Criterios de Filtro iniciales (iFC, en sus siglas en inglés), que se utilizan para activar la prestación, o la restricción, de los servicios del IMS. Las diferencias entre los servicios ofrecidos por el Perfil de Servicio-1 y el Perfil de Servicio-2 son específicas del operador, pero puede involucrar a diferentes servidores de aplicaciones (AS, en sus siglas en inglés), e incluso a diferentes esquemas de tarifas / calificación.

En el ejemplo mostrado en la figura 1, la Identidad Pública del Usuario -1 está asociada con un Perfil de Servicio -1, mientras la Identidad Pública de Usuario -2 y la Identidad Pública de Usuario -3 están asociadas con el Perfil de Servicio -2. En un escenario típico, la Identidad Pública de Usuario -1 podría ser una identidad que el usuario da a sus amigos y familiares, por ejemplo, "Gran_Pepe@priv.operador.com", mientras la Identidad Pública de Usuario – 2 y la Identidad Pública de Usuario – 3 podrían ser las identidades que el usuario da a los contactos de negocios, por ejemplo, "+46111222333@operador.com" o "pepe.negro@operador.com".

3GPP define el concepto denominado "Conjunto de Registro Implícito" para identificar un conjunto de PUI que

trabajan como un grupo, y que se registran y se dan de baja juntas cuando cualquiera de las PUI del conjunto se registra o se da de baja. 3GPP requiere que el HSS envíe el Conjunto de Registro Implícito a la S-CSCF tras el registro de un usuario o al terminar una llamada. Se ha entendido que, en el registro, el HSS identifica todas las PUI dentro del Conjunto de Registro Implícito, y luego identifica todos los Perfiles de Servicio asociados con estas PUI. Los Perfiles de Servicio (o datos seleccionados de los Perfiles de Servicio) que contienen las PUI con las que están asociados, se envían luego a la S-CSCF. Como resultado de esta operación, la S-CSCF conoce todas las PUI que pertenecen al mismo Conjunto de Registro Implícito, así como sus Perfiles de Servicio.

Un caso de uso posible del IMS conlleva una colección de usuarios que tienen una suscripción a nivel de grupo del IMS, pero en el que los propios usuarios individuales no están suscritos y de la que el IMS no es consciente. Es deseable permitir la marcación directa interna y externa a los usuarios. Esto podría suceder, por ejemplo, en el caso de una empresa que está abonada al IMS y que tiene estaciones individuales de empleados o terminales conectados a una centralita privada de IP (IP-PBX, utilizando siglas en inglés). Los terminales de los empleados pueden estar provistos o no de clientes del SIP. En este último caso, la IP-PBX realiza una traducción entre la señalización SIP y la no SIP. Aunque podría ser posible, por supuesto, que el IMS grabe una PUI individual para cada terminal (dentro del mismo Conjunto de Registro Implícito), esto se convierte en ineficaz mientras el tamaño del grupo se hace grande. La TISPAN del ETSI define una red empresarial como tal, como una Red Empresarial de Próxima Generación (NGCN, en sus siglas en inglés).

Es posible incluir en el Conjunto de Registro Implícito asociado con una suscripción, una Identidad Pública de Usuario comodín. "Comodín" se entiende aquí en el sentido de una Identidad Pública de Usuario que contiene un símbolo o un símbolo que representa uno o más caracteres no especificados. La Identidad Pública de Usuario comodín tiene un perfil de servicio asociado con él. Cualquier nodo dentro del Subsistema Multimedia IP que realiza pruebas o tratamientos basados en el Conjunto de Registro Implícito, actúa sobre una Identidad Pública de Usuario recibida correspondiente con una Identidad Pública de Usuario comodín de la misma forma que si la Identidad Pública de Usuario recibida corresponde con una Identidad Pública de Usuario estándar dentro del Conjunto de Registro Implícito. En lugar de representar una gama de Identidades Públicas de Usuario que utilizan una Identidad Pública de Usuario comodín, tal gama puede ser representada en su lugar por un sub-dominio. Por ejemplo, una gama de Tel URI puede ser representada mediante un prefijo de marcación, mientras un margen del SIP URI puede ser representado mediante un dominio corporativo. Esto permite el enrutamiento desde y hacia usuarios de redes empresariales cuando la red empresarial está conectada a una red del IMS en el punto de referencia Gm.

Sin embargo, existe un requisito en la especificación publicada de TISPAN para Requisitos de Comunicaciones de Negocios (ETSI TS 181 019 (V2.0.0): Telecomunicaciones y Servicios y Protocolos convergentes en Internet para Redes Avanzadas (TISPAN, en sus siglas en inglés); Requisitos de Comunicaciones de Negocios)] que expresa que el dominio de confianza del operador debería ser capaz de extenderse en el dominio de la red empresarial, donde está preparado un tronco de negocio entre una red del IMS y una red empresarial de confianza. Una implicación de esto es que el P-CSCF en la red del IMS debe aceptar una cabecera de P-Identidad-Afirmada enviada desde la red empresarial sobre el punto de referencia Gm. La cabecera de P-Identidad-Afirmada es una cabecera de un mensaje del SIP que contiene un SIP URI y un nombre de pantalla opcional. La P-Identidad-Afirmada es una identidad que se utiliza entre entidades SIP de confianza, por lo general intermediarios, para llevar la identidad del usuario enviando un mensaje del SIP como fue verificado mediante autentificación. La P-Identidad-Afirmada se inserta en el campo de cabecera de un mensaje del SIP mediante una entidad del SIP una vez que el nodo ha autentificado al usuario originario de alguna manera. Una consecuencia de esto es que la P-Identidad-Afirmada no puede representar al usuario servido de origen de la red del IMS, ya que la P-Identidad-Afirmada contiene una identidad que es autentificada por la red distante / empresarial / privada.

La S-CSCF utiliza normalmente la P-Identidad-Afirmada para comprobar si se han puesto algunas restricciones relevantes al UE de origen, por ejemplo, si el UE tiene prohibido usar el servicio solicitado. El S-CSCF también utiliza la P-Identidad-Afirmada y el caso de llamadas para determinar los Criterios de Filtro Iniciales (IFC, en sus siglas en inglés) del UE. Suponiendo, por ejemplo, que el IFC requiere que la S-CSCF remita la INVITACIÓN a un AS particular, la S-CSCF incluye en el nivel superior de la cabecera de ruta del SIP la URI del AS. También incluye en el nivel subsiguiente su propia URI, junto con un Identificador de Diálogo Original (ODI, en sus siglas en inglés). La ODI es generada por la S-CSCF e identifica de forma única la llamada a la S-CSCF. El AS realizará él mismo la autentificación basada en la P-Identidad-Afirmada contenida en el mensaje. Se puede concluir de esto que la P-Identidad-Afirmada se utiliza en una red del IMS de origen para determinar el usuario servido, para que la red sea capaz de ejecutar las políticas y servicios adecuados para este usuario.

Como se ha descrito más arriba, cuando el dominio de confianza se extiende desde una red pública del IMS a otra red conectada a través de un punto de referencia Gm, la P-Identidad-Afirmada puede contener una identidad de usuario no conocida en la red del IMS. Sin embargo, surge un problema debido a que la P-Identidad-Afirmada también es utilizada por sistemas centrales originarios del SIV para determinar el usuario servido. Al enviar un mensaje que contiene una P-Identidad-Afirmada de un usuario que no representa al usuario actualmente servido por una P-CSCF, y en algunos casos, una P-Identidad-Afirmada que no es la identidad de un usuario del IMS conocido, los procedimientos actuales o fallarían, los procedimientos serían ejecutados para un usuario equivocado, o la P-

CSCF caería la P-Identidad-Afirmada que pertenece a un usuario diferente.

SUMARIO

El inventor ha ideado un método para permitir que una red del IMS extienda su dominio de confianza a otra red. Una P-CSCF en la red del IMS, después de recibir un mensaje del SIP desde el dominio de la empresa de confianza, inserta una cabecera nueva, denominada cabecera de P-Usuario-Servido, en el mensaje SIP antes de enviar el mensaje SIP a una S-CSCF. Opcionalmente, la P-CSCF sólo inserta la cabecera nueva cuando la P-Identidad-Afirmada en el mensaje SIP no coincide con la identidad de un Registro Implícito establecido que pertenece a la entidad de confianza. La cabecera de P-Usuario-Servido incluye la identidad del usuario servido. La identidad del usuario servido es una identidad por defecto perteneciente al sitio de red de confianza a través del cual el mensaje SIP entró en la red del IMS. Una S-CSCF que posteriormente recibe el mensaje SIP es luego consciente de que debe utilizar el campo de cabecera de P-Usuario-Servido para determinar el usuario servido y puede ignorar un campo de cabecera de P-Identidad-Afirmada con el propósito de determinar el usuario servido.

Según un primer aspecto de la invención, se proporciona un método para gestionar una comunicación de Protocolo de Inicio de Sesión (SIP, en sus siglas en inglés) dentro de una red de un Subsistema Multimedia IP (IMS, en sus siglas en inglés). Una Función de Control de Sesiones de Llamada de Proximidad (P-CSCF, en sus siglas en inglés) recibe un mensaje del SIP enviado desde una red distante. La P-CSCF añade al mensaje una cabecera adicional, que identifica una Identidad Pública de Usuario de una entidad de confianza en la red a distancia servida por una Función de Control de Sesiones de Llamada de Servicio en la red del IMS. Opcionalmente, la P-CSCF sólo inserta la nueva cabecera cuando la P-Identidad-Afirmada en el mensaje del SIP no coincide con la identidad de la entidad de confianza. La Identidad Pública de Usuario de la entidad de confianza se obtiene opcionalmente mediante la determinación de la identidad de un canal seguro en el que se recibió el mensaje. El mensaje se envía luego a la S-CSCF. La S-CSCF, y cualquier otro nodo al que se envía el mensaje, sabe de la presencia de la cabecera adicional para ignorar los contenidos de una cabecera de P-Identidad-Afirmada, que no puede incluir la Identidad Pública de Usuario servida por el S-CSCF, y en lugar de utilizar la Identidad Pública de Usuario de la entidad de confianza contenida en la cabecera adicional.

El mensaje del SIP se envía opcionalmente por medio de un tronco de negocios entre la red distante y la red del IMS, y la red distante tiene la confianza de la red del IMS. Debido a que la P-CSCF de la red del IMS confía en la red distante (esto puede ser denominado estando en el mismo dominio de confianza, véase el documento IETF RFC 3324 y RFC 3325), ésta confiará en la P-Identidad-Afirmada recibida desde esa red, y los nodos de la red del IMS que confían en la P-CSCF confiarán en la P-Identidad-Afirmada recibida desde ella, y así sucesivamente. Esto se denomina confianza transitiva. Los nodos de la red del IMS serán, por lo tanto, conscientes de que se puede confiar en la entidad de confianza.

Opcionalmente, la cabecera adicional que identifica el nodo de la red privada se obtiene de la información de suscripción relacionada con la Identidad Pública del Usuario de la entidad de confianza almacenada a un Servidor de Abonados Domésticos o, en el caso de una red de NGN, una Función de Servidor de Perfil de Usuario localizada en la red del Subsistema de Multimedia IP.

La información de suscripción relacionada con la Identidad Pública del Usuario de la entidad de confianza incluye, opcionalmente, un Conjunto de Registro Implícito. Opcionalmente un Conjunto de Registro Implícito incluye una Identidad Pública de Usuario comodín o Identidad Pública de Usuario representativa del subdominio de una gama de Identidades Públicas de Usuarios. Como otra opción, el mensaje del SIP es un mensaje de INVITACIÓN SIP enviado desde la entidad de confianza, en nombre de un usuario de la red distante.

Según un segundo aspecto de la invención, hay provisto un nodo de P-CSCF para su uso en una red del IMS. El nodo de Función de P-CSCF comprende un receptor para recibir un mensaje del SIP enviado desde una red distante. Hay provisto un procesador para añadir al mensaje una cabecera adicional, identificando la cabecera adicional una Identidad Pública de Usuario de una entidad de confianza en la red distante que está servida por una S-CSCF. La P-CSCF también incluye un transmisor para enviar el mensaje a la S-CSCF. La cabecera adicional puede ser utilizada por otros nodos de la red del IMS para informarles sobre el uso de información en la cabecera adicional para identificar el nodo servido, más que de la información contenida en la cabecera de P-Identidad-Afirmada.

La P-CSCF comprende opcionalmente medios para recibir información de suscripción en relación con la Identidad Pública del Usuario de la entidad de confianza de uno de un Servidor Doméstico de Abonados y una Función de Servidor de Perfiles de Usuario que se encuentra en la red del IMS.

La información de suscripción incluye, opcionalmente, un Conjunto de Registro Implícito, comprendiendo el Conjunto de Registro Implícito un subdominio de Identidad Pública de Usuario de comodín o una Identidad Pública de Usuario representativa de una gama de Identidades Públicas de Usuario.

De acuerdo con un tercer aspecto de la invención, se proporciona un nodo de S-CSCF para su uso en una red del

IMS. El nodo de S-CSCF comprende un receptor para recibir un mensaje de Protocolo de Iniciación de Sesión desde un nodo de P-CSCF, y un procesador para identificar la presencia de una cabecera adicional en el mensaje de Protocolo de Inicio de Sesión, identificando la cabecera adicional una Identidad Pública de Usuario de una entidad de confianza en una red distante servida por la Función de Control de Sesiones de Llamadas de Servicio. La S-CSCF incluye también medios para, en el caso de que se identifique la cabecera adicional, utilizar la Identidad Pública de Usuario de la entidad de confianza en esa cabecera para determinar el usuario servido en lugar de la cabecera de P-Identidad-Afirmada contenida en el mensaje del SIP. De este modo, los mensajes recibidos por el S-CSCF en que el usuario servido no es identificado por la cabecera de P-Identidad-Afirmada pueden ser tratados adecuadamente.

De acuerdo con un cuarto aspecto de la invención, se proporciona un servidor de aplicaciones (AS, en sus siglas en inglés) para su uso en una red del IMS. El AS comprende un receptor para recibir un mensaje del SIP, y un procesador para identificar la presencia de una cabecera adicional en el mensaje de Protocolo de Inicio de Sesión. La cabecera adicional identifica una Identidad Pública de Usuario de una entidad de confianza en una red distante servida por un S-CSCF en la red del IMS. El AS incluye además medios para, en el caso de que se identifique la cabecera adicional, utilizando la Identidad Pública de Usuario de la entidad de confianza contenida en esa cabecera para determinar el usuario servido en lugar de la P-Identidad-Afirmada.

La invención está definida según las reivindicaciones independientes 1, 8, 10 y 11.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 ilustra esquemáticamente las relaciones ilustrativas entre una suscripción de usuario del IMS y las Identidades Pública y Privada de Usuarios;

La figura 2 ilustra esquemáticamente en un diagrama de bloques un flujo de señalización entre una red empresarial y una red del IMS según una realización de la invención;

La figura 3 es un diagrama de flujo que muestra las operaciones básicas de una forma de realización de la invención;

La figura 4 ilustra esquemáticamente en un diagrama de bloques una P-CSCF según una realización de la invención;

La figura 5 ilustra esquemáticamente en un diagrama de bloques una S-CSCF según una realización de la invención;

La figura 6 ilustra esquemáticamente en un diagrama de bloques un Servidor de Aplicaciones según una realización de la invención.

DESCRIPCIÓN DETALLADA

Haciendo referencia a la figura 2, se ilustra esquemáticamente una red del IMS 1 y una red empresarial de confianza 2. La red empresarial 2 contiene una centralita (PBX, siglas en inglés de Private Branch eXchange), que se designa con IP-PBX. La IP-PBX se registra en la red del IMS 1, en nombre de un grupo de terminales de usuario. La IP-PBX recoge la dirección de la P-CSCF 3 de salida ubicada en la red del IMS 1 por medio de una búsqueda de DHCP (como se especifica en el IETF RFC 3263). La IP-PBX se registra en la red del IMS utilizando su propia PUI (en este ejemplo, "pbx1@operador.com"). El HSS 4 de la red del IMS 1 almacena información de suscripción de la IP-PBX, que incluye un Conjunto de Registro Implícito que incluye a todos los usuarios capaces de acceder a la red del IMS 1 a través de una IP-PBX. Además de las PUI de la IP-PBX y un tel URI asignado a la IP-PBX, el Conjunto Implícito de Registro contiene una PUI "comodín" que representa una amplia gama de PUI asociados con la centralita. En este ejemplo, la PUI comodín es "!x!@empresa2.com". El componente "!x!" de la PUI comodín indica que una PUI que tiene el sufijo especificado y cualquier prefijo coincidirá con la PUI comodín.

El HSS 4 envía el Conjunto de Registro Implícito a una S-CSCF 7 en una Respuesta de Asignación de Servidores junto con el(los) perfil(es) de servicio asociado(s). La S-CSCF 7 envía luego un mensaje de OK 200 a la IP-PBX a través de la I-CSCF (no mostrada) y la P-CSCF 3, con el mensaje de OK 200 que incluye un campo de P- URI-Asociado que identifica las PUI dentro del Conjunto de Registro Implícito que está asociado a la PUI de la PBX.

Teniendo en cuenta el caso de que un terminal en la red empresarial de confianza desea enviar una llamada a otro terminal, un primer terminal 5 que tiene la identidad de Cassandra@empresa3.com llama a un segundo terminal 6, que tiene la identidad Berto@empresa2.com. Un mensaje enviado desde el primer terminal 5 contiene en su cabecera la URI de Cassandra@empresa3.com en el campo "De" y Berto@empresa2.com en el campo "Para". El mensaje también incluye la P-Identidad-Afirmada de Cassandra@empresa3.com. Sin embargo, los mensajes enviados a Berto@empresa2.com van a ser remitidos a Alicia@empresa1.com.

El mensaje se devuelve a la IP-PBX para su transmisión a Alicia@empresa1.com, y la IP-PBX determina que este debe ser enviado a la P-CSCF 3 en la red del IMS 1. La IP-PBX envía un mensaje de INVITA a la P-CSCF 3, conteniendo el mensaje de invitación la URI de Alicia, la URI de Cassandra en el campo "De", y la URI de Berto en el campo "Para". El INVITA también contiene la P-Identidad-Afirmada de Cassandra.

Hay que tener en cuenta que existe una relación de confianza entre la IP-PBX en la red empresarial 2 y la red del

IMS 1. Debido a que la P-CSCF 3 recibe el INVITA del SIP en la asociación de seguridad que se creó durante el registro, la P-CSCF es consciente de que el INVITA se va a tratar, en nombre de pbx1@operador1.com. La P-CSCF 3 también es consciente de que el dominio de confianza de la red del IMS 1 se extiende a la IP-PBX en la red corporativa 2. La P-CSCF 3 pasa sin modificar la P-Identidad-Afirmada e inserta una nueva cabecera al INVITA, siendo la nueva cabecera referida como el "P-Usuario-Servido". La cabecera del P-Usuario-Servido contiene la URI de la IP-PBX, que es pbx1@operador1.com. Hay que tener en cuenta que en una realización, la P-CSCF 3 sólo insertará una cabecera de P-Usuario-Servido en el caso de que la P-Identidad-Afirmada no coincida con la identidad en la que se recibió el mensaje. En este ejemplo, la P-CSCF sólo insertará una cabecera de P-Usuario-Servido si la P-Identidad-Afirmada no es un elemento del Conjunto de Registro Implícito que pertenece a la entidad de confianza.

La P-CSCF 3 envía la INVITA del SIP que contiene la cabecera de P-Usario-Servido a la S-CSCF 7. Los iFC asociados con la suscripción de pbx1@operador.com pueden indicar que el INVITA va a ser tratado por un Servidor de Aplicaciones (AS, en sus siglas en inglés) 8 de reenvío de llamada. En este caso, la S-CSCF 7 realiza operaciones convencionales de añadir la URI del SIP del AS 8 como el URI superior de la cabecera de la ruta, y de incluir su propio URI del SIP debajo de la URI de AS en la cabecera de la ruta junto con el “identificador de diálogo original” (ODI, en sus siglas en inglés). El mensaje se envía luego al AS 8 través de la interfaz de ISC. La S-CSCF 7 mantiene información de estado para la sesión con la que se relaciona el INVITA. Esta información incluye la ODI y la identidad del Usuario servido.

El S-CSCF 7 también determina el usuario servido basándose en el P-Usuario-Servido, más que en la P-Identidad-Afirmada. Esto permite que la autentificación se base en la identidad de IP-PBX asociada con la IP-PBX, más que en la P-Identidad-Afirmada contenida en el INVITE del SIP.

Si la cabecera de P-Usuario-Servido no estuviera incluida en el INVITA del SIP, los nodos de la red del IMS intentarían llevar a cabo la autorización en la P-Identidad-Afirmada (en este caso, Cassandra@empresa3.com). Como Cassandra@empresa3.com no pertenece a la red del IMS ni a la red empresarial adjunta, la autentificación utilizando la P-Identidad-Afirmada fallaría.

La invención permite que la P-CSCF 3 se comunique con el usuario servido (Berto@empresa2.com) en un elemento de información por separado en el INVITA del SIP desde la identidad del usuario que origina la afirmación de la red (Cassandra@empresa3.com). La S-CSCF 7 utiliza esto para determinar el usuario servido. Esto permite que redes empresariales sean tratadas como redes de confianza.

La figura 3 es un diagrama de flujo que ilustra las operaciones básicas de una forma de realización de la invención. La siguiente numeración se refiere a la numeración de la figura 3:

S1. La P-CSCF recibe un mensaje del SIP desde la IP-PBX de la asociación de seguridad creada durante el registro;

S2. Al recibir el mensaje del SIP en la asociación de seguridad existente y al reconocer que esto viene de una entidad de confianza, y al determinar que la P-Identidad-Afirmada no pertenece al conjunto de identidades implícitas registradas, la P-CSCF añade la URL de la IP-PBX al mensaje del SIP en forma de una cabecera de P-Usuario-Servido y deja intacta una cabecera de P-Identidad-Afirmada opcionalmente existente, ya que la IP-PBX tiene una suscripción a la red del IMS y el usuario de origen afirmado por la red no puede tener una suscripción como esa;

S3. El mensaje del SIP que resulta de la operación 2 es enviado a la S-CSCF;

S4. La S-CSCF, siendo conscientes de la presencia de la cabecera del P-Usuario-Servido, ignora la P-Identidad-Afirmada y utiliza la cabecera de P-Usuario-Servido para determinar el usuario servido para el tratamiento de sus procedimientos. Si se activan los iFC para el usuario servido, el mensaje del SIP puede ser enviado a un AS;

S5. Si el mensaje es recibido posteriormente por un AS, el AS, siendo conscientes de la presencia de la cabecera del P-Usuario-Servido, utiliza la cabecera del P-Usuario-Servido para determinar el usuario servido para tratar los procedimientos pertinentes.

La figura 4 ilustra esquemáticamente una P-CSCF 3 según una realización de la invención. La P-CSCF 3 comprende un receptor 9 para recibir un mensaje del SIP de la IP-PBX. Una memoria 10 está provista para almacenar información de suscripción relacionada con la IP-PBX, y un procesador 11 está provisto para añadir una cabecera de P-Usuario-Servido al mensaje del SIP, identificando la cabecera de P-Usuario-Servido la suscripción relacionada con la IP-PBX. Un transmisor 12 está también provisto para enviar el mensaje del SIP a un nodo adicional tal como una S-CSCF.

La figura 5 ilustra esquemáticamente una S-CSCF 5 de acuerdo con una realización de la invención. La S-CSCF 7

comprende un receptor 13 para recibir un mensaje del SIP de la P-CSCF 3, y un procesador 14 para determinar si el mensaje del SIP contiene una cabecera de P-Usuario-Servido. Si una cabecera de P-Usuario-Servido está presente en el mensaje del SIP, luego la cabecera de P-Usuario-Servido se utilizará para determinar el usuario servido en lugar de la P-Identidad-Afirmada. Hay también provisto un transmisor 15 para enviar el mensaje a otros nodos de la red del IMS para su tratamiento posterior.

La figura 6 ilustra esquemáticamente un AS 8 según una realización de la invención. El AS 8 comprende un receptor 16 para la recepción de un mensaje del SIP, y un procesador 17 para determinar si el mensaje del SIP contiene una cabecera de P-Usuario-Servido. Si una cabecera de P-Usuario-Servido está presente en el mensaje del SIP, luego la cabecera de P-Usuario-Servido se utilizará para determinar el usuario servido en lugar de la cabecera de P-Identidad-Afirmada. El AS tiene también un transmisor 18 para enviar mensajes a otros nodos de la red del IMS.

Se apreciará por la persona experta en la materia que pueden hacerse diversas modificaciones a las realizaciones descritas más arriba sin apartarse del alcance de la presente invención. Por ejemplo, la descripción anterior se refiere a un nodo de IP_PBX en una red empresarial. Sin embargo, la invención también se aplica a un nodo de proximidad conectado mediante SIP o SIP B2BUA dispuesto en redes empresariales u otros tipos de red.

REIVINDICACIONES

1. Un método para gestionar una comunicación de Protocolo de Inicio de Sesión dentro de una red de Subsistema Multimedia IP, comprendiendo el método:

En una Función de Control de Sesiones de Llamada de Proximidad (3) que recibe un mensaje de Protocolo de Iniciación de Sesión enviado desde una entidad de confianza situada en una red distante, en la que el mensaje de Protocolo de Inicio de Función originado desde una entidad adicional cuya identidad ha sido afirmada por la entidad de confianza;
En la Función de Control de Sesiones de Llamadas de Proximidad (3), determinar que la identidad de la entidad de confianza no coincide con una identidad contenida en una P-Identidad-Afirmada del mensaje;
En el caso de tal determinación, en la Función de Control de Sesiones de Llamadas de Proximidad (3), añadir al mensaje una cabecera adicional, identificando la cabecera adicional una Identidad Pública de Usuario de una entidad de confianza en la red distante servida por una Función de Control de Sesiones de Llamadas de Servicio (7), y
Enviar el mensaje a la Función de Control de Sesiones de Llamadas de Servicio (7).

2. El método según la reivindicación 1, comprendiendo además la obtención de la Identidad Pública de Usuario de la entidad de confianza mediante la determinación de la identidad de un canal seguro en el que se recibió el mensaje.

3. El método según la reivindicación 1 o 2, comprendiendo además:

en la Función de Control de Sesiones de Llamadas de Servicio (7), identificar la presencia de la cabecera adicional y utilizar la Identidad Pública de Usuario de la entidad de confianza para determinar el usuario servido en lugar de la P-Identidad-Afirmada.

4. El método según una cualquiera de las reivindicaciones 1, 2 o 3, en el que el mensaje de Protocolo de Inicio de Sesión enviado desde una red distante se envía a través de un tronco de negocios.

5. El método según una cualquiera de las reivindicaciones 1 a 4, en el que la cabecera adicional que identifica la Identidad Público del Usuario se obtiene de la información de suscripción relacionada con la Identidad Pública de Usuario de la entidad de confianza almacenada en uno de los Servidores Domésticos de Abonados (4) y una Función de Servidor de Perfil de Usuario ubicada en la red del Subsistema Multimedia IP (1).

6. El método según la reivindicación 5, en el que la información de suscripción relacionada con la Identidad Pública del Usuario de la entidad de confianza incluye un Conjunto Implícito de Registro, comprendiendo el Conjunto Implícito de Registro un subdominio de una Identidad Pública de Usuario comodín o una Identidad Pública de Usuario representativa de una gama de Identidades Públicas de Usuario.

7. El método según la reivindicación 7, en el que el mensaje de Protocolo de Inicio de Sesión es un mensaje de INVITA de Protocolo de Inicio de Sesión

8. Un nodo de Función de Control de Sesiones de Llamadas de Red (3) para su uso en una red de Subsistema Multimedia IP (1), comprendiendo nodo de Función de Control de Sesiones de Llamadas de Red (3):

un receptor para recibir un mensaje de Protocolo de Iniciación de Sesión enviado desde una entidad de confianza situada en una red distante, en el que el mensaje de Protocolo de Iniciación de Sesión originado desde una entidad adicional cuya identidad ha sido afirmada por la entidad de confianza;
medios para recibir información de suscripción relacionada con la Identidad Pública de Usuario de la entidad de confianza desde uno de los Servidores Doméstico de Abonado (4) y una Función de Servidor de Perfil de Usuario situada en la red de Subsistema IP y para determinar que la identidad de la entidad de confianza no coincide con una identidad contenida en una P-Identidad-Afirmada del mensaje;
un procesador para, en el caso de tal determinación, añadir al mensaje una cabecera adicional, identificando la cabecera adicional una Identidad Pública de Usuario de una entidad de confianza en la red distante servida por una Función de Control de Sesiones de Llamadas de Servicio (7), y
un transmisor para enviar el mensaje a la Función de Control de Sesiones de Llamadas de Servicio.

9. El nodo de Función de Control de Sesiones de Llamadas de Red (3) según la reivindicación 8, en el que la información de suscripción relacionada con la Identidad Pública de Usuario de la entidad de confianza incluye un Conjunto de Registro Implícito, comprendiendo el Conjunto de Registro Implícito una Identidad Pública de Usuario comodín o un subdominio de Identidad Pública de Usuario representativo de una gama de Identidades Públicas de Usuario.

10. Un nodo de Función de Control de Sesiones de Llamada de Servicio (7) para su uso en una red del Subsistema Multimedia IP (1), comprendiendo el nodo de Función de Control de Sesiones de Llamadas de Servicio (7):

un receptor para recibir un mensaje de Protocolo de Iniciación de Sesión desde un nodo de Función de Control de Sesiones de Llamada de Red (3), el mensaje de Protocolo de Inicio de Sesión que origina desde un usuario en una red distante y que ha sido enviado por el nodo de Función de Control de Sesiones de Llamada de Red (3) a través de una entidad de confianza en una red distante;
un procesador para identificar la presencia de una cabecera adicional en el mensaje de Protocolo de Inicio de Sesión, identificando la cabecera adicional una Identidad Pública de Usuario de la entidad de confianza en la red distante servida por la Función de Control de Sesiones de Llamada de Servicio; y
medios para, en el caso de la cabecera adicional esté identificada, usar le Identidad Pública de Usuario de la entidad de confianza como el usuario servido en lugar de la P-Identidad-Afirmada.

11. Un Servidor de Aplicaciones (8) para su uso en una red de Subsistema Multimedia IP (1), comprendiendo el Servidor de Aplicaciones (8):

un receptor para recibir un mensaje de Protocolo de Inicio de Sesión, el mensaje de Protocolo de Inicio de Sesión que origina desde un usuario de una red distante y que ha sido enviado a un nodo de Función de Control de Sesiones de Llamada de Red (3) a través de una entidad de confianza en la red distante;
un procesador para identificar la presencia de una cabecera adicional en el mensaje de Protocolo de Inicio de Sesión, la cabecera adicional identificando una Identidad Pública de Usuario de la entidad de confianza en una red distante servida por una Función de Control de Sesión de Llamada de Servicio (7) en la red de Subsistema Multimedia IP (1), y
medios para, en el caso de que la cabecera adicional sea identificada, utilizar la Identidad Pública de Usuario de la entidad de confianza como usuario servido en lugar de la P-Identidad-Afirmada.

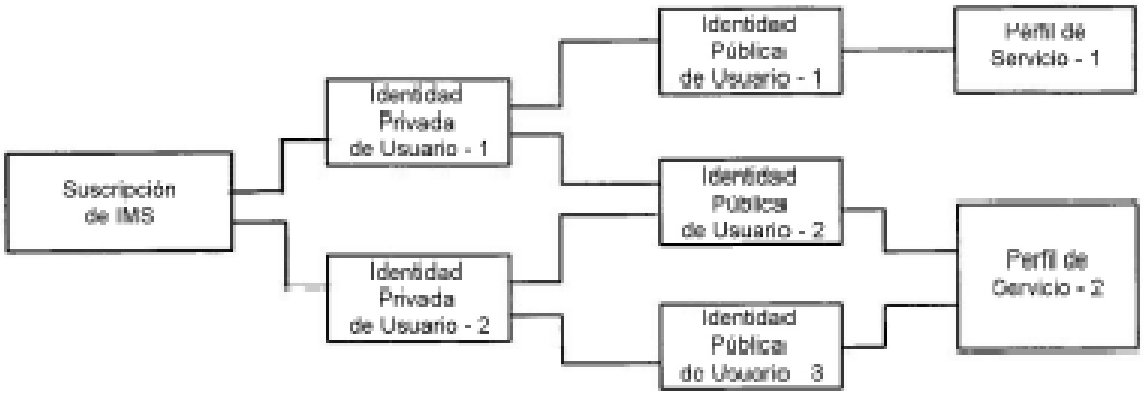
Suscripción de IMS
Identidad Privada de Usuario - 1
Identidad Privada de Usuario - 2
Identidad Pública de Usuario - 1
Identidad Pública de Usuario - 2
Identidad Pública de Usuario 3
Perfil de Servicio - 1
Perfil de Servicio - 2

Figura 1

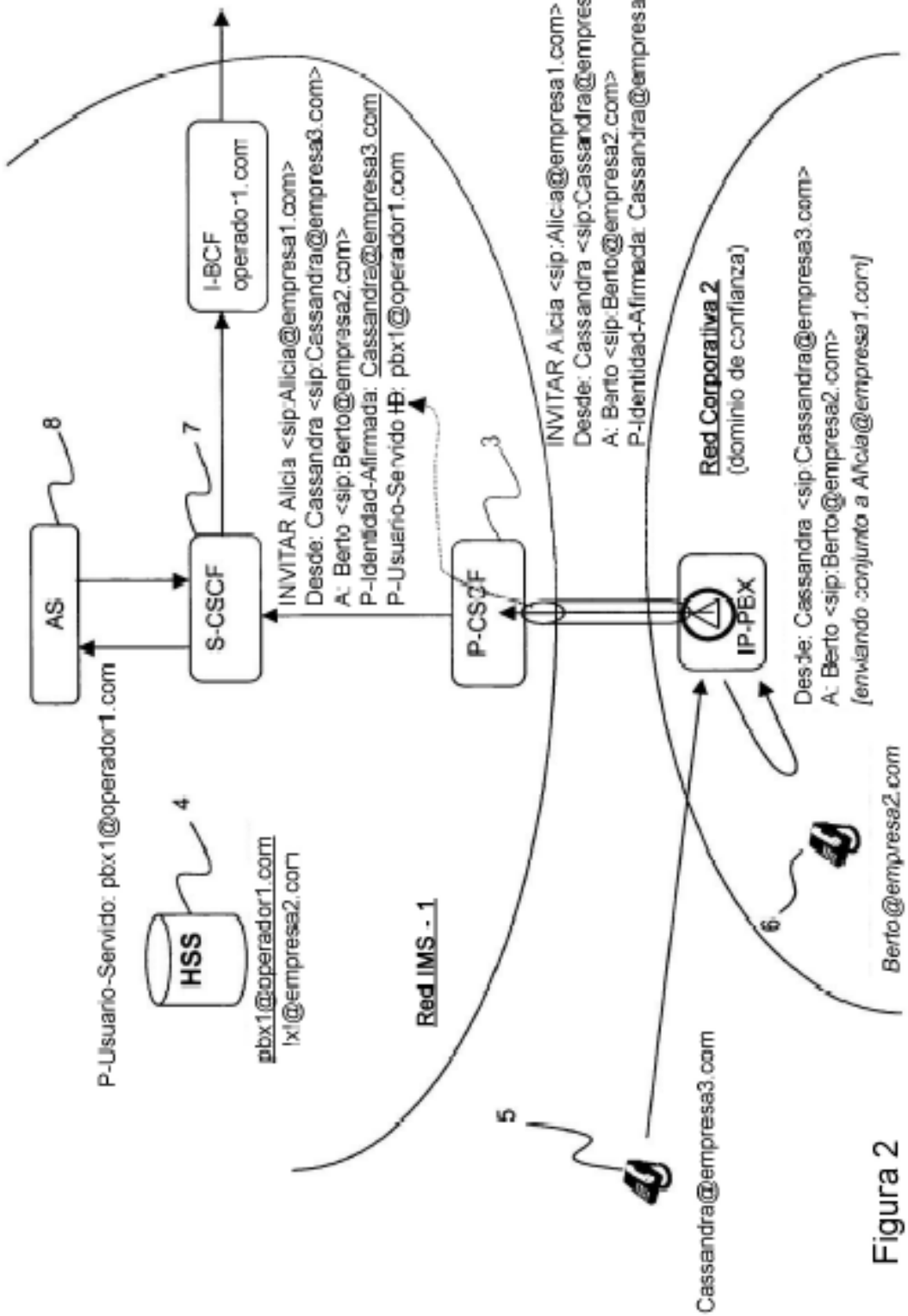
AS
8
S-CSCF
7
I-BCF
operador1.com
INVITAR Alicia <sip:Alicia@empresa1.com>
Desde: Cassandra <sip:Cassandra@empresa3.com>
A: Berto <sip:Berto@empresa2.com>
P-Identidad-Afirmada: Cassandra@empresa3.com
P-Usuario-Servido HB: pbx1@operador1.com
P-Usuario-Servido: pbx1@operador1.com
HSS
4
pbx1@operador1.com
lx1@empresa2.com
Red IMS - 1
P-CSCF
3
INVITAR Alicia <sip:Alicia@empresa1.com>
Desde: Cassandra <sip:Cassandra@empresa3.com>
A: Berto <sip:Berto@empresa2.com>
P-Identidad-Afirmada: Cassandra@empresa3.com
Red Corporativa 2
(dominio de confianza)
IP-PBX
Desde: Cassandra <sip:Cassandra@empresa3.com>
A: Berto <sip:Berto@empresa2.com>
(enviando conjunto a Alicia@empresa1.com)
6
Berto@empresa2.com
5
Cassandra@empresa3.com

Figura 2

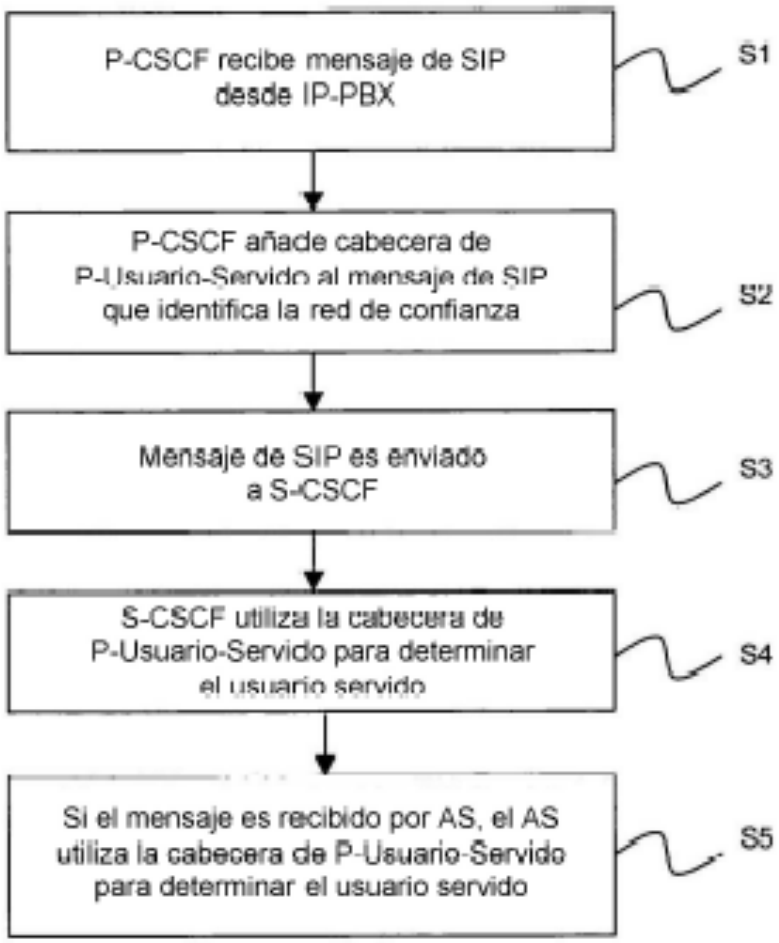

Figura 3

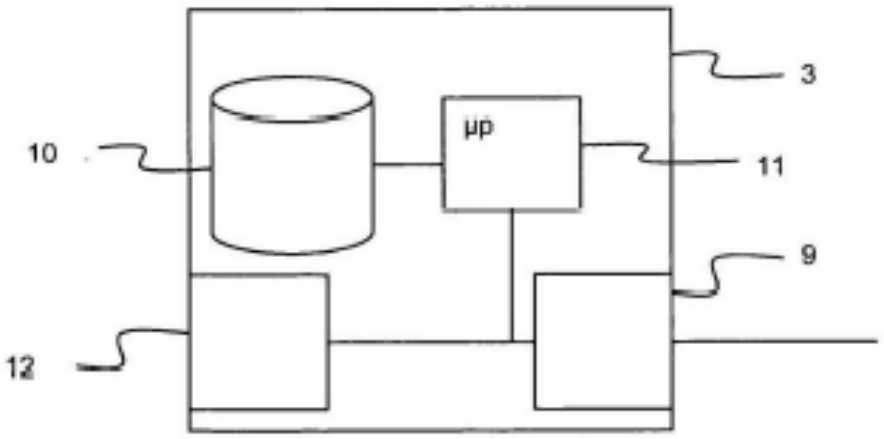

Figura 4

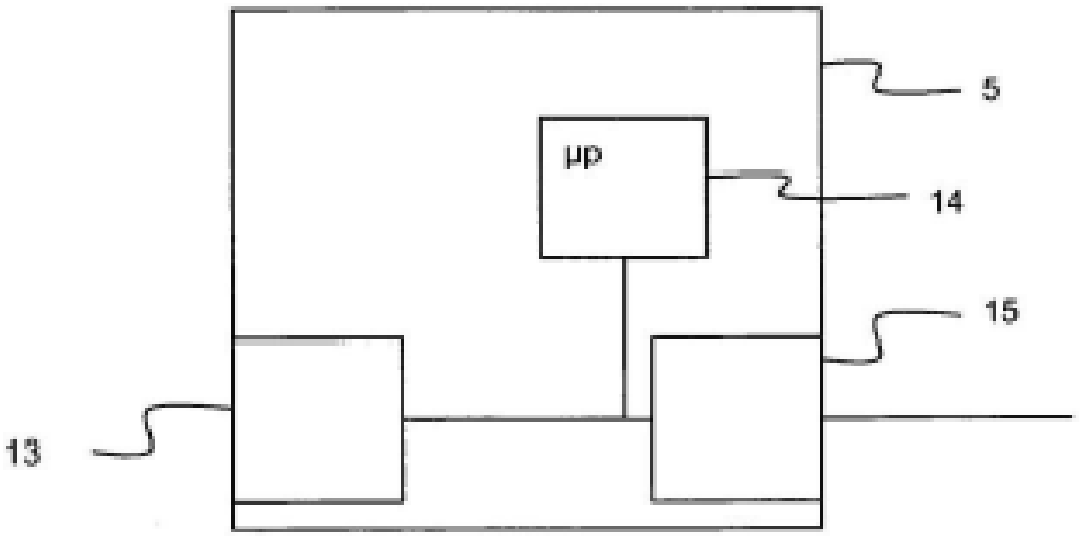

Figura 5

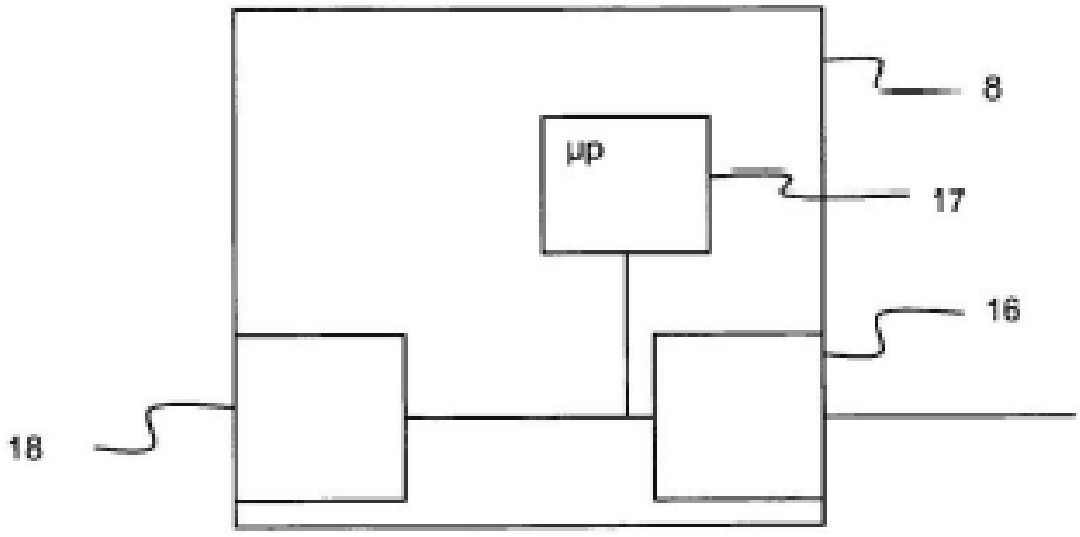

Figura 6