Seguridad en IP Multimedia Subsystem (IMS)

Por Ing. Mefístoles Zamora Márquez, Especialista B GRRHH, Dirección Territorial Camagüey, ETECSA, y Dr. Walter Baluja García, Profesor del Departamento de Telemática, ISJAE
mefi@cmg.etecsa.cu, walter@tesla.cujae.edu.cu

Versión de la ponencia del mismo título presentada en el III Seminario Internacional de Telecomunicaciones que sesionó durante la XII Convención y Exposición Internacional, Informática, La Habana, 2007.

IP Multimedia Subsystem IMS

La opción **Todo-IP** que pretende 3G UMTS —*Universal Mobile Telecommunications System*— no es suficiente para motivar un aumento del tráfico de datos en las redes móviles. De hecho, sólo proporciona beneficios a los operadores en lo que se refiere al ahorro de costes de infraestructura, mejor escalabilidad, mayor flexibilidad, y operación y mantenimiento más simplificado, pero no aumenta, por sí misma, el uso de servicios de datos. Por ello, la opción **Todo-IP** en 3GPP —3er *Generation Partnership Project*— aisladamente no tiene mayor interés. Ante esta situación, 3GPP, impulsado por las perspectivas de sus socios industriales, define e incorpora el Subsistema IP Multimedia —*IP Multimedia Subsystem* (IMS)— al núcleo de red móvil de la *Release* 5.

IMS es un sistema de control de sesión diseñado con tecnologías de Internet adaptadas al mundo móvil, que hace posible la provisión de servicios móviles multimedia sobre conmutación de paquetes —servicios IP multimedia—. El objetivo económico comercial de esta iniciativa es doble: aumentar los ingresos medios por abonado y reducir costes.

Fundamentos de los servicios IP multimedia y de 3GPP IMS

Las características más importantes de los servicios IP multimedia, que IMS hace posible, son las siguientes:

- La comunicación es orientada a sesión, y se realiza bien de un usuario a uno o varios usuarios o bien de un usuario a un servicio.
- La comunicación se efectúa en tiempo real o diferido.
- Las sesiones IP multimedia están compuestas por flujos y contenidos multimedia diversos, con el nivel de calidad de servicio adecuado: video, audio y sonido, texto, imagen y datos de aplicación.
- La identificación de usuarios, servicios y nodos se hace mediante URIs —*Uniform Resource Identifier*/Identificador Uniforme de Recurso—, lo que aumenta la usabilidad de los servicios frente a los abonados. Estos ya no tienen que manejar números de teléfono imposibles de recordar, sino nombres al estilo de los servicios de Internet, como es el caso del correo electrónico.

Por ejemplo, los servicios IMS pueden implementarse en una sola aplicación de usuario final que utilice, de manera coordinada y simultánea, la mensajería IP multimedia —instantánea y diferida—, los llamados servicios de presencia, la Web, las videoconferencias y llamadas de voz sobre IP —usuario a usuario o *multiparty*—, el *streaming*, la difusión multimedia, la descarga de contenidos, los juegos en red y cualquier otro servicio de Internet basado en TCP/IP —*Transmission Control Protocol/Internet Protocol*—, de forma muy similar a como operan las últimas versiones de los populares clientes de mensajería instantánea para PC —*Personal Computer*— e Internet, pero ofreciendo una Calidad de Servicio (QoS) garantizada y adaptada a cada flujo de datos, a la vez que permite al usuario disfrutar de la movilidad y características propias de su dispositivo personal 3G IMS.

Sin embargo, IMS no define las aplicaciones o servicios que pueden brindarse al usuario final, sino la infraestructura y capacidades del servicio que los operadores o proveedores de servicio pueden emplear para construir sus propias aplicaciones y producir su oferta de servicios. Sirvan como ejemplo determinados servicios finales:

- Los servicios heredados: llamadas básicas de voz, mensajería textual, mensajería multimedia, correo electrónico, entre otros.

◆ Los servicios multimedia avanzados: videoconferencia, audioconferencia monofónica o estereofónica, videoconferencia para personas sordas —video más texto en tiempo real—, multiconferencias en video, audio o texto, difusión de medios de televisión o radio, video bajo demanda, mensajería instantánea y *chat* multimedia, videojuegos interactivos multiusuario, servicio *push-to-talk* (*walkie-talkie*).

Estos servicios son ofrecidos con la misma calidad que percibe el usuario cuando se prestan a través de los sistemas tradicionales.

Por otro lado, como IMS fue diseñado para una red evolucionada de GSM —*Global System for Mobile Telecomunications*/Sistema Global para Comunicaciones Móviles—, hereda ciertas cualidades intrínsecas del mundo móvil, como son:

Las sesiones interoperador: los abonados de un operador IMS tienen la posibilidad de cursar sesiones IP multimedia con abonados localizados en la red 3G IMS de otro operador. La arquitectura de IMS, las entidades funcionales y sus protocolos se diseñan para realizar la interconexión con los sistemas IMS de otros operadores.

La itinerancia (*roaming*): IMS soporta *roaming* nativo, que puede definirse como la capacidad del sistema de admitir y dar servicio a abonados de otros operadores que emplean la misma tecnología, y con los que se tiene el acuerdo de negocio pertinente.

Cuando un abonado está en *roaming*, el subsistema IMS visitado encamina la señalización del abonado itinerante hasta el IMS nativo del abonado, desde donde se reencamina la sesión hacia su destino.

La interconexión con redes y servicios heredados: IMS contempla la interconexión con redes de circuitos SS7 —*Signaling System 7*— para servicios de llamadas de voz. Así, existen elementos IMS para el interfuncionamiento entre sesiones multimedia con componentes de audio y las redes PSTN —*Public Switched Telephone Network*/Red Telefónica Pública Conmutada—, GSM o el dominio de conmutación de circuitos de la propia red 3G. De esta forma, los abonados con la innovadora tecnología IMS siempre podrán seguir comunicándose con otros abonados "no-IMS".

La interconexión con redes IP multimedia externas e Internet: la futura Internet albergará servicios IP multimedia avanzados, especialmente para el caso de comunicaciones en tiempo real o con requisitos de calidad de servicio. IMS incorpora componentes para el interfuncionamiento con redes IP multimedia externas, de forma que los abonados IMS podrán mantener comunicaciones con usuarios de la Internet multimedia.

La seguridad integrada: uno de los factores clave del éxito de GSM fue que incorporaba intrínsecamente mecanismos de seguridad, soportados por la tarjeta SIM —*Subscriber Identity Module*/Módulo Identidad de Abonado—. IMS requiere autenticación de abonado y especifica sus propios mecanismos y arquitectura de seguridad, independientes de los propios de UMTS. Así, la suscripción IMS está soportada por una aplicación lógica llamada ISIM —*IMS Subscriber Identity Module*— que ejecuta funciones de autenticación de abonado durante su registro en IMS, además de contener datos de la suscripción de abonado, de igual forma que la SIM en GSM y la USIM —*Universal Subscriber Identity Module*— en 3G. La ISIM reside, junto con la aplicación USIM, en la tarjeta inteligente física. Por lo tanto, un abonado que desee acceder a IMS, deberá primeramente autenticarse y registrarse con el núcleo de red UMTS empleando la USIM, y, posteriormente, autenticarse y registrarse con IMS utilizando la ISIM.

La calidad de servicio: el subsistema GPRS —*General Packet Radio Service*/Servicio de Radio Genérico de Datos por Paquetes— de 3G hace uso de la arquitectura de QoS de UMTS, que define una jerarquía de portadoras adecuadas para servicios con diferentes requisitos de QoS. Así, se han definido nuevas funciones e interfaces opcionales en GPRS 3G de 3GPP *Release* 5 que permiten que IMS controle y autorice el uso de recursos del subsistema de transporte GPRS.

La provisión de servicios: IMS posibilita un desarrollo rápido y simplificado de servicios siguiendo el modelo de Internet. La arquitectura IMS cuenta con interfaces o pasarelas hacia servidores de aplicaciones. Las aplicaciones pueden modificar el transcurso de una sesión multimedia de una forma muy similar a como las aplicaciones de red inteligente pueden actuar y modificar una llamada de voz, con la ventaja de la simplicidad y facilidad del desarrollo de las aplicaciones Web.

Pueden establecerse una serie de criterios en la suscripción de usuarios IMS, de forma que el control de una sesión se traspase a un servidor de aplicaciones.

La tarificación y facturación: en la tarificación de servicios IP multimedia intervienen el sistema de facturación de GPRS y el sistema de facturación de IMS. Este último registra datos sobre la sesión IMS, tales como usuarios implicados, duración, componentes multimedia empleados y QoS autorizada, y los asocia a los correspondientes registros de tarificación de GPRS que se originaron como consecuencia del transporte de flujos multimedia y señalización de IMS en el subsistema de transporte GPRS. De ese modo, es posible facturar los servicios según la duración, los contenidos, volumen de datos, destino de la sesión o combinaciones de los anteriores. Por otro lado, el sistema soporta tanto tarificación *online* como *offline*, lo que se traduce en facturación postpago y prepago, necesaria para atender al mercado de clientes potenciales.

Tecnologías de IMS

Durante la especificación de IMS, aún en curso y evolución, 3GPP e

IETF —*Internet Engineering Task Force*/Grupo de Trabajo de Ingeniería de Internet— establecieron un acuerdo de trabajo que ha vinculado fuertemente el desarrollo del estándar IMS al trabajo de IETF. Este último ha tenido que acelerar la estandarización de los protocolos IP emergentes que se emplean en IMS, a la vez que han realizado especificaciones a medida y exclusivas para 3GPP. Estos protocolos se denominan:

Control de sesión —control de llamada IMS basado en SIP y SDP—

La señalización de IMS se efectúa mediante el protocolo SIP —*Session Initiation Protocol*/Protocolo de Inicio de Sección—, que IETF diseñó para la gestión de sesiones multimedia en Internet. A petición de 3GPP, IETF ha ido añadiendo al protocolo básico extensiones y cabeceras privadas para adaptar su uso a las necesidades del entorno móvil, y a las particularidades de una red de pago como UMTS. Por ello, se habla del perfil 3GPP del protocolo SIP, una variante personalizada para la red 3G IMS. SIP aporta las funciones para el registro, establecimiento, liberación y mantenimiento de sesiones IMS, lo que incluye funciones de enrutado de sesiones e identificación de usuarios y nodos, y, además, habilita todo tipo de servicios suplementarios. El protocolo SIP es similar en estructura a HTTP —*HyperText Transfer Protocol*—, incluso, comparte los códigos de respuesta. Esto facilita el desarrollo de servicios, puesto que es similar a construir aplicaciones Web. Tanto SIP como HTTP son protocolos de texto, que permiten incluir contenido MIME —*Multipurpose Internet Mail*—en el cuerpo de sus mensajes.

De este modo, los mensajes del protocolo SDP —*Session Description Protocol*/Protocolo de Sesión de Descripción— se transfieren en los mensajes SIP. El protocolo SDP, también diseñado por IETF, se emplea para describir la sesión que se negocia con SIP. Mediante SDP, los extremos de una sesión pueden indicar sus capacidades multimedia y definir el tipo de sesión que desea mantenerse. Con SDP, los extremos deciden qué flujos multimedia compondrán la sesión: a qué tipos de medios multimedia corresponden dichos flujos —audio, video, información—, qué *codecs* soportan y desean emplear para cada flujo, y cuál es la configuración específica de los *codecs* anunciados. La QoS se negocia mediante este intercambio de señalización, tanto en el establecimiento como durante la sesión en curso, si es necesario. Este dinamismo es una novedad en el mundo de las telecomunicaciones, donde la QoS es estática y viene impuesta por las redes y el servicio final solicitado.

Transporte de red (IPv6)

IMS se ha definido desde su origen como una red y un servicio fundamentado completamente sobre IPv6 —*IP version 6*—. El subsistema GPRS 3G que proporciona acceso a dicha red IPv6 ha visto modificadas sus especificaciones para soportar el transporte de datagramas IPv6 desde el terminal de usuario hasta IMS, así como otras funciones tales como la configuración y asignación de direcciones de red. Por otro lado, el terminal IMS ha de soportar el *snack* IPv6. La razón para que IPv6 sea un requisito básico es la previsión de la expansión paulatina de IPv6 en Internet. Como los mecanismos de interfuncionamiento IPv4/IPv6 iban a necesitarse igualmente, con independencia de la versión del protocolo escogida para IMS, 3GPP prefirió dar compatibilidad hacia atrás en lugar de hacia delante, y partir de la situación más avanzada técnicamente.

Además de las ya conocidas ventajas inherentes a IPv6 como QoS y seguridad integradas, autoconfiguración y mayor espacio de direccionamiento, el tráfico del plano de usuario se transfiere directamente entre terminales siguiendo el paradigma *peer-to-peer*. En la actualidad, 3GPP está estudiando la interoperación con las posibles implementaciones tempranas de IMS basadas en IPv4.[7]

Otros Protocolos

Además de SIP/SDP e IPv6, 3GPP emplea otros protocolos de IETF para la provisión de servicios IP multimedia, como son [8]:

- RTP —*Real Time Protocol*/Protocolo en Tiempo Real— y RTCP —*Real Time Control Protocol*/Protocolo de Control en Tiempo Real—, que se utilizan para el transporte de flujos IP multimedia del plano de usuario.
- COPS —*Common Open Policy Service*—, para el control de recursos QoS de GPRS mediante el uso de políticas.
- *Diameter*, para acciones relacionadas con la autorización, autenticación y tarificación. Principalmente se emplea como heredero de MAP para el diálogo con el nodo HSS —*Home Subscriber Server*— de IMS, que sustituye al tradicional HLR —*Home Location Register*—.
- RSVP —*Resource Reservation Protocol*— y DiffServ, para asegurar la QoS extremo a extremo, especialmente cuando la conectividad IP requerida se extiende más allá de la red móvil GPRS.
- MEGACO, para el control remoto de media *gateways*.

Arquitectura Funcional de IMS

La entidad funcional clave es el nodo CSCF —*Call State Control Function*— [9], que es básicamente un servidor SIP con funciones de *proxy*. El CSCF ejecuta tres roles diferentes en la operatividad de IMS [10], denominados:

1. Proxy CSCF (P-CSCF): es el punto de entrada al subsistema IMS y recibe directamente la señalización IMS desde el terminal, vía GPRS. Implementa las funciones de protección de señalización (seguridad) y el control de recursos del

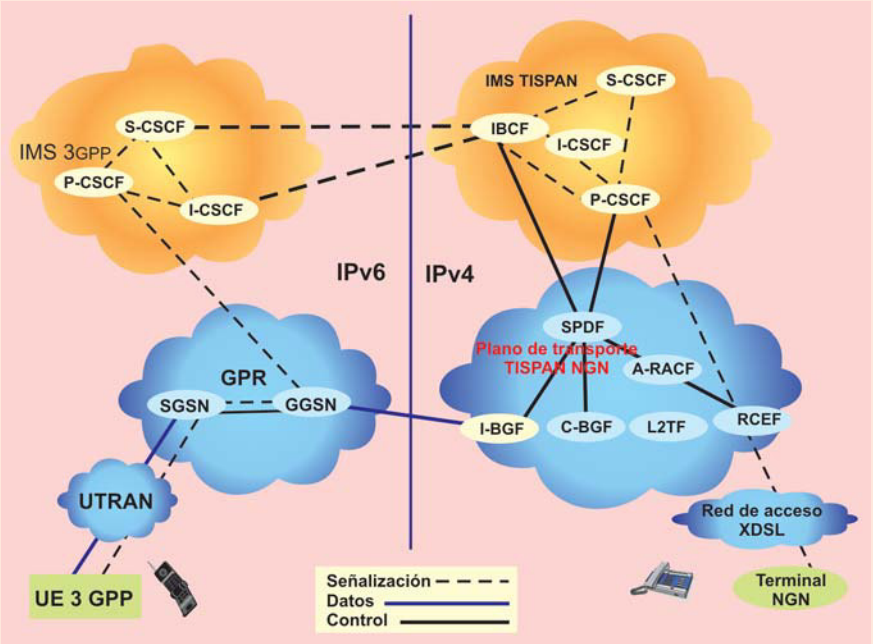

Figura 1 Arquitectura funcional IMS. Fuente: Mampaey, M., D. Hoefkens, and A. Bultinck (ver Bibliografía [5]).

◆ **MGCF** —*Media Gateway Control Function*—. Es parte de la arquitectura de interfuncionamiento de IMS con las redes de circuitos. En concreto, implementa el plano de control del *interworking*, traduciendo la señalización IMS SIP/SDP a SS7, y viceversa. Se encarga de controlar la operación del IM-MGW.

◆ **IM-MGW** —*IP Multimedia Media Gateway*—: implementa el plano de usuario de la arquitectura de interoperación de IMS con las redes de circuitos. Se encarga de la transcodificación de flujos IMS sobre IP a los datos de usuario en las redes TDM —*Time Division Multiplexing*— de circuitos.

◆ **Función de Recursos de Medios (MRF)**: este servidor de medios y puente de conferencia proporciona el soporte para audio y videoconferencia, anuncios multimedia y proceso de medios —por ejemplo, transcodificación—.

◆ **Los servidores de aplicación y las pasarelas hacia el plano de servicios**: 3GPP define interfaces IMS entre el S-CSCF y el plano de servicios. La señalización puede desviarse hacia el plano de servicio según una serie de criterios que se recogen en el perfil de abonado, que el HSS alberga y que el S-CSCF descarga durante el registro de cada abonado.

IMS en NGN TISPAN

Mientras los avances en las redes móviles se suceden continuamente, los operadores fijos asisten a un mercado en retroceso que paulatinamente abandona los servicios clásicos de telefonía fija hacia los móviles. Este hecho ha provocado la aparición de diversas iniciativas de estandarización de la evolución de la red fija, bajo el paradigma de NGN. De todas estas iniciativas, la más importante es la emprendida en el 2004 por el Comité TISPAN de ETSI, que para evolucionar los servicios PSTN/ISDN —*Public Switched Telephone Network/Integrated Switched Digital Network*— directamente ha adoptado por reutilizar el subsistema de 3GPP. [12]

Aunque la percepción de los servicios y la tecnología en los mundos fijo y móvil es convergente en IMS, el empleo y expansión técnico de este sistema es distinto. Esto se debe a las restricciones de las tecnologías de subsistema de transporte. En *roaming*, es el nodo en la red visitada que se encarga de enrutar la señalización de registro y sesión desde los terminales en itinerancia hasta la red IMS nativa. Además, ejecuta las funciones comunes a los demás CSCF: el procesado y enrutado de señalización, la consulta del perfil de usuario en el HSS y la tarificación.

2. Serving CSCF (S-CSCF): a cada usuario registrado en IMS se le asigna un S-CSCF. Este se encarga de enrutar las sesiones destinadas o iniciadas por el usuario, así como del registro y autenticación del abonado IMS, de la provisión de servicios IMS mediante el desvío de señalización a los servidores de aplicación, de emplear las políticas del operador de red y de generar registros de tarificación.[11]

3. Interrogating CSCF (I-CSCF): es un nodo intermedio que da soporte a la operación IMS. El ICSCF ayuda a otros nodos a determinar el siguiente salto de los mensajes SIP y a establecer un camino para la señalización. Durante el registro, el P-CSCF se ayuda del I-CSCF para determinar el S-CSCF que ha de servir a cada usuario. En situaciones de *roaming* y en sesiones interred, el I-CSCF es el punto de entrada cono-cido por la red IMS externa y también indica el siguiente salto para la señalización. Opcionalmente, el I-CSCF efectúa funciones de ocultación de la topología de red IMS ante redes externas, de forma que los elementos ajenos a IMS no puedan averiguar cómo se gestiona la señalización internamente.

Otros nodos de relevancia en IMS

◆ **HSS** —*Home Subscriber Server*—: hereda las funciones del HLR—*Home Location Register*—, de manera que almacena y gestiona el perfil del servicio IMS del abonado, recopila las claves de seguridad y genera vectores de autenticación, registra el estado de los abonados y almacena el nodo S-CSCF con el que el abonado se ha registrado.

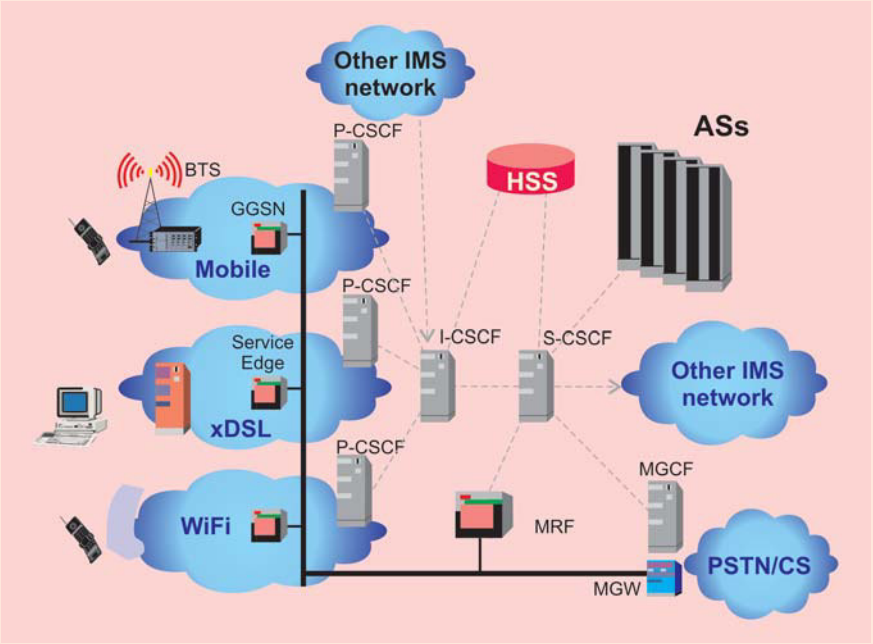

Figura 2 IMS 3 GPP e IMS TISPAN y su interconexión. Fuente: Mampaey, M., D. Hoefkens, and A. Bultinck (ver Bibliografía [5]).

acceso NGN y 3G, y a los diferentes requisitos y servicios que ofrecen los operadores fijos y móviles en este ámbito.

Mientras que en 3G hay una red de transporte GPRS y un subsistema IMS que utiliza IPv6, en TISPAN puede encontrarse una red de acceso xDSL y un subsistema IMS NGN que usan IPv4. En ambos casos se interconectarían en el plano de control y transporte. Se trata de un diagrama simétrico, es decir, la interconexión no se ve afectada por el hecho de que una red u otra sea la de origen en la sesión interoperador.

En el subsistema de control IMS de ambos, las funciones CSFC son las entidades SIP —*Session Initiation Protocol*— que gestionan la señalización de establecimiento de sesiones.

En el subsistema de transporte 3G, los nodos SGSN —*Serving GPRS Support Node*— y GGSN —*Serving GPRS Support Node*— proporcionan y controlan la conectividad IP que permite transferir datagramas entre los terminales móviles y las redes de paquetes.

En el transporte de NGN TISPAN, las entidades SDPF y A-RACF componen el denominado subsistema RACS —*Resource and Admission Control System*—, que realiza el control de admisión y reserva de recursos. [12]

La interconexión a nivel de control y transporte se realiza por dos nuevos elementos, el I-BCF—*Interconnection Border Control Function*—, en el plano de control y el I-BGF —*Interconnection Border Gateway Function*— en el plano transporte, definidos por TISPAN para que el operador NGN IMS pueda aplicar mecanismos de control en la frontera con otros dominios. Estos nodos realizan funciones de *firewall*, ocultación de topología y extremo *DiffservK* [5]. Sin embargo, su principal función es permitir la interconexión transparente entre el IMS NGN y otras redes externas, a través de las conversiones entre direcciones IP de distintas versiones.

Por lo tanto, para realizar la interconexión considerando estos requisitos de versiones IP y el control de frontera, el I-BCF ha de mediar en el intercambio de señalización de las entidades IMS-NGN con el 3G. En el plano transporte, cuando empiece el intercambio de medios, los medios IPv6 del Terminal 3G dirigen a la I-BGF, que los transforma en paquete IPv4 para entregárselos al terminal NGN.

TISPAN en su modelo para las NGN coloca la arquitectura IMS en la capa de control, no sólo para garantizar la convergencia entre redes fijas y móviles, sino también por las potencialidades que brinda y su fácil implementación. [13]

Seguridad en IMS

La convergencia fijo-móvil al mundo IP va aparejada a una convergencia de los aspectos de seguridad. Aunque es esencial no descuidar la seguridad como se define para el IMS móvil, los operadores fijos tienen necesidades específicas. Buscan conservar las inversiones existentes —en las instalaciones de cliente y operador— teniendo en cuenta la gran base instalada en las redes fijas, disminuir el umbral para la aceptación de clientes de IMS y acelerar su expansión, pero con la sustitución de los servicios heredados.

El 3GPP produjo un conjunto completo de especificaciones para seguridad IMS, que muestran un alto nivel de madurez. El método lógico y eficiente es usar especificaciones 3GPP como base donde se identifica la convergencia. La intención principal es extrapolar la seguridad TISPAN desde el método del 3GPP.

La seguridad es un aspecto fundamental de la arquitectura IMS de 3GPP. Se basa en un concepto de capas que en el IMS se diseña como una superposición una red móvil 2,5/3G independiente de la tecnología de acceso y con su propia autorización/autenticación de usuario y protección de flujo de comunicación. El objetivo es asegurar todas las sesiones IMS entre los abonados y los servidores de llamadas IMS y entre los servidores de llamadas. Se basa en un método de seguridad *hop by hop* donde:

- El primer tramo entre el abonado y el P-CSCF se asegura con un contexto de seguridad individual para cada abonado [2].
- Los tramos entre CSCFs se protegen globalmente para todas las sesiones: *Network Domain Security* (NDS) [5].

El primer tramo requiere una seguridad muy grande, debido a que proporciona a los usuarios un canal de señalización directo al corazón de la infraestructura de control de IMS. Las principales necesidades para la seguridad en el primer tramo son:

- La necesidad de autenticar al usuario para prevenir el robo de la identidad de usuario.
- La necesidad de autorizar y proteger la integridad de la señalización de usuario para prevenir el ToS —*Theft of Service*— y los ataques maliciosos explotando la señalización.

La seguridad en el primer tramo se basa en la aplicación ISIM sobre una UICC —*UMTS Integrated Circuit Card*— en el terminal. Reutiliza un mecanismo muy probado en campo definido por acceso UMTS para proteger los accesos de radio sensibles.

El AKA —*Authentication and Key Agreement Protocol*— permite la autenticación y el acuerdo de claves mediante un código secreto común compartido entre el abonado —aplicación ISIM— y la red (AuC/HSS). En el registro del IMS, el usuario se autentica usando un intercambio de mensajes SIP *Digest* AKA. Los siguientes intercambios se protegen por el modo de transporte IPsec —Seguridad de Protocolo Internet— entre el abonado y el P-CSCF usando claves de cifrado e integridad derivadas del código secreto compartido y del valor objetivo.

La seguridad de los dominios de red para protocolos basados en IP (NDS/IP) es menos de una facilidad específica IMS. NDS/IP propone una arquitectura de seguridad y herramientas que permiten a los operadores IMS estructurar su propia red IMS en zonas de seguridad y tener mecanismos de seguridad interoperables para intercambios con otros operadores. Para dicho efecto, NDS/IP introduce la noción de interfaz intradominios (Zb), que representa la interfaz entre componentes IMS en el mismo dominio de seguridad y la de interdominios (Za) que representa la existente entre dos dominios de seguridad diferentes. La interfaz Zb puede asegurar la señalización encapsulándola en un túnel IPsec —una opción del operador—. Los nodos en los diferentes dominios de seguridad conectados por la interfaz Za deben comunicarse a través de una pareja de componentes SEG —Pasarela de Seguridad— en cada borde del dominio. Los SEGs deben asegurar los intercambios entre dominios usando túneles IPsec *peer-to-peer* (ver figura 3).

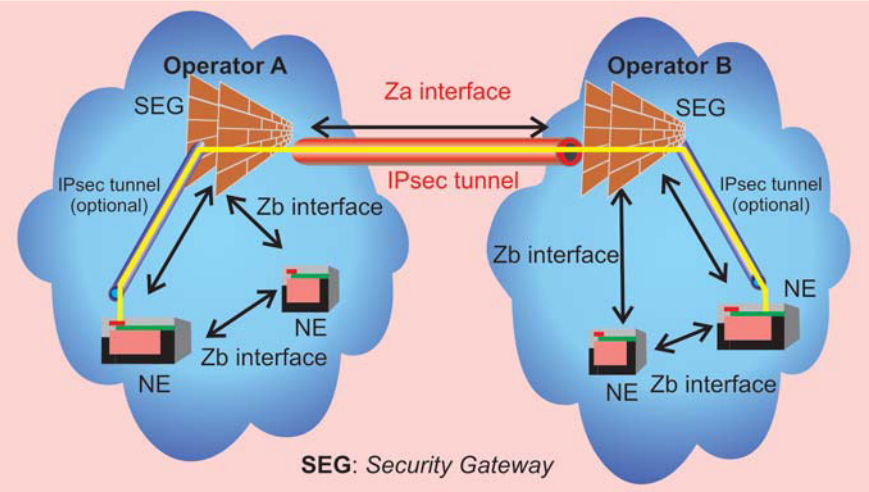

Figura 3 Dominios de seguridad

El protocolo IKE —Intercambio de Claves Internet— se usa para negociar, establecer y mantener SA—Asociación de Seguridad— y túneles ESP seguros asociados.

TISPAN definió el NASS —*Network Access SubSystem*— y el RACS —*Resource Admission Control Subsystem*— para control de la conectividad IP en la capa de transporte.

HSS se redefine en el UPSF —*User Profile Server Function*— que todavía incluye los datos de autenticación de usuario y configuración de sistema, pero sustituye el HLR con datos específicos de otros subsistemas tales como PES —PSTN *Emulation Subsystem*—. El SLF —Función Localizadora de Abono— permite localizar al UPSF que contiene los requeridos datos de configuración de usuario en una múltiple configuración UPSF.

Mediante el UAAF —*User Access Authorization Function*— y su asociado PDBF —*Profile DataBase Function*— de repositorio de datos, el NASS [14] registra, autentica y autoriza el acceso del CPE —Equipo en las Instalaciones del Cliente— a la red fija. El NACF —*Network Access Configuration Function*— [13] asigna direcciones IP al CPE y también le proporciona las direcciones de contacto de los servicios, por ejemplo, la dirección IP del P-CSCF —función de control de sesión de llamada intermediaria o Proxy— para el servicio IMS. El CLF —*Connectivity Session Location and Repository Function*— vincula toda la información NACF y UAAF con la información de localización para soporte de RACS, operaciones de servidores de aplicaciones y subsistemas de control de servicio [13].

La seguridad intradominios es responsabilidad exclusiva del operador pero no es obvia. La protección en los bordes del dominio no es suficiente, porque la experiencia ha mostrado que muchos ataques se lanzan desde dentro de la red. El principio de separación donde los tipos de flujo —señalización,

gestión y medios— y los tipos de nodo se aíslan y protegen individualmente, reducirá la magnitud de un ataque. Las bases de datos tienen que concentrarse en zonas que estén muy protegidas por cortafuegos. Nuevas reglas administrativas controlarán las posibles fuentes de ataques internos [5].

Se concibe y propone utilizar la Arquitectura de Seguridad para redes de Telecomunicaciones, que constituye una herramienta para realizar las tareas de seguridad en estas redes. La arquitectura es sencilla, general y flexible, lo cual garantiza que sea aplicable a cualquier red de telecomunicaciones, incluyendo las NGN como tendencia predominante en el sector. Además, se presenta más como una forma de organizar las labores de seguridad no como una combinación de mecanismos de defensa sino como un trabajo continuo de planificación, implantación y mantenimiento de la seguridad.

Conclusiones

Las NGN, el protocolo IP e Internet están cambiando el modelo de las comunicaciones modernas. El IMS puede proporcionar nuevos servicios de comunicación multimedia persona a persona más allá de los disponibles en las actuales redes 3G. Como IMS se basa en IP, combinará servicios de datos y de telecomunicaciones, conservando lo mejor de los mundos de paquetes y circuito conmutado. Como IMS se diseñó para los operadores de red, guarda el control de llamada multimedia con los operadores de móviles que pueden así obtener una mayor parte de la cadena de valor —acceso, aplicación y servicios, intermediación, pago— y convertirse en **proveedores de telecomunicaciones IP**.

IMS es tanto un reto como una oportunidad como base para los negocios de servicios y aplicaciones de telefonía en la próxima década. A pesar de sus facilidades, presenta los típicos problemas de seguridad de las redes IP, existen normas y propuestas de seguridad por parte de organismos internacionales, fabricantes y operadores de comunicaciones [15].

Finalmente, se recomienda utilizar esta Arquitectura de Seguridad que ofrece una perspectiva completa del trabajo de gestión, los elementos y tareas fundamentales de seguridad, y otros aspectos que facilitan su implementación en las redes de telecomunicaciones actuales, incluyendo las NGN.

Referencias bibliográficas

[1] Baluja, W. y Llanes, A. "Estado actual y tendencias del enfrentamiento del fraude en las redes de telecomunicaciones". *Ingeniería Electrónica, Automática y Comunicaciones*, vol. XXVI, no. 2 (2005): 45.

[2] Goossens, P., L. W., and W. Y. "Convergencia de servicios y su impacto en la arquitectura y evolución de la red: el ejemplo chino". *Revista de Telecomunicaciones de Alcatel* (1er trimestre 2003): 1-10. Disponible en: http://www.alcatel.com/atr. (Consulta: agosto/2006).

[3] Paridaens, O., Gamm, B., and Howard, B. "Seguridad en la arquitectura de redes IP". *Revista de Telecomunicaciones de Alcatel* (2do trimestre 2001): 122-128. Disponible en: http://www.alcatel.com/atr. (Consulta: agosto/2006).

[4] Hills, D. and Mercouroff, N. "Usar la convergencia fijo-móvil como ventaja competitiva". *Revista de Telecomunicaciones de Alcatel* (4to trimestre 2005): 281-285. Disponible en: http:// www.alcatel.com/atr. (Consulta: agosto/2006).

[5] Mampaey, M., Hoefkens, D., and Bultinck, A. "Seguridad de IMS de 3GPP A NGN de TISPAN". *Revista de Telecomunicaciones de Alcatel* (4to trimestre 2005): 303-308. Disponible en: http://www.alcatel.com/atr. (Consulta: agosto/2006).

[6] B. Howard, O.P., Gamm, B. "Seguridad de la información: amenazas y mecanismos de protección". *Revista de Telecomunicaciones de Alcatel* (2do trimestre 2001): 117-121. Disponible en: http://www.alcatel.com/atr. (Consulta: agosto/2006).

[7] Fernández, D.M., Llanos, D.L., and Martínez, J.A.G. "IMS: la clave para el despegue de UMTS". *Comunicaciones de Telefónica I+D*, no. 33 (2004): 31-142. Disponible en: http://http://www.tid.es/presencia/publicaciones. (Consulta: septiembre/2006).

[8] 3GPP, *IP Multimedia Subsystem (IMS); Stage 2*, 2005, **3GPP TS 23.228,** V7.1.0 *Release* 7. Disponible en: http://http://www.3gpp.org. (Consulta: septiembre/2006).

[9] Vriendt, J.D., Hanson, G., and Urie, A. "Estrategias de migración de red hacia el IMS". *Revista de Telecomunicaciones de Alcatel (4to trimestre 2005)*: 291-296. Disponible en: http:// www.alcatel.com/atr. (Consulta: agosto/2006).

[10] Ericsson *IMS – IP Multimedia Subsystem*, 2004, 284 23 — 3001 Uen Rev A,

[11] Vega, A.M. *IP Multimedia Subsystems (IMS) – the Open Industry Standard Supporting the Next Generation of Converged Network Services,* 2005, ABC XX-007.v1. Disponible en: http:// www.lucent.com. (Consulta: septiembre/2006).

[12] Fernández, D.M., Jular, A.S. y Villarribia, S.F. "Estudio de la interconexión entre redes fijas y móviles en el plano de control mediante los estándares IMS de 3 GPP y NGN de TISPAN". *Comunicaciones de Telefónica I+D*, no. 37 (2005): 111-117

[13] ETSI, *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables*, 2005, **EG 202 387,** V1.1.1. Disponible en: http:// www.etsi.org. (Consulta: septiembre/2006).

[14] 3GPP, *Security Threats and Requirements*, 2001, **3GPP TS 21.133 V4.1.0,** *Relase* 4. Disponible en: http://http://www.3gpp.org. (Consulta: septiembre/2006).

[15] García, W. B. Arquitectura y sistema para la gestión de seguridad en las redes de telecomunicaciones, 2006. Tesis para obtener el grado de Doctor en Ciencias Técnicas, CUJAE, Departamento de Telemática.

Nota editorial: se ha decidido hacer una excepción en relación con las normas para las referencias bibliográficas y bibliografías; por su particularidad, se ha respetado la forma en que las han utilizado los autores.