(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 339 808**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04W 4/00 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06819070 .1**
(96) Fecha de presentación : **03.10.2006**
(97) Número de publicación de la solicitud: **2070287**
(97) Fecha de publicación de la solicitud: **17.06.2009**

(54) Título: **Suministro de información de acceso en una red de comunicación.**

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm, SE

(45) Fecha de publicación de la mención BOPI:
25.05.2010

(72) Inventor/es: **Lindholm, Fredrik;**
Terrero Díaz-Chirón, María Esther y
Esteban-Vares, Nuria

(45) Fecha de la publicación del folleto de la patente:
25.05.2010

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Suministro de información de acceso en una red de comunicación.

Campo de la invención

La presente invención se refiere al suministro de información de acceso en una red de Subsistema Multimedia IP.

Antecedentes de la invención

Los servicios Multimedia IP proporcionan una combinación dinámica de voz, vídeo, mensajería, datos, etc., dentro de la misma sesión. Haciendo crecer el número de aplicaciones básicas y los medios que son posibles combinar, crecerá el número de servicios ofrecidos a los usuarios finales, y se enriquecerá la experiencia de comunicación interpersonal. Esto conducirá a una nueva generación de servicios de comunicaciones multimedia personalizados y abundantes, incluyendo los denominados servicios "Multimedia IP de combinación" que se consideran en más detalle debajo.

El Subsistema Multimedia IP (IMS) es la tecnología definida por el Proyecto de Cooperación de Tercera Generación (3GPP) para proporcionar servicios Multimedia IP sobre redes de comunicaciones móviles (3GPP TS 22.228, TS 23.218, TS 23.228, TS 24.228, TS 24.229, TS 29.228, TS 29.229, TS 29.328 y TS 29.329 Comunicados 5 a 7). El IMS proporciona las características clave para enriquecer la experiencia de comunicación persona a persona del usuario final a través del uso de Activadores de Servicio IMS estandarizados, que facilitan nuevos servicios de comunicación persona a persona (cliente a cliente) abundantes así como servicios persona a contenido (cliente a servidor) sobre redes basadas en IP. El IMS hace uso del Protocolo de Inicio de Sesiones (SIP) para establecer y controlar las llamadas o sesiones entre los terminales de usuario (o terminales de usuario y servidores de aplicación). El Protocolo de Descripción de Sesiones (SDP), transportado por la señalización SIP, se usa para describir y negociar los componentes del medio de la sesión. Mientras que SIP fue creado como un protocolo usuario a usuario, el IMS permite a los operadores y proveedores de servicios controlar el acceso del usuario a los servicios y facturar a los usuarios en consecuencia.

La Figura 1 ilustra esquemáticamente cómo el IMS se integra en la arquitectura de red móvil en el caso de una red de acceso del Servicio General de Radio por Paquetes (GPRS)/Paquetes Conmutados (PS). Las Funciones de Control de Sesión de Llamada (CSCFs) funcionan como intermediarios SIP dentro del IMS. La arquitectura 3GPP define tres tipos de CSCFs: la CSCF (P-CSCF) Intermediaria que es el primer punto de contacto dentro del IMS para un terminal SIP; la CSCF de Servicio (S-CSCF) que proporciona los servicios al usuario a los que el usuario está abonado; y la CSCF de Interrogación (I-CSCF) cuyo papel es identificar la S-CSCF correcta y reenviar a esa S-CSCF una solicitud recibida desde un terminal SIP a través de una P-CSCF. Por supuesto, se puede acceder al IMS desde otros tipos de redes de acceso, por ejemplo una red de Red de Área Local Inalámbrica (WLAN).

En algunas circunstancias, es deseable proporcionar información de acceso del usuario, que incluye información sobre la tecnología usada para acceder a la red, y la ubicación del usuario, a un Servidor de Abonado Local (HSS). Un ejemplo de esto está donde el control de acceso depende del Punto de Acceso (AP) usado para acceder a la red. Un AP puede ser una estación base de una WLAN o un Nodo B de la red celular 3GPP. Puede ser deseable permitir a los operadores de redes IMS controlar qué APs se puedan usar para acceder a sus redes. Por ejemplo, un operador de red puede haber negociado una tarifa especial con una compañía que depende de los empleados de la compañía que acceden a la red IMS del operador solamente a través de los APs del operador de red. Para controlar el acceso a una red dependiendo del AP usado, la información de acceso se debe almacenar en el perfil del usuario en el HSS.

Otro ejemplo de un escenario donde es deseable proporcionar la información de acceso a un HSS surge de la Convergencia Fija Móvil (FMC). Un usuario que tiene una suscripción a una red IMS puede tener múltiples identidades de usuario, algunas de las cuales se pueden usar para acceder a una red usando un servicio de línea fija y algunas de las cuales se pueden usar para acceder a una red usando un servicio móvil. Las capacidades de los servicios móviles y fijos pueden diferir, y así la información de acceso del usuario se requiere para ser almacenada en el perfil del usuario para mostrar qué tipo de red de acceso o AP fue usado para acceder a la red IMS. Esto permitirá que los servicios disponibles sean determinados dependiendo del perfil del usuario y las capacidades del AP o la red de acceso.

Los mecanismos están disponibles para proporcionar información de acceso al HSS. Uno de tales métodos es para que el Equipo de Usuario obtenga la dirección de Control de Acceso al Medio (MAC) del AP e incluya ésta en un mensaje de REGISTRO SIP. La dirección MAC entonces se puede usar para identificar la ubicación del usuario al HSS. No obstante, este planteamiento requiere señalización además de enviar un mensaje de REGISTRO SIP para obtener la dirección MAC del AP.

La publicación "Permitir la ejecución del servicio en IMS en base al tipo de Red de Acceso", MOTOROLA (IP.com número IPCOM000136021D) publicada el 3 de mayo de 2006 y la WO2006/100459 A2 exponen los métodos para controlar el acceso al servicio IMS.

Compendio de la invención

Cuando un usuario accede a una red de Subsistema Multimedia IP, el Equipo de Usuario (UE) incluye una cabecera de Información de Red de Acceso P (PANI) en cada mensaje enviado durante un procedimiento de registro, por ejemplo un mensaje de REGISTRO SIP (ver la ETSI ES 283 003 V1.1.1). La cabecera PANI es una cabecera definida 3GPP e indica a la red IMS sobre qué tecnología de acceso el UE se une al IMS, y también la ubicación del usuario. En el momento presente, la PANI se puede enviar desde el UE a una Función de Control de Sesión de Llamada (CSCF), o alternativamente, para algún acceso, la CSCF Intermediaria añade la ubicación en base al conocimiento local.

Los inventores de la presente invención han comprendido que enviando la información de acceso de la PANI, o los contenidos completos de la PANI en sí misma, al Servidor de Abonado Local, un registro persistente de la información de acceso para una sesión se puede almacenar en el perfil de usuario, y esta información se puede usar para controlar el acceso a la red dependiendo de la información de acceso, o determinar los servicios disponibles para el usuario en base a las capacidades de la tecnología de la red de acceso y la ubicación usada (denominada como información de acceso).

De acuerdo con un primer aspecto de la invención, se proporciona un método de control de acceso a los servicios de un Subsistema Multimedia IP de acuerdo con la reivindicación 1.

Es preferible que el mensaje sea un mensaje de REGISTRO SIP.

En una realización preferente de la invención, el método además comprende la verificación de la cabecera de Información de Red de Acceso P o la información de acceso obtenida de allí. El paso de verificación puede comprender comparar la cabecera de Información de Red de Acceso P o la información de acceso obtenida de allí con una gama de cabeceras de Información de Red de Acceso P que se pueden usar por la Función de Control de Sesión de Llamada. Alternativamente, el paso de verificación puede comprender obtener la información de ubicación de una función de registro de ubicación móvil y comparar la información de ubicación obtenida con la información de acceso obtenida de la cabecera de Información de Red de Acceso P.

También se proporciona un método de control de acceso a los servicios de un Subsistema Multimedia IP por un usuario, en base a la ubicación del usuario, el método que comprende:

proporcionar la información de acceso a un Servidor de Abonado Local usando el método descrito arriba;

comparar la información de ubicación obtenida a partir de la información de acceso con la información de autorización almacenada en una base de datos, la información de autorización que comprende información que identifica las ubicaciones de acceso permitido y/o prohibido para el usuario; y

dependiendo del resultado de la comparación, permitir o denegar el acceso a los servicios del Subsistema Multimedia IP.

Además, se proporciona un método de determinación de los servicios disponibles para un usuario desde un Servidor de Aplicaciones en base a la información de acceso del usuario, el método que comprende:

proporcionar la información de acceso a un Servidor de Abonado Local usando el método descrito arriba;

transmitir la información de acceso desde el Servidor de Abonado Local al Servidor de Aplicaciones; y

comparar la información de acceso con los servicios disponibles y, en base a la comparación, determinar qué servicios poner a disposición del usuario.

Adicionalmente, se proporciona un método de filtrado de un perfil de usuario en una red de Subsistema Multimedia IP basado en la información de acceso del usuario, el método que comprende:

proporcionar la información de acceso a un Servidor de Abonado Local usando el método descrito arriba;

en el Servidor de Abonado Local, filtrar el perfil de usuario en base a la información de acceso.

Se proporciona un método de suministrar un perfil de usuario a una Función de Control de Sesión de Llamada que comprende:

filtrar el perfil de usuario usando el método descrito arriba; y

entregar el perfil de usuario filtrado a una Función de Control de Sesión de Llamada.

De acuerdo con un segundo aspecto de la presente invención, se proporciona una Función de Control de Sesión de Llamada de Interrogación para usar en un Subsistema Multimedia IP de acuerdo con la reivindicación 9.

De acuerdo con un tercer aspecto de la presente invención, se proporciona un Servidor de Abonado Local para usar en un Subsistema Multimedia IP de acuerdo con la reivindicación 10.

Es preferible que el Servidor de Abonado Local además comprenda los medios para actualizar un perfil de usuario con los contenidos recibidos.

Breve descripción de los dibujos

La Figura 1 ilustra esquemáticamente un Subsistema Multimedia IP;

La Figura 2 ilustra una secuencia de señalización para el intento de registro de un Punto de Acceso no permitido;

La Figura 3 ilustra una secuencia de señalización para obtener la información de acceso de un Servidor de Abonado Local;

La Figura 4 ilustra una secuencia de señalización para notificar una Función de Control de Sesión de Llamada de la información de acceso del usuario; y

La Figura 5 ilustra esquemáticamente un ejemplo conocido de un conjunto de Identidades de Usuario Públicas y Privadas Multimedia IP asociadas con una suscripción del Subsistema Multimedia IP.

Descripción detallada de las realizaciones preferentes

Como se describe arriba, una cabecera de Información de Red de Acceso P (PANI) se puede generar en el Equipo de Usuario (UE) del usuario e incorporar en cada mensaje enviado por el UE, o alternativamente la cabecera PANI se añade a un mensaje por la CSCF Intermediaria (P-CSCF). La información contenida en la cabecera PANI se muestra en la Tabla 1. La cabecera PANI incluye información que identifica el tipo de red de acceso (por ejemplo 3GPP-UTRAN-FDD, 3GPP-GERAN, ADSL etc.) sobre la que se anexa el UE a la red IMS, y la ubicación del usuario.

En el caso donde el UE accede a la red IMS a través de una red de acceso inalámbrico y una Función de Control de Sesión de Llamada Intermediaria conforme con las especificaciones de 3GPP Comunicado 6, la cabecera PANI no se verifica. La red IMS asume que el UE ha insertado la información de acceso correcta en la cabecera PANI. Por otra parte, donde el UE accede a la red IMS a través de una red de línea fija, la P-CSCF verifica que la información contenida en la cabecera PANI es correcta, y si no, sustituye la cabecera PANI con la cabecera PANI correcta.

Cuando un usuario intenta acceder a una red IMS, el UE envía un mensaje de REGISTRO SIP a la P-CSCF. El mensaje de REGISTRO SIP incluye una cabecera PANI. La P-CSCF, en lugar de eliminar la cabecera PANI, la permite para que se envíe a la Función de Control de Sesión de Llamada de Interrogación (I-CSCF) dentro del mensaje REGISTRO. En la presente invención, la I-CSCF envía entonces un mensaje de Petición de Autorización de Usuario (UAR) al Servidor de Abonado Local (HSS), e incluye o bien la PANI o bien la información de acceso obtenida de la PANI en el mensaje de UAR.

Un mensaje de UAR es un mensaje estándar enviado desde la I-CSCF al HSS que, entre otras cosas, solicita autorización para el usuario. Los códigos de comando de Forma Backus-Naur Aumentada (ABNF) para enviar esta información son como sigue, donde la “Información de Acceso” es el nuevo elemento de información:

```
Message Format
< User-Authorisation-Request> ::= < Diameter Header: 300, REQ, PXY, 16777216 >
        < Session-Id >
        { Vendor-Specific-Application-Id }
        { Auth-Session-State }
        { Origin-Host }
        { Origin-Realm }
        [ Destination-Host ]
        { Destination-Realm }
        { User-Name }
        *[ Supported-Features ]
        { Public-Identity }
        { Visited-Network-Identifier }
        [ User-Authorisation-Type ]
        [Access-Information]
        *[ AVP ]
        *[ Proxy-Info ]
```

Del mismo modo, otros intercambios de mensajes de Diámetro entre una S-CSCF y el HSS, y entre un Servidor de Aplicaciones (AS) y el HSS se pueden ampliar para incluir la información de acceso.

Como se describe arriba, donde un usuario intenta registrarse a través de una red de acceso móvil, la cabecera PANI no se puede verificar antes de ser enviada al HSS. En este caso, la lógica para verificar la cabecera PANI se proporciona para verificar la cabecera PANI en la I-CSCF, la CSCF de Servicio (S-CSCF) o el Servidor de Aplicaciones (AS) que envía la cabecera PANI al HSS. Esta lógica se puede realizar comprobando si se puede confiar en la cabecera PANI comprobando la P-CSCF usada contra una lista configurada. Si la cabecera PANI no es de confianza, la lógica o bien comprueba si la cabecera PANI está dentro de un conjunto de cabeceras PANI que se pueden usar por la P-CSCF, o bien comprueba con la función de registro de ubicación móvil y compara la ubicación contenida en la cabecera PANI con la ubicación dada por la función de registro de ubicación móvil.

Una vez que se ha recibido la cabecera PANI por el HSS, el HSS puede almacenar la información de acceso en el perfil de usuario relativa a la ubicación de acceso o tecnología de acceso usada para acceder a la red.

La información de acceso se puede usar para comprobar si el usuario está autorizado para registrarse en la red IMS desde la red de acceso usada. Con referencia a la Figura 2, la autorización de acceso se controla por la I-CSCF y el HSS. La I-CSCF recibe un mensaje de REGISTRO SIP desde el Equipo de Usuario, el mensaje de REGISTRO SIP que incluye una cabecera PANI. La I-CSCF envía una petición de Consulta Cx (UAR) que contiene la cabecera PANI y la Identidad Pública Multimedia IP (IMPU) del usuario al HSS. El HSS compara la PANI recibida con una lista almacenada de PANIs autorizadas, y toma una decisión sobre si permitir el acceso o no en base a esa comparación. El HSS puede controlar la autorización en base a distintos parámetros. Por ejemplo, el usuario puede ser autorizado para acceder a la red desde una de una pluralidad de ubicaciones distintas.

Autorizando al usuario a través de la I-CSCF, ciertos usuarios, por ejemplo aquéllos que solamente usan métodos débiles de autenticación, se les puede impedir acceder a la red IMS central. Como ejemplo, el acceso se puede limitar solamente a las peticiones de acceso que son altamente de confianza.

Además, el HSS puede definir dinámicamente las Capacidades del Servidor para la selección de la S-CSCF en base al acceso usado e identificado en la PANI.

Otro uso para la información de acceso almacenada está en permitir a un Servidor de Aplicaciones (AS) recuperar la información de usuario a partir del HSS que puede ser relevante para un acceso particular. Esto puede permitir a un AS adecuar el servicio a un usuario en base a la información de acceso. Con referencia a la Figura 3, el AS recibe un SIP INVITE desde el UE para acceder a un servicio particular. El AS envía un mensaje Sh-pull al HSS. La petición Sh-pull incluye un valor de la Referencia de Datos AVP para solicitar la información de acceso almacenada en el perfil del usuario en el HSS. El HSS recibe el mensaje Sh-pull y recupera la información de acceso solicitada. La información de acceso se incluye con la respuesta Sh-pull enviada desde el HSS al AS.

Otro uso de esta invención es que el AS puede adecuar el servicio proporcionado al usuario dependiendo de la información de acceso recibida. El AS puede proporcionar la información de acceso de usuario en una consulta al HSS, y el HSS responde con un perfil personalizado para ese usuario en base a la información de acceso del usuario. Por ejemplo, la tecnología de acceso usada para acceder a la red puede establecer limitaciones en el tipo de datos que se pueden incluir en el servicio.

La información de acceso almacenada también se puede usar por el HSS para filtrar el perfil requerido por un usuario para un acceso dado. Por ejemplo, si un usuario se registra para un servicio desde un acceso de línea fija, se pueden omitir las partes del servicio que son relevantes solamente para el acceso móvil en la descarga del perfil. Esto aumenta la eficiencia de los procedimientos de activación del servicio en la S-CSCF, ya que se reduce el número de desencadenantes que se deben evaluar por la S-CSCF. Otra información se puede incluir en el perfil, tal como la hora del día y el método de autenticación, además de la información de acceso. Con referencia a la Figura 4, un UE envía un mensaje de REGISTRO SIP a una S-CSCF. La S-CSCF envía una Petición de Asignación de Servidor (SAR) al HSS, la SAR que contiene las Identidades Públicas Multimedia IP (IMPU) del usuario. El HSS filtra el perfil de las IMPU para ese acceso y devuelve una respuesta de SAR a la S-CSCF que contiene un perfil de Servicio (SP), que incluye activadores de los Criterios de Filtro Inicial. La S-CSCF usa el SP para adecuar el servicio.

El almacenamiento persistente de la información de acceso en un perfil del usuario en el HSS también se puede usar para soportar el manejo de identidades múltiples. Con referencia a la Figura 5, se ilustra esquemáticamente un ejemplo conocido de un conjunto de Identidades de Usuario Públicas y Privadas Multimedia IP asociadas con una suscripción al Subsistema Multimedia IP. En este ejemplo, un usuario que tiene una suscripción IMS tiene dos Identidades Privadas Multimedia IP (IMPIs), IMPI-1 e IMPI-2. La IMPI-1 tiene dos Identidades de Usuario Públicas Multimedia IP (IMPUs), IMPU-1 e IMPU-2, asociadas con ella. La IMPI-2 tiene una IMPU, IMPU-3 asociada con ella. La IMPU-1 se asocia con un primer perfil de servicio, mientras que la IMPU-2 y la IMPU-3 están cada una asociadas con un segundo perfil de servicio. En este ejemplo, se puede acceder a la IMPU-2 simultáneamente por el acceso de línea fija y un acceso móvil. Proporcionando el HSS con la información de acceso, la red se hace consciente de la tecnología de acceso usada para acceder a la red. Esto permite, por ejemplo, el uso de distintos métodos de autenticación para cada IMPU, dependiendo de la información de acceso proporcionada al HSS.

Se apreciará por las personas expertas en la técnica que se pueden hacer varias modificaciones a las realizaciones descritas arriba sin salir del alcance de la presente invención.

TABLA 1

P-Access-Network-Info =	"P-Access-Network-Info" HCOLON access-net-spec * (COMMA access-net-spec)
access-net-spec	= access-type * (SEMI access-info)
access-type	= "IEEE-802.11" / "IEEE-802.11a" / "IEEE-802.11b" / "IEEE-802.11g" / "3GPP-GERAN" / "3GPP-UTRAN-FDD" / "3GPP-UTRAN-TDD" / "ADSL" / "ADSL2" / "ADSL2+" / "RADSL" / "SDSL" / "HDSL" / "HDSL2" / "G.SHDSL" / "VDSL" / "IDSL" / "3GPP2-1X" / "3GPP2-1X-HRPD" /token
access-info	= cgi-3gpp / utran-cell-id-3gpp / dsl-location / np / ci-3gpp2/ extension- access-info
extension-access-info	= gen-value
cgi-3gpp	= "cgi-3gpp" EQUAL (token / quoted-string)
utran-cell-id-3gpp	= "utran-cell-id-3gpp" EQUAL (token / quoted-string)
dsl-location	= "dsl-location" EQUAL (token / quoted-string)
np	= "network-provided"
ci-3gpp2	= "ci-3gpp2" EQUAL (token / quoted-string)

REIVINDICACIONES

1. Un método para controlar el acceso a servicios de una red del Subsistema Multimedia IP basado en una ubicación del usuario, el método que comprende:

transmitir un mensaje desde el Equipo de Usuario a una Función de Control de Sesión de Llamada de Interrogación, el mensaje que incluye una cabecera de Información de Red de Acceso P;

transmitir información de acceso que comprende la información de ubicación contenida en la cabecera de Información de Red de Acceso P desde la Función de Control de Sesión de Llamada de Interrogación a un Servidor de Abonado Local,

en el Servidor de Abonado Local, almacenar la información de acceso recibida;

en el Servidor de Abonado Local, comparar la información de ubicación recibida obtenida a partir de la información de acceso con la información de autorización almacenada en una base de datos, la información de autorización que identifica ubicaciones de acceso permitidas y/o prohibidas para el usuario; y

dependiendo de los resultados de la comparación, permitir o denegar el acceso a la red del Subsistema Multimedia IP.

2. El método de acuerdo con la reivindicación 1, en donde el mensaje es un mensaje de REGISTRO SIP.

3. El método de acuerdo con la reivindicación 1 o 2, que comprende verificar la cabecera de Información de Red de Acceso P o la información de acceso obtenida desde allí.

4. El método de acuerdo con la reivindicación 3, en donde el paso de verificación comprende comparar la cabecera de Información de Red de Acceso P o la información de acceso obtenida desde allí con una gama de cabeceras de Información de Red de Acceso P que se pueden usar por la Función de Control de Sesión de Llamada de Interrogación.

5. El método de acuerdo con la reivindicación 3, en donde el paso de verificación comprende obtener la información de ubicación de una función de registro de ubicación móvil y comparar la información de ubicación obtenida con la información de acceso obtenida de la cabecera de Información de Red de Acceso P.

6. El método de acuerdo con cualquiera de las reivindicaciones 1 a 5, el método que además comprende:

transmitir la información de acceso desde el Servidor de Abonado Local a un Servidor de Aplicaciones; y

comparar la información de acceso con los servicios disponibles y, en base a la comparación, determinar qué servicios poner a disposición del usuario.

7. El método de acuerdo con cualquiera de las reivindicaciones 1 a 5, el método que además comprende, en el Servidor de Abonado Local, filtrar un perfil de usuario en base a la información de acceso.

8. El método de acuerdo con la reivindicación 7, que además comprende entregar el perfil de usuario filtrado a la Función de Control de Sesión de Llamada de Interrogación.

9. Una Función de Control de Sesión de Llamada de Interrogación para usar en un Subsistema Multimedia IP que comprende:

los medios de entrada para recibir un mensaje enviado desde el Equipo de Usuario, el mensaje que comprende una cabecera de Información de Red de Acceso P; y

los medios de salida para enviar a un Servidor de Abonado Local parte o la totalidad de los contenidos de la cabecera de Información de Red de Acceso P.

10. Un Servidor de Abonado Local para usar en un Subsistema Multimedia IP que comprende:

los medios de entrada para recibir parte o la totalidad de los contenidos de una cabecera de Información de Red de Acceso P enviada desde una Función de Control de Sesión de Llamada de Interrogación;

los medios de almacenamiento para almacenar dichos contenidos de la cabecera de Información de Red de Acceso P; y

comparar los medios para comparar la información de ubicación contenida en la información de acceso con la información de autorización almacenada en una base de datos, la información de autorización que identifica las ubicaciones de acceso permitidas y/o prohibidas para el usuario.

11. El Servidor de Abonado Local para el uso en un Subsistema Multimedia IP como se reivindica en la reivindicación 10, que además comprende los medios para actualizar un perfil de usuario con los contenidos recibidos.

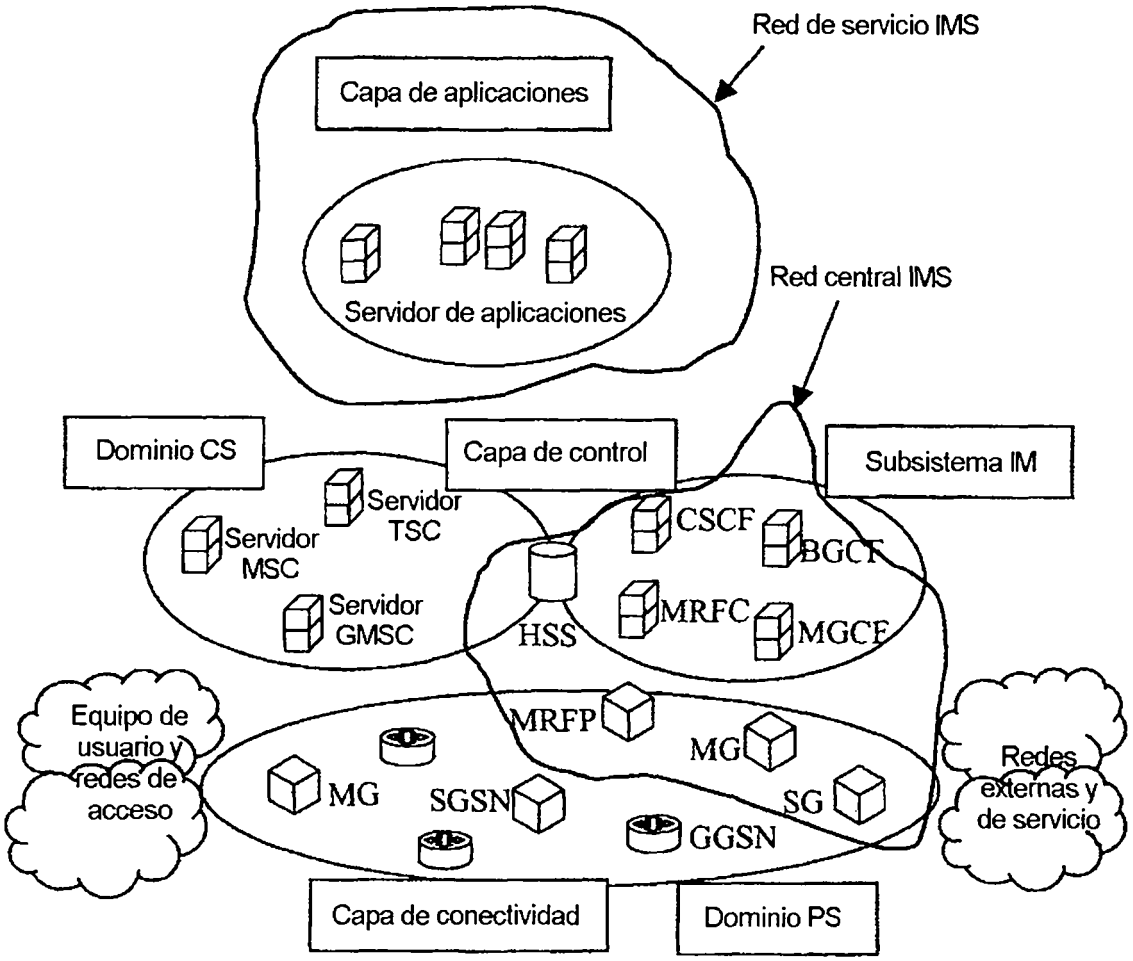
Red de servicio IMS
Capa de aplicaciones
Servidor de aplicaciones
Red central IMS
Dominio CS
Capa de control
Subsistema IM
Servidor TSC
Servidor MSC
Servidor GMSC
HSS
CSCF
BGCF
MRFC
MGCF
Equipo de usuario y redes de acceso
MRFP
MG
SGSN
MG
SG
GGSN
Redes externas y de servicio
Capa de conectividad
Dominio PS

Figura 1

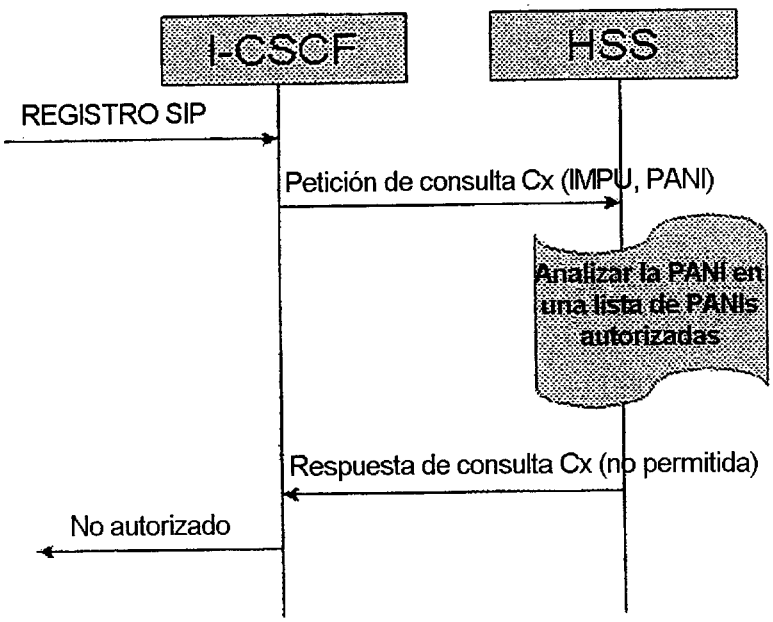

Figura 2

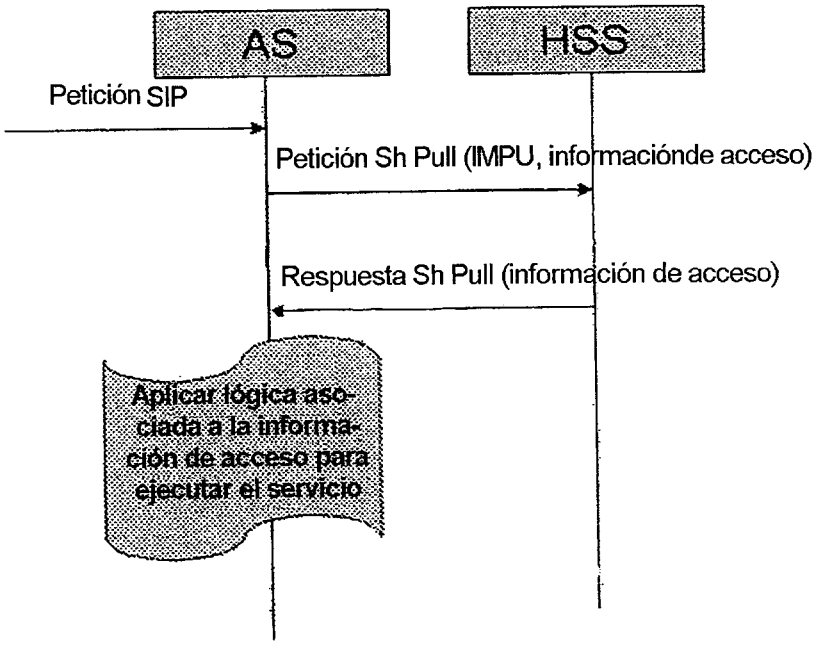

Figura 3

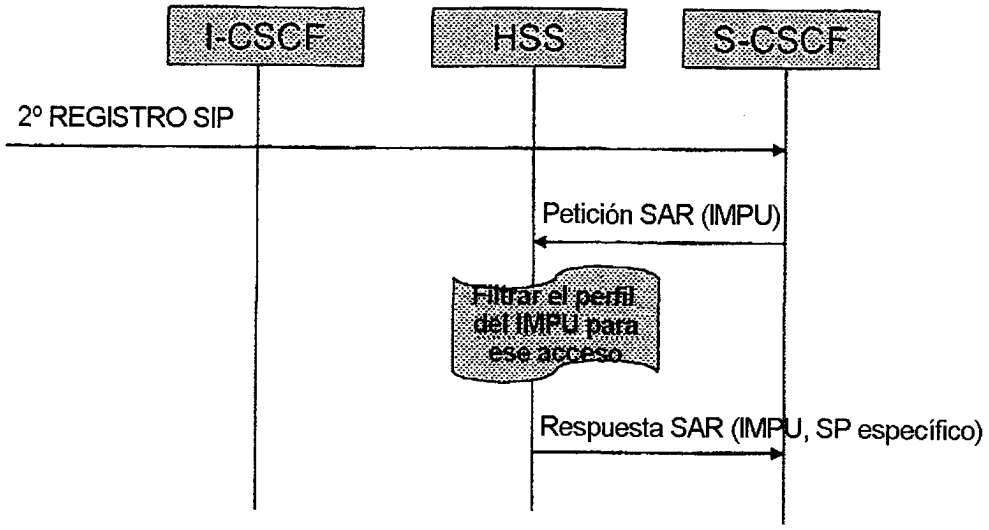

Figura 4

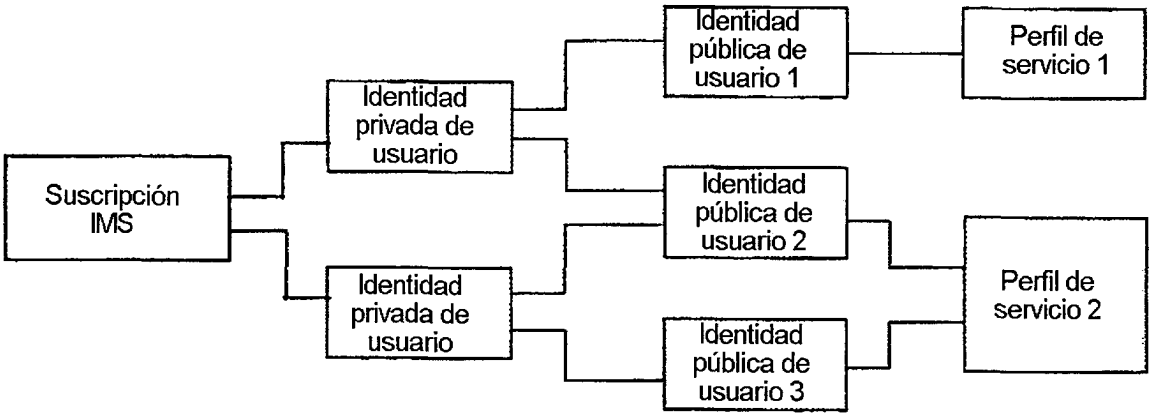

Figura 5 (Técnica anterior)