



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 360 036**

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

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **01980804 .7**

96 Fecha de presentación : **05.11.2001**

97 Número de publicación de la solicitud: **1332597**

97 Fecha de publicación de la solicitud: **06.08.2003**

54 Título: **Presencia con información de localización espacial.**

30 Prioridad: **08.11.2000 US 246779 P**

45 Fecha de publicación de la mención BOPI:
31.05.2011

45 Fecha de la publicación del folleto de la patente:
31.05.2011

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

72 Inventor/es: **Costa Requena, José**

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

ES 2 360 036 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

DESCRIPCIÓN

Presencia con información de localización espacial

Campo técnico

La presente invención se refiere a las telecomunicaciones y, más particularmente, a la presencia y mensajería instantánea.

La invención se relaciona también con el nuevo UMTS (Sistema de Telecomunicaciones Móviles Universal) basado en la señalización de la capas de aplicación. La invención muestra una solución para la implementación de Mensajería Instantánea y de la misma manera como Servicio de Presencia a través de un protocolo de control en la capa de aplicación. Utiliza un nuevo formato de información de localización definido para comunicar la localización espacial del usuario denominado "Contenido Útil de Localización Espacial". Proporciona medios y procedimientos de información a las entidades de red acerca de la información de localización del usuario.

Antecedentes de la invención

La presencia es un concepto promovido en varios documentos del Equipo de Trabajo de Ingeniería de Internet (IETF) como la suscripción a y la notificación de cambios en un estado de comunicación de un usuario. El estado puede por ejemplo consistir en una serie de medios de comunicación, direcciones de comunicación y estados que ese usuario. Un protocolo de presencia proporciona un servicio de ese tipo sobre una red IP. Se ha propuesto una extensión del Protocolo de Inicio de Sesión (SIP) por J. Rosenberg y col. para el control de presencia en el WG IMPP titulado "SIP Extensions for Presence" y que se puede encontrar en draft-rosenberg-impppresence-00.txt, 15 de junio de 2000. El SIP es del WG SIP y se describe en RFC 2543 por Handley y col., titulado "SIP: Session Initiation Protocol" 6 de agosto de 2000 que se encuentra en draft-ietf-sip-rfc2543bis-01.ps. Es un protocolo de control (señalización) de la capa de aplicación para la creación, modificación y finalización de sesiones con uno o más participantes.

La mensajería instantánea se usa ampliamente hoy en día pero principalmente usando un sistema propietario para intercambiar contenido entre un conjunto de participantes en tiempo real. Desafortunadamente, el usuario de tal sistema propietario está fuertemente ligado al proveedor y no puede usar el servicio con finalidades distintas de las ofrecidas por el proveedor, mucho menos interoperar con otros servicios de mensajería instantánea. En efecto, la presencia del usuario está fuertemente ligada al sistema propietario y los usuarios no pueden salir de este estrecho corsé. Esto representa un problema. Las extensiones SIP se han propuesto también para mensajería instantánea ("SIP extension for Instant Messaging") en draft-rosenberg-impp-im-00.txt, 15 de junio de 2000, también por J. Rosenberg y col. del WG IMPP del IETF. En ese documento, se proporcionan motivaciones sobre por qué el SIP es una plataforma ideal para mensajería instantánea (IM), por qué la IM se deberían separar completamente de la presencia y cómo realizar la IM con SIP. Las extensiones SIP para la indicación de mensaje en espera se han propuesto asimismo en el draft-mahy-sip-message-waiting-00.txt del IETF, de julio de 2000.

Se ha propuesto por lo tanto en el IETF usar el SIP para el registro del usuario y usar el mismo mecanismo para notificar al usuario acerca de un mensaje en espera.

También el documento de Schulzrinne H y col.: "The Session Initiation Protocol: Internet-centric Signaling", IEEE Communications Magazine, 10 de octubre de 2000 explica las características principales de un intervalo de extensiones potenciales del Protocolo de Inicio de Sesión (SIP). El SIP está indicado principalmente para establecer sesiones entre humanos identificados por identificadores similares a e-mail o números de teléfonos, pero cualquiera que se pueda direccionar mediante un nombre de recurso puede participar en una sesión SIP. El proceso de establecimiento de la sesión involucra el descubrimiento de un usuario dondequiera que se localice de modo que se pueda entregar al usuario una descripción de la sesión.

El documento "Basic SLoP Architecture Proposal" por J. Loughney y col., del 15 de julio de 2000, IETF draft-loughney-spatial-arch-00.txt propone una arquitectura simple que soporta el transporte de la información de localización espacial para permitir a los servicios basados en la información de localización espacial interoperar. El intercambio de información de localización es atractivo para el intercambio de información entre dispositivos tanto en redes cableadas como inalámbricas.

El documento de borrador de Internet "Spatial Location Protocol Requirements" (31 de julio de 2000) por B. Rosen, Mari Korkea-aho, Mika Ylianttila, Rohan Mahy, Kenji Takahashi y Stephen Farrel también se refiere al Protocolo de Localización Espacial (SLoP). Los requisitos presentados en este documento se refieren a las siguientes situaciones: Representación de la Localización, Codificación del Mensaje, Negociación de la Representación, Descubrimiento del Servidor, Transporte, Seguridad y Política.

Por lo tanto un problema es cómo implementar la presencia y la mensajería para redes IP cableadas e inalámbricas.

Divulgación de la invención

Un objeto de la presente invención es proporcionar una forma de transportar la información de localización espacial que pertenece a dispositivos conectados a redes cableadas e inalámbricas.

5 Otro objeto de la presente invención es proporcionar una solución para implementar la mensajería instantánea y la presencia usando una señalización de control de la capa de aplicación.

Otro objeto es aplicar dichas soluciones a los sistemas de telecomunicaciones móviles.

De acuerdo con un primer aspecto de la invención, se proporciona un procedimiento como se define en la reivindicación 1.

10 De acuerdo con un segundo aspecto de la invención, se proporciona un sistema como se define en la reivindicación 8.

De acuerdo con un tercer aspecto de la invención, se proporciona un procedimiento como se define en la reivindicación 3.

De acuerdo con un cuarto aspecto de la invención, se proporciona un procedimiento como se define en la reivindicación 14.

15 De acuerdo con un quinto aspecto de la invención, se proporciona un servidor de presencia como se define en la reivindicación 15.

De acuerdo con un sexto aspecto de la invención, se proporciona un sistema como se define en la reivindicación 16.

Por lo tanto, la invención resuelve el problema del transporte de la localización del usuario dentro de redes IP cableadas e inalámbricas mediante el uso de un protocolo de control de la capa de aplicación.

20 La presente invención también proporciona una solución de mensajería que utiliza el protocolo de señalización de la capa de aplicación para la información al usuario acerca de los mensajes entrantes.

Para el servicio de presencia, hace uso de un nuevo identificador de datos promovido en el IETF para el almacenamiento y mantenimiento de la información de localización del usuario cuando el usuario se está trasladando. Este enfoque usa el Contenido Útil de Localización Espacial (SLoP) para hacer seguimiento de la localización del usuario en cualquier momento. Por ello se usará el SIP para el registro de esa información en los servidores de Localización que normalmente están localizados conjuntamente al lado del servidor SIP actuando como un registrador de SIP. De ahí que, un Agente de Usuario del SIP registrará su información de localización espacial siguiendo el formato SLoP en el registrador del SIP. Esa información se almacenará en el Servidor de Localización y estará disponible para el resto de CSCF (Función de Control del Estado de Llamadas (servidores SIP)) en caso de llamadas de emergencia u otros servicios tales como mensajería instantánea.

35 Para el servicio de mensajería instantánea, se utilizará el SIP para la notificación al usuario acerca de cualquier evento para el que él se haya registrado previamente que quiere estar al tanto de él. Una vez que el usuario se ha suscrito para recibir cualquier nuevo mensaje, cuando sucede ese evento el servidor del SIP enviará un mensaje de notificación indicando que tiene un mensaje nuevo. Véase el documento de IETF draft-mahy-sip-message-waiting-00.txt. (SIP Extensions for Message Waiting Indication por Rohan Mahy y Ilya Slain). La innovación en la presente invención se basa en el uso del mismo mecanismo pero accediendo a la información de SLoP. En base a esta información, el Centro del Servicio de Mensajería conoce exactamente la situación del usuario y puede enviar el mensaje NOTIFICACIÓN directamente al servidor SIP correcto. Por ello, se contactará con el usuario inmediatamente sin ningún retraso.

40 El servidor del Registrador del SIP recibe la información de localización desde el Agente de Usuario del SIP (UA). Esa información se debería actualizar frecuentemente desde el UA del SIP cada vez que el usuario se traslada o actualiza su localización. El servidor del SIP que contiene la información de SLoP será consultado por el Servicio de Mensajería para determinar la localización exacta del usuario. El servidor del SIP devolverá al Centro del Servicio de Mensajería la localización de ese usuario y el mecanismo de señalización para acceder a ese usuario. En este caso, 45 el usuario se ha registrado a través del servicio de Registro del SIP, de modo que el acceso se debería realizar con la señalización SIP. En otra situación en la que el usuario se haya trasladado en GSM, H.323 o cualquier otro dispositivo, el SIP indicará al centro del servicio de mensajería la nueva localización y cómo puede ser alcanzado.

Realmente, en los sistemas UMTS nuevos no hay forma de comunicar al terminal sobre tales eventos. Incluso no hay ningún mecanismo posible para mantener la localización del usuario actualizada. La presente invención proporciona los medios para implementar tales nuevos servicios que dependen de la localización. La presente invención supera ambos problemas, primero la localización y segundo la notificación. Un ejemplo simple es el servicio de mensajería instantánea. Otros muchos servicios podrían hacer uso de esta solución.

La presente invención se aparta de forma única de las soluciones existentes en el sentido de que puede

proporcionar múltiples instancias de información necesarias para mantener al usuario completamente localizado e informarle acerca de cualquier evento importante.

Estos y otros objetos, características y ventajas de la presente invención serán más evidentes a la luz de la descripción detallada de un mejor modo de realización de la misma, como se ilustra en los dibujos adjuntos.

5 **Breve descripción de los dibujos**

La Figura 1 muestra una metodología y aparato para llevar a cabo la presente invención en la que se proporciona un servicio de presencia a través de una red de protocolo de Internet, así como muestra la mensajería instantánea y la presencia actuando conjuntamente como servicios complementarios en una red IP.

La Figura 2 muestra la sintaxis de un mensaje de REGISTRO SIP, de acuerdo con la presente invención.

10 La Figura 3 muestra un ejemplo de una solicitud de REGISTRO SIP que es aplicable a la solicitud de registro mostrada en la Figura 10.

La Figura 4 muestra un ejemplo de un mensaje de INVITACIÓN aplicable también al mensaje de invitación mostrado en la Figura 10.

15 La Figura 5 muestra los campos principales que se pueden insertar en la cabecera de los datos del contenido útil de localización espacial.

La Figura 6 muestra una sintaxis propuesta que incluye la cabecera y un cuerpo, que muestra tanto el formato como los atributos de la información de localización espacial.

La Figura 7A muestra el registro del SIP usando SLO.

La Figura 7B muestra el proceso de registro que incluye el descubrimiento del servidor.

20 La Figura 7C muestra la edición de tercera generación de la arquitectura 2000.

La Figura 7D muestra la posición del SIP-SS dentro del CPS.

La Figura 8 muestra un caso de usuario del servidor de presencia, de acuerdo con la presente invención.

La Figura 9 muestra un modelo de la arquitectura de red GPP.

La Figura 10 muestra varios mensajes para el registro de usuario, de acuerdo con la presente invención.

25 La Figura 11 muestra un mecanismo de mensajería instantánea básica para implementar la mensajería instantánea a través de redes IP.

La Figura 12 muestra el entrelazado para mensajería instantánea, de acuerdo con la presente invención.

La Figura 13 muestra otro ejemplo de entrelazado de la mensajería instantánea, de acuerdo con la presente invención.

30 La Figura 14 muestra un ejemplo de mensajería instantánea a través de redes completamente IP en donde no hay necesidad de conversiones.

La Figura 15 muestra un ejemplo de presencia y mensajería usadas en conjunto entre sí.

La Figura 16 muestra otro ejemplo de presencia y mensajería instantánea usadas conjuntamente.

Mejor modo de realizar la invención

35 La Figura 1 ilustra una metodología y aparato para realizar la presente invención en la que actúan conjuntamente la mensajería instantánea y la presencia como servicios complementarios en redes IP. Se muestra una primera pluralidad de usuarios 2 ya registrados en un primer servidor de presencia 4. Los registros se realizaron previamente mediante una pluralidad correspondiente de solicitudes de registro desde la primera pluralidad de usuarios al servidor de presencia 4 por medio de un primer servidor central 6. Las solicitudes de registro incluyen información
40 relacionada con un estado correspondiente de las comunicaciones de cada uno de la pluralidad de usuarios. Los cambios en el estado de las comunicaciones del usuario se pueden cambiar por ese usuario mediante el nuevo registro con el servidor de presencia 4 por medio del servicio central 6.

Se muestra con líneas discontinuas cómo se suscribieron una segunda pluralidad de usuarios 8 a un servidor de mensajería 10. Estas suscripciones de usuarios fueron realizadas previamente en el servidor de mensajería 10
45 proporcionando una pluralidad correspondiente de solicitudes de suscripción desde la segunda pluralidad de usuarios por medio del servidor central 6 al servidor de mensajería 10. Las solicitudes de suscripción pueden, por

ejemplo, haber incluido información relacionada con una solicitud correspondiente de notificación de un evento o conjunto de eventos de los que el usuario desea tener noticia. Las solicitudes de suscripción se pueden actualizar en cualquier momento desde los usuarios 8 al servidor de mensajería por medio del servidor central 6.

Se debería indicar que la segunda pluralidad de usuarios 8 incluye usuarios desde la primera pluralidad de usuarios 2. Visto desde otra perspectiva, la primera pluralidad de usuarios incluye usuarios de la segunda pluralidad de usuarios. Algunos usuarios tanto en la primera como en la segunda pluralidad de usuarios 2, 8 se muestran registrados en el mismo servidor de presencia 4 y suscritos en el mismo servidor de mensajería 10. Estos usuarios tienen un uso muy directo y por lo tanto eficiente del servidor de presencia 4, el servidor central 6 y el servidor de mensajería 10 para la utilización tanto de presencia como de mensajería. Se debería comprender sin embargo, que otros usuarios pueden estar registrados en otros servidores de presencia, otros servidores centrales y otros servidores de mensajería y continuar utilizando las ventajas de presencia y mensajería usados conjuntamente en la red IP. Por ejemplo, algunos de los usuarios de la primera pluralidad de usuarios 2 se muestran registrados en el servidor de presencia 4 pero suscritos en un segundo servidor de mensajería 12. De la misma manera, algunos de la segunda pluralidad de usuarios 8 se muestran suscritos en el servidor de mensajería 10 pero registrados en un segundo servidor de presencia 14. El segundo servidor de mensajería 12 y el segundo servidor de presencia 14 son capaces de comunicarse con un segundo servidor central 16 que por sí mismo es capaz de comunicar con el primer servidor central 6 de modo que todos los usuarios de la primera pluralidad 2 puedan comunicar con todos los usuarios de la segunda pluralidad 8 usando tanto los servicios de mensajería como de presencia disponibles en general y no restringidos a un área limitada. Los diversos servidores, así como los diversos usuarios mostrados en la Figura 1, se pueden distribuir en un área amplia. Los servidores y algunos de los usuarios pueden ser fijos, pero algunos de los usuarios pueden ser móviles. Por lo tanto es ventajoso para las finalidades de la presente invención que todos los usuarios sean capaces de contactar con los servicios ofrecidos por tales servidores de presencia y mensajería para la utilización solamente de esos servicios, así como otros servicios, tal como servicios basados en la localización que pueden actuar en conjunto tanto con el servidor de presencia como con servidor de mensajería o con ambos.

El servidor de presencia se puede hacer dentro de un servicio particularmente potente mediante el registro de la información de localización espacial de los usuarios que utilizan en él un protocolo de control en la capa de aplicación. Esto se mostrará en detalle a continuación.

Se debería comprender que los servicios de mensajería y presencia se pueden combinar entre sí o con el servidor central tanto individualmente como conjuntamente. Por ejemplo, la Figura 1 muestra el primer servidor central 6 y el primer servidor de mensajería 10 combinados en un único primer servidor 18 que combina las funciones de servidor central y de servidor de mensajería. De modo similar, la Figura 1 muestra el segundo servidor de mensajería 12 y el segundo servidor central 16 combinados en un único segundo servidor 20 que combina las funciones de un servidor de mensajería y un servidor central. Tales funciones pueden tener muchas formas diferentes que se describirán por medio de varios ejemplos. Por ejemplo, un usuario invitador 22 proporciona un mensaje de invitación sobre una línea de señal 24 al primer servidor central 6 invitando a un intercambio de contenido con un usuario invitado 26. En respuesta al mismo, el primer servidor central 6 proporciona una consulta de presencia sobre una línea 28 al primer servidor de presencia 4. El usuario 26, que ya se había registrado en el servidor de presencia 4 como se indica por la línea de conexión lógica 30, el primer servidor de presencia 4 devuelve la información de presencia con relación al usuario registrado 26 sobre la línea 28 al primer servidor central 6. El primer servidor central 6 es receptivo a la información de presencia sobre el usuario registrado 26 para su uso en la decisión de si el contenido propuesto para intercambio con el usuario 22 se debería enviar al usuario invitado 26, almacenar o rechazar. Si el primer servicio central decide que el contenido se debería enviar, el primer servidor central 6 hará que se envíe el contenido al usuario 26. Esto puede ser una transferencia directamente desde el usuario 22 al usuario 26 o puede ser a través de una ruta de transporte especificada.

Se debería comprender también que si el usuario invitado se ha registrado en el segundo servidor de presencia 14, tal como un usuario 32, entonces el primer servidor central 6 respondería al mensaje de invitación sobre la línea 24 mediante una comunicación con el segundo servidor central 16 sobre una línea 34. El segundo servidor central 16 proporcionaría una consulta de presencia sobre una línea 35 al segundo servidor de presencia 14 con la misma finalidad que la descrita previamente en conexión con la consulta sobre la línea 28 enviada al primer servidor de presencia 4. Teniendo múltiples servidores centrales y múltiples servidores de presencia a lo largo de muchas áreas diferentes, pueden estar disponibles en general varios servicios de presencia. En el ejemplo que se acaba de mencionar, tanto el primer servidor central 6 como el segundo servidor central 16 pueden tomar la decisión de si se debería enviar el contenido al usuario invitado 32 y se puede efectuar un control apropiado de la transferencia, almacenaje o rechazo desde cualquiera de ellos.

Ventajosamente, el mensaje de invitación sobre la línea 24, la consulta de presencia sobre la línea 28 o sobre la línea 35, se comunican de acuerdo con un protocolo de control de la capa de aplicación, tal como el protocolo de inicio de sesión (SIP) conocido por RFC 2543.

Además del uso de la presencia para decidir si el contenido se debería enviar al usuario invitado, almacenar o rechazar, es ventajoso de acuerdo con la presente invención utilizar un servicio de mensajería para la suscripción de los usuarios mostrada en la Figura 1 de tal manera que puedan proporcionar información sobre sus preferencias de

mensajería. En tal caso, por ejemplo, el primer servidor central 6 es receptivo al mensaje de invitación sobre la línea 24 para proporcionar también una consulta de suscripción sobre una línea de señal 36 al primer servidor de mensajería 10. Como se muestra en la Figura 1, el usuario invitado 26 tiene una conexión lógica 37 con el primer servidor de mensajería 10, por la que el usuario 26 se suscribió previamente a un servicio de mensajería proporcionado por el primer servidor de mensajería 10. En consecuencia, el primer servidor de mensajería 10 responde a la consulta de suscripción sobre la línea de 36 proporcionando una información de notificación en relación al servicio de suscripción suscrito por el usuario 26 indicativo de las preferencias del usuario. Éste podría incluir, por ejemplo, la notificación de un evento en el que el servidor central es receptivo a la información de notificación para su uso en la decisión de si el contenido se debería enviar al usuario invitado, almacenar o resaltar. De nuevo, la consulta de suscripción y la información de notificación se pueden intercambiar sobre la línea de señal 36 de acuerdo con un protocolo de control de aplicación, tal como el conocido SIP.

Presencia y localización espacial aplicadas al SIP

La información de presencia con relación a un usuario registrado puede incluir la información de localización espacial. Se describen a continuación los requisitos básicos para proporcionar la información de localización espacial de los dispositivos conectados a las redes IP cableadas e inalámbricas. De acuerdo con las enseñanzas de la presente invención, el Protocolo de Inicio de Sesión (SIP) se puede usar como Información de transporte y Localización Espacial (SLO) como el formato de datos insertado en el contenido útil SIP. Véase el documento IETF-draft-loughney-spatial-arch-00.txt titulado "Basic SLoP Architecture proposal" para una información detallada de la información que define una arquitectura SLoP. La descripción a continuación introduce la relación entre el SIP para el registro y transporte de los datos y la SLO como la estructura de información de localización. También se describe la integración de ambos elementos y la dependencia entre ellos. El resultado es una arquitectura común para proporcionar la información de localización de usuario a través de las redes IP. También se muestra la relación entre los elementos de red involucrados en la arquitectura y la funcionalidad global.

Como se ha mencionado anteriormente, el SIP es un protocolo de señalización en la capa de aplicación usado para la creación, modificación y finalización de sesiones multimedia entre diferentes partes. Se usa principalmente como un protocolo de control de llamada en la telefonía IP. La SLO es una estructura de datos definida para portar la información de localización de usuario. Define una estructura de datos que incluye la información de localización, requisitos de seguridad, mecanismos de política y entidades involucradas que forman una arquitectura completa. Se incluye en los requisitos para el intercambio de la estructura SLO entre entidades, una necesidad de unos medios de transporte, que deben ser escalables y seguros. En la presente invención el SIP usado como el protocolo de transporte para los datos SLO satisface estos requisitos.

La invención muestra como efectuar un servicio común para proporcionar la localización de usuario siguiendo la estructura SLO, usando el SIP como el mecanismo de transporte. Se desvela en el presente documento cómo las entidades SIP satisfacen los requisitos de la arquitectura SLO mientras proporcionan todos los requisitos necesarios para la definición SLO. Básicamente, la invención muestra cómo se pueden complementar la SLO y el SIP para realizar un servicio de localización de usuario global.

El protocolo SIP y todas las entidades involucradas en una sesión SIP son conocidos a partir de RFC 2543 pero se describirán brevemente a continuación. También se describen los mensajes SIP y los mecanismos proporcionados por el SIP para el direccionamiento e implementación de la movilidad del usuario.

A continuación se describe más abajo la SLO, en donde se explican los requisitos para la definición de una arquitectura común para proporcionar los datos SLO a través de redes IP. Se describe la estructura SLO y las diferentes partes del mensaje adoptadas para proporcionar una información de localización completa. Tercero, se ilustra cómo tanto la arquitectura SIP como la SLO se adaptan conjuntamente, el primero como el medio de transporte para la segunda. Los requisitos de la SLO se describen en el contexto de las funcionalidades SIP existentes. Finalmente, se muestran algunos escenarios básicos de cómo el SIP y la SLO se comportarán conjuntamente.

Introducción al SIP

El protocolo de inicio de sesión (SIP) es un protocolo de control en la capa de aplicación que puede establecer, modificar y finalizar sesiones o llamadas multimedia. El SIP se basa en texto, usando la codificación ISO 10646 en UTF-8 en todo él. Esto hace al SIP flexible y extensible y, dado que se usa para la iniciación de conferencias multimedia más que para el suministro de datos, la sobrecarga por un uso basado en texto no es significativa. La sintaxis del mensaje es similar a HTTP pero el SIP en su lugar puede portar la transacción usando tanto UDP como TCP. El mensaje puede ser tanto una Solicitud como una Respuesta y se crea siguiendo el formato de D. Crocker, "Standard for the format of ARPA Internet text messages", RFC 822, IETF, agosto de 1982.

Entidades SIP

Las entidades involucradas en una sesión SIP son el Agente del Usuario, el servidor Proxy, el servidor de Redireccionamiento, el servidor de Registro y el servidor de Localización.

El Agente de Usuario (UA) puede actuar como un cliente (UAC) que es una aplicación cliente que inicia una solicitud de SIP. El Agente de Usuario puede actuar también como servidor (UAS) que es una aplicación de servidor que contacta con el usuario cuando se recibe una solicitud SIP y se devuelve una respuesta en nombre del usuario.

- 5 El servidor de Proximidad es una entidad intermedia que se comporta como un cliente y un servidor simultáneamente. Puede interpretar y modificar la solicitud antes de su envío a otros servidores.

El servidor de Redireccionamiento es una entidad que recibe la solicitud y mapea la dirección a la que se dirigió inicialmente el mensaje en cero o más nuevas direcciones. A continuación, el cliente debería tratar de nuevo el uso de nuevas direcciones devueltas desde el servidor de Redireccionamiento para contactar al comunicante o a otro servidor de SIP que pueda manejar el mensaje en caso de requisitos especiales.

- 10 El servidor de Registro es un servidor que acepta el registro del usuario (mensaje REGISTRO) y que puede poner esta información a disposición a través del servidor de localización. El servidor de Localización es un elemento usado por los servidores de Redireccionamiento o Proximidad para obtener información sobre la localización posible del llamado. Puede incluir el servidor de Registro o cualquier protocolo de registro móvil disponible para esta finalidad.

15 Estructura del mensaje

El mensaje consiste en una línea de comienzo, uno o más campos de cabecera, una línea vacía (retorno del carro, avance de línea, CRLF) y un cuerpo opcional. Se muestran tres ejemplos en las Figuras 2, 3 y 4:

- 20 Básicamente, la línea de comienzo indica si es una Solicitud (INVITACIÓN, RECONOCIMIENTO, OPCIONES, DESPEDIDA, CANCELAR, REGISTRO, etc.) o una Respuesta (100 Informativa, 200 Éxito, 300 Redirección, 400 Error de cliente, 500 Error de servidor o 600 Fallo global).

La cabecera del mensaje se compone por múltiples cabeceras que indican, el Origen ("De:"), Destino ("A:"), Identificador de la Llamada ("ID de llamada:"), Secuencia del Mensaje ("Sec C:"), Vía de la Transacción ("Vía:"), longitud ("Longitud contenido:") y contenido ("Tipo-de-Contenido:") del cuerpo si se lleva en el mensaje.

- 25 Finalmente, el cuerpo del mensaje puede contener cualquier tipo de datos y su interpretación depende del tipo de mensaje. Generalmente el contenido del cuerpo puede contener una descripción de la sesión que sigue un formato específico tal como el Protocolo de Descripción de la Sesión (SDP), texto o scripts XML. El campo de cabecera del tipo de contenido da el tipo de medio del cuerpo del mensaje. Si el cuerpo tiene una codificación concreta se indica en el campo de cabecera "Codificación del contenido". La longitud del contenido se da en el campo de cabecera "Longitud del contenido".

30 Direccionamiento SIP

- 35 Las entidades seleccionadas por SIP son usuarios en alojamientos y se identifican por una URL SIP, véase T. Berners-Lee, R. Fielding y L. Masinter, "Uniform resource Locators (URL)", RFC 1738, IETF, diciembre de 1994. El URL toma una forma tal como *user@host* en donde la parte del usuario debe ser un nombre de usuario o un número teléfono y el alojamiento debería ser o bien un nombre de dominio o una dirección de red. Los URL del SIP se usan dentro de los mensajes SIP para indicar el originador (De), el destino actual en la línea de comienzo (Solicitud de URL) y el receptor final (A) de una solicitud SIP. Su interpretación sigue las guías de RFC 2396 "Uniform resource identifier (URI)", IETF, agosto de 1998, por T. Berners-Lee y col. y la sintaxis se describe usando la forma de Backus-Naur aumentada, usando caracteres reservados dentro de cualquier componente URI.

- 40 El URL del SIP se usa para la localización de un usuario en base a la búsqueda DNS SRV. El cliente solicita al servidor de DNS que incluye los registros de dirección, la dirección de destino. Si el DNS no devuelve ningún registro de dirección, significa que no se puede localizar al usuario final. Otros protocolos alternativos para la localización del usuario son finger (RFC 1288 D. Zimmerman, "The finger user information protocol", RFC 1288, IETF, diciembre de 1991), rwhois (RFC 2167 S. Williamson, y col. "Referral who is (rwhois) protocol v. 1.5." (RFC 2167, IETF 1997), LDAP (RFC 1777 W. Yeong y col. "Lightweight directory access protocol", RFC 1777, IETF, marzo de 1995) y otros protocolos basados en emisión múltiple disponibles para determinar si se puede alcanzar a un usuario. Es posible recibir una lista de localizaciones porque el usuario se ha podido registrar en varios alojamientos simultáneamente o porque el servidor de localización tiene una información no precisa. La forma de contactar con los usuarios en tales casos es probar cada una de las direcciones listadas hasta que se localiza al usuario.

Movilidad SIP

- 50 El SIP soporta de modo transparente el mapeado de nombres y servicios de redireccionado que le permiten una *movilidad personal*. La movilidad personal es la capacidad del usuario final para originar y recibir llamadas y acceder a servicios suscritos en cualquier terminal en cualquier localización y la capacidad de la red para identificar a los usuarios finales cuando se trasladan. La movilidad personal se basa en el uso de una identificación personal única basada en el URL del SIP mencionado anteriormente.

55

El SIP también soporta movilidad de terminal mediante solicitudes de sustitución y redireccionamiento a la localización actual en donde el usuario está adscrito. Este proceso se ha descrito brevemente anteriormente, en el que se usa los posibles URL donde se supone que el usuario puede ser alcanzado. Con el SIP el usuario puede registrar su localización actual o incluso el perfil de servicio requerido para la sesión. En el proceso de registro, el usuario puede proporcionar su identificación personal para conseguir una movilidad personal. Posteriormente, para la localización del usuario, el SIP necesita el servidor de localización, que puede usar el DNS, LDAP o cualquier otro mecanismo similar para la obtención de la dirección en donde se localiza el cliente.

SIP y SLO

El usuario se puede registrar temporalmente en el servidor del SIP local en donde estará adjunto durante un cierto período de tiempo. Ese registro sólo indica que el usuario está localizado en ese punto. Para los nuevos servicios que se conviertan en realizaciones (Servicios Basados en Localizaciones, Llamadas de Emergencia, etc.) el usuario necesita proporcionar una información más detallada de su situación. Usando el marco proporcionado por SIP, es más efectivo que en el mismo proceso de registro el usuario inserte más información sobre su localización.

Tal información y los requisitos para registrar esa información pueden seguir los requisitos de arquitectura definidos en el grupo de trabajo de la SLO. Véase Haitao Tang, "A Proposal for the Version-01 BOF Charter", 21 de febrero de 2000 situado en <http://www.nre.nokia.com/ip-location/charter-v01-00.txt>. Véase también IETF draft-tand-islif-reg-00.txt para "Problems and Requirements of Some IP Applications Based on SLO Information" por Tang y col., febrero de 2000.

Por ello, un simple registro SIP se convierte en más efectivo usando los datos de SLO como contenido útil. En esta forma, el identificador de usuario usado en el SIP (URL) se puede enlazar a una información más completa sobre la localización geográfica del usuario. Esta finalidad se puede efectuar mediante la adición del SLO como el tipo de contenido de SIP durante el registro. A continuación se proporcionan vías adicionales en relación con las entidades y condiciones para el uso de la estructura SLO apropiadamente.

Introducción a SLO

Un servicio de presencia puede proporcionar dirección a una información de Localización Espacial (SLO) de establecimiento, intercambio, y utilización de dispositivos IP. El objetivo es dejar a los dispositivos y aplicaciones direccionables por IP que sean capaces de establecer/adquirir y proporcionar los datos de localización espacial que se relacionan consigo mismos y otras partes cuando se permite. La seguridad es un requisito fundamental para muchas situaciones de intercambio de datos y servicios. Véase el documento de estatutos BOF por H. Tang. Las restricciones principales para cualquier implementación serán la seguridad y la escalabilidad.

Esto último es importante para proporcionar un servicio de confianza en general, en donde toda la información sea fiable. Para esta situación es importante establecer varios canales de seguridad entre la entidad que proporciona o solicita la información y la entidad que almacena y recupera esa información para otros servicios (emergencia, servicios personales, señalización, etc.).

Para obtener cierta seguridad en los medios de comunicación se pueden usar los protocolos de seguridad existentes y mecanismos de cifrado tales como 3DES, SSL, IPsec, PGP, etc. Dado que el SIP se elige para el transporte de la SLO, ya proporciona un canal seguro que usa el PGP.

El otro problema es la escalabilidad y es tan importante como la seguridad. En la arquitectura presente se han considerado todos los diversos escenarios así como la cantidad de información a intercambiar. Se ha analizado asimismo el tipo de datos intercambiados entre las posibles entidades en diferentes escenarios y sus actualizaciones. Obviamente, un usuario fijo sólo necesita proporcionar su localización una vez y estará permanentemente allí. Posteriormente se considera una entidad móvil (terminal IP, teléfono, etc.) y en este caso el usuario proporciona su localización inicial con la posibilidad de traslado espacial. Por ello, tras la notificación de la localización inicial se ha de hacer un seguimiento de sus movimientos, aunque las actualizaciones de la localización se solicitan periódicamente. La periodicidad de las actualizaciones depende de la velocidad del terminal, es decir, si el usuario está andando el periodo de actualización puede ser más largo que si el usuario se está moviendo con otros medios de locomoción (coche, bicicleta, etc.). Se han de tener en cuenta estas consideraciones para el tráfico generado en cada situación y el protocolo elegido para esas actualizaciones.

Arquitectura de localización espacial

A continuación se identifican los requisitos básicos para el diseño de la arquitectura básica. Se describen las principales características que debería contener el servicio en su diseño esencial. Se ha de considerar que en el mercado actual hay muchas posibilidades de proporcionar un servicio similar. Considerando que la intención de la presente invención es proporcionar una infraestructura común que se vaya a usar en todo el mundo y en dispositivos múltiples, ha de ser flexible, escalable y segura. Estas propiedades son cruciales para satisfacer los requisitos de varios proveedores de servicios y llegar a ser bien aceptada como el instrumento común para proporcionar localización espacial.

Representaciones de localización espacial

- 5 Soporta diferentes representaciones/expresiones de datos de localización. Por razones de interoperabilidad, tiene un sistema de localización absoluto como el formato soportado por todos los comunicantes del servicio. Lista todos los sistemas distintos de localización absolutos con sus formatos de datos, que pueden estar soportados por los elementos del servicio en una forma opcional. También da soporte a localizaciones descriptivas en donde no se define sintaxis y norma en el alcance de la arquitectura actual.

Mecanismo de negociación de representación

- 10 Hay provisto un mecanismo de negociación de la representación. El mecanismo soporta la selección del sistema de localización y del formato de datos deseado entre dos comunicantes. La negociación de la localización descriptiva se considera durante el registro de la localización. Una vez que el usuario registra su localización, indicará el formato de ese dato. En el caso de que una tercera parte necesite solicitar esa información será notificada acerca del formato de información de la localización (esos formatos serán especificados previamente y notificados públicamente).

Mecanismos de seguridad

- 15 Hay un mecanismo de autenticación seleccionado/definido entre dos comunicantes SLoP, para garantizar la integridad/autenticidad/accesibilidad (por ejemplo, no interferencias ni ciertos ataques DOS) de las partes involucradas. El uso de los mecanismos de autenticación y/o cifrado será ajustable por el punto final de servicio (el usuario puede habilitar o inhabilitar el uso de los mecanismos). Éste se realiza por sesión o por punto final. El diseño primario para la seguridad en la arquitectura es punto a punto.

Mecanismos de política

- 20 Hay un lenguaje de especificación de política seleccionado/definido para especificación de las varias políticas que son relevantes para la arquitectura. Se define un PIB para todos los comunicantes. La instancia de política para un objetivo debería estar disponible para el servidor que representa el objetivo, mientras que la instancia de política dice como servirá un servidor a la localización espacial del objetivo.

Mecanismo de descubrimiento del servidor

- 25 Hay dos aspectos de este asunto. El mecanismo de descubrimiento para que el objetivo encuentre el servidor en donde puede registrar sus datos de SLO. En segundo lugar, hay un mecanismo de descubrimiento seleccionado/definido para un cliente para hallar el servidor apropiado para un objetivo dado cuando es necesario.

- 30 El descubrimiento de servidor es un aspecto importante para los problemas de escalabilidad. Hay diferentes enfoques para obtener el servidor de localización más cercano o su equivalente. La primera elección es usar una dirección preconfigurada estática del servidor en donde está suscrito el usuario. La elección opcional sería usar mensajes de difusión múltiple para localizar el servidor de localización más cercano para establecer la conexión inicial. Hay muchas alternativas para alcanzar un mecanismo de emisión múltiple eficiente (Hussein F. Salama y col. "Evaluation of Multicast Routing Algorithms for Real Time Communication on High-Speed Networks", N.C. State University.) Tras ser localizado, el servidor presentará un mecanismo de política para la autorización del usuario para continuar con el servicio.

35 En el caso de uso del SIP como el protocolo de control, ya proporciona un mecanismo de descubrimiento del servidor para ambos casos, es decir para el Objetivo y el Cliente que tratan de contactar con el Servidor de Localización bien para el registro o bien para obtener información de localización.

Mecanismo de transmisión y fiabilidad

- 40 El diseño del mecanismo de fiabilidad queda afectado por el protocolo de transporte debajo de la arquitectura de Localización Espacial. Varios protocolos de transporte tienen diferentes niveles de fiabilidad. Si se selecciona TCP, no hay necesidad de tener este mecanismo extra. Sin embargo, TCP parece demasiado "pesado" para algunos servicios. Dado que este servicio debe ser independiente del tipo de comunicación y se debería garantizar la comunicación, el protocolo de transporte cuidará de este asunto. El protocolo de transporte también ha de asegurar la seguridad para los diferentes mecanismos de acuerdo con el dispositivo de usuario y el proveedor de servicio. En este punto el SIP usa UDP o TCP independientemente en base a los requisitos del usuario.

Mecanismo de codificación del mensaje

- 50 Hay un mecanismo de codificación seleccionado/definido para la codificación/decodificación de todos los mensajes. Todos los usuarios deben soportar el mecanismo de codificación.
- Los usuarios soportan el mecanismo de codificación básico seleccionado como por defecto para todas las transacciones. Se define un esquema estándar basado en una cabecera y un cuerpo de mensaje. Ambos se codifican usando un lenguaje basado en texto tal como XML. En la cabecera se definen los campos predeterminados necesarios para la transacción del protocolo que incluye la información de cifrado y en el cuerpo se

inserta la información de acuerdo con el mensaje específico. El uso de un lenguaje extensible permite extensiones posteriores con nuevas cabeceras o características. De esta forma tiene la fiabilidad de la codificación del formato XML y la extensibilidad del lenguaje basado en texto. En el caso concreto de que el cuerpo esté portando información de localización se puede insertar usando el lenguaje de marcado geográfico (GML) (Geography by Markup Language (GML) v1.0 OGC Document Number: 00-029.12 de mayo de 2000. <http://www.opengis.org/techno/specs/00-029/GML.html>. La denominación propuesta se basa en los identificadores de recursos uniformes (URI) (véase RFC 2396) y sigue la sintaxis definida para la ID de Información Objetivo (TID) y la ID de Acceso de registros Objetivo (TAD) en Tang y co, "Serving Spatial Information over Internet" y en el "Target Naming Scheme" establecido en IETF draft-tangspatial-target-00.txt. Estas definiciones componen el identificador para datos persistentes (TID) y finalidades de itinerancia entre los servidores de Localización (TAD). Preferiblemente, tanto el TID como el TAD estarán presentes en las cabeceras de todos los mensajes del SL.

Adicionalmente, el mensaje contendrá preferiblemente la representación de Localización Especial descrita y los atributos descritos a continuación.

Entidades SLO

Estas definiciones se basan en los requisitos de arquitectura identificados para proporcionar información SLO.

Cliente es el elemento que solicita la Localización Física de otro elemento (denominado Objetivo). Puede ser o bien un dispositivo de usuario que solicita la localización de otro terminal o una aplicación que necesita obtener los datos de la localización del usuario para proporcionar servicios adicionales (servicios Basados en la Localización, notificaciones de Emergencia, etc.). El Cliente se comporta como un Objetivo cuando está proporcionando la información de SL.

Objetivo es el elemento cuya localización física solicita el Cliente. Puede tener capacidades para resolver su localización o no. En el caso del equipo más simple, enviará a su servidor la estructura de localización espacial dentro de la información geográfica. En este caso la estructura de datos incluye los requisitos del usuario e información básica y dentro de qué datos se incluyen los derechos para servidor para la resolución de la localización Objetivo y rellenado de la estructura de Localización Espacial.

Interfaz de Usuario (UI) es lo que el usuario utiliza para interactuar con el servidor de localización (LPS). El UI se implementa típicamente como una parte integral de un terminal móvil o como una aplicación sobre un servidor WEB y/o WAP que pertenece a un proveedor de red. Por lo tanto, el UI se implementa físicamente en el llamado Objetivo y en base a la nomenclatura del SIP será un Agente de Usuario SIP.

El Servidor de Localización (LS) almacena y distribuye la información de localización relacionada con un terminal específico. Se implementa típicamente en el terminal o en un servidor en un lugar arbitrario, no necesariamente propiedad de un proveedor de red. El servidor de localización interactúa directamente con la interfaz de usuario. Por ello, el LS recibirá la información de localización y presumiblemente usará protocolos bien formados y fiables para proporcionar esa información al Cliente en caso de que el Objetivo haya especificado este requisito cuando se almacenó su información de localización en el LS. De la misma manera la información de localización se proporciona directamente al Cliente desde el LS.

La función de posicionamiento (PF) determina la localización de un terminal dado. Típicamente es una función integral del terminal, por ejemplo en base al GPS, a Servicios de Información de Localización (LIS) (M. korkea-aho "Some Scenarios for an ISL Architecture" 10 de marzo de 2000, IETF draft-korkea-aho-islscenarios-00.txt) o a Sistema de Posicionamiento Local (LPS) (J.M. Polk y col. "Spatial Location Protocol Location Server Authentication" 10 de marzo de 2000, IETF draft-polk-slploc-auth-server-00.txt) proporcionado por un Proveedor de Red, por ejemplo basado en la información de la célula de radio o un mecanismo de triangulación. Puede estar localizado en el Objetivo (UA de SIP) o en el LS si el Objetivo no tiene estas capacidades.

El Usuario de Información (IU) es típicamente un servicio de valor añadido, un servicio de salvamento que pueda acceder a la información de localización del usuario previa autenticación. Se comporta como cliente cuando está accediendo al LA para saber la información de localización del usuario que se ha solicitado por cualquier elemento externo tal como un enrutador, protocolo de señalización, servicio de salvamento, etc. Y el IU se comportará también como una entidad de servidor cuando activa dicho interfaz para el acceso a servicios de Directorio o instalaciones locales (taxis, restaurantes, etc.). En este caso el IU conocerá la localización del usuario a través del LA y cuidará de solicitar los servicios necesitados por el usuario.

Estructura de los mensajes

El formato de los mensajes se define de acuerdo con las necesidades de localización. La parte importante del mensaje corresponde a la información de localización, que se puede definir de diferentes formas dependiendo del dispositivo. Se mencionó en la sección de Requisitos que esta información sería negociada de acuerdo con las capacidades del dispositivo del usuario. El formato del mensaje se basa en una cabecera y un cuerpo. Por ello, la cabecera contendrá los datos por omisión o seguridad y otras propiedades. El cuerpo del mensaje llevará la información de localización o cualquier otro dato. Si el dispositivo no tiene capacidades para el cálculo de la

localización, entonces el cuerpo puede estar vacío y el mensaje es sólo un receptor de las demandas del usuario acerca de su información. Los campos principales insertados en la cabecera podrían contener los datos mostrados en la Figura 5.

5 Aparte de estos campos es necesario considerar también otros para realizar el contrato inicial, actualizar los cambios y el resto del comportamiento del protocolo.

La Figura 6 representa la sintaxis propuesta en base a la codificación del mensaje presentada en la sección anterior que describe la arquitectura de localización espacial. Contiene las partes de cabecera y cuerpo, en donde el primero contiene el identificador del objetivo y los datos esenciales de la estructura y el último incluye los datos de localización y atributos identificados en esta sección.

10 Arquitectura de Localización espacial usando SIP

En base a los requisitos y elementos de arquitectura ilustrados se desvela una arquitectura en base al protocolo de señalización SIP. Se elige el SIP como protocolo de transporte dado que puede trabajar tanto con TCP como con UDP. Consecuentemente este enfoque incorporará mecanismos de seguridad y fiabilidad. En esta divulgación el formato de datos SLO será parte del contenido útil del protocolo y se indicará en una de las cabeceras del protocolo que está aportando los datos SL.

Representación de la localización espacial

En consecuencia, la información de SLO será parte del cuerpo del mensaje SIP. Este cuerpo contendrá el mensaje de localización con la estructura y atributos definidos anteriormente. El SIP se usa como un mecanismo de transporte simple que se extenderá bien dado que se ha adoptado como protocolo de Control de Llamadas para la Señalización de Telefonía IP. El contenido del cuerpo en el mensaje SIP se indica en la cabecera de "Tipo de contenido". El IANA permite el registro de nuevos tipos de contenidos y se indicarían en una forma similar a "Tipo-de-Contenido: aplicación/SLO". El SIP permite el cifrado del contenido útil completo en caso de que se requiera una alta tasa de seguridad.

25 La Figura 7A ilustra un ejemplo de un registro SIP en donde está usando el SLO como contenido útil. Después de recibir el registro SIP sobre la línea 70, el Proxy SIP 72 realiza el registro y comprueba los datos SLO y si está presente, está almacenado en una base de datos 74 que puede ser el servidor de Localización SIP y desde ahí se puede recuperar si es necesario para ejecutar cualquier servicio suplementario.

Mecanismo de seguridad

30 El protocolo SIP ha definido varios enfoques de seguridad basado en punto a punto y salto a salto. Los servidores SIP pueden requerir la autenticación del usuario previa a cualquier acceso. La arquitectura SLO descansará en el protocolo de transporte para este asunto, el usuario sólo indica la tasa de seguridad designada y el SIP cuidará de ello. Los servidores habilitados para SIP autenticarán y cifrarán los datos de acuerdo con las restricciones definidas por el usuario.

35 Si el usuario trata de registrarse y no le está permitido el registrador devolverá una respuesta "401 No autorizado". Indica que el registro requiere una autorización previa usando cualquiera de los mecanismos definidos en el SIP. El usuario ha de reenviar de nuevo la solicitud incluyendo la cabecera "Autorización" donde se añade el credencial que contiene la información de autenticación.

40 La seguridad del SIP se implementa básicamente usando dos enfoques, usando esquemas básicos y de compendio HTTP, J. Franks y col. "HTTP authentication: Basic and digest access authentication," RFC 2617, IETF, junio de 1999 así como usando PGP J. Callas y col. "Open PGP message format" RFC 2440, IETF, noviembre de 1998.

El primer enfoque usa las cabeceras "Proxy-Autorización", "WWW-Autenticado" y "Autorización" en varios mensajes en base al RFC 2617. El registrador devolverá una respuesta 401 que indica que necesita estar autenticado. Entonces el usuario devuelve el registro que incluye la cabecera "Autorización" con la información relevante.

45 El último enfoque usa la sintaxis en base al mecanismo de autenticación PGP. Se basa en el modelo de que el cliente se autentifica a sí mismo con una solicitud firmada con la clave privada del cliente. El servidor puede asegurar entonces el origen de la solicitud si tiene acceso a la clave pública que debería estar firmada por una tercera parte de confianza. Los algoritmos de este esquema se basan en RFC 2440. Las cabeceras involucradas en la transacción son la "Autorización", "WWW-Autenticado" y "Clave-respuesta" para proporcionar la clave pública del usuario extraída del llavero PGP.

Descubrimiento del servidor

En este punto el SIP proporciona el mecanismo de descubrimiento del servidor usando la configuración predefinida con las consultas de emisión múltiple a un servidor DHCP. Cuando se inicia el terminal de usuario obtendrá inmediatamente la dirección de su servidor SIP más cercano. Otra característica de descubrimiento también en el

protocolo SIP es resolver la dirección del servidor SIP más cercano usando los registros SRV desde el DNS.

Una vez que el usuario tiene la dirección del servidor puede enviar el mensaje de REGISTRO SIP que contiene la información SL en su cuerpo. El servidor de Registro que se comporta como el Servidor de Autenticación (AUS) requerido en la arquitectura SLO autentifica el mensaje inicial. Si el servidor de SIP contactado no es un Servidor de Localización (LS) el mensaje tiene una cabecera específica para el descubrimiento del servidor de localización. Estará indicado en la cabecera de SIP "Requiere" enviada en el mensaje REGISTRO. Por ello, para indicación de que el mensaje entrante contiene Información Espacial y necesita ser procesado por un Servidor de Localización, el REGISTRO SIP tendrá la siguiente cabecera: "Requiere: servidor SLO". Esto indica que el usuario está registrando su localización y necesita un Servidor de Localización Espacial para manejar este dato. En caso de que el servidor contactado no tenga capacidades de SL el usuario recibirá una respuesta de vuelta en donde la cabecera "Contacto:" incluye la dirección de un nuevo servidor de SIP, que puede gestionar ese mensaje. Un ejemplo sería como este: "Contacto: slo-server.nokia.com".

Una vez que el usuario haya contactado con el registro de SIP el cliente debería comenzar el registro en el que incluirá el SLO en el contenido útil.

Después de esto, el usuario conoce la dirección del Registrador donde pueden enviar la solicitud, que incluye los datos de SLO. Ahora, es necesario establecer una transacción segura para proporcionar la información al Registrador. El SIP manejará la seguridad de las transacciones durante el registro en base al mecanismo descrito en la sección anterior "Mecanismo de seguridad".

El proceso completo se representa en la Figura 7B que muestra las diferentes etapas hasta que tiene éxito el registro. Los mensajes 1 y 2 son justamente el descubrimiento del servidor SIP independientemente de si es capaz de SLO o no. Los mensajes 3 y 4 se envían cuando el usuario está tratando de registrar la información SLO en el Registrador de SIP pero desafortunadamente, en el ejemplo ilustrado, no tiene capacidades de SLO. En su lugar, la respuesta 4 indica la localización del servidor SIP más cercano que puede manejar un mensaje SLO. Finalmente, en los mensajes 5 y 6 el registro se consigue y los datos de SLO se almacenan en el servidor de SLO que puede ser accedido por cualquier otro servicio que use SIP o cualquier otro Protocolo de Acceso a Directorio.

Negociación de la representación

Tras haber sido contactado el Servidor de Localización Espacial realiza una negociación de representación. La arquitectura SLO tiene un formato por omisión pero debería comprender otros formatos que se hayan negociado previamente. En caso de que la información recibida no se puede interpretar o provenga de un dispositivo no IP, el servidor SLO necesitará contactar con la Pasarela de Localización Espacial (SLG) para producir la información recibida en el contenido útil de SIP. Finalmente, si no hay forma de que el servidor SLO maneje el mensaje, devolverá un mensaje SIP de error como: "SIP/2.0 501 No implementado" o "SIP/2.0 503 Servicio no disponible".

Dado que el SLO es un servicio nuevo, continúa existiendo la posibilidad de que el Registrador de SIP contactado no soporte esta característica. Hay dos posibilidades, la primera es tratar de registrarse con el Registrador de SIP más cercano y esperar a su respuesta y la otra solución sería usar el mensaje OPCIONES para consultar previamente las capacidades del Registrador. En el primer caso, si el Registrador puede manejar un mensaje SLO el registro tendrá éxito, en caso contrario el Agente de Usuario recibe una respuesta 300 con la dirección de un SLO capacitado como Registrador SIP. En el otro caso, el Agente de Usuario necesita negociar esta capacidad por el Registrador. El cliente enviará un mensaje OPCIONES al Registrador para indicación de que necesita un Registrador en base a SLO. El Registrador puede devolver una respuesta 200 OK, que significa que puede manejar este tipo de registro. En caso contrario, el Registrador devuelve una respuesta 300 Múltiples Opciones, que significa que se puede acceder a las capacidades requeridas a través de proxy dado en el campo "Contacto:".

Escenarios

Los escenarios se pueden visualizar tal como se describen en IETF draft-polk-slp-loc-auth-server-00.txt titulado "ISL Architectural Considerations" 8 de marzo de 2000 por S. Nyckalgard y J. Loaghtney. Básicamente, los dispositivos basados en SIP han de ser diferenciados de los aparatos IP generales.

En primer lugar se necesita una búsqueda para hallar el servidor al que se debe dirigir el mensaje. Como se ha mencionado anteriormente, el Objetivo puede usar un mecanismo de emisión múltiple para buscar el Servidor de Localización más cercano a su localización actual. En caso de un dispositivo habilitado para SIP usará el mecanismo de descubrimiento del servidor SIP ya descrito.

El Objetivo es por omisión un dispositivo basado en IP y durante esta fase el Objetivo proporcionará su nueva dirección asignada y sus capacidades de dispositivo al Servidor de Localización. El LS responderá al Objetivo o bien con su propia dirección en caso de que satisfaga los requisitos del dispositivo de usuario o le devolverá la dirección del Servidor Proxy de Localización que será capaz de traducir los requisitos del objetivo al formato de mensaje estándar del protocolo. El Servidor de Localización o Servidor Proxy de Localización (LPS) será por ello la entidad que cuidará de este primer contacto con el Objetivo de acuerdo con la decisión tomada después de la fase de Negociación de Representación.

Si el servidor Proxy cuida de esta fase será necesario mantener un registro (caché) del Servidor de Localización específico que tiene el perfil de usuario. Esos registros se actualizarán y replicarán entre los diferentes Proxy para estar al tanto de los respectivos LS que manejan la información de cada Objetivo (Autorización, facturación, etc.). Véase J. Luciani y col., "Server Cach Synchronization Protocol (SCSP)" IETF RFC 2334, abril de 1998.

- 5 Después de que el LPS haya descubierto el Objetivo comenzará la fase de Negociación. Por un lado el Objetivo proporcionará su identificación y requisitos de servicio al LPS y por otro lado el Proxy (basado en su tabla de registro) contactará con el Servidor de Localización que maneja la información privada de ese usuario. El LPS recibirá de vuelta una aceptación del LS o no, en caso de denegación del servicio para ese usuario.

- 10 Adicionalmente, tras la fase de negociación el LS continuará el procedimiento de servicio a través del Proxy o directamente. Este proceso se ha descrito ya en la sección anterior para los dispositivos habilitados para SIP.

- 15 Anteriormente se identificó la necesidad de mantener una tabla de registro en el LPS para el contacto con el LS al que ese usuario se ha suscrito. Las etapas básicas serían Descubrimiento del Servicio, Negociación del Servicio y Ajuste del Mecanismo de Política. La última etapa se realiza después de que o bien el LS o bien el LPS hayan confiado en el Objetivo. En este estado el Objetivo ajusta la política que se ejecutará con cualquier Cliente que trate de solicitar su información de localización. Esto significa que el Objetivo puede hacer su información globalmente disponible o totalmente privada. En el último caso será necesario establecer un canal seguro para la transmisión de su información entre el Cliente que solicita la información y el servidor. Sin embargo, si el Objetivo ha designado la información como totalmente pública cualquier Cliente no confirmado puede solicitar su información de localización.

Escenario de Itinerancia

- 20 Este escenario es similar al escenario básico con la diferencia de que el usuario está en itinerancia en una localización diferente. Esto significa que el usuario ya está registrado en su servidor de SL local y ha asignado un ID de Acceso al registro Objetivo (TAD) para ese objetivo. Por ello, el servidor local ha almacenado tanto el ID de información del Objetivo (TID) como el TAD. Puede haber más de un TAD para un TID dado. El TAD puede depender del tiempo o del lugar y está adjunto sólo temporalmente al servidor visitado. Ahora, el objetivo trasladado a una localización diferente va a actualizar sus datos. El proceso es el mismo pero ahora el mensaje SIP porta la estructura SL en el contenido útil incluyendo el TAD en lugar del TID. Este es el TAD por defecto asignado al objetivo por el servidor local y sirve como registro por defecto que accede al ID. En situaciones de itinerancia, el servidor de localización visitado se convierte en el servidor de localización actual que representa al objetivo. Después de la autenticación y la negociación de representación el servidor visitado asigna un TAD temporal para la objetivo e informa a su servidor de localización por defecto del TAD temporal actual del objetivo. El servidor de localización por defecto del objetivo puede ligar entonces los dos TAD (el predeterminado y el temporal).
- 30

Adicionalmente, para encontrar el punto actual de fijación del Objetivo, se usará el TAD que indica la dirección asignada. El TAD apuntará inequívocamente a la localización actual del Objetivo.

Conclusiones sobre la Aplicación de Información de Localización Espacial al SIP

- 35 La inclusión de los datos de la SLO como parte del contenido útil SIP durante el registro se ha desvelado anteriormente. La colocación de este nuevo elemento en la transacción SIP mejora el servidor de localización comparado con técnicas anteriores. El usuario que se ha registrado usando los datos SLO hace disponible su localización para otros servicios y también especifica cómo puede ser alcanzada. Consecuentemente, una vez que servidor de Localización obtiene la información del usuario en base a los datos SLO, puede enviar los mensajes directamente a la situación correcta en la que está localizado el usuario en ese momento. Evita la información redundante recibida del servidor de localización cuando el usuario esté registrado en varios lugares. El Comunicante evita el envío de múltiples solicitudes tratando de contactar con el usuario.
- 40

- 45 La información de localización del usuario se puede almacenar en diferentes tipos de bases de datos para estar disponible globalmente para otras finalidades. Se accederá a esas bases de datos usando otro procedimiento que requerirá autorización y una Denegación de servicio en caso de que el usuario en los datos de SLO lo haya definido así. El acceso a los datos se puede realizar dependiendo de las bases de datos usadas pero está abierta a la decisión de los implementadores. Esta parte del servicio se considera también en los requisitos SLO como la transacción entre el servidor de SLO o proxy y el Cliente SLO. Una solución adecuada sería usar el SIP también para esta finalidad, extendiendo el protocolo con algunas cabeceras específicas para la solicitud de la información de localización del usuario.
- 50

Adicionalmente, éste nuevo servicio deja abierta el marco para el desarrollo de nuevos servicios basados en la localización y otros futuros. Los clientes SLO accederán a los datos para proporcionar esos servicios basados en la localización.

- 55 En resumen, esta divulgación establece los procedimientos para el registro de la solicitud de información SLO en bases de datos globales usando el SIP.

Una implementación de la mensajería instantánea y presencia usando el SIP

Introducción

La siguiente realización implementa la Mensajería Instantánea y la Presencia usando un protocolo SIP para varias realizaciones que incluyen una realización de telecomunicaciones móviles particularmente adecuada pero no necesariamente restringida a los servicios de generaciones siguientes.

El SIP se define como el protocolo de señalización para redes UMTS en la Función de Control del Estado de Llamada (CSCF), que es parte del elemento de la red Servidor de Procesamiento de Llamadas (CPS). La intención de lo que sigue es proporcionar una descripción completa del SIP como el protocolo de señalización para el control de llamadas entre CSCF dentro del Proceso de Mensajería y Presencia. El entorno es la arquitectura de referencia 3G.IP y la edición 2000 del 3GPP arquitectura All-IP, que se representa la Figura 7C.

Los servicios de señalización SIP se implementan en el subsistema de Señalización de Gestión de Llamada y Movilidad (CMS) en el CPS de acuerdo con la Figura 7B.

SERVIDOR DE PRESENCIA

La generación 3GPP está usando el SIP para señalización pero tiene que manejarse con los sistemas existentes. La nueva arquitectura ha de soportar la herencia de otros servicios previos tales como SMS y tiene que mejorarlos con nuevas características.

La base del servicio de presencia es en primer lugar definir una estructura de datos común en la que se especifique la información de localización del usuario. Se prefiere XML como el marco para esa finalidad. Se presenta un buen ejemplo en el borrador "An XML Format for Presence Buddy Lists" por Rosenberg y col. en draft-rosenberg-impp-buddylist-00.txt. Dentro del mismo contexto el IETF está trabajando en la definición de un formato específico para la información de localización espacial por J. Loughney y J. Costa-Requena "Basic SloP Architecture Proposal", IETF draft-loughney-spatial-arch-00.txt.

Esta parte de la divulgación se enfoca principalmente en el segundo enfoque que se diseña para llevar una información de localización basada en coordenadas, ID de célula del móvil en cada momento y otros similares. Ese formato proporciona un soporte general para la inserción de los datos de usuario e información adicional para alcanzarlo.

Como se ha explicado anteriormente, en esta divulgación se propone usar el SIP como protocolo de transporte para llevar ese formato de datos o bien en XML o bien en otro formato concreto.

Para esa finalidad se muestra el uso de un nuevo atributo Tipo-de-Contenido para la indicación de que el SIP contiene esa información en el contenido útil tal como:

Tipo-de-contenido: Info-de-presencia/TID

Lo que sigue es un ejemplo que usa un servicio de presencia. Se describe una situación específica en la que el usuario registra su información para estar disponible para otro usuario o hacer uso de los servicios basados en la localización. Los ejemplos muestran cómo se realiza el registro completo y el mecanismo de seguridad proporcionado por el SIP para soporte de la privacidad del usuario.

Descripción de la figura:

Con referencia ahora a la Figura 8 se muestra un registro de usuario con datos de localización:

El usuario (Quex) registró su información en el servidor de presencia a través del CSCF de SIP. Por ello, el servidor de presencia tiene conocimiento completo de ese usuario. Sabe que está registrado y que su información espacial está disponible si es necesario para los Servicios Basados en la Localización.

El UA del SIP utiliza el formato de los datos de localización denominado TID (o cualquier otro formato basado en XML) y el Tipo-de-Contenido indicará el tipo de formato que se lleva en el contenido útil.

El usuario indica en la estructura TID el nivel de publicidad que desea dar a esa información. En este caso no permitirá a otro usuario acceder a esa información. Por ello, este dato se mantiene oculto en base a las especificaciones del usuario. En caso de servicios de emergencia este dato se recupera sin ningún obstáculo con la autorización previa. Un ejemplo de formato de datos para información de localización se presenta en el Apéndice 3.

Después de este proceso el SIP recibirá esa información y registrará la localización del usuario. En este punto el registrador de SIP necesitará interactuar con el HSS (véase la Figura 9) o almacenar este dato y hacerlo globalmente disponible para otras redes. En la siguiente sección se muestran las diferentes entidades para almacenamiento de la información de localización en UMTS.

Ahora, el usuario se registra y el sistema conoce donde está localizado. Si hay otro usuario tratando de encontrar dónde está, el servidor de presencia o el CSCF SIP responsable volverá a intentar esa información. Esa solicitud se autentifica usando el mecanismo de seguridad SIP. Será recuperada la localización del usuario si el usuario dio derechos para que este nuevo usuario lo hiciera. Esto se especificó durante el registro del usuario usando los atributos del mensaje descritos en el Apéndice 4.

Información de localización de usuario en UMTS

La Figura 9 muestra un modelo de arquitectura de Red GPP. Las entidades principales a considerar se refieren particularmente a las transacciones de movilidad como sigue:

Gestor de movilidad. Asume la Gestión del Traspaso entre redes. Interactúa con el Servidor de Localización y con el Registrador de Suscripción Local.

Gestor de sesión (SM). El SM establece y gestiona las Sesiones, el Estado y los traspasos por medio y a través de varias redes, lleva los recursos requeridos para llamada/sesión tal como anuncios, puenteado, transferencias, etc. Recoge los estados de la sesión y la información de fin de Estado y la pasa al Agente de Servicio. También comunica con el Gestor de Recursos para una funcionalidad de control de la pasarela dentro de varias pasarelas dependientes del medio. Adicionalmente, se incluyen las siguientes funciones: enrutado de llamadas, gestión de sesión y estado, traducción de direcciones de consulta, traducción del protocolo de señalización entre el control de llamadas heredadas y el protocolo de control de llamadas de red IP (por ejemplo, ISUP) y el protocolo de control IP (por ejemplo, SIP, H.323).

Pasarelas de Señalización de Itinerancia. La Pasarela de Señalización de Itinerancia asume la transformación de la señalización de paquetes (SIP, MGCP, etc.) a y desde la señalización ISUP y TCAP en las redes de circuitos conmutados. Se entrelaza con el Gestor de Sesión. La GW SIG proporciona una interfaz entre todas las redes IP y la red SS7 de señalización heredada.

Servidor de localización. El servidor de localización proporciona un registro de la Información de Localización, Centro de Posicionamiento Móvil (MPC) (información GPS, de triangulación y célula/sector). También incluye una interfaz con el PDE (Equipo de Determinación de la Posición) para recoger la información GPS (por ejemplo WAG, agente extranjero, dirección IF, etc.). El LS contiene también un Marcador de Registro para indicar si el abonado o dispositivo se ha registrado en una o más redes específicamente definidas. El servidor de localización actualiza la Base de Datos de Localización en el HSS.

Registro del Equipos. El Registro de Equipos es una base de datos de información de equipos, que incluye pero sin limitarse a un registro de equipos robado. El Registro de Equipo es parte del Servicio de Abonado Local.

Registrador de Localización Local. El Registrador de Localización Local contiene los datos del perfil de abonado (recursos/derechos utilizables en servicios entre dominios, de servicios de prioridad IP, SLA, etc.) que se pueden referenciar en tiempo real o descargar en un registro.

A partir de estas definiciones el elemento más relevante es el Servidor de Abonado Local (HSS) donde se almacenan los datos de los usuarios. El LS recibe y recupera la información directamente del HSS. El LS está también estrechamente conectado con el Gestor de Movilidad, que es parte de la Función de Control del Estado de Llamadas (CSCF). Por ello, el CSCF recibirá el registro y lo recuperará en el HSS a través del LS. En el LS se puede realizar algún tipo de traducción en caso de diferentes formatos de localización. Si se requiere compatibilidad hacia atrás, es necesario extraer la información de la estructura TID y crear las estructuras normales usadas en el HSS. Esta clase de adaptación se realizará de acuerdo con las diferentes implementaciones.

Varias alternativas de implementación (PS)

Se usa el SIP como la señalización para el control de llamadas entre CSCF para servicios de Presencia y Mensajería. El contenido útil SIP es la parte más adecuada del mensaje para el transporte de esa información. El SIP facilita la privacidad de los datos en el sentido de que se puede cifrar el contenido útil completo.

La idea básica de este enfoque es permitir la interoperatividad hacia atrás con todos los sistemas de redes mejoradas SIP. Por ello, para evitar enormes cambios en las implementaciones existentes se decidió definir esta nueva característica usando mecanismos ya existentes. El SIP por sí mismo proporciona esta característica utilizando las cabeceras para finalidades específicas. Esto da una gran flexibilidad. El Agente de Usuario definirá esta información que se inserta en el registro inicial dentro del cuerpo de SIP. De esta forma el paquete está completamente cifrado de punto a punto y no hay necesidad de ningún esfuerzo de normalización para la definición de cualquier nueva cabecera específica para esta finalidad.

La cabecera de Tipo-de-Contenido SIP especifica el contenido del cuerpo del mensaje. En este caso indicará que está llevando información de presencia usando TID o cualquier otro formato basado en XML (Ejemplo: "Tipo-de-

Contenido: presencia/TID”).

Hay muchas posibilidades:

Tipo-de-contenido: presencia/TID. Como se muestra en la Figura 2, el usuario proporciona la información de localización siguiendo el formato TID (Apéndice 3).

5 **Tipo-de-contenido: presencia/GML-GIS.** El usuario está usando otro formato que sigue la estructura GIS.

Tipo-de-contenido: presencia. En este caso el usuario está indicando que desea hacer su presencia públicamente disponible y el Servidor rellenará esta información en base a su perfil de servicio. Esto está indicado para pequeños dispositivos en los que no se puede implementar un sistema completo para el cálculo del posicionamiento (GPS) y el Servidor lo hará por él. El Servidor puede usar cualquier sistema disponible (ID de célula) para resolver la localización del usuario y rellenar los datos del usuario.

Ejemplos de flujo del mensaje de Presencia

A continuación se describen varios casos de usuarios y flujos de mensajes para ilustración del servicio de presencia de acuerdo con la presente invención.

15 Cuando llega una nueva llamada al Gestor de Sesión este desnudará el paquete para comprobar las cabeceras SIP. En el caso de que sea un mensaje de registro será notificado al Gestor de Movilidad. El MM comprobará si el tipo de contenido es igual a “presencia/???”. En este caso el MM obtendrá el paquete SIP y comprobará si contiene el atributo definido en el presente documento (TID, GML_GIS, o está vacío). Si es este el caso, esos valores serán almacenados o actualizados en el HSS para futuras transacciones.

20 Para posteriores transacciones, el MM accede a esa información almacenada en el HSS si se requiere para la gestión de las sesiones entrantes en base al perfil del usuario. En otro caso, el CSCF está gestionando un nuevo establecimiento de llamada y el paquete SIP no contiene estos nuevos atributos. En base a la cabecera Tipo-de-contenido SIP, el LS actualizará los datos de registro del usuario almacenados en el Registro de Localización Local. El perfil de usuario se actualiza con la información SDP y se almacena de acuerdo con el formato de las redes heredadas. Las redes heredadas descargarán directamente la información requerida desde el HLR.

25 La Figura 10 presenta un ejemplo de flujo de llamada durante una transacción del servicio de Presencia. La primera etapa es el Registro y Autenticación del Terminal SIP y la utilización del paquete de contenido útil SIP para proporcionar la Información de Identificación del Usuario dentro del Registro.

30 En este caso, estamos tratando con un terminal móvil que usa UMTS. El usuario necesita un pequeño almuerzo y no tiene suficiente conocimiento acerca de los servicios disponibles en los alrededores. Para la obtención del servicio adecuado para su localización actual necesita registrar 100 su situación como se indica. Posteriormente, el usuario solicita 120 un servicio específico y recibe la respuesta 130 con el servicio adaptado a su situación física.

35 Volviendo a referirnos a la Figura 3, el Terminal SIP cifrará la Identidad del Usuario y localización del Sistema para su envío en la solicitud de REGISTRO. La solicitud de REGISTRO puede estar cifrada o no en base a los requisitos del usuario. Si al usuario no le importa que cualquiera pueda conocer su localización la solicitud irá en texto plano. En otro caso, el SIP contiene el campo Autorización (por ejemplo después de una respuesta 401 Requerida Autenticación) y se cifra la Información de Localización (TID).

40 El CSCF (con las capacidades Proxy/Registro SIP) aceptará el registro del usuario. Adicionalmente, el CSCF envía la información del usuario o bien al HSS (Interfaz de señal Cx) o bien al Servidor de Presencia si tal entidad existe, como se muestra. Después de esto el usuario está registrado y su situación está disponible para otros servicios. Si el Servidor de Presencia no existe, entonces el HSS se comportará de modo similar a un Servidor de Presencia. En este punto es un asunto de reutilizar o no entidades existentes sobrecargadas.

45 En este punto el usuario solicita el servicio específico mencionado anteriormente, que para ser completado, será esencial para el centro de servicio basado en la Localización tener el conocimiento de su localización que ya está disponible en el HSS. Por ello, el usuario envía una INVITACIÓN para la apertura de una sesión donde pregunta por alguna información. Es necesario definir un atributo para indicar la naturaleza de esta Solicitud. De ahí que en el Tipo-de-contenido estará definido el atributo “Solicitud-Servicio” como se muestra en la Figura 4.

50 El CSCF recibe el mensaje y comprueba la información de ese usuario o bien en el HSS o bien en el Servidor de Presencia. Si el usuario tiene una información de localización almacenada, el CSCF realiza una consulta al servidor de los Servicios Basados en la Localización sin revelar la identidad del usuario que necesita la información. El CSCF sólo realiza una consulta para un servicio concreto en un lugar específico.

El servidor LBS responderá con la información de acuerdo solamente a los requisitos indicados en la consulta por parte del CSCF (servicio-localización). Por ello, se mantiene segura la privacidad del usuario en el CSCF.

Finalmente, una vez que el CSCF recibe la respuesta del LBS, se envía al usuario. El formato es similar a la solicitud

pero en este caso la información se lleva en la respuesta 200 OK. Después de esto el usuario traducirá la información y devolverá el ACUSE al CSCF que cerrará la sesión.

MENSAJERÍA INSTANTÁNEA (IM)

Se describirán ahora las realizaciones de un servicio de Mensajería Instantánea en unos pocos ejemplos.

- 5 La funcionalidad se basa en los procedimientos SUSCRIPCIÓN/ NOTIFICACIÓN del SIP para el envío de la notificación al usuario cuando llega un mensaje nuevo.

10 Considere un primer ejemplo en el que un usuario no desea ser perturbado durante un periodo de tiempo pero desea estar al tanto de cualquier evento en caso de que algo anormal suceda. La ventaja de este enfoque es que el usuario puede estar informado constantemente sin establecer una sesión completa. De nuevo, se resalta que la característica importante es que no requiere ningún procedimiento SIP nuevo, usa justamente el marco existente y define nuevos atributos para las cabeceras SIP.

Mecanismo de IM básico (véase la figura 11)

15 Esta parte muestra el mecanismo básico usado para implementar el Servicio de Mensajería Instantánea a través de redes IP. En este caso no hay cambios entre diferentes redes. El único inconveniente es que el servicio ha de tratar con la traducción entre diferentes proveedores de servicios de implementaciones del servicio similares.

El usuario utiliza el procedimiento SUSCRIPCIÓN con el CSCF para recibir notificaciones acerca de ciertas clases de eventos. El tipo de evento se indica en la cabecera **Evento** y en este caso sería un **"Evento: Mensaje"**.

20 Cada vez que el CSCF al que se suscribe el usuario recibe un mensaje se notificará al usuario mediante el procedimiento NOTIFICACIÓN. En la cabecera Evento se indica el tipo de **Evento** y en el **"Tipo-de-Contenido"** se indica el tipo de mensaje (mensaje de voz, texto SMS, imagen SMS, etc.).

En caso de que el mensaje provenga de otro sistema o proveedor el mensaje se recibirá en el CSCF que lo almacenará en el Servidor de Mensajería Instantánea.

25 (IMS/MMSC). Si el mensaje se origina en otra red, es necesaria una etapa intermedia para adaptar el formato de mensaje. Desde el punto de vista del usuario esto estará oculto y sólo hará una SUSCRIPCIÓN a algún **"Evento"** específico y recibirá la NOTIFICACIÓN cuando tenga lugar.

30 Finalmente el usuario recibe una notificación acerca de un nuevo mensaje. En la cabecera Desde del SIP se indica el origen de ese mensaje. En la de Contacto se indica el punto en el que el mensaje puede recogerse (puede ser o bien en la dirección del Servidor de Mensajería o bien en la URL donde está almacenada la información). En el Tipo-de-Contenido se indicaría la naturaleza del mensaje, si es un mensaje de voz, imagen, video clip, etc.

IM Entrelazado

35 Esta parte muestra aproximadamente la situación en la que el mensaje o información proviene de otro tipo de red. En tal caso, como se ha mencionado anteriormente, es necesario realizar una traducción de formato o incluso de señalización. En este punto la pasarela de Señalización para la PSTN por la pasarela de Señalización de Itinerancia, en el caso de GSM o redes móviles se convierte en importante.

El primer ejemplo se muestra en la Figura 12 e ilustra una llamada que viene de una red PSTN.

La primera etapa es la suscripción del usuario para tenerle al tanto de cualquier suceso pero sin que sea perturbado.

40 La llamada de teléfono va a través de la pasarela (SIP/GW). La GW convierte la llamada de voz normal en un mensaje de INVITACIÓN SIP y va a través de la red hasta que alcanza el CSCF en el que se registró el usuario final.

El CSCF recibe la llamada SIP normal y en base a los requisitos del usuario no procede con la continuación de llamada normal. En su lugar, convierte la información entrante en un mensaje de voz.

El CSCF almacena el mensaje en el Servidor de Mensajería.

45 Finalmente el CSCF enviará un mensaje de NOTIFICACIÓN al usuario con las características del evento que recibió y que fue dirigido a él. El mensaje indicará el **"Tipo-de-Contenido: mensaje de voz"** y donde puede ser recogido en el **"Contacto: sip.messgecentre.nokia.com"**.

La Figura 13 es similar con la diferencia de que el origen es un bien conocido Servicio de Mensajes Cortos (SMS) de las redes GSM. En este caso necesitara una GW de Señalización de Itinerancia (véase también la Figura 9) para la conversión del mensaje en una transacción SIP. La R-SGW encontrará donde está localizado el usuario y enviará la

INVITACIÓN SIP normal con la información del mensaje hacia ese usuario. A partir de ahí el procedimiento similar al caso previo.

Se suscribe el usuario

El mensaje se origina en la red GSM.

- 5 El mensaje alcanza el centro SMS y desde ahí la GW de Señalización de Itinerancia en donde se convierte en una transacción SIP. En este punto hay dos posibilidades. El mensaje se inserta en el cuerpo de una INVITACIÓN SIP y su naturaleza se indica en el **Tipo-de-contenido**. En caso contrario, el SMS se ajusta directamente con el procedimiento de MENSAJE SIP ya definido.

Desde ahí, el mensaje SIP se dirige al CSCF en donde se registró el usuario.

- 10 Ahora el procedimiento es similar a los casos previos. El mensaje se almacena en el centro de mensajería y se notifica al usuario como se muestra en la Figura 13.

El último ejemplo de IM se muestra en la Figura 14 en la que se muestra una transacción de red totalmente IP. Es decir, no hay necesidad de conversiones. La señalización se basa en SIP a todo lo largo de ella y la llamada va a través de las redes mejoradas SIP sin cambios.

- 15 Presencia y Mensajería

En esta parte se muestran un par de ejemplos en donde se implementa tanto el Servicio de Presencia como de Mensajería para proporcionar un servicio completo. El servidor de presencia comprobará los requisitos del usuario y actúa en base a ellos. Esto ahorra recursos de red de acuerdo con la especificación del perfil de usuario.

Ejemplo 1 (véase la Figura 15)

- 20 Inicialmente todos los usuarios (jefe, abogada, esposa) están suscritos proporcionando su información, incluyendo los requisitos de servicio. Algunos de ellos están libres y otros ocupados pero desean estar al tanto de cualquier suceso. Por ello en este punto la información del usuario se almacena en el Servidor de Presencia.

Uno de los usuarios está ocupado (abogada) y no desea ser perturbado. En su lugar, ella se suscribirá al servicio de mensajería para recibir notificaciones en cualquier caso.

- 25 La suscripción se consigue en el Servicio de Mensajería.

El tercer usuario (esposa) desea establecer una transacción con dos personas (jefe, abogada) al mismo tiempo. Ella inicia la sesión SIP con ambos.

- 30 La solicitud invitación SIP llega al CSCF pero en lugar de ser enviada el CSCF comienza primero a buscar la información acerca de los usuarios finales. El CSCF solicita al Servidor de presencia cualquier pista acerca de los usuarios invitados.

El CSCF descubre en base a la respuesta desde el servidor de presencia que uno de los usuarios está disponible (jefe) y el otro está ocupado (abogada).

- 35 En este punto el CSCF devuelve al usuario originador (esposa) una respuesta que indica el estado de cada uno de ellos. Este mecanismo es diferente de la transacción normal en la que la INVITACIÓN se enviaría sin ninguna comprobación.

El usuario (esposa) que inició la sesión previa, en base a la respuesta de realimentación desde el CSCF, decide enviar un mensaje a ambos usuarios finales en lugar de establecer una llamada directa.

El mensaje llega al CSCF y comprobar los perfiles de usuario en relación con sus preferencias. Una vez más lo comprueba y se da cuenta de que uno de ellos no desea ser perturbado.

- 40 El mensaje se envía directamente al usuario (jefe) que específico durante el registro que estaba libre.

El mensaje se almacena para el tercer usuario (abogada) que está ocupado. En su lugar ella recibirá una notificación de que el mensaje está esperando para ser recogido.

Conclusión:

- 45 Con la combinación de ambos mecanismos se puede proporcionar un servicio más completo al usuario y ahorrará algunos recursos de red en algunos aspectos.

Ejemplo 2 (véase la Figura 16)

Este ejemplo usa una combinación similar de ambos sistemas de Presencia y Mensajería para la definición del servicio innovador.

- 5 Los usuarios ilustrados (esposo, esposa) trataron de hacer una reserva para cenar en un restaurante pero estaba completamente ocupado. Dejaron su información de contacto para el caso de una cancelación. A continuación está el flujo de mensajes para la implementación de tal servicio:

Los usuarios se registran con su información en el Servidor de Presencia. A partir de entonces todos sus datos están disponibles para su solicitud por parte del CSCF.

- 10 Uno de los usuarios (esposa) está ocupado pero ella decide suscribirse para la notificación de cualquier mensaje porque tiene una buena intuición.

La suscripción de la esposa se registra en el Servidor de Mensajería.

De pronto, se cancela una mesa. El camarero comprobará la lista de reservas en el ordenador y automáticamente (con un clic) envía un mensaje a las personas de acuerdo con el orden listado en el ordenador.

- 15 El CSCF con estado al PC del Restaurante recibe la solicitud y comprueba el estado del usuario en el servidor de mensajería.

En base a la información desde el MS el mensaje se envía directamente a uno de los usuarios (esposo).

El otro usuario (esposa) está ocupado pero ella recibirá una notificación del mensaje. La notificación incluirá suficiente información (en la cabecera Sujeto) para saber si el mensaje es importante o no para ser recogido desde el centro de mensajería.

- 20 Aunque la invención se ha mostrado y descrito con respecto al mejor modo de realización de la misma, se debía comprender por los expertos en la técnica que lo precedente y varios otros cambios, omisiones y adiciones en la forma y detalle de los mismos se pueden realizar sin separarse del alcance de la invención.

Apéndices**Apéndice 1**

- 25 Abreviaturas

API Interfaz de Programación de Aplicaciones

AuF Función de Autenticación

BCC Control de Llamada Básico

BCSM Modelo de Estado de Llamada Básico

- 30 BHCA Intento de Llamada en Hora de Ocupación

CC Control de Llamada

CPS Servidor de Procesamiento de Llamada

CS Circuito Conmutado

CSCF Función de Control del Estado de Llamada

- 35 E- GGSN Nodo Mejorado de Soporte de la Pasarela GPRS

E- SGSN Nodo Mejorado de Soporte del Servicio GPRS

ETSI Instituto de Normas de Telecomunicaciones Europeo

FFS Para Estudio Adicional

GK Guarda

- 40 GGSN Nodo de Soporte de la Pasarela GPRS

GPRS Servicio General de Paquetes Vía Radio

	GSM	Sistema Global para Telecomunicaciones Móviles
	GW	Pasarela
	HLF	Función de Localización Local
	HLR	Registro de Localización Local
5	HPoA	Punto de Conexión H.323
	HSS	Servidor de Abonado Local
	HTML	Lenguaje de Marcado de Hipertexto
	HTTP	Protocolo de Transferencia de Hipertexto
	IANA	Autoridad de Asignación de Números de Internet
10	I-CSCF	Interrogación de la Función de Control del Estado de Llamada
	IETF	Grupo de Trabajo de Ingeniería de Internet
	IMSI	Identidad de Abonado Móvil Internacional
	IP	Protocolo de Internet
	IPTE	Terminal IP
15	ITU	Unión Telecomunicaciones Internacional
	IWF	Función de Entrelazado
	LAN	Red de Área Local
	LCS	Servicio de Localización
	MBone	Columna de Emisión Múltiple
20	MD5	Compendio de Mensajes, ver. 5 del algoritmo
	MGCF	Función de Control de Pasarela de Medios
	MGW	Pasarela de Medios
	MRF	Función de Recursos de Medios
	MT	Terminal Móvil
25	NNI	Interfaz Entre Redes
	NPoA	Punto de Conexión de Red
	O-CSCF	Función de Control del Estado de la Llamada de Origen
	PDP	Protocolo de Paquetes de Datos
	PDU	Unidad de Datos del Protocolo
30	PPP	Protocolo Punto a Punto
	PLMN	Red Móvil Terrestre Pública
	PSTN	Red Telefónica Conmutada Pública
	PTP	Punto a Punto
	QoS	Calidad de Servicio
35	RAN	Red de Acceso Vía Radio
	RN	Número de Itinerancia
	R-SGW	Pasarela de Señalización de Itinerancia

	RSVP	Protocolo de Reserva de Recursos
	RTCP	Protocolo de Control en Tiempo Real
	RTP	Protocolo en Tiempo Real
	RTSP	Protocolo de Transmisión Continua en Tiempo Real
5	RTT	Tiempo de Ida y Vuelta
	SAP	Protocolo de Anuncio de Sesión
	SCN	Red de Circuitos Conmutados
	SCP	Protocolo de Control de Sesión
	SCTP	Protocolo de Control de Transmisión Continua
10	S-CSCF	Función de Control del Estado de Llamada en Servicio
	SDP	Protocolo de Descripción de Sesión
	SGSN	Nodo de Soporte GPRS en Servicio
	SIP	Protocolo de Inicio de Sesión
	SLoP	Contenido útil de Localización Espacial
15	SPD	Base de Datos de Perfiles en Servicio
	SS7	Sistema de Señalización 7
	TA	Dirección de Transporte (dirección IP + número de puerto TCP/UDP)
	TCP	Protocolo de Control de Transporte
	TE	Equipo Terminal
20	TID	ID de Acceso al registro Objetivo
	TAD	ID de Acceso al registro Objetivo
	T-SGW	Pasarela de Señalización del Transporte
	UA	Agente de Usuario
	UAC	Cliente del Agente de Usuario
25	UAS	Servidor del Agente de Usuario
	UDP	Protocolo de Paquetes de Datos de Usuario
	UMS	Servidor de Movilidad de Usuario
	UMTS	Sistema Universal de Telecomunicaciones Móviles
	UNI	Interfaz Usuario a Red
30	URL	Localizador Uniforme de Recursos
	VLF	Función de Localización de Visitante
	VoIP	Voz sobre IP

Apéndice 2

Términos

35 **Usuario:** Una persona u otra entidad autorizada por un abonado para usar algunos o todos los servicios a los que se ha suscrito ese abonado.

Identidad de Usuario: un código o cadena de un formato preestablecido particular que identifica de modo

único a un usuario a través de una infraestructura multiusuario, multiservicio.

Papel de servicio del usuario: papel que tiene un usuario en el alcance de un servicio particular.

Identidad del papel de servicio del usuario: un código o cadena de un formato preestablecido particular que identifica de modo único a una instancia en un papel de servicio del usuario.

5 **Traspaso:** se denomina adicionalmente *sin saltos* cuando el cambio de localización del terminal no da como resultado un retardo o pérdida de los datos comunicados que finalmente se percibirían por el usuario como una degradación de la calidad de servicio. Los traspasos sin salto pueden depender por ello de muchos factores, incluyendo el tipo de servicio y la robustez de la presentación del servicio contra pérdida de datos en el terminal.

10 **Terminal móvil H.323:** un terminal móvil que implementa las funciones de terminal H.323 tal como se define la norma H.323.

Punto de conexión H.323: el guarda con el que se registra el terminal H.323.

Terminal móvil: un terminal que puede cambiar su punto de conexión a la red y/o punto de conexión H.323.

15 **Punto de conexión a la red:** la dirección por la que los paquetes alcanzan un punto final.

Servicios: existen diferentes tipos de servicios, se puede distinguir:

Proporcionados en la capa de aplicación hacia los abonados, y por ello denominados aplicaciones; el tipo de servicios a los que normalmente se refiere dentro del alcance del problema de movilidad.

20 Proporcionados por una capa más baja del protocolo de comunicaciones hacia una capa del protocolo más alta por medio de un punto de acceso de servicio (SAP) definido, típicamente algún tipo de servicio de transporte.

Movilidad del servicio: capacidad para que un usuario utilice un servicio particular (abonado) independientemente de la localización del usuario y del terminal que se usa para esa finalidad.

25 **Abonado:** una persona u otra entidad que tiene una relación contractual con un proveedor de servicios a nombre de uno o más usuarios. (Un abonado es el responsable del pago de los cargos debidos a ese proveedor de servicios.)

Movilidad de proveedor de servicios: la capacidad de un usuario para cambiar los proveedores de servicios y mantener la misma identidad de usuario.

30 **Perfil de terminal de usuario:** información específica del usuario, posiblemente contenida en una base de datos multiusuario, que indica qué terminales está usando un usuario, tanto de forma temporal como permanente.

Identidad del terminal: un código o cadena de un formato preestablecido particular que identifica de modo único un terminal.

35 **Movilidad del terminal:** la capacidad de un terminal para cambiar la localización, punto de conexión a la red y punto de conexión H.323 mientras sigue siendo manteniendo la comunicación. La *movilidad de terminal discreta* (itinerancia del terminal): la capacidad de un terminal para realizar cambios de localización discretos. Es decir, para cambiar la localización mientras no haya transmisiones continuas de medios activas. *Movilidad de terminal continua* (traspaso): la capacidad de un terminal para cambiar la localización mientras están activas transmisiones continuas de medios.

40 **Movilidad del usuario:** definida como la capacidad de un usuario para mantener la misma identidad de usuario independientemente de los terminales y tipos de terminales y asimismo el *punto de conexión a la red*.

45 **Perfil de servicio de usuario:** información específica del usuario, contenida posiblemente en una base de datos multiusuario, indica aquellos servicios a los que un usuario está suscrito y datos de configuración personales para los respectivos servicios. Nótese que los servicios particulares pueden usar un perfil de terminar como entrada para la operación de servicio.

Gestión de la movilidad: el conjunto de funcionalidades necesarias para proporcionar Movilidad de Usuario, de Terminal y de Servicio.

50 **Dominio administrativo local:** el dominio administrativo que se relaciona por una suscripción a la red de usuarios H.323 móvil. El dominio administrativo local contiene permanentemente datos específicos del

usuario incluyendo la información de localización, autenticación y perfil de servicio relacionada con la red de usuario H.323 móvil.

Dominio administrativo visitado: el dominio administrativo que no es el dominio administrativo local y que está dando servicio a un usuario de red H.323 móvil activo.

5 **Dominio administrativo en servicio:** El dominio administrativo (local o visitado) que da servicio a un Usuario de red H.323 móvil activo.

TID: ID de información objetivo. Este es un identificador basado en URL que contiene toda la información de localización de cualquier usuario. Se fija al punto de suscripción.

10 **TAD:** ID de acceso al registro objetivo. Esta es una URL que enlaza la localización momentánea del usuario con su registro fijo (TID).

SLoP: contenido útil de localización espacial. Es la definición del formato del mensaje en el que se almacena la información de localización. Se basa principalmente en TID o TAD dependiendo de si el usuario se sitúa en su punto usual de conexión o está en una localización temporal.

Apéndice 3

15 **Visión Global del TID y TAD:**

Para obtener la localización espacial de un objetivo, debe haber un procedimiento para identificar y referirse al objetivo. Dos identificadores del objetivo son los siguientes: (1) ID de Información del Objetivo (TID) y (2) ID de Acceso al Registro Objetivo (TAD).

20 El TID sirve como un identificador de recursos persistente, independiente de la localización, válido incluso después de la existencia del objetivo. Por otro lado, el TAD está formado generalmente con la información de contacto, procedimientos de manejo, etc., para el repositorio de la información de localización del objetivo. El TAD sólo puede decirle dónde/cómo obtener la información de localización del objetivo dado. Puede haber más de un TAD para un TID dado. Puede ser dependiente del tiempo/lugar, no persistente, etc.

25 Por ejemplo el TID de Mike Lee puede incluir información tal como "Nombre: Mike Lee, Sexo: varón, Nacionalidad: xyz, ID: 221166-3355, etc.". El TAD de Mike Lee puede incluir información tal como "Identidad: un subconjunto del TID (por ejemplo su nombre y número de ID), Acceso: el procedimiento de contacto y dirección de su oficina de registro social o del repositorio que tiene su información de localización, etc.".

30 Un identificador de recursos uniforme (URI) es una cadena compacta de caracteres para la identificación de un recurso abstracto o físico. Es un identificador muy adecuado para los objetivos descritos en el presente documento (sección 2). Hay varios subconjuntos bien conocidos de URI, tal como el nombre de recursos uniforme (URN), el localizador de recursos uniforme (URL), etc.

35 Como subconjunto del URI, el URN es un identificador de recursos con los requisitos específicos para permitir la identificación de un recurso independientemente de la localización, así como la longevidad de la referencia. Un TID puede estar muy bien denominado con un URN. Por ejemplo, el TID basado en URN del automóvil de Mike Lee puede ser:

"urn:espacioNombre-xyz: coche=abc-888, estadoregistro = nnn, propietario =mike.lee, nacionalidad =xyz,id=221161-3355,email=mike.lee@hardcom.com,pstn=+358405021988".

40 El TID basado en URN del automóvil de Mike Lee se puede mantener en el repositorio de registro original del automóvil en el estado nnn. El TID basado en URN del automóvil de Mike Lee puede depender de donde está localizado actualmente el automóvil. Por ejemplo,

(1) cuando el automóvil no está actualmente en el país xyz, su TAD puede ser: "slop:coche=abc-888,registro=estade=nnn@coche1.find.gov:5888;validedhasta= 31.8.2000",

(2) cuando el automóvil está actualmente en el país xyz, su TAD (predeterminado) puede ser: "slop:abc-888@vehicle.supervizado. eu:transporte=tcp:2008",

45 en el que "slop" es el protocolo o esquema para el acceso a la información de localización.

Apéndice 4

Atributos del formato de datos a considerar:

50 El formato de los mensajes se decide de acuerdo con las necesidades de localización. La parte importante del mensaje corresponde a la información de localización, que se puede definir de diferentes formas dependiendo del dispositivo. Los campos principales podrían contener los datos siguientes:

Coordenadas: indica la localización geográfica del usuario. Pueden ser datos GPS o de cualquier otro formato dependiendo de los últimos diseños.

Precisión: la precisión de la información.

Tiempo de vida: es el tiempo durante el que es válida la información en el mensaje.

5 **Tipo de dispositivo:** para saber qué clase dispositivo está proporcionando la información y si es capaz de proporcionar información adicional si es necesario. Se puede definir como un móvil, teléfono fijo, dispositivo IP o un simple mecanismo de supervivencia que proporciona datos GPS.

10 **Estatismo del dispositivo:** Define como de estático es el dispositivo en una escala de 0 a 10, es decir, puede ser totalmente fijo o móvil con una elevada velocidad. Este campo se usa principalmente para determinar el periodo de latencia entre actualizaciones. Un dispositivo con este campo igual a 0 indica que está fijo y solo necesita actualizarse tras un periodo prolongado de tiempo o incluso no se necesita actualizar, solo se le deja el tiempo de vida hasta que expira.

Estado del dispositivo: para indicar en qué estado está realmente el dispositivo. Puede ser fijo, móvil, cambiando el alcance de LA y otros posibles estados.

15 **Transparencia de información:** indica el grado de privacidad de la información contenida el mensaje. Puede tener una escala de 0 a 10 dependiendo de si el usuario desea hacer su información totalmente transparente a otros usuarios (10) o totalmente opaca (0). En ese caso el LA recibirá la información pero no podrá replicar los datos en relación a la localización de ese usuario (excepto para los servicios de emergencia).

20

REIVINDICACIONES

1. Un procedimiento, que comprende:

la recepción de un mensaje de señalización en la capa de aplicación (70) desde un usuario (26) que se registra para un servicio de presencia proporcionado a través de una red de protocolo de Internet, la comprobación de dicho mensaje (72) para la extracción de la información de localización espacial de dicho usuario (26), el almacenamiento de dicha información de localización espacial extraída (74) de dicho usuario, y proporcionar acceso a dicha información de localización espacial de dicho usuario a uno o más servicios basados en la localización, en el que dicha información de localización espacial está contenida en dicho mensaje como contenido útil de localización espacial de acuerdo con un protocolo de inicio de sesión (SIP), proporcionándose dicho servicio de presencia a dicho usuario de acuerdo con dicha información de localización espacial de dicho usuario, y en el que dicho acceso a dicha información de localización espacial de dicho usuario se proporciona a dichos uno o más servicios basados en la localización sin proporcionar acceso a la información asociada de identidad del usuario.

2. El procedimiento de la reivindicación 1, en el que dicha información de localización espacial de dicho usuario se proporciona a uno o más de otros usuarios en conjunto con un servicio de mensajería proporcionado a dichos otros usuarios.

3. Procedimiento, que comprende:

construcción de un mensaje de señalización en la capa de aplicación que contiene información de localización espacial de un usuario, estando contenida dicha información de localización espacial en dicho mensaje como un contenido útil de localización espacial de acuerdo con el protocolo de inicio de sesión, que proporciona dicho mensaje de señalización en la capa de aplicación (100) para el registro de dicho usuario en un servicio de presencia sobre una red de protocolo de Internet, en el que dicha información de localización espacial de dicho usuario es extraída por un servidor de presencia (4) que proporciona dicho servicio de presencia a dicho usuario de acuerdo con dicha información de localización espacial, y en el que el acceso a dicha información de localización espacial de dicho usuario se proporciona a uno o más servicios basados en la localización sin proporcionar acceso a la información asociada de identidad del usuario.

4. El procedimiento de la reivindicación 3, en el que dichos uno o más servicios basados en la localización se proporcionan a dicho usuario de acuerdo con dicha información de localización espacial de dicho usuario.

5. El procedimiento de la reivindicación 3, en el que dicho mensaje de señalización en la capa de aplicación (100) incluye proporcionar seguridad a dicha información de localización espacial mediante cifrado.

6. El procedimiento de la reivindicación 3, en el que dicho proporcionar dicho mensaje de señalización en la capa de aplicación (100) incluye proporcionar seguridad para dicha información de localización espacial mediante la inclusión de información de seguridad para su uso por dicho servicio de presencia en el manejo de dicha información de localización espacial.

7. El procedimiento de la reivindicación 3, en el que dicha información de localización espacial se proporciona a uno o más de otros usuarios en conjunto con un servicio de mensajería a dichos otros usuarios.

8. Un sistema de red en comunicación con un dispositivo terminal (TE), que comprende:

un servidor (72), configurado para recibir un mensaje de señalización en la capa de aplicación (100) para el dispositivo terminal (TE) que registra (30) a un usuario de dicho dispositivo (TE) en un servicio de presencia (4) proporcionado a través de una red de protocolo de Internet, para comprobar dicho mensaje de señalización en la capa de aplicación (100) para la extracción de información de localización espacial de dicho usuario y para proporcionar acceso a dicha información de localización espacial de dicho usuario a uno o más servicios basados en la localización, y un almacén de datos (74), configurado para almacenar dicha información de localización espacial extraída de dicho usuario, en el que dicha información de localización espacial está contenida en dicho mensaje de señalización en la capa de aplicación (100) como un contenido útil de localización espacial de acuerdo con un protocolo de inicio de sesión, proporcionándose dicho servicio de presencia a dicho usuario de acuerdo con dicha información de localización espacial de dicho usuario, y en el que el acceso a dicha información de localización espacial de dicho usuario se proporciona a dichos uno o más servicios basados en la localización sin proporcionar acceso a la información asociada de identidad del usuario.

9. El sistema de red de la reivindicación 8, en el que dicho sistema de red se configura para proporcionar información de localización espacial de dicho usuario a uno o más de otros usuarios en conjunto con un servicio de mensajería proporcionado a dichos otros usuarios.

10. Un aparato (TE) en comunicación con un sistema de red, que comprende:

- 5 un procesador, configurado para construir un mensaje de señalización en la capa de aplicación que contiene información de localización espacial de un usuario, estando contenida dicha información de localización espacial en dicho mensaje como un contenido útil de localización espacial de acuerdo con un protocolo de inicio de sesión,
- 10 una interfaz de comunicación (Um, Uu), configurada para proporcionar dicho mensaje de señalización en la capa de aplicación al sistema de red para el registro de dicho usuario con un servicio de presencia proporcionado a través de una red de protocolos de Internet,
- 15 en el que dicha información de localización espacial de dicho usuario se extrae por el sistema de red al proporcionar dicho servicio de presencia a dicho usuario de acuerdo con dicha información de localización espacial,
- y en el que se proporciona acceso a dicha información de localización espacial de dicho usuario a uno o más servicios basados en la localización sin proporcionar acceso a la información asociada de identidad del usuario.

11. El aparato de la reivindicación 10, en el que dicho aparato se configura para recibir uno o más servicios basados en la localización proporcionados a dicho usuario de acuerdo con dicha información de localización espacial de dicho usuario.

12. El aparato de la reivindicación 10, en el que dicha información de localización espacial contenida en dicho mensaje de señalización en la capa de aplicación (100) se asegura mediante cifrado.

13. El aparato de la reivindicación 10, en el que dicha información de localización espacial contenida en dicho mensaje de señalización en la capa de aplicación (100) se asegura mediante la inclusión de información para su uso por el servicio de presencia en el manejo de dicha información de localización espacial.

14. Procedimiento, que comprende:

- el registro de una primera pluralidad de usuarios (2) a un servicio de presencia (4) en respuesta a una correspondiente pluralidad de solicitudes de registro de la primera pluralidad de usuarios, en el que una solicitud de registro incluye información relacionada con un estado de comunicaciones de un usuario;
- 30 la recepción del mensaje de invitación (24) desde un usuario invitador (22) registrado en dicho servicio de presencia para intercambiar contenido con un usuario invitado (26) también registrado en el servicio de presencia;
- proporcionar una consulta de presencia en respuesta a dicho mensaje de invitación para la obtención de un estado de comunicaciones actualizado de dicho usuario invitado; y
- 35 la determinación, en base a dicho estado de comunicaciones actualizado de dicho usuario invitado, de si dicho contenido se debería enviar a dicho usuario invitado, almacenar o rechazar,
- en el que dicho estado de comunicaciones pertenece a una localización espacial del usuario, dicha solicitud de registro, dicha consulta de presencia y dicho mensaje de invitación se comunican de acuerdo con un protocolo de inicio de sesión y en el que dicha localización espacial está contenida en dicha solicitud de registro como un contenido útil de localización espacial y dicha localización espacial se extrae de la solicitud de registro en el registro.
- 40

15. Un servidor de presencia (4), que comprende:

- un procesador, configurado para registrar una pluralidad de usuarios (2) a un servicio de presencia en respuesta a una correspondiente pluralidad de solicitudes de registro de la pluralidad de usuarios (2), en el que una solicitud de registro incluye información relacionada con un estado de comunicaciones de un usuario;
- 45 un almacenamiento de datos, configurado para almacenar estados de comunicación de los usuarios registrados; y
- una interfaz de comunicaciones, configurada para recibir un mensaje de invitación desde un usuario invitador (22) registrado en dicho servicio de presencia para intercambiar contenido con un usuario invitado (26) registrado en dicho servicio de presencia y proporcionar una consulta de presencia en respuesta a dicho mensaje de invitación para la obtención de un estado de comunicaciones actualizado de dicho usuario invitado (26);
- 50 en el que dicho procesador se configura adicionalmente para determinar, en base a dicho estado de comunicaciones actualizado de dicho usuario invitado (26), si dicho contenido se debería enviar a dicho usuario invitado (26), almacenar o rechazar,
- 55 en el que dicho estado de comunicaciones pertenece a una localización espacial del usuario, dicha solicitud de registro, dicha consulta de presencia y dicho mensaje de invitación se comunican de acuerdo con un

protocolo de inicio de sesión y en el que dicha localización espacial está contenida en dicha solicitud de registro como un contenido útil de localización espacial.

16. Sistema, caracterizado por que comprende:

5 un servidor central (6), receptivo a un mensaje de invitación (24) de un usuario invitado (22) para intercambiar contenido con un usuario invitado (26), para proporcionar una consulta de presencia (28); y un servidor de presencia (4), receptivo a dicha consulta de presencia, para proporcionar información de presencia (28) en relación a un usuario (26) registrado (30),
 10 en el que dicho servidor central (6) es receptivo a dicha información de presencia en relación con dicho usuario invitado (26) registrado en dicho servidor de presencia, para su uso en la decisión de si el contenido se envía a dicho usuario invitado (26), se almacena o se rechaza, en el que dicha consulta de presencia y mensaje de invitación se comunican de acuerdo con un protocolo de control de la capa de aplicación y en el que dicha información en relación a la presencia pertenece a una localización espacial de dicho usuario.

17. El sistema de la reivindicación 16, en el que dicho servidor central (6) es receptivo también a dicho mensaje de invitación para proporcionar una consulta de suscripción (36) y en el que dicho sistema comprende además un
 15 servidor de mensajería (10), receptivo a dicha consulta de suscripción, para proporcionar información de notificación (36) en relación a una consulta desde un abonado suscrito para la notificación de un evento y en el que dicho servidor central (6) es receptivo a dicha información de notificación para dicho uso en la decisión de si dicho contenido se debería enviar a dicho usuario invitado (26), almacenar o rechazar.

18. El aparato de la reivindicación 17, en el que dicho protocolo de control de aplicación es un protocolo de inicio de
 20 sesión (SIP).

19. El aparato de la reivindicación 18, en el que dicha información en relación a la presencia y que pertenece a dicha localización espacial de dicho usuario se comunica como un contenido útil de localización espacial.

20. El aparato de la reivindicación 16, en el que dicha información en relación a la presencia y que pertenece a dicha localización espacial de dicho usuario se comunica como un contenido útil de localización espacial.

25

FIG. 1

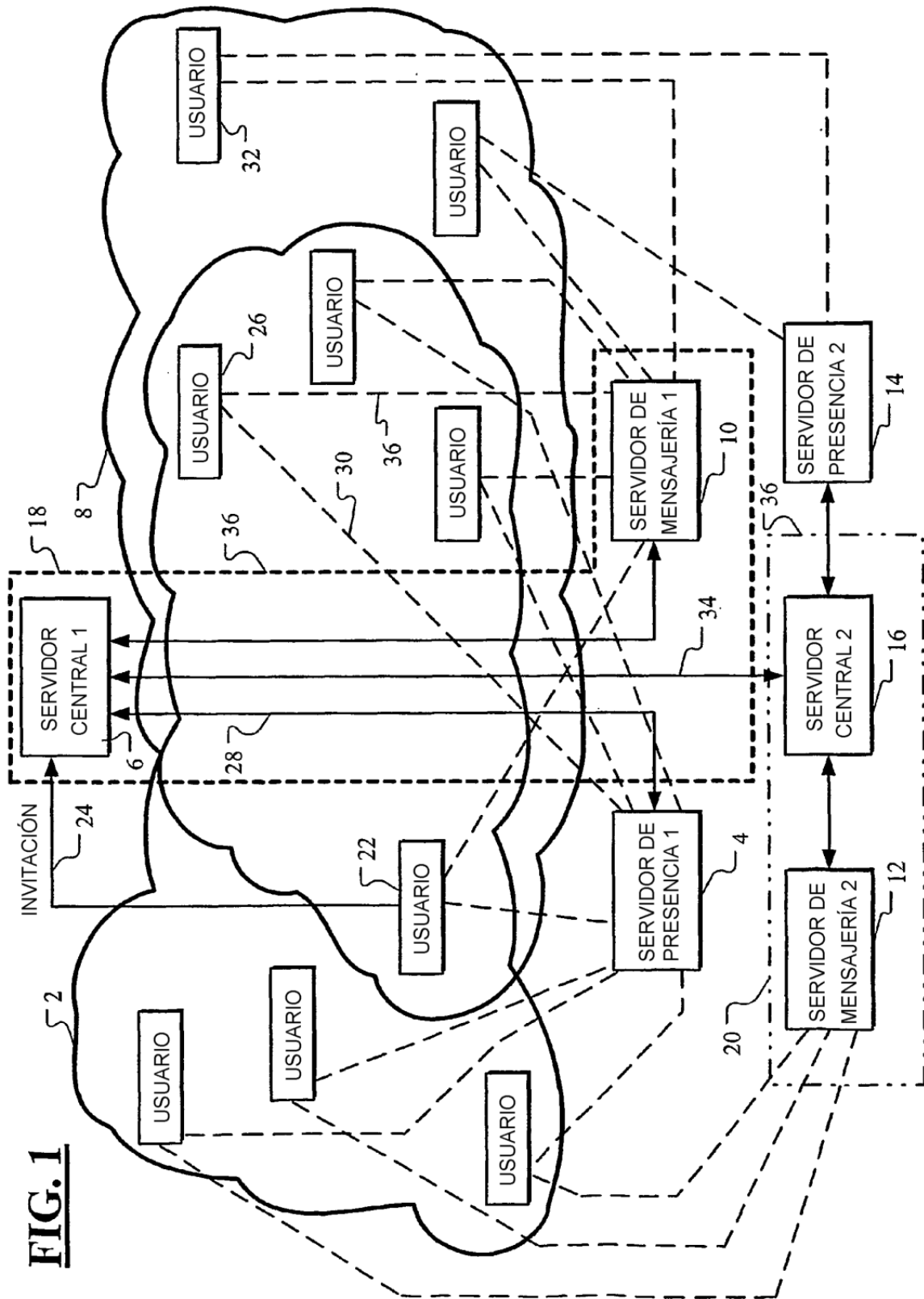


FIG. 2

REGISRO sip: Solicitud URI SIP/2.0
A través de: dirección SIP/2.0/UDP IP
De: sip. dirección pública[user@domain]
[E: 164 dirección@dominioCSCF; usuario=telef]
A: sip: dirección pública [user@domain]
[E: 164 dirección@dominioCSCF; usuario=telef]
ID llamada local: local-ID@host
CSeq: 1 REGISTRO
Contacto: <sip:user@IP dirección:puerto; transporte=udp/tcp>
Autorización: UMTS <RES valor en formato HEX>
Longitud Contenido: X
Expira: delta-segundos
Tipo de Contenido: presencia/TID

<urn: nombrespacio-xyz:car=abc-888,
estado registro= nnn, propietario=mike.lee,
nacionalidad= xyz,id=221161-3355,
email=mike.lee@hardcom.com,
pstn=+358405021988.....>

FIG. 3

Registro sip: i-cscsf.nokia.com SIP/2.0
A través de: SIP/2.0/UDP i-cscf.nokia.com
De: sip: Road_user@dominioCSCF; usuario=telef
A: sip: Road_user@dominioCSCF; usuario=telef
ID llamada: my_host@host
CSeq: 1 REGISTRO
Contacto: <sip:joe@nokia.com:5060; transporte=udp>
Autorización: UMTS <RES valor en formato HEX>
Longitud Contenido: X
Expira: delta-segundos
Tipo de Contenido: aplicación/TID
&

CIFRADO
<urn: nombrespacio-xyz:car=abc-888,
estado de registro= nnn, propietario=mike.lee,
nacionalidad= xyz,id=221161-3355,
email=mike.lee@hardcom.com,
pstn=+358405021988

INVITACIÓN sip: i-cscsf.nokia.com SIP/2.0
A través de: SIP/2.0/UDP i-cscsf.nokia.com
De: sip: Road_user@dominioCSCF; usuario=telef
A: sip: Road_user@dominioCSCF; usuario=telef
ID llamada: my_host@host
CSeq: 1 INVITE
Contacto: <sip:joe@nokia.com:5060;transporte=udp>
Autorización: UMTS<RES valor en formato HEX>
Longitud Contenido: X
Expira: delta segundos
Tipo de Contenido: solicitud servicio/NML

< Aquí se define un script XML que define el tipo de servicio solicitado en esta sesión que sigue a DTD XML basado en Nokia>

FIG. 4

Dato	-WGS84	(Obligatorio)
Coordinadas	- Latitud-	(Obligatorio)
	- Longitud	(Obligatorio)
	- Altitud por encima del elipsoide de referencia a WGS84	(Opcional)
	- Altitud sobre el nivel medio del mar	(Opcional)
Precisión de Localización	- Precisión horizontal, por el radio de un círculo desde el punto posicionado	(Opcional)
	- Precisión de altitud, por el alcance desde el punto posicionado	(Opcional)
Hora	-Hora de la medición/fija	(Obligatorio)
Velocidad	-Velocidad en tierra	(Opcional)
	- Velocidad vertical	(Opcional)
Dirección	- Dirección del movimiento	(Opcional)
Recorrido	- Dirección desde la posición actual al destino definido	(Opcional)
Orientación	- Orientación horizontal	(Opcional)
	-Orientación vertical (pendiente)	(Opcional)
Atributos sin especificar	- Atributo que permiten alguna extensibilidad	(Opcional)

FIG. 5

FIG. 6

```

<SL-info>
  <Cabecera>
    <TID>
      urn:username@company.com, propietario=jose,id=2342112,
      email=jose.Costa-Requena@nokia.com, pstn=+358405201815
    </TID>
    <Seguridad: 10/>
    <Transparencia: 0/>
    <Firma: aZWQAd22aFg&"£4/>
    <Tiempo de vida: 3000 seg.>
  </Cabecera>
  <Cuerpo>
    <Descripción-Localización>
      Estoy sentado en una terraza en el segundo piso de la Torre Eiffel
    </Descripción-Localización>
    <Precisión: 5m/>
    <Tipo-dispositivo: móvil/>
    <Estado-dispositivo: en movimiento/>
    <Estática-Dispositivo: 7/>
    <Cálculo-Coordenadas: Habilitadas/>
    <Codificacion-Coordenadas: SGMl/>
    <Datos-Coordenadas>
      Aquí viene un script SGMl indicando las coordenadas geográficas x,y,z
    </Datos-Coordenadas>
  </Cuerpo>
</SL-info>

```

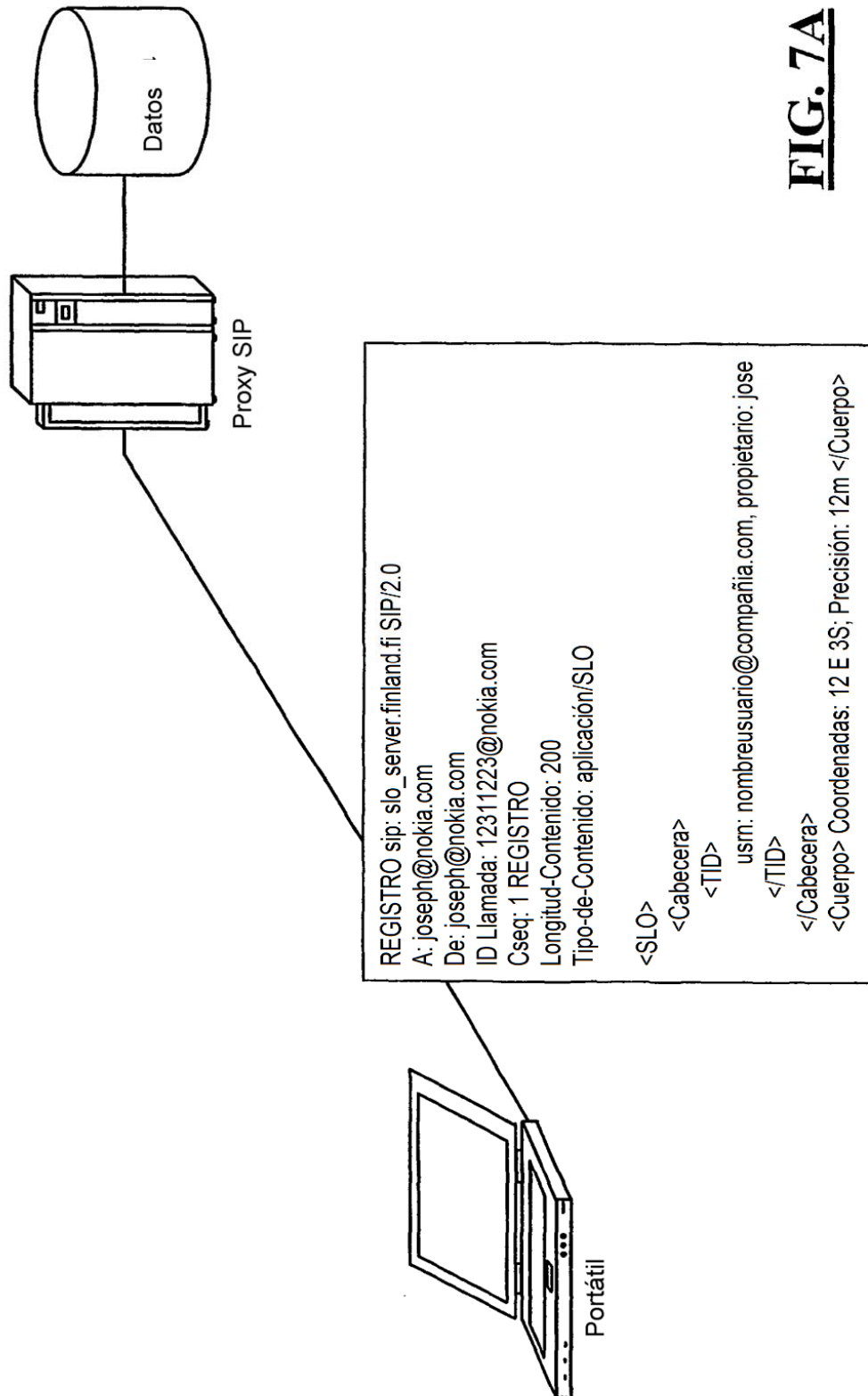
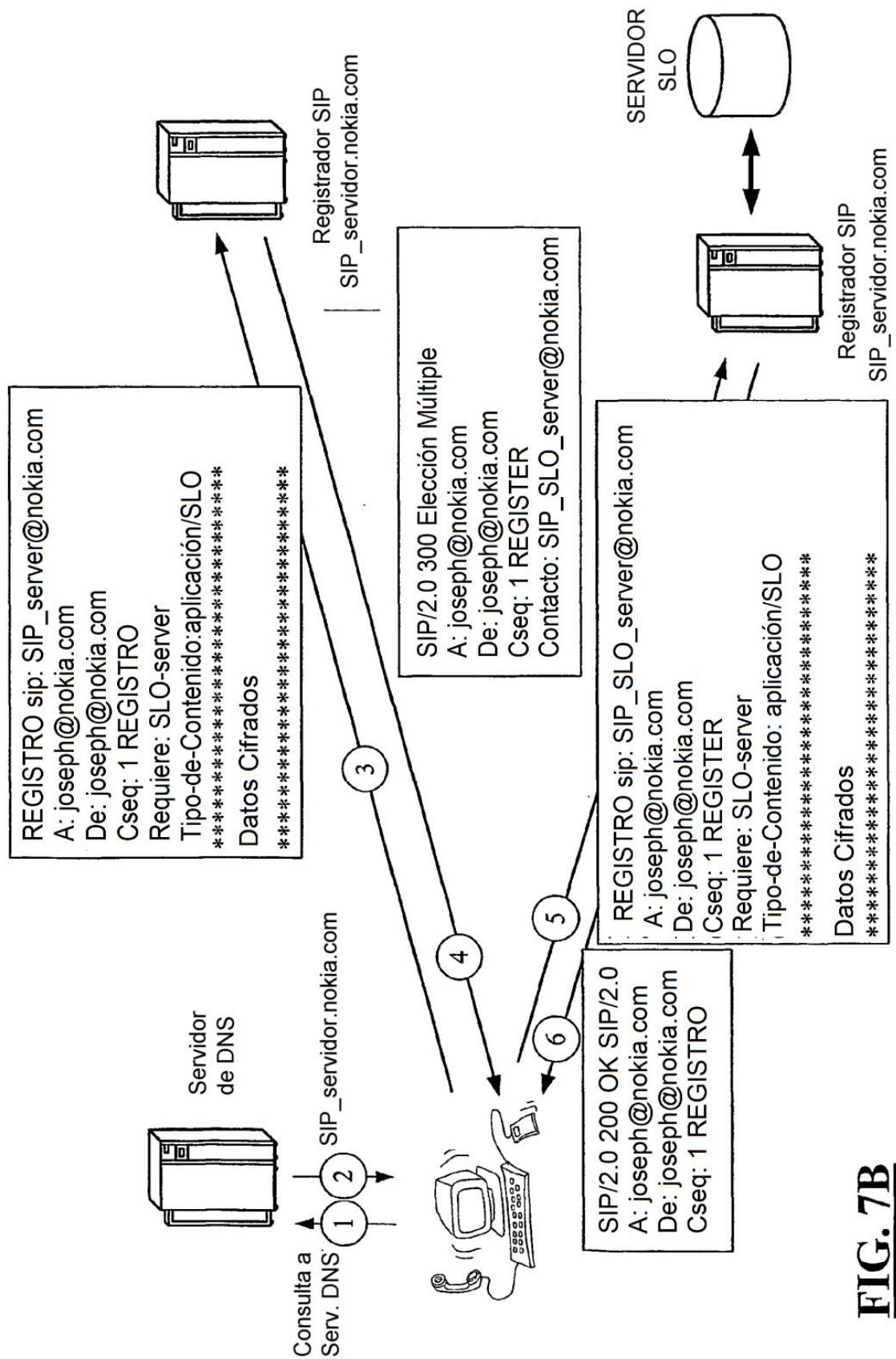


FIG. 7A

**FIG. 7B**

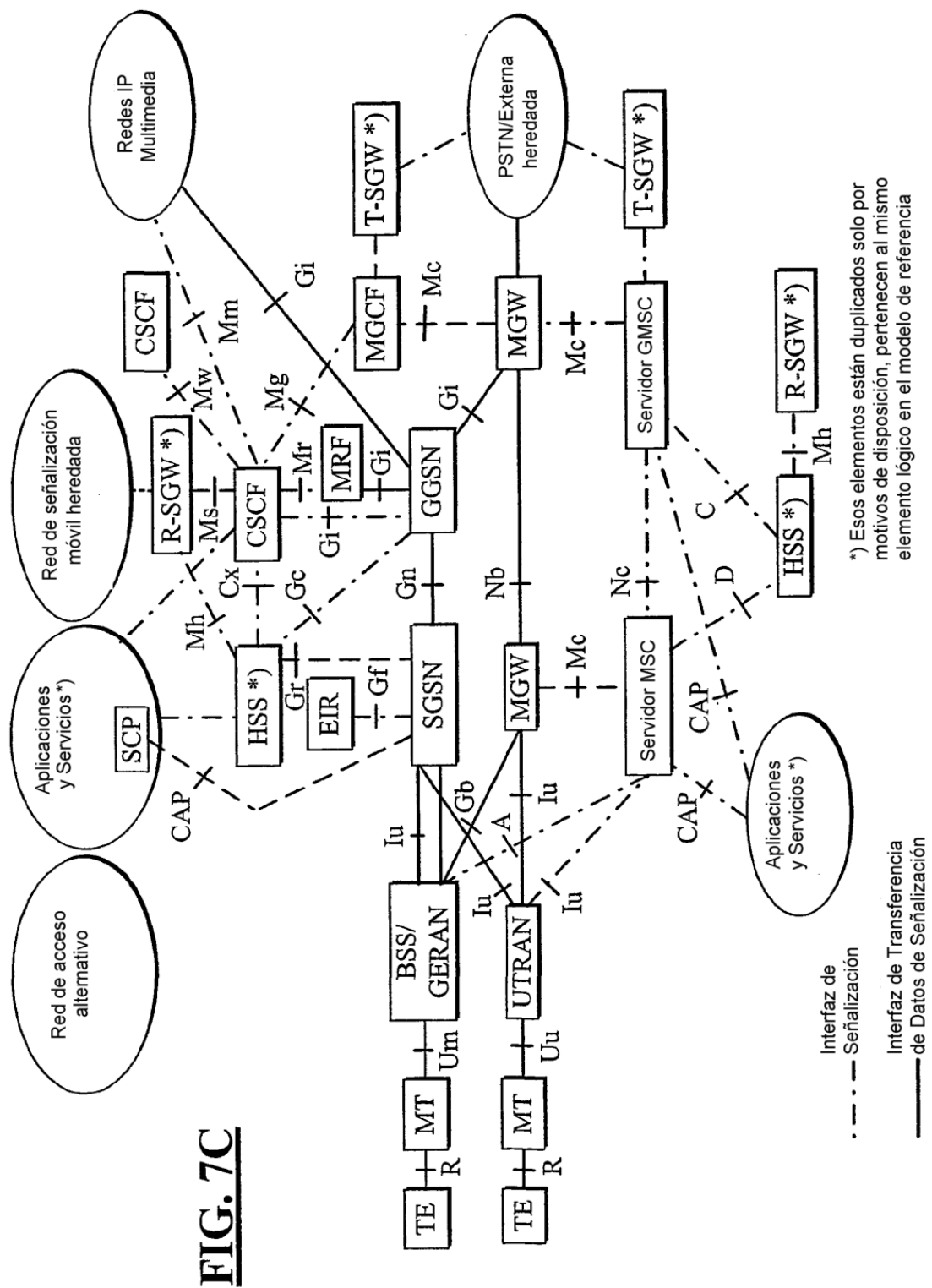
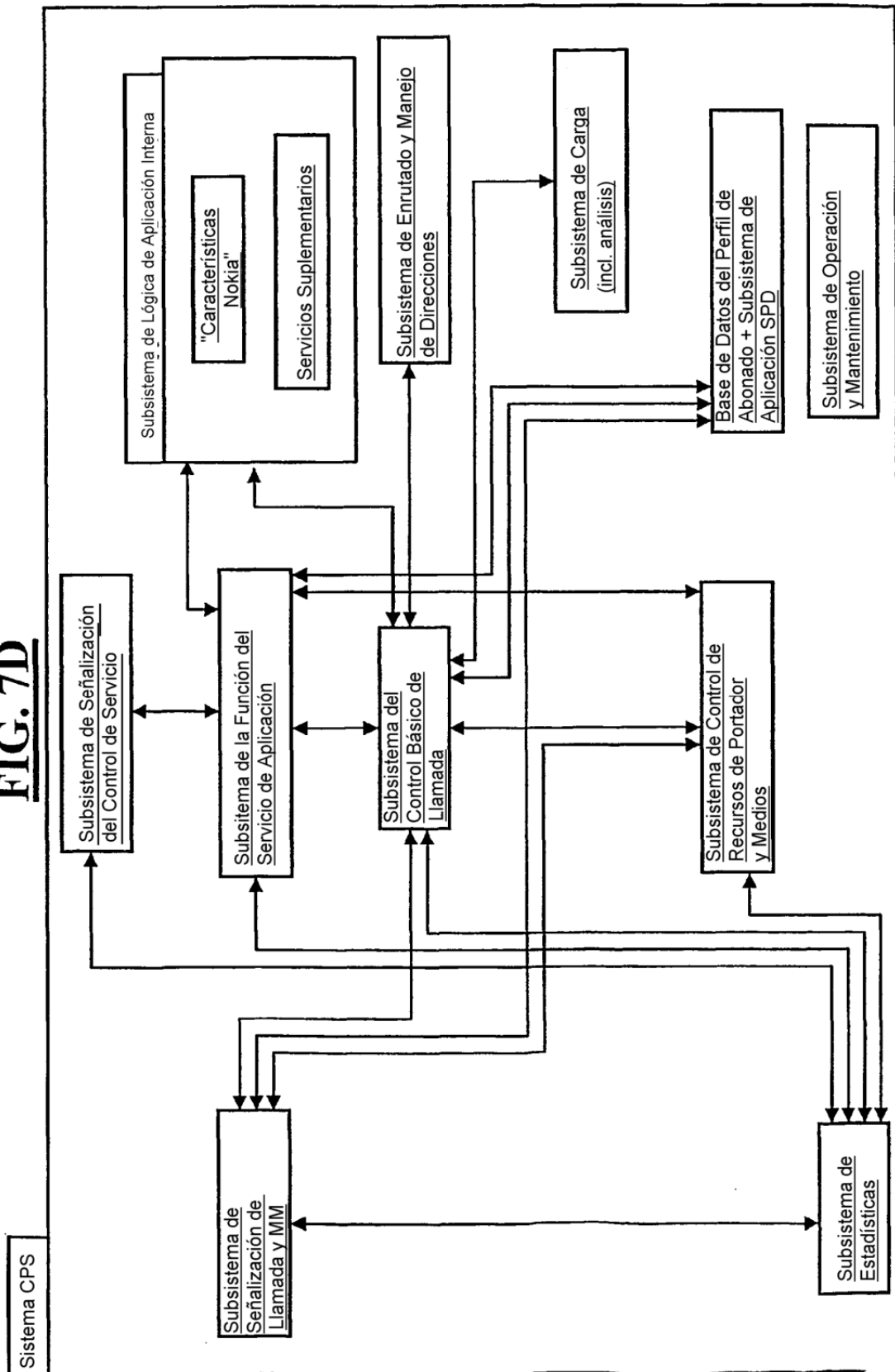
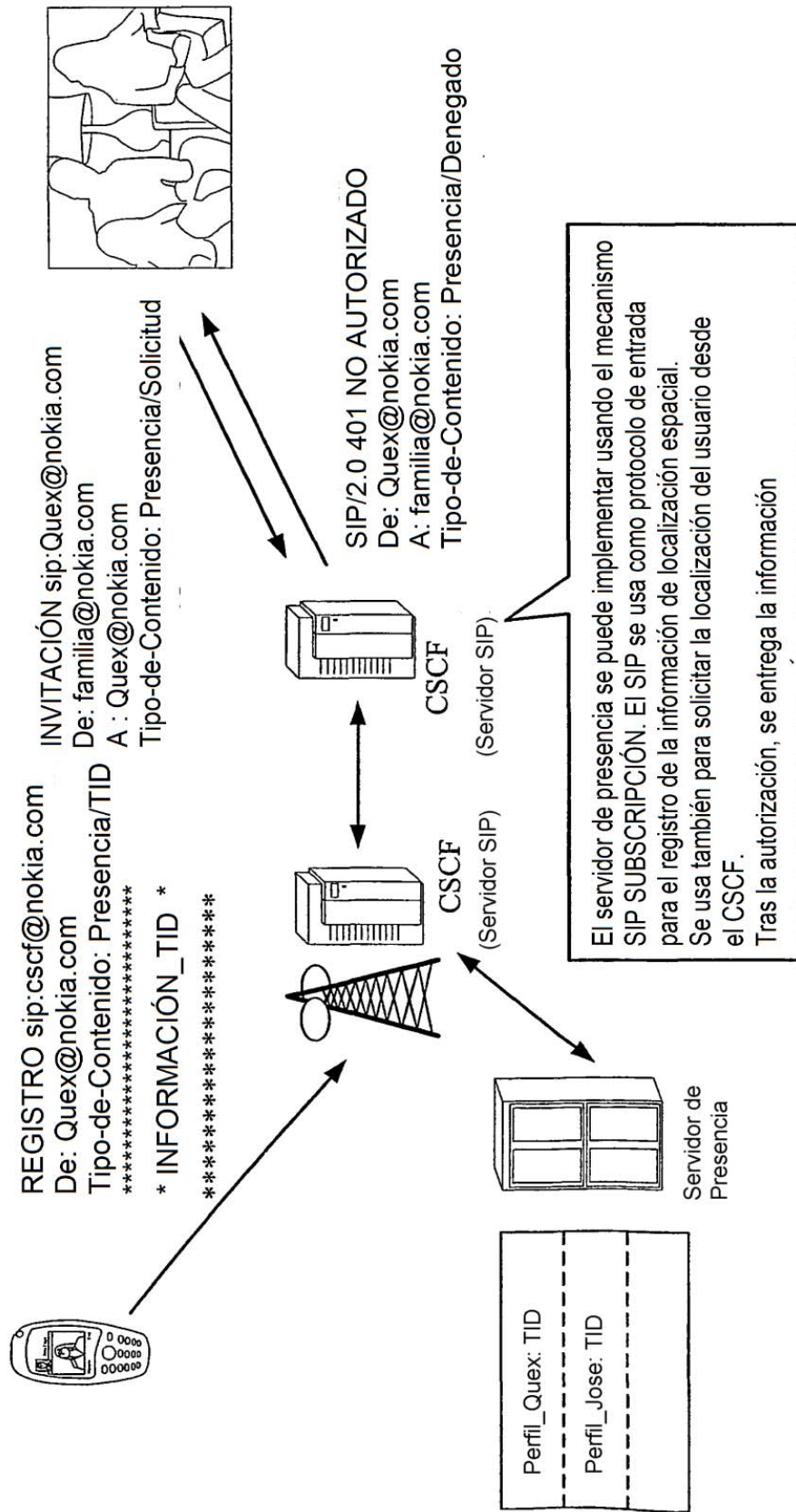


FIG. 7D

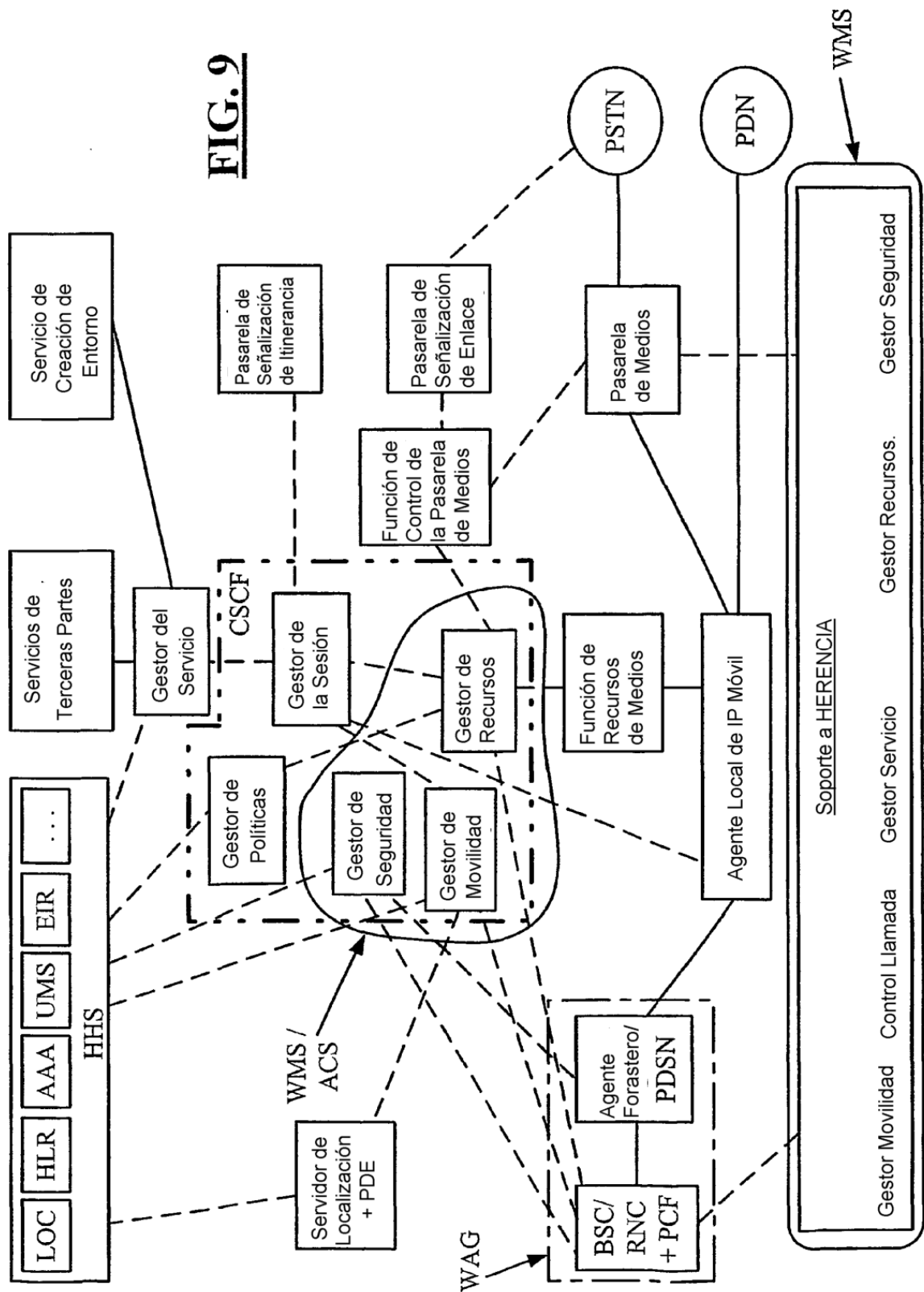


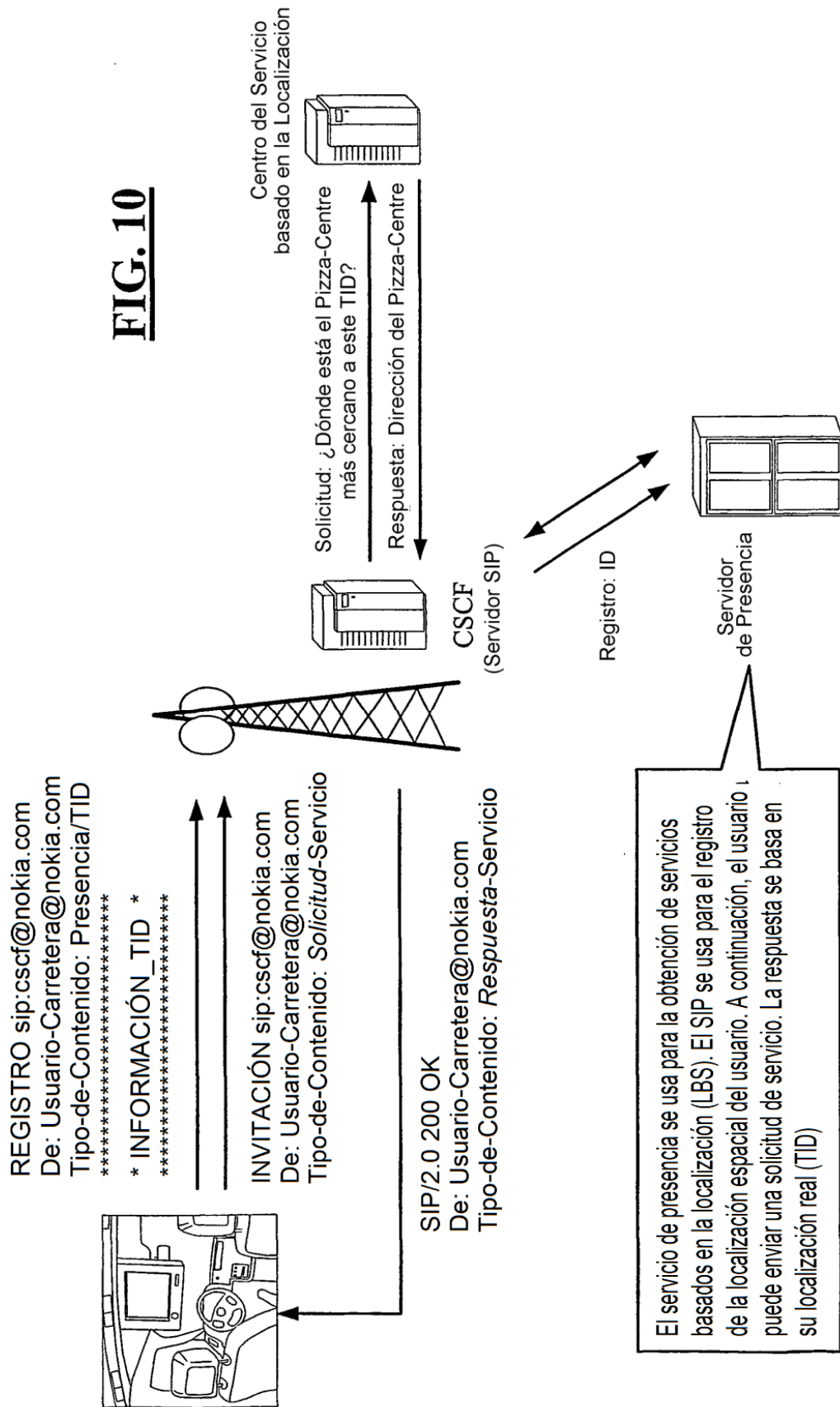


TID: Identificador de Información Objetivo da la información de localización del usuario en base a GPS u otro mecanismo

FIG. 8

FIG. 9





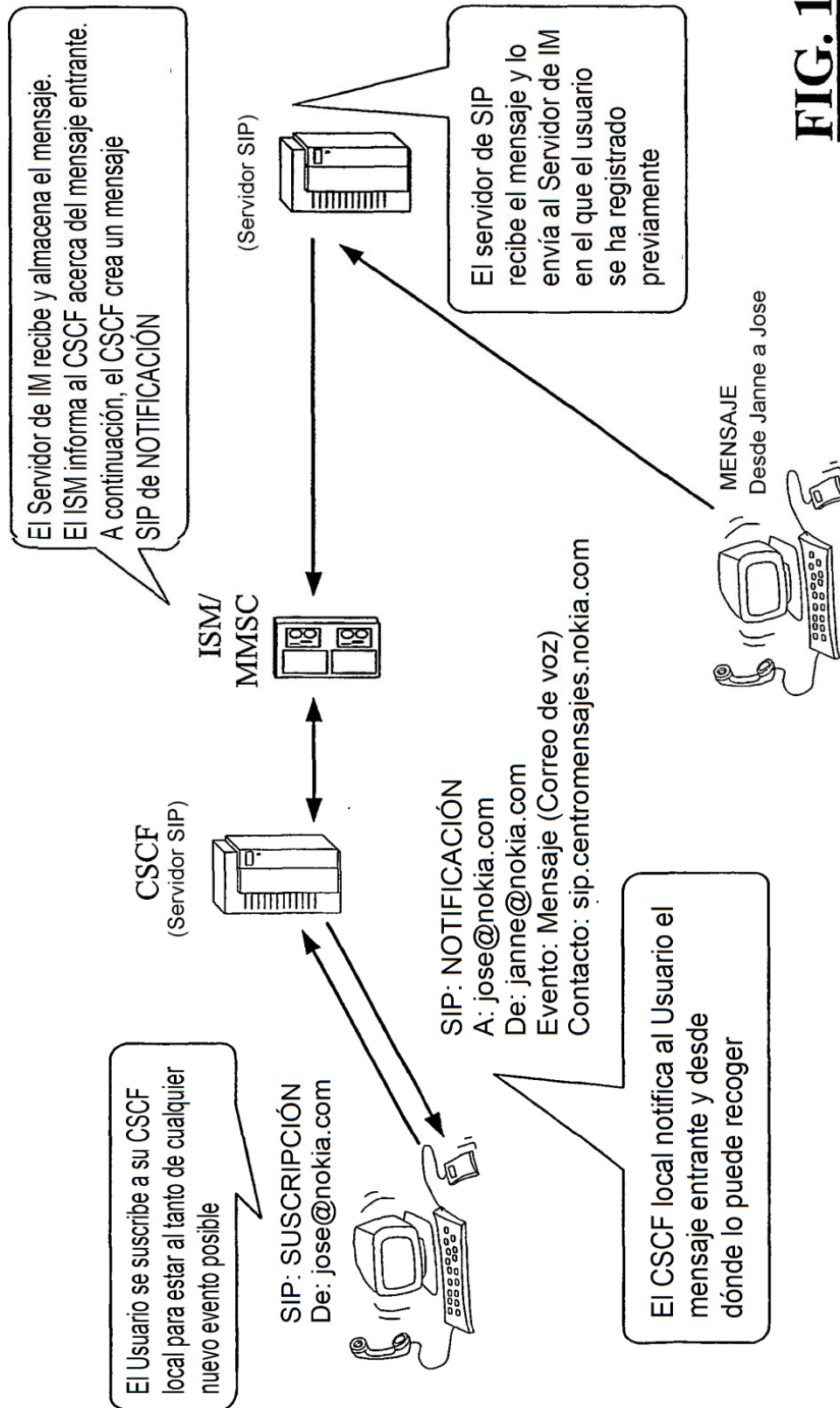


FIG. 11

FIG. 12

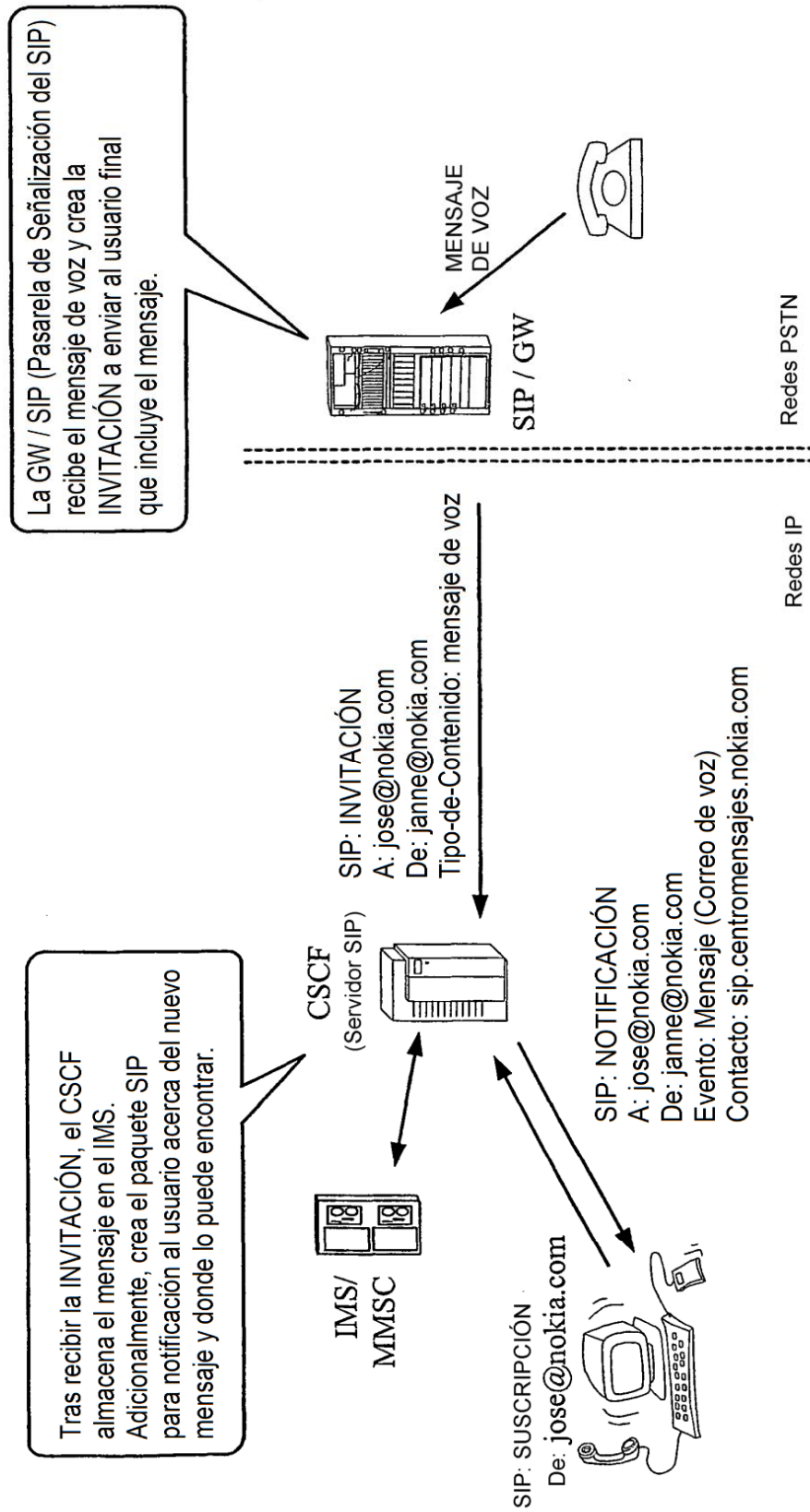
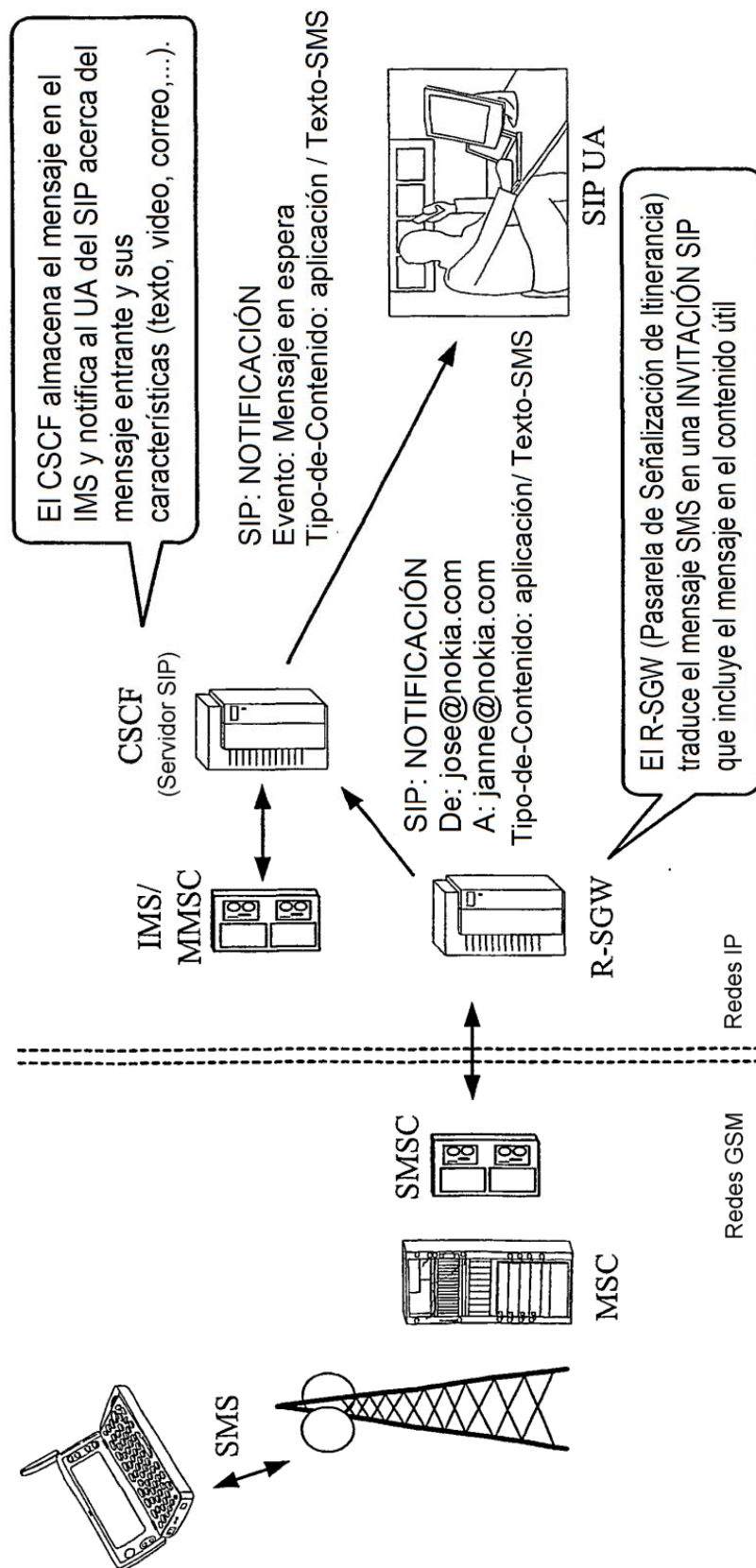
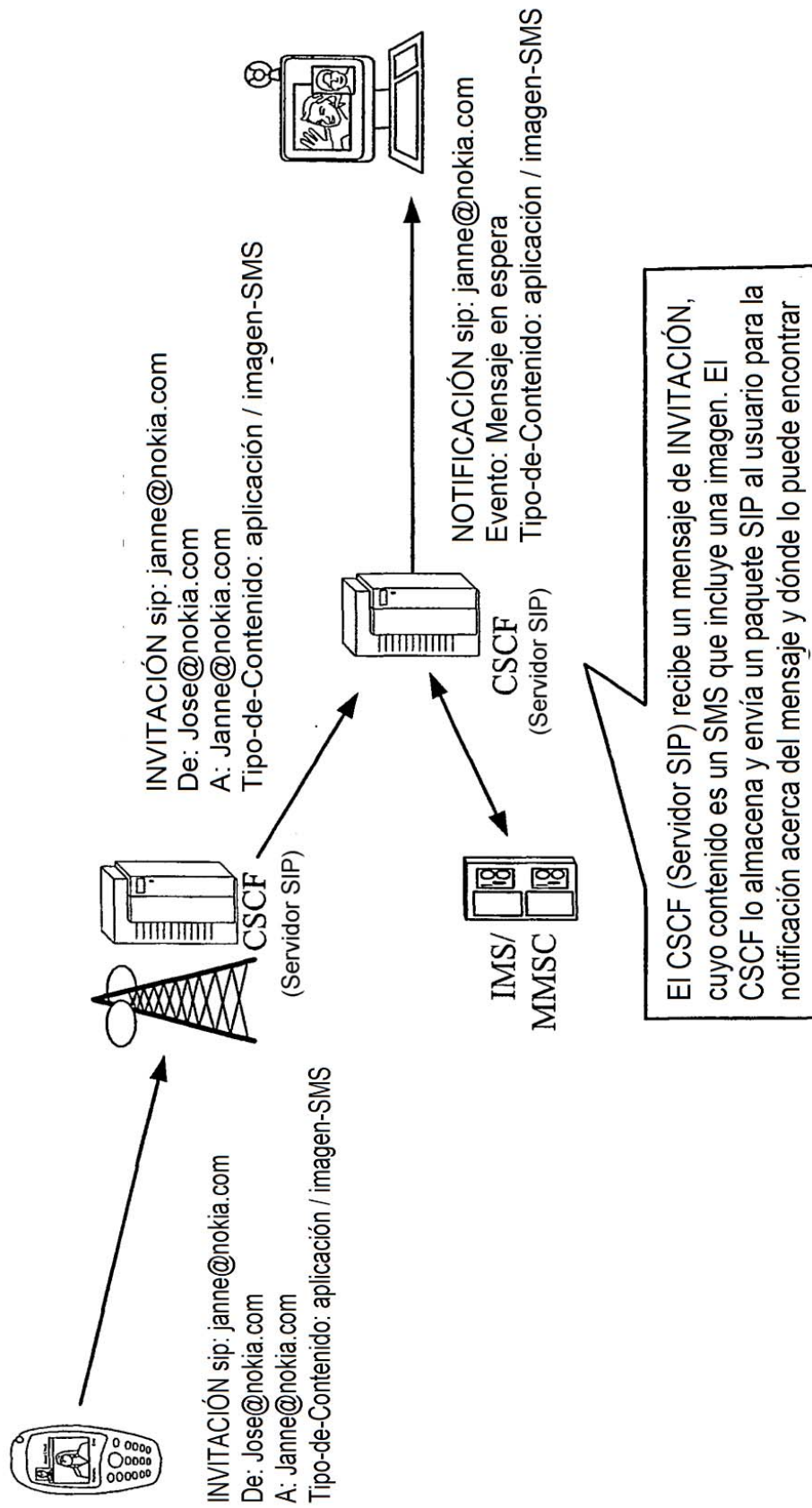
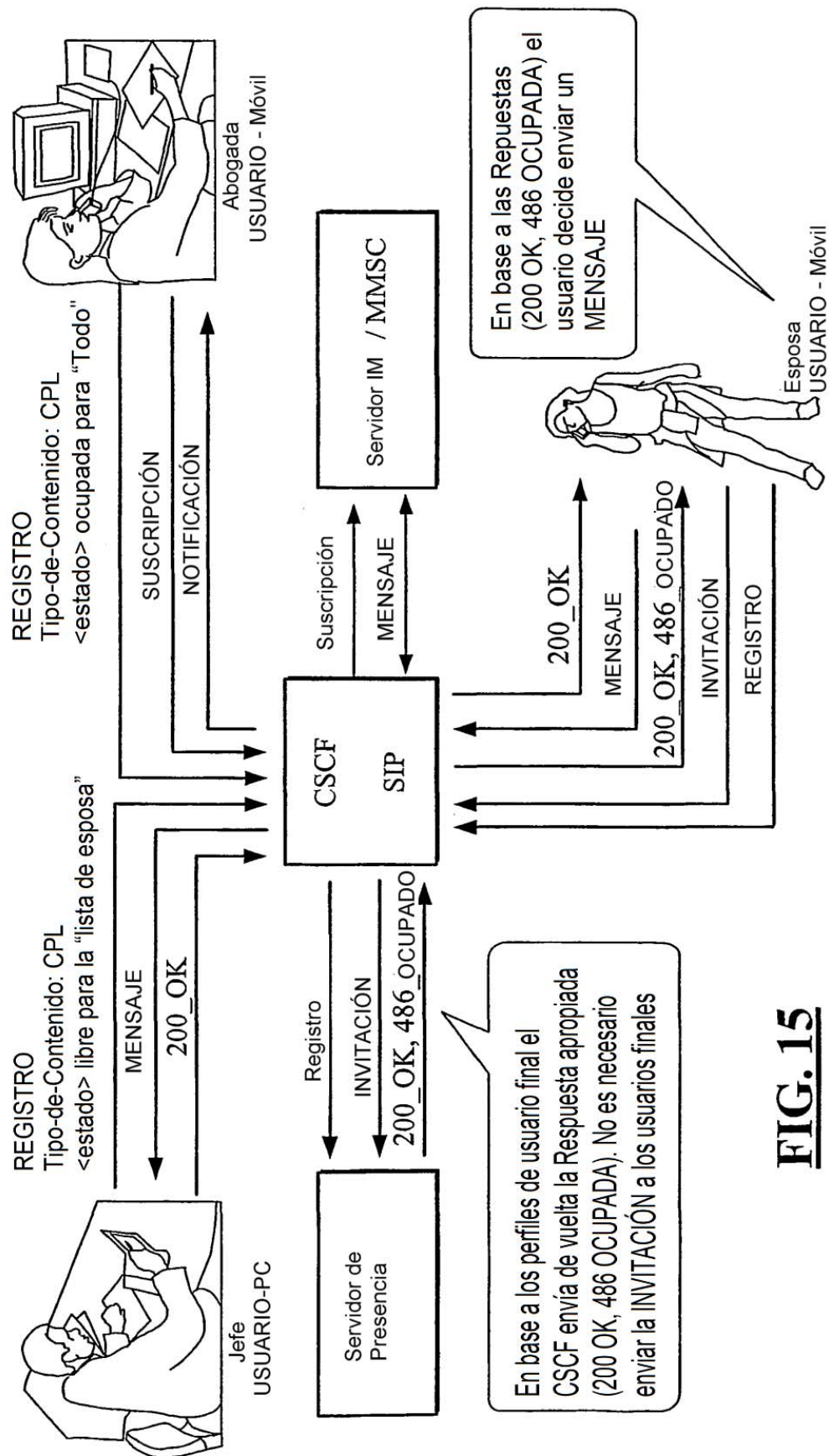


FIG. 13

**FIG. 14**

**FIG. 15**

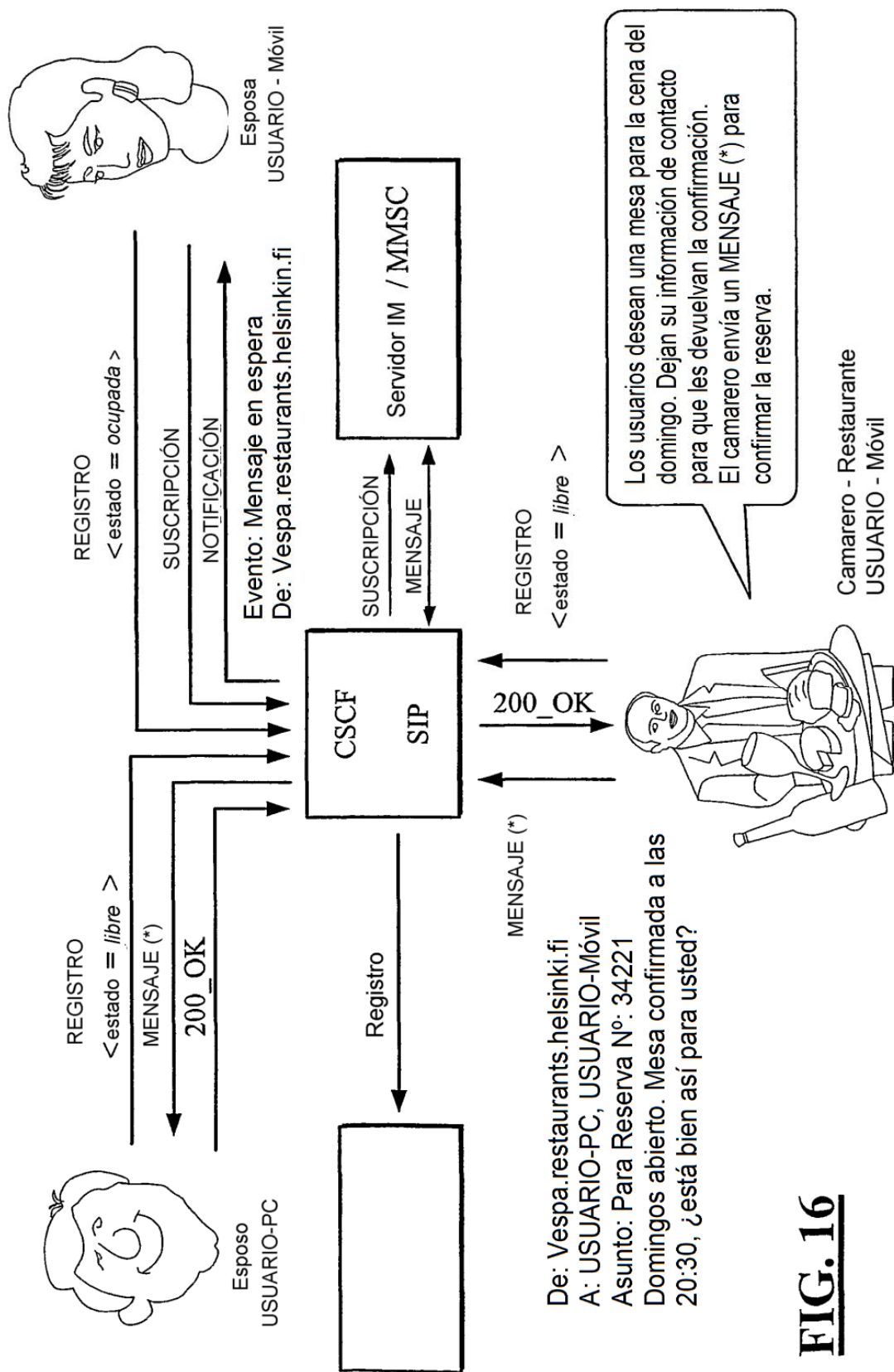


FIG. 16