ESPECIFICACIÓN DE AGENTES IP MÓVILES PARA PROCESOS AAA EN AMBIENTES 3G

ALEXANDER GALVIS QUINTERO

LUIS ALEJANDRO FLETSCHER BOCANEGRA

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE TRANSMISIÓN

GRUPO NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES

POPAYÁN

2001

ESPECIFICACIÓN DE AGENTES IP MÓVILES PARA PROCESOS AAA EN AMBIENTES 3G

ALEXANDER GALVIS QUINTERO
LUIS ALEJANDRO FLETSCHER BOCANEGRA

Monografía presentada como requisito parcial para optar al título de Ingeniero en Electrónica y Telecomunicaciones.

DIRECTOR: Ing. OSCAR J. CALDERÓN C.

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TRANSMISIÓN
GRUPO NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2001

TABLA DE CONTENIDO

TABLA DE FIGURAS

INTRODUCCIÓN

La “Sociedad de la Información Móvil” rápidamente se ha hecho una realidad; las redes avanzadas capaces de altas velocidades de transferencia de datos ya se han empezado a construir, y una vasta selección de nuevos y excitantes servicios serán habilitados para usuarios móviles, lo cual impone un reto para el mejoramiento de los procesos y la optimización en el uso de los recursos de la red. Dentro de esta tendencia aparecen los Sistemas de Tercera Generación (3G), los cuales combinan una amplia gama de servicios de alto ancho de banda con la posibilidad de disponer de ellos a través de un terminal móvil. Para el usuario esta característica de movilidad ofrece amplios beneficios, pero es indispensable que todos los procesos que se llevan a cabo para proveerla sean transparentes para dicho usuario y se realicen de forma ágil, segura y eficiente; es decir, que sin importar la ubicación geográfica del usuario, éste obtenga acceso a los servicios de telecomunicaciones a los cuales está suscrito sin que necesariamente sepa quien los provee y sin perder continuidad en el acceso al recurso; para lo cual la red debe verificar la identidad de un terminal que se encuentra en su área de cobertura, este proceso es conocido como autenticación y es de gran relevancia en la gestión de la movilidad en estos sistemas.

Una de las alternativas para superar el reto de mejorar los procesos relacionados con la movilidad en las Redes de Tercera Generación es la aplicación de la tecnología de Agentes Móviles, la cual ha sido ampliamente probada y ha arrojado excelentes resultados en ambientes como Internet, gracias a sus características de eficiencia y desempeño.

El alcance del presente proyecto es desarrollar un modelo teórico para la aplicación de Agentes IP Móviles en el proceso de Autenticación, que cumpla con los requerimientos impuestos por las Redes de Tercera Generación para la adecuada prestación de servicios. El modelo está compuesto por dos Agentes y un conjunto de características que definen su comportamiento para el caso particular en que un Terminal Móvil se encuentra fuera de su propia red y necesita negociar las características de prestación del servicio con el operador del área en la cual se encuentra ubicado.

A continuación se presenta la organización de la monografía:

CAPITULO I – ASPECTOS DE SEGURIDAD EN SISTEMAS MÓVILES DE TERCERA GENERACIÓN (3G)

En este capítulo se abordan de forma genérica los conceptos relacionados con las Redes de 3G, haciendo énfasis en los aspectos concernientes a la seguridad de dichos sistemas.

CAPITULO II – AGENTES MÓVILES

Se presenta un estudio de la tecnología de agentes móviles, su funcionamiento y utilización en diferentes ambientes, así como la aplicabilidad de estos conceptos en procesos que se llevan a cabo en los Sistemas de Tercera Generación.

CAPITULO III – PROCESOS AAA EN AMBIENTES 3G

Capítulo en el que se estudiarán y analizarán los procedimientos de autenticación, autorización y tarificación implementados para la prestación de servicios de forma segura en Sistemas de Tercera Generación.

CAPITULO IV – MODELADO DE AGENTES IP MÓVILES PARA PROCESOS AAA EN AMBIENTES 3G

Capítulo central de la monografía donde se realizará la especificación (definición, análisis y diseño) de dos agentes IP móviles que brindarán soporte en la tarea específica de autenticación, en las redes que presten servicios de Tercera Generación. Dicha especificación se hace aplicando el paradigma orientado a objetos y el modelado se hace mediante el Lenguaje de Modelamiento Unificado (UML: Unified Modeling Language).

CONCLUSIONES Y RECOMENDACIONES

En este apartado se consignan los resultados obtenidos durante el desarrollo del proyecto y el aporte que este entrega, así como recomendaciones para futuras implementaciones y desarrollos relacionados.

ANEXO A

Aquí se consignan los diagramas de colaboración para cada caso de uso y los pseudocódigos mediante los cuales se implementan las clases de diseño.

ANEXO B

Este anexo contiene los diferentes diagramas de colaboración correspondientes a los casos de uso del par de Agentes Móviles.

ANEXO C

Aquí se presenta el diccionario del sistema, el cual complementa la etapa de análisis.

1. ASPECTOS DE SEGURIDAD EN SISTEMAS MÓVILES DE TERCERA GENERACIÓN (3G)

1.1 Introducción

Los sistemas de comunicaciones han evolucionado conforme pasa el tiempo, es así como de la telefonía tradicional con hilos se ha dado paso a un nuevo esquema donde el medio de transmisión es el aire y la principal ventaja para el usuario es la total movilidad, este nuevo esquema es conocido como tecnología inalámbrica (sin hilos) o simplemente sistemas inalámbricos.

Dentro de la evolución de los sistemas inalámbricos se han conocido hasta ahora tres generaciones, cada una de las cuales ha marcado un hito en la historia de las telecomunicaciones y han estado caracterizadas por ciertos rasgos tecnológicos que las han distinguido de las demás. Es así como la primera generación estaba basada en estándares analógicos donde solo era posible la transmisión de voz. Años después surge la segunda generación, la digital, utilizada hoy en día, donde los teléfonos celulares constituyen pequeños dispositivos capaces de reconocer comandos de voz, enviar y recibir mensajes de texto, procesar datos en aplicaciones de agenda, directorio telefónico, calculadora, entre otras, convirtiéndose en un servicio popular y de demanda masiva. Finalmente, se encuentra la llamada tercera generación (3G) donde se espera que los usuarios puedan tener en su terminal servicios de voz y aplicaciones multimediales, con capacidad de movilidad mundial y convergencia total. En la figura 1.1 se observa la evolución de los sistemas inalámbricos a través de los años. Es conveniente aclarar que al hablar de 3G, Redes 3G, Sistemas Móviles 3G y Ambientes 3G, se estará haciendo referencia al mismo concepto.

El advenimiento de la nueva generación de sistemas inalámbricos y la convergencia de servicios han incrementado la preocupación por los esquemas de seguridad que deberán adoptarse para garantizar la integridad y confidencialidad de la información,

puesto que la cantidad de usuarios involucrados y el tipo de datos a manejar serán factores críticos en la prestación de los servicios, siendo necesario implementar mecanismos de seguridad confiables que sirvan de soporte a los nuevos requerimientos. El presente capítulo estudia los aspectos relacionados con la seguridad en los sistemas de Tercera Generación, haciendo énfasis en lo concerniente a la prestación de los servicios, ya que estos servirán como base para el desarrollo de este proyecto.

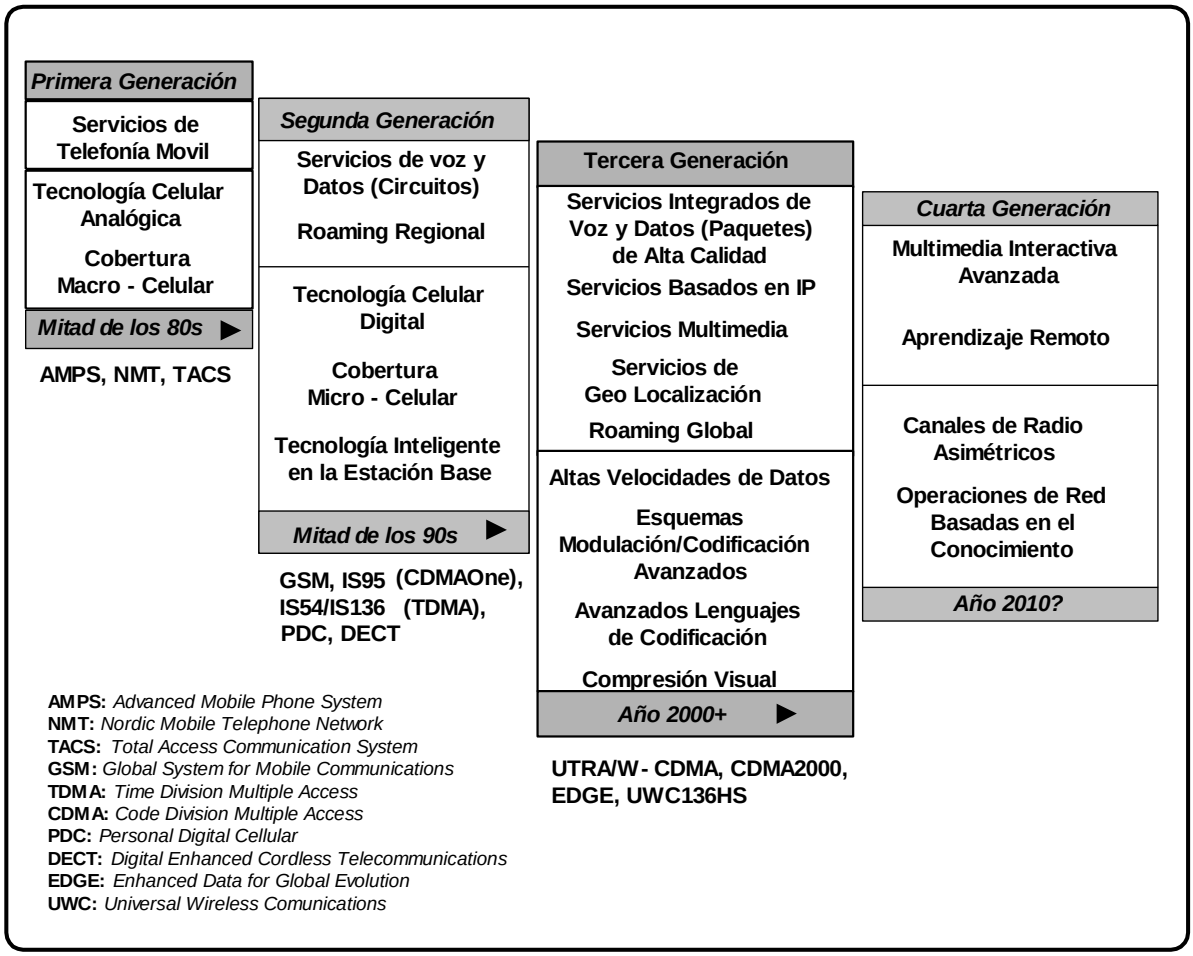


Figura 1.1 Evolución de los sistemas inalámbricos

1.2 Definición de Sistemas 3G

Tercera generación (3G) es el término genérico utilizado para la próxima generación de sistemas de comunicación móvil. Los Sistemas 3G proporcionarán servicios que aumentarán las capacidades de aquellos disponibles hoy en día (voz, texto y datos), combinando alta velocidad de acceso móvil de hasta 144 kbps en servicios IP. De

igual forma permitirá un sinnúmero de servicios, que no estaban disponibles anteriormente para usuarios móviles, tales como:

- Aplicaciones de Negocios: Comercio electrónico, Negocio a Negocio (B2B: Business to Business), Negocio a Consumidor (B2C: Business to Consumer), entre otros
- Banca electrónica y aplicaciones de ventas al por menor
- Aplicaciones de vídeo: video-conferencias y video por demanda
- Mensajería unificada
- Tarjetas electrónicas
- Juegos electrónicos
- Cotizaciones de bolsa en vivo y resultados deportivos
- Capacidad para descargar y ver video, audio y archivos MP3
- Consulta a bases de datos

Debido a la naturaleza de estos servicios y a las características particulares de las comunicaciones inalámbricas, los Sistemas de Tercera Generación tienen que incorporar algunas medidas de seguridad para evitar la fácil recepción de información por parte de usuarios distintos al destinatario previsto, al igual que impedir el acceso fraudulento a los servicios.

1.2.1 Características de los Sistemas Móviles de Tercera Generación

La comunicación móvil de tercera generación se diferencia de las existentes primera y segunda generación en los siguientes aspectos:

- *Movilidad global.* Los Sistemas 3G brindarán a los usuarios un alto grado de movilidad. Actualmente la mayor parte de dispositivos móviles están restringidos a desplazamientos dentro de un país o en el mejor de los casos a lo largo de todo un continente, pero con el advenimiento de 3G esta capacidad dejará de ser de carácter regional y se trasladará a un entorno mundial (roaming global), donde sin importar el lugar en que se esté o el proveedor que dé soporte, se podrá contar con el servicio de manera transparente para el usuario.

- *Posee la capacidad de soportar servicios multimedia.* Los Sistemas 3G poseen la capacidad para soportar aplicaciones que requieren gran ancho de banda,

en especial servicios de Internet. Los actuales servicios de comunicaciones móviles soportan voz, y con el desarrollo de nuevos sistemas, podrán proveer servicios de datos a 100 Kbps - 200 Kbps. El sistema de comunicación móvil de Tercera Generación tendrá mucha mayor capacidad de servicios que la segunda generación, soportando voz y datos en servicios multimedia, y podrá proveer ancho de banda de acuerdo con las necesidades (bajo demanda).

- *Evolución y Migración.* Los Sistemas de Tercera Generación tienen capacidad para coexistir con otros tipos de sistemas inalámbricos que se encuentren en servicio. Dentro de este entorno se debe considerar entonces:

    - Flexibilidad para evolución de los sistemas y migración de usuarios desde un Sistema Móvil pre3G hasta un Sistema Móvil 3G.
    - Compatibilidad de servicios entre un Sistema Móvil 3G y la red fija de telecomunicaciones, por ejemplo la Red Telefónica Pública Conmutada (PSTN: Public Switching Telephone Network) o la Red Digital de Servicios Integrados (ISDN: Integrated Services Digital Network).
    - Provisión de una estructura para la continuidad y expansión de servicios de las redes móviles como también acceso a servicios y facilidades de la red fija.
    - Arquitectura abierta que permita la fácil introducción de avances tecnológicos, por ejemplo canceladores de interferencia para mejorar la capacidad de enlace y de diferentes aplicaciones.
    - Habilidad para coexistir e interactuar con un sistema pre3G.

Dentro de los requerimientos técnicos que deben tener los Sistemas 3G se pueden enumerar los siguientes:

- Altas tasas de datos de por lo menos 144 Kbps en vehículos, 384 Kbps caminando y de 2 Mbps en ambientes de baja movilidad y de interiores.
- Transmisión de datos de manera simétrica y asimétrica.
- Servicios de conmutación por paquetes y en modo circuito, tales como tráfico del Protocolo de Internet (IP: Internet Protocol) y video en tiempo real.
- Buena calidad de voz (comparable a la calidad de una línea fija alambrada).
- Mayor capacidad y mejor utilización del espectro comparado con los sistemas actuales inalámbricos de segunda generación.

- Servicios simultáneos para usuarios finales y terminales, es decir, para servicios multimedia.
- La incorporación sin traumatismos de sistemas celulares de segunda generación y coexistencia e interconexión con servicios móviles por satélite.
- Itinerancia, inclusive itinerancia internacional, entre distintos operadores de Redes 3G.

1.2.2 Composición de los sistemas

Al más alto nivel, un sistema 3G puede describirse mediante un conjunto de subsistemas funcionales que toman decisiones e interactúan entre sí para dar soporte a usuarios 3G inalámbricos, estos subsistemas funcionales son:

- Subsistema funcional *Módulo de Identidad de Usuario (UIM: User Indentity Module)*

  Las funciones UIM soportan la seguridad y los servicios de usuario. Las funciones pueden residir en una tarjeta física removible para un terminal móvil o pueden estar integradas en el propio terminal móvil.

- Subsistema funcional *Terminal Móvil (MT: Mobile Terminal)*

  Las funciones MT proporcionan la capacidad de comunicar el UIM con la red de acceso radioeléctrico a la vez que soportan los servicios y la movilidad de usuario.

- Subsistema funcional *Red Central (CN: Central Network)*

  Las funciones CN proporcionan la capacidad de comunicación con la RAN y otras CN así como las funciones necesarias para soportar servicios de usuario y movilidad de usuario.

- Subsistema funcional *Red de Acceso Radioeléctrico (RAN: Radioelectric Access Network)*

  Las funciones RAN proporcionan la capacidad de comunicación con el MT y la CN. Las funciones en la RAN actúan como puente, direccionador y pasarela según las necesidades con objeto de intercambiar información entre la CN y el MT.

La figura 1.2 muestra la relación entre los diferentes subsistemas funcionales de los Sistemas 3G.

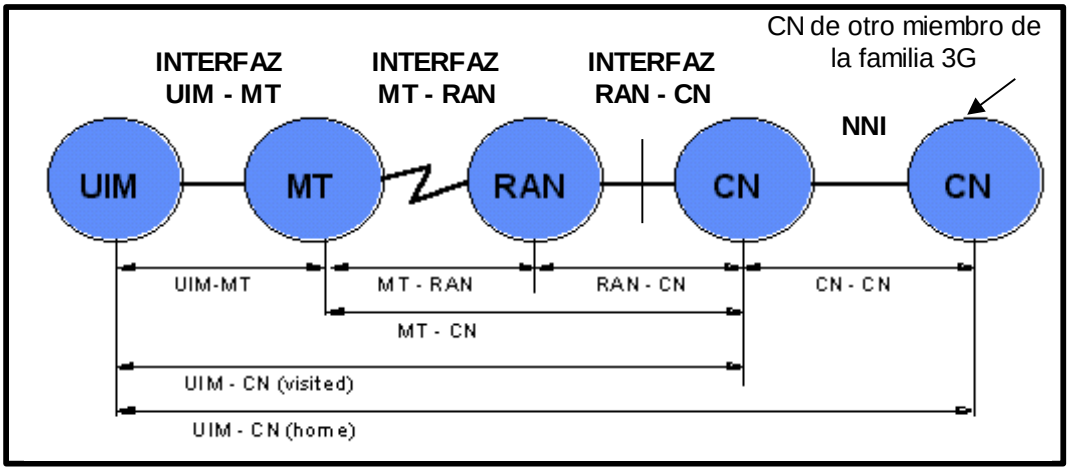


Figura 1.2 Subsistemas Funcionales de los Sistemas 3G

Estos subsistemas funcionales se presentan con fines de modelización y pueden implementarse como una o más plataformas físicas en diversas configuraciones. Los subsistemas funcionales se descomponen después en elementos funcionales más pequeños que se describen en el modelo funcional de red para 3G.

De igual forma dentro de los Sistemas 3G se pueden distinguir diferentes tipos de dominios con los que los móviles deben interactuar, estos dominios son:

- *Dominio Administrativo.* Es una intranet o una colección de redes, computadores y bases de datos bajo una administración común. Se pude asumir que las entidades computacionales operan en una administración común y comparten las asociaciones de seguridad creadas administrativamente.

- *Dominio Local.* Es un dominio administrativo que contiene la infraestructura de Autenticación, Autorización y Tarificación (AAA: Authentication, Authorization and Accounting) de interés inmediato para un cliente IP móvil cuando está fuera de casa.

- *Dominio Foráneo.* Es un dominio administrativo visitado por un cliente móvil IP, y contiene la infraestructura necesaria para soportar las operaciones que conlleven a habilitar el registro del móvil IP.

1.2.3 Aplicaciones y Servicios

A la hora de hablar de aplicaciones se encuentra un portafolio bastante amplio, inclusive ilimitado, sin embargo se pueden enumerar las siguientes:

- *Aplicaciones en Internet*. Dentro de este campo de servicios podemos encontrar navegadores Web, correo electrónico, videoteléfono, juegos y comercio electrónico entre otros.

- *Acceso a Intranet*. Esta gama de servicios hace referencia a aplicaciones como la transferencia de archivos, acceso a bases de datos e información empresarial.

- *Aplicaciones Humanas*. Son todas aquellas aplicaciones encaminadas al usuario tradicional y de gran popularidad hoy en día, entre las cuales tenemos las postales electrónicas, servicios de chat, buzón de mensajes, televisión y el audio “mp3”.

- *Aplicaciones Especializadas*. Este tipo de servicios hace referencia a todos aquellos que no forman parte de las expectativas de los usuarios comunes, sino por el contrario de un grupo con necesidades específicas; por ejemplo las aplicaciones de tele-medicina, tele-educación, tele-vigilancia, servicios de posicionamiento, servicios de bolsa, entre otros.

- *Comercio electrónico móvil*. En esta área podemos encontrar servicios como la reserva de tiquetes, transacciones bancarias, pago de cuentas y compra de artículos.

Un elemento que es importante destacar es la posibilidad de trabajar con herramientas como el Protocolo de Aplicación Inalámbrico (WAP: Wireless Application Protocol), que da acceso a los usuarios móviles a distintos servicios basados en Internet, lo que es un ejemplo de datos en ambientes móviles. La figura 1.3 muestra los diferentes servicios de los que podrá disponer un usuario en los Sistemas 3G.

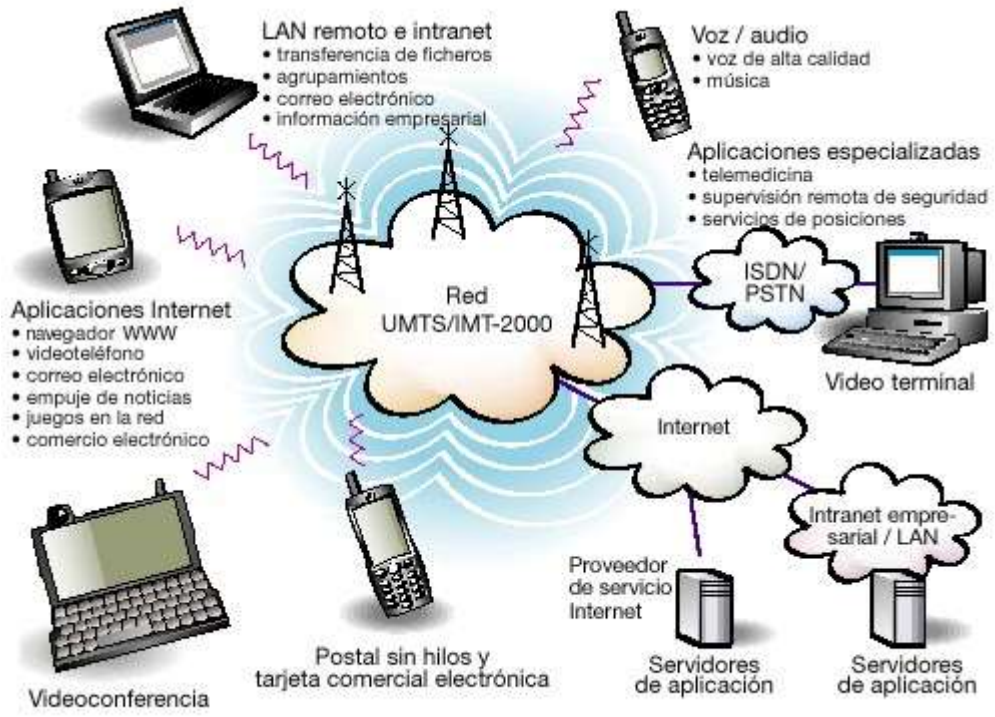


Figura 1.3 Aplicaciones de Usuario de Tercera Generación

Esta nueva dimensión de comunicación móvil está destinada a poner servicios de Internet en los bolsillos de cientos de millones de personas, así WAP sirve también como el inicio de una plataforma de desarrollo de aplicaciones inalámbricas dentro de la arquitectura Cliente/Servidor.

1.3 Seguridad en los Sistemas 3G

La seguridad en los Sistemas 3G es uno de los campos que ha despertado mayor interés debido al tipo de aplicaciones que se proveerán y a la clase de información que será manejada (números de tarjetas de crédito, transacciones financieras, información corporativa, entre otros) siendo por lo tanto necesario implementar mecanismos que brinden un alto nivel de confiabilidad en la prestación de los servicios y que permitan aprovechar al máximo las ventajas de estos sistemas.

1.3.1 Conceptos básicos sobre seguridad

Antes de profundizar en lo concerniente a los Sistemas de Tercera Generación, es necesario aclarar ciertos aspectos relacionados con la seguridad, los cuales serán

objeto de estudio y punto de partida para los desarrollos que se realicen posteriormente en este campo. Estos aspectos son:

- *Amenazas.* Una amenaza es toda acción, operación o hecho no autorizado que podría afectar adversamente al sistema. Involucra la determinación de cualquier tipo desautorizado de acceso, cambio, destrucción, revelación, interrupción, bloqueo o hurto de los medios que constituyen el sistema

- *Vulnerabilidad.* Indica un aspecto sensible dentro del sistema que puede ser aprovechado por un intruso.

- *Ataque.* Es un procedimiento heurístico basado en una vulnerabilidad, el cual tiene como fin causar amenaza.

- *Riesgo.* Se detecta al evaluar o estimar la proximidad o debilidad de un sistema, para que le sea causado daño.

De igual forma es necesario identificar los diferentes actores que tienen relación con el nivel de seguridad que pueda proveer el sistema, ya que serán ellos quienes interactúen con el mismo. Entre estos actores tenemos:

- Usuarios
- Red
- Proveedor de servicios de red
- Protocolos de comunicación
- Administrador de la red
- Personas externas
- Cuerpos de auditoria

Otro aspecto de fundamental importancia en la seguridad de un sistema es lo referente a los mecanismos que se utilicen para garantizar la protección de información; una de las herramientas comúnmente utilizadas, y quizás la de mayor relevancia para nuestro proyecto, es la criptografía la cual ha sido utilizada a través de los años para mandar mensajes confidenciales cuyo propósito es que sólo las personas autorizadas puedan entender el mensaje.

La criptografía es la técnica de convertir un texto inteligible, texto plano (plaintext), en otro llamado criptograma (ciphertext) cuyo contenido de información es igual al anterior pero sólo lo pueden entender las personas autorizadas. Para encriptar se debe transformar un texto mediante un método cuya función inversa únicamente conocen las personas autorizadas, utilizando para ello un algoritmo secreto o un algoritmo público que utiliza una palabra llamada clave como elemento de control (la cual es conocida sólo por las personas autorizadas), esta clave debe ser imprescindible para la encriptación y desencriptación.

Las técnicas de criptografía moderna se pueden clasificar en dos según el tipo de clave utilizada:

Criptografía simétrica o de clave secreta. Se caracteriza por hacer uso de la misma clave para encriptar y desencriptar, toda la seguridad está basada en la privacidad de esta clave secreta, llamada simétrica porque es la misma para el emisor y el receptor. El emisor del mensaje genera una clave y después la transmite mediante un canal seguro a todos los usuarios autorizados a recibir mensajes. La distribución de claves es un gran problema para los sistemas simétricos, hoy en día se resuelve mediante sistemas asimétricos montados únicamente para transmitir claves simétricas.

Criptografía de clave pública o asimétrica. Se basa en la utilización de claves distintas para encriptar y desencriptar, una de ellas se hace pública y la otra es privada de cada usuario. Así todos los usuarios de la red tienen acceso a las claves públicas, pero únicamente a su clave privada, lográndose utilizar para confidencialidad (como los sistemas simétricos) y autenticación, además de solucionar el problema de la distribución de claves simétricas.

Los sistemas de clave pública realizan la encriptación de forma diferente para cada tipo de servicio:

- *Confidencialidad.* El emisor encripta el texto con la clave pública del receptor y el receptor lo desencripta con su clave privada. Así cualquier persona puede enviar un mensaje encriptado, pero sólo el receptor, que tiene la clave privada, y el emisor, que lo ha creado, pueden descifrar el contenido.

- *Autenticación.* Se encripta el mensaje o un resumen de éste mediante la clave privada y cualquier persona puede comprobar su procedencia utilizando la

clave pública del emisor. El mensaje es auténtico porque sólo el emisor verdadero puede encriptar con su clave privada.

1.3.2 Propiedades de la información que protege la seguridad

La Seguridad del sistema debe encaminarse fundamentalmente a salvaguardar las siguientes propiedades de la información:

- *Privacidad.* La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la privacidad es la divulgación de información confidencial sobre los usuarios 3G.

- *Integridad.* La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de violación a la integridad es la modificación no autorizada del valor facturado por la prestación de un servicio.

- *Disponibilidad.* La información debe estar en el momento que el usuario requiera de ella. Un ataque a la disponibilidad es la Negación de Servicio (DoS: Denial of Service), es decir, dejar fuera de funcionamiento total o parcialmente a un servidor e impedir de esta manera que se le de servicio a los usuarios del sistema.

1.3.3 División de las áreas de administración de la seguridad

Para simplificar, es posible dividir las tareas de administración de seguridad en tres grandes campos. Estos campos son:

Autenticación

Hace referencia a la necesidad de establecer las entidades que pueden tener acceso al universo de recursos que el sistema puede ofrecer.

Autorización

Es el hecho de que las entidades autorizadas a tener acceso a los recursos, tengan acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.

Auditoria

Se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este campo el mantener estadísticas de acceso, estadísticas de utilización y políticas de acceso a los recursos.

1.3.4 Objetivos generales de seguridad

Dentro de los requisitos que se espera que cumplan los sistemas móviles de Tercera Generación se tienen:

- La seguridad proporcionada a un usuario 3G y a un proveedor de servicio u operador 3G, debe ser comparable a la seguridad proporcionada por las redes fijas contemporáneas.
- Los aspectos jurídicos, reglamentarios y comerciales de la seguridad que caracteriza a los Sistemas 3G deben facilitar la disponibilidad de servicio a escala mundial.
- La seguridad que han de proporcionar las Redes 3G debe estar normalizada adecuadamente para soportar interfuncionamiento y transito mundial seguro entre diferentes proveedores de servicio y/u operadores de red.
- Se debe prever la adopción de disposiciones de modo que sea posible la interceptación legal de la comunicación radioeléctrica del usuario de acuerdo con la legislación nacional.
- Los Sistemas 3G no deben utilizar disposiciones de seguridad que sean características inherentes del diseño de la interfaz radioeléctrica, de modo que se pueda adoptar cualquier diseño de interfaz radioeléctrica sin disminuir la seguridad y la privacidad.

1.3.5 Identificación de las amenazas

A continuación se identifican las amenazas asociadas con la prestación y utilización de los servicios en los Sistemas 3G; dichas amenazas se pueden dividir en las siguientes categorías:

- Amenazas intencionales
- Amenazas accidentales
- Amenazas administrativas

Amenazas Intencionales

Son las que hacen los intrusos maliciosos. Se pueden clasificar a su vez en tres categorías:

- Uso fraudulento
  - Robo del terminal móvil
  - Imitación. Copia de los datos secretos de usuario a un terminal móvil fraudulento.
  - Intromisión. Interrupción de una llamada después de que se ha establecido pero antes de que el terminal móvil legítimo haya iniciado la conversación.

- Amenazas a la integridad
  - Manipulación coherente de los datos de usuario. La información de la comunicación es manipulada intencionalmente de modo que esta tenga un significado diferente al original, pero que todavía parezca significativa a los usuarios.
  - Registro malicioso de la ubicación. El intruso intenta registrar a un usuario legítimo en una ubicación errónea.
  - Manipulación maliciosa del perfil de servicio del usuario

- Amenazas a la confidencialidad, privacidad y anonimato
  - Revelación de identidades de usuario
  - Revelación de la ubicación de usuarios
  - Escucha furtiva de la comunicación del usuario

Amenazas Accidentales

Son las causadas por errores operacionales del usuario, errores de transmisión, fallas en el sistema, errores cometidos por personal administrativo y operativo, entre otros.

Amenazas administrativas

Son las causadas por la falta de administración y gestión de seguridad, el abuso de privilegios, etc. Posiblemente este tipo de amenazas no se relacionen con la interfaz radioeléctrica. Entre ellas tenemos:

- Intromisión en la base de datos del abonado/usuario

- Intento de registro de credenciales de usuario en otras redes
- Intromisión en la base de datos del sistema o funciones de control de red.

Todas estas amenazas conducen a la necesidad de implantar mecanismos que garanticen la confidencialidad y autenticidad de la información que se está transportando, al igual que la autenticidad de quienes pretenden registrarse en la red. Entre dichos mecanismos se encuentran los denominados procesos AAA, los cuales hacen parte de la temática tratada en las siguientes secciones y serán objeto de un estudio más detallado en capítulos posteriores.

1.3.6 Requerimientos de seguridad de los Sistemas 3G

A continuación se indican los requerimientos de seguridad que se aplican a una o más de las partes que interactúan en los Sistemas 3G.

En sentido general, los requerimientos de seguridad del sistema se pueden relacionar con una o más de las siguientes prestaciones de seguridad:

- Confidencialidad.
- Autenticación.
- Integridad.
- Autorización y control de acceso.
- Privacidad y anonimato.
- Disponibilidad del servicio.
- Limitación de eventos.
- Informe de eventos.

Los requisitos del servicio para la seguridad de los Sistemas 3G se agrupan en las siguientes categorías:

Requisitos relacionados con el servicio

Las prestaciones de seguridad proporcionadas para la protección de los usuarios deben ser cómodas y fáciles para el usuario y en la medida de lo posible deben ser transparentes a ellos y requerir un mínimo de interacción en cada llamada. De igual forma la prestación de dicha seguridad no debe aumentar significativamente los tiempos de establecimiento del servicio.

Requisitos relacionados con el acceso

Debe ser muy difícil para un intruso suplantar a un usuario, proveedor del servicio u operador de red, en la comunicación con otros usuarios u operadores de red. De igual forma se debe reducir al mínimo la posibilidad de que un intruso pueda tener acceso a la información que circula por un canal y pueda leerla, modificarla, almacenarla o limitar de alguna forma la prestación del servicio.

Requisitos relacionados con la interfaz radioeléctrica

Se debe garantizar el no descifrado de las comunicaciones de los usuarios a través de una interfaz radioeléctrica 3G, independiente del tipo de servicio que se esté prestando. Igualmente no debe ser posible para un intruso identificar al usuario o localizarlo físicamente, mediante interceptación en una interfaz radioeléctrica.

Requisitos relacionados con el terminal

Se debe brindar la posibilidad de que un proveedor del servicio u operador de red identifiquen un terminal móvil no autorizado, robado o imitado y que registren e impidan el acceso de este equipo a los servicios. Igualmente debe reducirse al mínimo la posibilidad de que un intruso obtenga identidades de terminales móviles, y en particular, información de autenticación de un terminal móvil 3G.

Requisitos relacionados con la tasación

Se deben brindar los mecanismos para que la tasación y tarificación de los servicios sea la establecida por los operadores, de igual forma se debe garantizar que intrusos no tendrán acceso a la información de tarificación evitando así posibles manipulaciones y operaciones fraudulentas.

Requisitos operacionales de red

La seguridad que han de proporcionar los Sistemas 3G debe estar normalizada adecuadamente para proporcionar interfuncionamiento y transito internacional seguro; sin embargo, dentro de los mecanismos de seguridad se debe permitir la independencia máxima entre las partes que intervienen en el funcionamiento de los Sistemas 3G, así como la máxima libertad para que todos los participantes tengan sus propias políticas y mecanismos de seguridad. Otro aspecto a tener en cuenta es que dichos mecanismos de seguridad deben requerir el mínimo posible de conexiones de señalización de larga distancia en tiempo real.

Requisitos de gestión de seguridad

Las claves y dispositivos de seguridad que sean implementados deben ser gestionados y actualizados de manera fácil y segura. De la misma forma se deben tener mecanismos seguros para registrar eventos asociados con usuarios o abonados 3G y para gestionar las claves de seguridad entre los proveedores de servicios y al interior de los mismos.

1.3.7 Seguridad proporcionada por los Sistemas 3G

Una prestación de seguridad es un proceso que brinda cierto grado de protección contra una o varias posibles amenazas a la seguridad y que por lo general posee una de las siguientes propiedades:

- Prevención
- Informe
- Limitación
- Restablecimiento
- Disuasión

Las prestaciones de seguridad se han clasificado en esenciales y facultativas, y se clasifican también en prestaciones relacionadas con el usuario y prestaciones relacionadas con el proveedor del servicio.

Las prestaciones de seguridad relacionadas con el usuario son proporcionadas con una ventaja de seguridad directa para los usuarios 3G, mientras que las prestaciones de seguridad relacionadas con el proveedor del servicio son proporcionadas para que satisfagan las necesidades de seguridad global del sistema que afectan solo indirectamente a los usuarios.

A continuación se describen las prestaciones de seguridad proporcionadas por los Sistemas de Tercera Generación:

Prestaciones de seguridad esenciales relacionadas con los usuarios.

Los Sistemas de Tercera Generación proporcionan las siguientes prestaciones de seguridad esenciales relacionadas con el usuario:

- *Control de acceso para datos de abonado y de perfil del servicio.* Prestaciones por las cuales se imponen restricciones al acceso a los datos personales y al perfil de servicio almacenados en la red de un usuario o abonado 3G.

- *Autorización de acción de usuario ó de terminal.* Prestaciones por la cuales las diversas acciones de un usuario ó terminal móvil 3G tienen distintos grados de restricción. Ello requiere que un usuario ó terminal móvil 3G tiene que estar autorizado para ejecutar sus acciones.

- *Confidencialidad de datos de usuario e información de señalización.* Prestaciones por las cuales los datos de un usuario y la información de señalización 3G están protegidos contra su revelación en la interfaz radioeléctrica, en la prestación de cualquiera de los servicios.

- *Confidencialidad de identidad y ubicación de usuario.* Prestaciones por las cuales se protege la identidad de un usuario 3G y su ubicación física contra su revelación en una interfaz radioeléctrica.

- *Autenticación de identidad de usuario y de terminal.* Prestaciones por las cuales se verifica que la identidad del usuario y del terminal móvil son las alegadas.

- *Verificación de titular del Módulo de Identidad de Usuario (UIM).* Prestación por la cual se autentica al usuario humano del UIM. Esta prestación solo se aplica cuando el UIM se utiliza para la asociación de usuario relacionada con los terminales móviles que utilizan esta tecnología.

- *Integridad de datos de transacción.* Prestación por la cual el usuario y el proveedor de servicio 3G pueden tener cierta seguridad de que los datos transmitidos desde el otro lado en una transacción no han sido modificados en el canal.

- *Integridad de ubicación de usuario y de terminal móvil.* Prestaciones por las cuales el proveedor del servicio propio, el proveedor del servicio visitado y/o el operador de red pueden tener cierta seguridad de que la información relacionada con la ubicación del usuario y del terminal móvil no puede ser modificada por intrusos.

- *Distribución segura de identidad de usuario y su información de seguridad asociada.* Prestación por la cual la identidad del usuario 3G y su información de seguridad asociada puede distribuirse con seguridad al UIM por el proveedor de servicio propio en el momento del registro del usuario. Esta prestación solo se aplica cuando se utiliza el UIM para la asociación de usuario relacionada con terminales móviles 3G (posiblemente sin relación directa con la interfaz radioeléctrica).

- *Distribución segura de identidad de terminal móvil y su información de seguridad asociada.* Prestación por la cual la identidad de terminal móvil 3G y su información de seguridad asociada puede distribuirse con seguridad al terminal móvil, si son asignadas por el gestor del terminal, o al gestor de terminal, si son asignadas por los fabricantes del terminal, en el momento del registro del terminal móvil (posiblemente sin relación directa con la interfaz radioeléctrica).

Prestaciones de seguridad facultativas relacionadas con los usuarios.

Los Sistemas 3G pueden proporcionar las siguientes prestaciones de seguridad facultativas relacionadas con los usuarios:

- *Autenticación de proveedor de servicio.* Prestación por la cual se verifica que la identidad de un proveedor de servicio 3G es la alegada.

- *Reautenticación de usuario y de terminal.* Prestaciones por las cuales se verifica de nuevo que la identidad de un usuario o de un terminal móvil es la alegada. Esta prestación puede ser invocada repetidamente o en cualquier momento.

- *Informes de evento de usuario.* Prestación por la cual el usuario recibirá avisos o indicaciones en momentos críticos durante el funcionamiento de los servicios (por ejemplo, información sobre tasas acumuladas y que su comunicación no está cifrada).

- *Acceso de abonado al perfil de servicio.* Prestación por la cual el abonado tiene acceso directo y limitado al perfil de servicio personal de sus usuarios

asociados, y mediante la cual puede restringir el acceso a servicios entre otras aplicaciones más.

Prestaciones de seguridad esenciales relacionadas con la prestación del servicio.

Los Sistemas 3G proporcionan las siguientes facilidades esenciales de seguridad relacionadas con la prestación de los servicios:

- *Denegación al usuario de acceso al servicio.* Prestación por la cual el proveedor del servicio niega el acceso al servicio a un determinado usuario.

- *Reserva de datos de abonado.* Prestación por la cual el proveedor de servicio puede restablecer datos relativos a usuarios o abonados después de un fallo.

- *Represión del fraude y de los abusos en la red.* Prestación por la cual se facilita a un operador de red, con el que el proveedor del servicio o el gestor del terminal tienen relación, los datos necesarios para que proceda a la represión del fraude y de los abusos en su red.

Prestaciones de seguridad facultativas relacionadas con la prestación del servicio.

Los Sistemas 3G proporcionan las siguientes prestaciones de seguridad facultativas relacionadas con la prestación de los servicios:

- *Registro de eventos.* Prestación por la cual el proveedor de servicio puede registrar actividades relacionadas con el usuario o el abonado 3G.

- *Denegación de acceso al servicio a terminales móviles.* Prestación por la cual el proveedor de servicio y/u operador de red puede denegar a un terminal móvil acceso a un determinado servicio.

1.3.8 Arquitectura de seguridad

Basadas en una arquitectura de protocolos diferente a la manejada hasta ahora, las Redes de Tercera Generación inician un proceso encaminado a la implementación de

un protocolo para el control de sesión y señalización en servicios de voz y multimedia basados en IP, denominado Protocolo de Iniciación de Sesión (SIP: Session Initiation Protocol). Uno de los requerimientos de mayor relevancia para poder implementar el SIP es la definición de una arquitectura de seguridad que proteja la señalización para el control de la sesión.

Como ya se ha visto, la arquitectura de red 3G se encuentra basada en el concepto de dominio, el cual se encarga de agrupar las entidades funcionales de red. Desde el punto de vista del SIP, el Equipo de Usuario (UE: User Equipment) proporciona la funcionalidad de un agente usuario del SIP, y el subsistema IM se convertiría en el proxy del SIP, mientras que los registros y servidores de ubicación brindan soporte para el roaming global. Por tanto existen varias amenazas para los mensajes enviados entre el SIP y las diferentes entidades de red móvil. Los siguientes apartados brindan una apreciación global de la arquitectura de seguridad utilizada actualmente para la introducción de los SIP y los requerimientos de seguridad necesarios.

La arquitectura de seguridad que protege la primera fase de implementación de Sistemas 3G ofrece a las redes móviles la autenticación mutua de entidades y el establecimiento de llaves de sesión entre un UE viajero y la red.

En lo concerniente a la interfaz aérea, la cual se convierte en la sección más expuesta de las redes móviles, todos los datos enviados entre un UE y la red visitada son opcionalmente encriptados en la capa de enlace, aumentando la longitud de la clave utilizada hasta ahora para encriptar este tipo de comunicaciones (pasando de 40 a 128 bits), lo que hace prácticamente imposible su descifrado.

Además de la encriptación, es obligatorio proteger la integridad de los datos de señalización que van por la interfaz aérea (más precisamente, la confidencialidad y protección de la integridad se extienden más allá del Controlador de la Red Radio (RNC: Radio Network Controller), cubriendo también las partes de la red fija). La señalización de la que se habla anteriormente es la utilizada para controlar las portadoras en los circuitos y la conmutación de paquetes en los diferentes dominios del Sistema Universal de Telecomunicaciones Móviles (UMTS: Universal Mobile Telecommunications System), la cual es diferente de la señalización de control de sesión para un protocolo de capa de aplicación como SIP.

El protocolo utilizado para la autenticación y el establecimiento de llaves es llamado protocolo de Autenticación y Acuerdo de Llaves en UMTS (UMTS-AKA: UMTS Authentication and Key Agreement). Dicho protocolo está basado en llaves secretas a largo plazo compartidas entre el USIM y el centro de autenticación en la red local.

Dentro de la ejecución de este protocolo son generadas llaves de sesión de corto tiempo de vida (corto tiempo de validez). Como consecuencia, a todos los mensajes de señalización enviados entre el UE y la red foránea se les brindará protección de integridad utilizando para ello procedimientos de encriptación, basados en las llaves de sesión generadas. Una diferencia mayor entre UMTS-AKA y otros protocolos de encriptación como el Intercambio de Llaves en Internet (IKE: Internet Key Exchange) es que UMTS-AKA se ha diseñado especialmente para escenarios viajeros. Según 3GPP (3GPP: 3G Partnership Project), IKE no cumple los requerimientos para estos escenarios.

La autenticación involucra tres partes: el UE foráneo, la redes foráneas y la red local. Las entidades encargadas de la autenticación son el USIM y un Centro de Autenticación en la red local del usuario donde ellos comparten la llave secreta de largo plazo. Sin embargo, la red local delega el control de la autenticación a la red visitada (foránea), principalmente por razones de desempeño. Aquí, se requiere confianza mutua entre la red visitada y la red local, manejo realizado dentro de un llamado "acuerdo de roaming".

El UE y el Centro de Autenticación también establecen llaves de sesión entre ellos. El Centro de Autenticación transfiere como consecuencia las llaves de sesión codificadas a la red visitada que finaliza la confidencialidad e integridad por el UE. Utilizando las llaves de sesión, las redes visitantes demuestran al UE que están autorizadas por la red local para servir al UE.

La delegación del control de la autenticación y el traslado de las llaves de sesión a la red visitada es realizada por los vectores de transferencia de autenticación del centro de autenticación de la red visitada. Éstos vectores de autenticación contienen pares de pregunta-respuesta y las respectivas llaves de sesión. Normalmente varios vectores de autenticación para un USIM específico son transferidos a la red visitada dentro de un simple requerimiento a la red local, lo que reduce significativamente la carga de dicha red y de la red local, para las autenticaciones subsecuentes, minimizando el retraso de las operaciones de los usuarios móviles.

1.3.9 Requerimientos de seguridad para el SIP

Como un requisito general, cualquier arquitectura de seguridad debe permitir diferentes mecanismos para la seguridad de acceso a dominio (es decir, UE-SIP NE) en el terminal móvil y seguridad de dominio de red (es decir, SIP NE-SIP NE) en el otro extremo. Esto a consecuencia de los diferentes requerimientos del sistema y los diferentes papeles de entidades SIP que forman parte de una u otra sección de la red.

Requerimientos de seguridad de acceso a dominio

En lo referente a la seguridad de acceso a dominio debe ser soportada la autenticación mutua y el intercambio de llaves entre el usuario móvil (representado por el USIM) y el lado de la red. La clave de largo plazo compartida que es usada para la autenticación y la llave intercambiada sólo deben ser conocidas por el USIM y la red local; de igual forma debe garantizarse la protección de integridad y la confidencialidad entre el usuario móvil y el SIP NE (SIP Network Entity) en el lado de la red.

Otro requerimiento importante es el hecho de que se deben proveer mecanismos seguros para delegar la integridad o confidencialidad a un SIP NE específico. Además debe proveerse un mecanismo seguro para la delegación de la entidad de control de la autenticación y gestión de llaves. Esto se debe al hecho de que el control de integridad, confidencialidad y autenticación requeridos, no necesariamente son transportados fuera de la red local, o por la misma entidad. De igual forma debe proporcionarse también un transporte seguro para las claves de sesión convenidas al SIP NE que determinará la integridad y confidencialidad de los usuarios.

Igualmente se debe asegurar confidencialidad para la identidad del usuario. Debe ser posible ocultar la identidad de un usuario móvil, u otros datos que puedan derivarse de esta entidad, o que permita rastrear al usuario o derive su ubicación, mientras gestionó el acceso al dominio (el inconveniente aquí radica en el hecho de que la identidad del usuario debe ser enviada antes de la llave de sesión para que pueda establecerse la protección de la confidencialidad).

Es crucial que para mantener la compatibilidad de los sistemas cualquier mecanismo de seguridad del SIP debe ser independiente de la tecnología de acceso que proporcione conectividad IP y movilidad.

Requerimientos de seguridad en el dominio de la red

Una vez superada la parte concerniente al acceso al dominio se deben considerar los requerimientos de seguridad al interior de este, donde inicialmente se debe soportar la autenticación mutua y la gestión de llaves entre SIP NEs de diferentes subsistemas IM. Este mecanismo soportará la autenticación basada en el intercambio previo de las llaves confidenciales compartidas (en lugar de utilizar un método de llaves públicas).
De la misma forma debe proveerse protección de integridad y confidencialidad entre SIP NEs de diferentes subsistemas IM.

Otro aspecto que se debe tener en cuenta es la integridad extremo a extremo y confidencialidad entre SIP NEs dentro del mismo subsistema IM, así como la confidencialidad de la identidad de los usuarios en el dominio de la red.

Requerimientos del sistema de seguridad

Finalmente, en términos globales, el sistema de seguridad debe garantizar que cualquier mecanismo criptográfico que deba ser ejecutado por el dispositivo móvil especialmente para la autenticación y el intercambio de llaves en el USIM, no debe utilizar criptografía de llave pública, es decir, sólo debe permitirse criptografía de llave simétrica. La interfaz aérea está limitada por el ancho de banda y la probabilidad de error. Los mecanismos de seguridad para la interfaz aérea deben poder tratar los retrasos causados por bajos anchos de banda o altas tasas de errores.

En lo referente a las soluciones de seguridad se debe garantizar que cualquier solución de seguridad implementada debe ser escalable a grandes cantidades de usuarios y debe poder soportar un gran número de Redes Móviles de Carácter Público (PLMN: Public Land Mobile Network) diferentes (dominios de confianza diferentes). De la misma forma se debe garantizar el roaming global, por ejemplo, un usuario móvil debe poder acceder a una red foránea sin contacto previo entre el usuario móvil y la red visitada (manejo realizado por el protocolo UMTS AKA).

Cualquier protocolo para la autenticación e intercambio de claves debe ser eficaz. Debe minimizar el número de operaciones para identificar a un usuario móvil en una red foránea, disminuyendo así la carga de la red.

Se debe proveer un almacenamiento seguro para las llaves a largo plazo utilizadas para seguridad en subsistemas IM, en el lado correspondiente al usuario móvil y a la red local. Igualmente se debe garantizar la ejecución de algoritmos de seguridad. Algoritmos que requieren acceso a las llaves a largo plazo se ejecutarán en las mismas entidades en que dichas llaves se almacenen.

Lo consignado anteriormente se convierten en los requerimientos de seguridad que hasta el momento se han establecido para garantizar la confidencialidad y correcto funcionamiento de los sistemas de Tercera Generación.

Es conveniente recordar que a pesar de que este es uno de los puntos más críticos en la especificación de los nuevos sistemas, todavía se encuentra en etapa de desarrollo y pruebas, siendo de particular interés la aplicación de la tecnología de Agentes Móviles que por sus características de funcionamiento se convierte en una excelente opción para servir de soporte a la prestación de las aplicaciones de seguridad necesarias para garantizar los requerimientos especificados.

2. AGENTES MÓVILES

El acelerado desarrollo de los sistemas de telecomunicaciones y la creciente necesidad de contar con mecanismos que brinden una conectividad global y permitan acceder a la información en cualquier momento, lugar y forma han llevado al desarrollo de nuevas tecnologías que faciliten la obtención y tratamiento de dicha información de una manera ágil y eficiente. Dentro de este entorno surge el concepto de Agente Inteligente (InA: Intelligent Agent), el cual establece una serie de mecanismos que pretenden dar un paso más allá en el tratamiento informático distribuido, añadiendo características como la localización o la situación, y permitiendo la interacción dinámica de componentes autónomos y heterogéneos.

Los agentes son una de las tecnologías con mayor auge en la actualidad y sus aplicaciones pueden observarse en múltiples campos. Disciplinas como inteligencia artificial, interacción humano–computadora, sistemas distribuidos, ingeniería de software, redes y sistemas autónomos, han fundado las bases para el surgimiento de esta prometedora tendencia.

2.1 Definición de Agente

Actualmente hay tres disciplinas informáticas fundamentales en el desarrollo y definición de agentes:

- Inteligencia artificial.
- Programación orientada a objetos y programación concurrente.
- Diseño de interfaces hombre-máquina.

El término *agente* posee numerosas definiciones que sin duda están influenciadas de acuerdo a las áreas en las que éstos se han aplicado. Sin embargo en términos generales los "agentes son procesos autónomos o semi-autónomos que realizan una misión bien definida".

Seguidamente se indicará, a modo de ejemplo, algunas de las definiciones de agente más utilizadas:

- Según el Diccionario de la Lengua Española:

"Agente: Del lat. *agens, -entis*, p. a. de *agere*, hacer.
adj. Que obra o tiene virtud de obrar. …
m. Persona o cosa que produce un efecto.
Persona que obra con poder de otro …".

- Según el Grupo para la Gestión de Objetos (OMG: Object Management Group):

"Un agente es un programa de computador que actúa autónomamente en nombre de una persona u organización".

- Según Lange y Oshima

“Los agentes son, desde el punto de vista del usuario final, programas que lo asisten y que actúan a su favor. La funcionalidad de los agentes consiste, entonces, en permitirles a los usuarios delegarles tareas que interactúen con información. “

- Según I.B.M. Aglets:

"Los agentes inteligentes son entidades programadas que llevan a cabo una serie de operaciones en nombre de un usuario o de otro programa, con algún grado de independencia o autonomía, empleando algún conocimiento o representación de los objetivos o deseos del usuario".

Aunque anteriormente se han indicado las principales acepciones del término agente, ninguna de ellas puede tomarse con carácter general, sino que consideraremos como claves para una definición adecuada las características más básicas:

Situación: localización en un determinado entorno.
Flexibilidad: sus acciones no están prefijadas.
Autonomía: puede actuar sin intervención directa del hombre o de otro programa.

En este punto también existe cierta controversia, ya que los investigadores en Inteligencia Artificial consideran que un agente ideal debería tener tres cualidades: *posibilidad de cooperar con otros agentes o programas, capacidad de aprendizaje y ser autónomo.*

Es así como tomando en cuenta los anteriores conceptos se podría dar una posible definición:

"Se puede definir un agente Inteligente como un programa que puede actuar en nombre de un usuario o de otro programa y puede hacer esto con cierto grado de independencia. Como tal, un agente puede comprender los objetivos de su usuario y tomar la iniciativa para alcanzarlos. El agente puede operar y reaccionar de forma autónoma utilizando las capacidades incorporadas para negociar con otros agentes o puede actuar de acuerdo a su entorno. Sin embargo, el usuario puede en cualquier momento definir las fronteras dentro de las cuales permite que el agente negocie y tome decisiones."

2.2 Tipos de Agentes

Por supuesto, hay multitud de clasificaciones que dependen del punto de vista del investigador. Aunque es posible considerar la más común, realizada a partir de la enumeración de las características que cumple un agente.

- Movilidad: capacidad de transportarse de una máquina a otra.
- Reacción: actuación sobre el entorno mediante un comportamiento estímulo/respuesta.
- Proacción: toma la iniciativa para alcanzar sus objetivos.

- Sociabilidad o cooperación: capacidad de comunicarse con otros agentes, programas o personas.
- Aprendizaje o adaptación: comportamiento basado en la experiencia previa.
- Continuidad temporal: ejecución continua en el tiempo.
- Carácter: inclusión de estados de creencia, deseo e intención.

Teniendo en cuenta que un agente cumple las características mínimas de situación, flexibilidad y autonomía, expuestas anteriormente, se puede considerar, por ejemplo, agentes móviles con aprendizaje; agentes reactivos y sociables; agentes móviles proactivos y sociables; etc.

Desde el punto de vista de la Inteligencia Artificial se hace una clasificación a tres niveles:

- Agentes móviles o estáticos.
- Agentes reactivos o proactivos.
- Agentes cooperativos, autónomos, con aprendizaje o con una mezcla de dichas características:
    - Agentes de interfaz: autónomos y con aprendizaje.
    - Agentes colaboradores: autónomos y cooperativos.
    - Agentes ideales: autónomos, cooperativos y con aprendizaje.

2.3 Diferencia entre Agentes Móviles y Agentes Estáticos

Antes de examinar más a fondo el concepto de agente móvil, es importante conocer las diferencias principales entre los conceptos de agentes estáticos y agentes móviles, definidos por el Grupo Gestión de Objetos (O.M.G.:Object Management Group) en sus Utilidades para la Interoperación entre Sistemas de Agentes Móviles.

2.3.1 Agente Estático

Es aquél que sólo puede ejecutarse en la máquina donde fue iniciado. Si éste necesita interactuar con otros agentes o programas o requiere cierta información que no se encuentra en el sistema, la comunicación puede llevarse a cabo mediante cualquier método de interacción para objetos distribuidos, como la Arquitectura

genérica para Mediación de Requerimientos de Objetos (CORBA: Common Object Request Broker Architecture) o el Método de Invocación Remota (RMI: Remote Method Invocation) de Java.

2.3.2 Agente Móvil

Es aquél que no está limitado al sistema donde se inició su ejecución, siendo capaz de transportarse de una máquina a otra a través de la red. Esta posibilidad le permite interactuar con el objeto deseado de forma directa sobre el sistema de agentes donde se halla dicho objeto. También puede utilizar los servicios ofrecidos por el sistema multiagente destinatario.

Las tareas de búsqueda y tratamiento de la información en Internet tienen últimamente una gran importancia en el desarrollo de sistemas basados en agentes móviles. Debido al rápido crecimiento de la Red, el proceso de encontrar los datos más convenientes para un usuario resulta excesivamente tedioso y complejo. En nuestro caso, puede enviarse un agente a los destinos más interesantes para el usuario, localizar y filtrar la información deseada siguiendo las normas dictadas por éste y traerla consigo al computador de origen, permitiendo ahorrar tiempo de conexión y ancho de banda y, por lo tanto, dinero. De igual forma en los futuros Sistemas de Tercera Generación donde el usuario podrá encontrarse en cualquier lugar del planeta y solicitar acceso a información y recursos distantes geográficamente, esta tecnología será de gran utilidad dadas sus características y potencial de funcionamiento.

Los agentes móviles suelen programarse normalmente en lenguajes interpretados o generadores de código intermedio, Telescript, Java, Tcl, ya que éstos dan un mejor soporte a entornos heterogéneos, permitiendo que los programas y sus datos sean independientes de la plataforma utilizada.

La **seriación** es el proceso típico por el que se representa el estado completo de un agente mediante una serie que puede ser fácilmente transportada por la red. El proceso de decodificación de dicha serie en el agente se denomina **diseriación**.

2.4 Antecedentes

Los agentes de red o agentes móviles han sido desarrollados como un método alternativo para el paradigma de Llamadas a Procedimientos Remotos (RPC: Remote Procedure Call), una interacción común entre un cliente y un servidor utilizando RPC.

En RPC, el servidor B ofrece un conjunto de servicios así como los recursos y procedimientos necesarios para la ejecución de dichos servicios. El cliente A requiere un servicio *X* así que le envía una petición remota por medio de un mensaje (que incluye los argumentos necesarios para la ejecución del servicio *X*) al servidor B. Como respuesta, B atiende la solicitud del servicio ejecutando el procedimiento correspondiente y accesando los recursos involucrados. El servicio produce un resultado que es enviado de regreso al cliente por medio de una interacción adicional y provoca que el cliente que hasta este momento había estado bloqueado en espera de una respuesta a su solicitud, reanude su ejecución. La figura 2.1 ilustra el concepto del paradigma RPC.

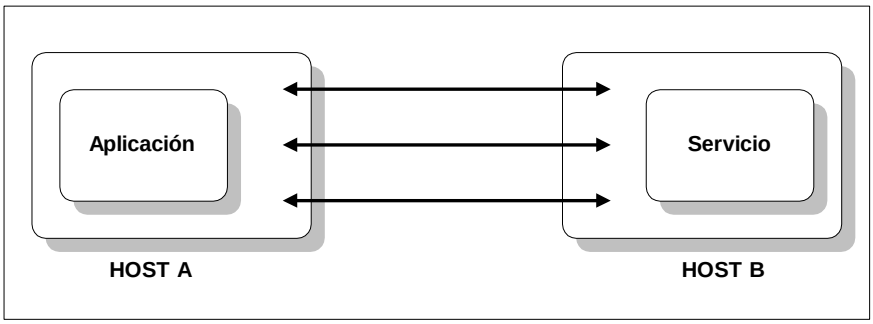


Figura 2.1 Esquema basado en RPC

La característica principal de RPC es que, en cada interacción entre el cliente y el servidor se entablan dos actos de comunicación, uno para enviarle al servidor la petición y los argumentos correspondientes y otra para enviar los resultados de la petición. Este tipo de interacción puede incrementar dramáticamente el tráfico de la red si el número de clientes y/o el número de peticiones de servicios se incrementan.

Una alternativa a RPC es la Programación Remota (RP: Remote Programming), también referenciado como *modelo basado en agentes móviles* [Sanchez 1997]. En este tipo de comunicación, al enviar el cliente A una petición para la ejecución de un servicio, no solamente manda los argumentos necesarios para la ejecución de tal

servicio sino que manda el procedimiento requerido para su ejecución. Cada mensaje que la red transporta contiene un procedimiento que la computadora receptora ejecuta y los datos (argumentos) necesarios para su ejecución. Estos datos reflejan el estado actual del procedimiento. El procedimiento comienza su ejecución en el cliente pero continua en el servidor. El procedimiento y su estado son llamados un *agente móvil.* La figura 2.2 ilustra el concepto del uso de agentes móviles.

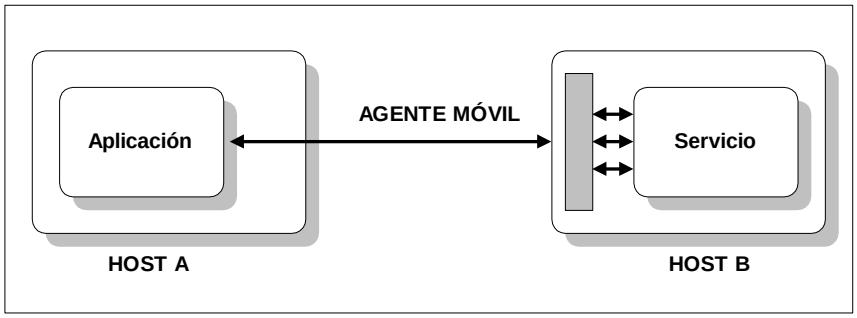


Figura 2.2 Esquema basado en Agentes Móviles

La primera ventaja de RP es el desempeño. Cuando una computadora cliente tiene trabajo que hacer en un servidor remoto, puede enviar el trabajo y supervisarlo localmente utilizando un agente, en vez de estar enviando continuamente instrucciones sobre la red.

La segunda ventaja de RP es la personalización. Un agente móvil permite que el cliente personalice la funcionalidad del servidor. Pueden enviarse nuevos procedimientos con poco esfuerzo. RP puede ayudar a automatizar procesos de instalación. Se puede codificar en un programa un proceso de instalación y transferirlo a un conjunto de nodos de la red. En cada nodo el programa puede analizar las características de la plataforma local de hardware/software y ejecutar la configuración correcta. RP ayuda a incrementar la flexibilidad del servidor, manteniendo limitado el tamaño y la complejidad del mismo. Cada cliente es responsable de la correcta especificación del servicio que necesita y debe ser descrito en el código enviado al servidor remoto.

Por su naturaleza, RP permite especificar qué procesos complejos deben ejecutarse de forma remota, y si los servicios tienen que ser ejecutados en un servidor que es alcanzable solamente a través de una conexión lenta (por ejemplo, vía modem), se puede enviar el programa para su ejecución y no se necesitaría mantener una

conexión permanente con el servidor, excepto para la transmisión del resultado final. En la figura 2.3 se puede observar como se realiza el proceso de operación de los Agentes Móviles al no disponer de una conexión.

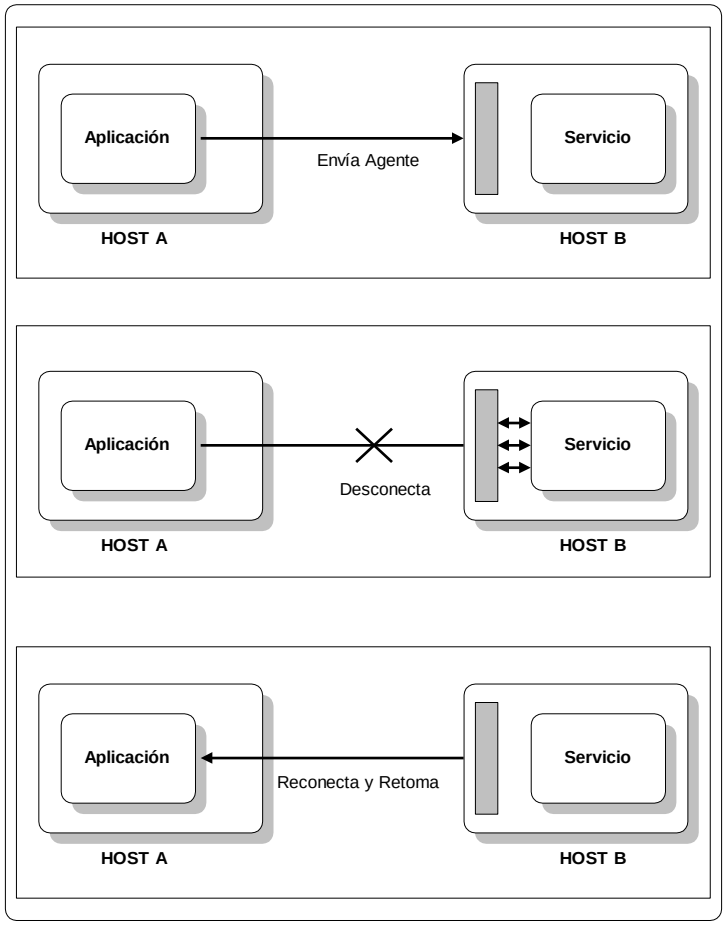


Figura 2.3 Operación de Agentes Móviles sin conexión

Todos estos beneficios de la programación remota, hacen de los agentes móviles una tecnología muy atractiva para el desarrollo de nuevos sistemas.

2.5 Definición de Agente Móvil

Existen en la literatura diversas definiciones de lo que es un agente móvil. Para [Gray 1995a], un *agente transportable* es un programa que puede migrar de una máquina a otra en una red heterogénea. Este tipo de agente debe ser portable a través de plataformas, debe ser capaz de elegir cuando y donde transportarse a si mismo, debe

ser capaz de duplicarse a si mismo, y debe poder comunicarse con otros agentes para intercambiar información.

Según [Nwana 1996], los *agentes móviles* son procesos computacionales de software capaces de moverse en Redes de Area Amplia (WAN: Wide Area Network) tales como el www, interactuando con diferentes hosts, recolectando información en nombre de su dueño y regresando a casa después de ejecutar las tareas delegadas por su usuario. Esas tareas pueden ir desde una reservación de vuelo hasta el manejo de una red de telecomunicaciones. Los *agentes móviles* son agentes porque son autónomos y cooperan. Por ejemplo, pueden cooperar o comunicarse con otros agentes, intercambiando datos o información.

Para [Kotay y Kotz 1994] los *agentes transportables* son aquellos que soportan el movimiento de computo cliente a un sitio donde se encuentra un recurso remoto. Son capaces de suspender su ejecución, transportarse ellos mismos a otro host en la red, y reanudar la ejecución desde el punto en el cual ellos fueron suspendidos. Consumen pocos recursos de red y pueden soportar sistemas que no tienen una permanente conexión a la red, tales como computadores portátiles o dispositivos inalámbricos.

[Ghezzi y Vigna 1994], definen al *agente móvil* como un componente que contiene al menos un hilo de ejecución, el cual es capaz de autónomamente migrar a un sitio diferente.

Para [Vitek 1996], un *agente móvil* es un conjunto de objetos ejecutando un cálculo en nombre de un usuario. Este cálculo es realizado en una plataforma de ejecución de agentes la cual controla la ejecución del agente. Un agente puede requerir moverse causando que su calculo sea interrumpido y reanudado en otra máquina.

[White 1996], plantea que un *agente móvil* es un programa:

- Una persona u organización enviste con su autoridad
- Puede correr sin supervisión por un largo periodo de tiempo (por ejemplo una semana)
- Puede conocer e interactuar con otros agentes
- Puede ejecutarse en diferentes sistemas de computo y en diferentes etapas de su vida.

En resumen se puede decir que un agente móvil es un programa o proceso con las siguientes características:

- Es autónomo o semi-autónomo de manera que él decide como, cuando y a donde migrar.
- Esta orientado a ejecutar tareas, a veces en nombre del usuario y otras basándose en los cambios de su ambiente.
- Se envía como objeto, a través de plataformas conservando además de su código, los datos y su estado de ejecución.
- Es asíncrono, debido a que tiene su propio proceso o hilo de ejecución. Por tanto, el agente se ejecuta asincrónicamente respecto a los otros procesos que se estén ejecutando en el nodo.
- Es capaz de comunicarse con su dueño, con otros agentes y con el medio. Puede operar sin conexión, es decir, que puede ejecutar sus tareas aun cuando la conexión a red no este funcionando; si el agente necesita trasladarse y la red no esta activa, el agente puede esperar o desactivarse hasta que la conexión se restablezca.
- Puede suspender su ejecución, transportarse a otro host y reanudar su ejecución desde el punto en el cual se suspendió.
- Es capaz de duplicarse.
- Puede reaccionar a cambios en su ambiente, modificando su conducta debido a las acciones generadas por otros agentes, debido a su experiencia propia o por la intervención directa del programador o usuario.

En la figura 2.4 podemos observar el funcionamiento de un agente móvil.

2.6 Paradigmas de la Computación en Redes

Los Agentes Móviles pueden revolucionar el diseño y desarrollo de los sistemas distribuidos puesto que proveen un poderoso y uniforme paradigma de computación en redes. Para poner esto en perspectiva, se observa una apreciación global y comparación de tres paradigmas de programación para computación distribuida: *cliente-servidor*, *código por demanda* y *agentes móviles*.

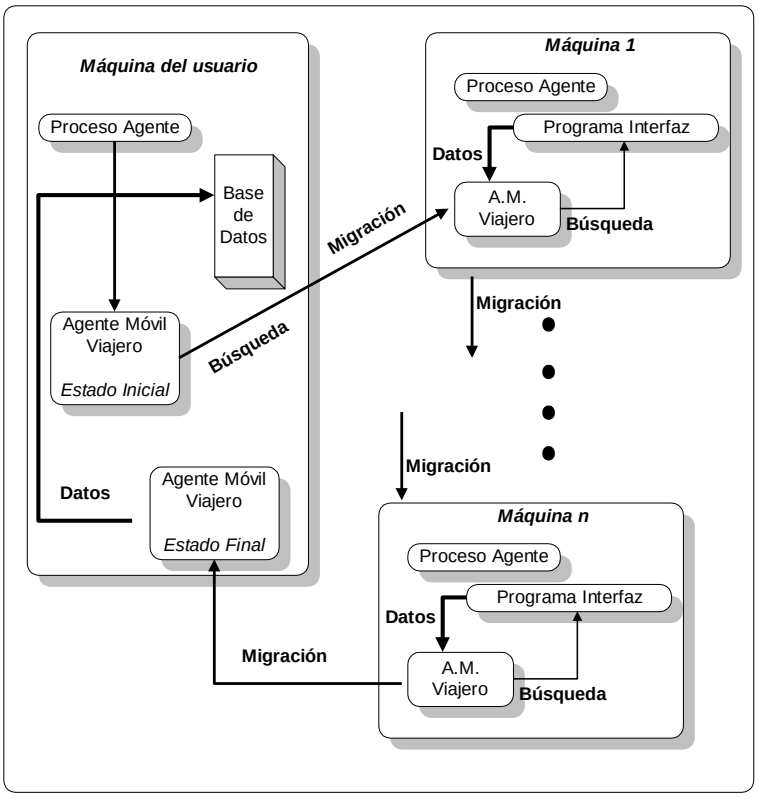


Figura 2.4 Funcionamiento de un Agente Móvil

2.6.1 Paradigma Cliente-Servidor

En el paradigma Cliente – Servidor (figura 2.5), un servidor provee un conjunto de servicios que brindan acceso a algunos recursos (por ejemplo bases de datos). El código que implementa esos servicios es organizado localmente por el servidor. Se dice que el servidor tiene el "Know-How". Finalmente, es el servidor por si mismo quien ejecuta el servicio y así, es él quien tiene la capacidad de procesamiento.

Muchos sistemas distribuidos han sido basados en este paradigma, existe un amplio rango de tecnologías que lo soportan como Llamada a Procedimientos Remotos (RPC: Remote Procedure Calling), Arquitectura Común para Mediación de Solicitudes de Objeto (CORBA: Common Object Request Broker Architecture) y el Método de Invocación Remota (RMI: Remote Method Invocation).

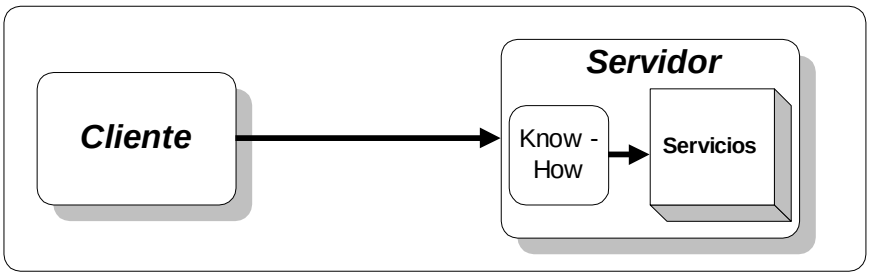


Figura 2.5 Paradigma Cliente – Servidor

2.6.2 Paradigma de Código por Demanda

De acuerdo a este paradigma (figura 2.6), el cliente toma el "Know-How" cuando lo necesita y lo puede bajar desde un host en la red. Una vez el cliente recibe el código, la computación es transportada hacia él. El cliente posee la capacidad de procesamiento y los recursos locales.

Los applets y servlets Java son excelentes ejemplos prácticos de este paradigma. Los applets son bajados en navegadores web y ejecutados localmente, mientras que los servlets son subidos a los servidores web remotos y ejecutados allí.

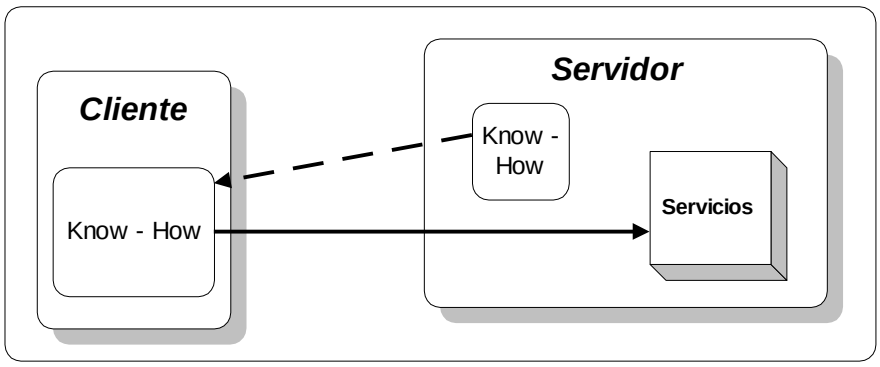


Figura 2.6 Paradigma de código por demanda

2.6.3 Paradigma de Agentes Móviles

Una característica clave del paradigma de Agentes Móviles (figura 2.7), es que ningún host en la red permite un alto grado de flexibilidad para poseer una mezcla de "Know-How", recursos y procesadores. Sus capacidades de procesamiento pueden ser combinadas con recursos locales. El "Know-How" (en la forma de Agentes Móviles) no está atado a un solo host sino que está disponible a lo largo de la red.

Si se comparan estos tres paradigmas se puede ver la tendencia cronológica hacia una mayor flexibilidad. El cliente y el servidor han emergido y han llegado a ser un host. El applet y el servlet, sirviendo como extensiones de clientes y servidores, respectivamente, se han combinado y mejorado con la emergente tecnología de agentes móviles.

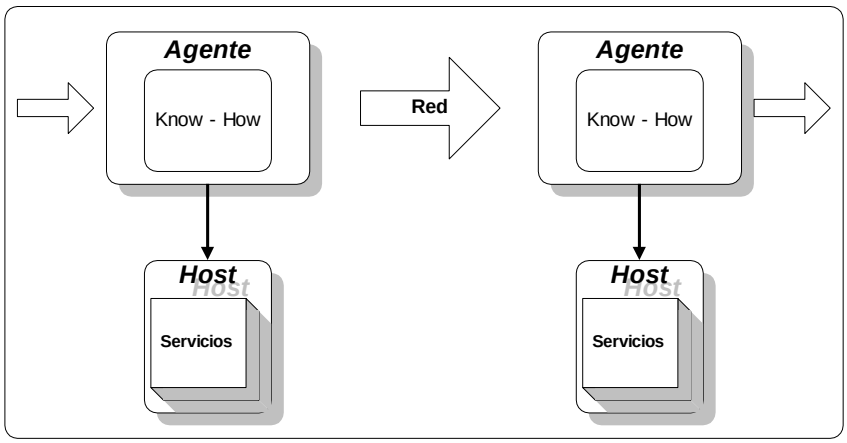


Figura 2.7 Paradigma de Agentes Móviles

2.7 Infraestructura para Agentes Móviles.

Para ser útil un agente necesita interactuar con su nodo y otros agentes, debe accesar información que la máquina ofrece y/o negociar con otros agentes sobre el intercambio de servicios e información. Los agentes deben ser también capaces de moverse dentro de redes heterogéneas de computadoras. Esto es posible solamente si existe un marco de trabajo común para operaciones de agentes a través de la red completa, es decir, una infraestructura de agentes estandarizada.

Esta infraestructura debe ofrecer soporte básico para la movilidad y comunicación de agentes. También debe proteger a la computadora de accesos no autorizados y salvaguardar la integridad de los agentes, tanto como sea posible [Lingnau et al. 1995] En esta sección se describen algunas de las infraestructuras planteadas por diversos autores.

2.7.1 Infraestructura para Agentes Móviles según Crystaliz.

Crystaliz Inc., sugiere un modelo común [Crystaliz 1997], que extrae las características más generales de los sistemas de agentes móviles que existen con el fin de estandarizar y promover interoperabilidad entre dichos sistemas.

El *Sistema de Agentes* es una plataforma que puede crear, interpretar, ejecutar, transferir y terminar agentes. Un *lugar* es donde el agente reside, es un contexto en un Sistema de Agentes en el cual un agente puede ejecutarse. Toda la comunicación entre Sistemas de Agentes se hace a través de la *Infraestructura de Comunicación (CI: Communication Infrastructure)*.

Se han identificado 3 tipos de interacción de agentes:

- C*reación de agentes remotos.* Un programa cliente interactúa con el Sistema de Agentes, pidiéndole crear un agente de una clase particular.
- *Transferencia de agentes.* Cuando un agente decide transferirse a otro Sistema de Agentes, el Sistema de Agentes le crea una solicitud de viaje.
- *Invocación de métodos de agentes.* Un agente puede invocar el método de otro agente u objeto si está autorizado para hacerlo y tiene una referencia al objeto.

Dentro de las funciones de un Sistema de Agentes podemos enunciar las siguientes:

- Transferir un agente, lo cual puede incluir iniciar una transferencia de agente, recibir un agente, y transferir *clases.*
- Crear un agente.
- Proporcionar nombres únicos a los agentes.
- Soportar el concepto de región (conjunto de sistemas de agentes).
- Hallar un agente móvil.
- Asegurar un ambiente seguro para operaciones de agentes.

2.7.2 Infraestructura para Agentes Móviles según Lingnau.

[Lingnau et al. 1995] propone una infraestructura para agentes móviles basada en el Protocolo de Transferencia de Hypertexto (http:: HiperText Transfer Protocol) el cual proporciona movilidad al agente a través de redes heterogeneas, así como comunicación entre agentes.

Soporta agentes escritos en diversos lenguajes y permite implementar una variedad de esquemas de interacción basados en un mecanismo general para comunicación de agentes. La base de esta infraestructura es la noción de *Servidor de Agentes*.

El Servidor de Agentes es un programa que corre en cada computadora, el cual es accesible a los agentes y está a cargo de que los agentes corran en esa computadora. Sus tareas incluyen aceptar agentes, crear ambientes de ejecución apropiados, ejecutar los agentes y terminarlos. También debe organizar la transferencia a otros nodos, manejar la comunicación entre agentes, así como entre los agentes y sus dueños y hacer autenticación y control de acceso para todas las operaciones del agente. Participa también en el manejo de operaciones de red.

Cada Servidor de Agentes conoce sobre otros Servidores de Agentes en su "vecindario" y esta información la hace disponible para los agentes, quienes la utilizan para elegir un nuevo destino, en el momento en que ellos deciden dejar la maquina. Para cada agente corriendo en un servidor, existe un ambiente de ejecución adecuado. El *ambiente de ejecución* es la interfaz entre el agente y su nodo y permite que los recursos de la maquina estén disponibles para el agente de una manera controlada.

2.7.3 Infraestructura para Agentes Móviles según Stone.

[Stone et al. 1996] propone un sistema de agentes cuyas componentes principales son los agentes móviles, un lenguaje de agentes, Lugares de Reunión de Agentes (AMP: Agent Meeting Places), y una maquina.

El *agente* puede ser escrito en varios lenguajes de programación y puede transportar conocimiento expresado en varias formas. El agente debe ser capaz de entablar un dialogo con el *lugar de reunión de agentes* hasta que se ejecute o se rechace. Un agente puede ejecutarse hasta su terminación o puede elegir suspender su actividad y moverse a otro lugar de reunión de agentes y continuar su ejecución ahí.

- *Lugar de Reunión de Agentes* (AMP: Agent Meeting Places). Un AMP ofrece servicio para los agentes móviles que entran allí.
- Una *máquina* es un programa residente en el servidor que implementa el marco de trabajo del agente manteniendo y ejecutando los AMPs que contiene,

así como los agentes que ocupan esos AMPs. En general, la máquina es un interprete para el lenguaje utilizado en la implementación del ambiente de trabajo del agente. La máquina se comunica con el nodo a través de 3 aplicaciones de Interfaz de Programa de Aplicación (API: Application Program Interface). Los APIs son utilizados para manejar almacenamiento, transportar agentes y comunicarse con las aplicaciones externas.

2.7.4 TACOMA: una Infraestructura para Agentes Móviles.

A continuación se presenta una infraestructura particular para agentes móviles, llamada TACOMA. Esta infraestructura se compone *de agentes, folders, portafolios y gabinetes.* Los agentes TACOMA [Johansen et al. 1995b] desarrollados en la Universidad de Troms y la Universidad de Cornell, están escritos en Tcl/Horus el cual es una versión del lenguaje Tcl que proporciona comunicación y tolerancia a tallas. La abstracción mas importante en TACOMA es la operación *meet* la cual se utiliza para que un agente ejecute otro agente. Este es un concepto vital utilizado para la comunicación y sincronización entre agentes. La operación *meet* debe tener un punto de entrada en el sitio de destino.

En TACOMA, no es posible interrumpir la ejecución de agentes. El agente que migra se ejecuta desde el comienzo del programa en vez de continuar después del punto de migración. Esto hace difícil escribir un agente que deba preservar el estado de información mientras migra a través de una secuencia de maquinas.

TACOMA no proporciona mecanismos de seguridad y su componente Horus no esta disponible en la mayoría de las plataformas. Características notables de TACOMA son el dinero electrónico que es utilizado para pagar los servicios, agentes guardaespaldas que inicializan agentes perdidos y agentes de rompimiento que proporcionan programación y servicios de directorio. Requiere que el programador explícitamente capture la información del estado antes de migrar. El sistema TACOMA proporciona soporte para procesos móviles, que recorren los nodos de una red para realizar una tarea [Johansen et al. 1995a].

En TACOMA los agentes se comunican utilizando archivos compartidos o *"folders"* [Hylton et al. 1996]. Existen varios folders de interés, por ejemplo, un folder CODE contiene el código fuente de un agente, el cual es vital para la transferencia de

agentes. Similarmente, un folder DATA contiene los datos que pueden ser asociados con el agente en el folder CODE. La colección de folders asociados con un agente forman un *"portafolio",* un agente puede acarrear un portafolio mientras se esta moviendo. Existen folders estacionarios que son necesarios para propósitos de almacenamiento de datos permanentes, para eso se utilizan los *"gabinetes".* La principal diferencia entre los gabinetes y los portafolios es que los gabinetes son estacionarios mientras que los portafolios son móviles.

Un agente TACOMA puede causar que otro agente sea ejecutado invocando la operación *meet* y llamando a un agente fuente y a un portafolios. El efecto de la operación es terminar la invocación de *meet y* entonces comenzar a ejecutar el agente destino con el portafolio especificado [Johansen et al~ 1995b].

Las cuatro arquitecturas presentadas y otras como la de [Reza et al. 1996], [Kato et al. 1997], [Lange y Change 1996] y [Straber et al. 1996], tienen en común el hecho de que para poder ejecutar un agente, se necesita de un ambiente adecuado y de un sistema o servidor de agentes que controle el acceso al ambiente. Dicho sistema debe ser capaz de monitorear las instrucciones a ser ejecutadas por los agentes y debe proveer las facilidades para migración y recepción de agentes, así como mecanismos para que los agentes se conozcan e intercambien datos.

2.8 Movilidad de un Agente

El proceso para transferir un agente de un sistema a otro se realiza en tres fases:

Iniciación de la transferencia.

- El agente identifica el destino deseado, realiza una petición de viaje al sistema y si es aceptada recibe el permiso para ejecutar la transferencia.
- El sistema suspende la ejecución del agente e identifica el estado y las partes del agente que serán enviadas. Se realiza la conversión en serie del código y del estado del agente (seriación) y se codifica según el protocolo establecido.
- El sistema hace la autenticación del agente.
- Se realiza la transferencia.

Recepción del agente

- El sistema destinatario acredita al cliente.
- Se realiza la decodificación del agente y la conversión de serie a código y estado del agente (diseriación).
- El sistema crea la instancia del agente, restaura su estado y continúa la ejecución.

Transferencia de otras clases (sólo en sistemas orientados a objetos).

- Este proceso es necesario cuando el agente se mueve de un sistema a otro, cuando el agente se crea remotamente o cuando necesita otros objetos. La transferencia de las clases puede realizarse completamente junto con el viaje del agente o hacer peticiones de carga cuando sea preciso.

2.9 Interoperabilidad entre Sistemas Multiagentes.

La normalización en el proceso de interconexión de agentes móviles se aplica a dos niveles:

- Interoperabilidad entre lenguajes de programación.
- Interoperabilidad entre sistemas escritos en el mismo lenguaje.

La primera de ellas resulta muy compleja de alcanzar y continúa aún en proceso de estudio, mientras que el segundo caso está siendo normalizado por CORBA. Para alcanzar el grado de interconexión deseado las Facilidades para la Interoperabilidad entre Sistemas de Agentes Móviles (MASIF: Mobile Agent System Interoperability Facility) de CORBA definen los siguientes conceptos:

- **Lugar.** Contexto dentro de un sistema donde puede ejecutarse un agente; por lo tanto, un agente viaja de un lugar a otro, ya sea en el mismo sistema o en otro distinto.
- **Localización.** Va asociada con un lugar, indicando el nombre y la dirección que ocupa en la agencia.
- **Localidad.** Propiedad de cercanía al destino, ya sea en el mismo computador o en la misma red.

- **Infraestructura de comunicación.** Provee servicios de transporte al sistema.
- **Autoridad.** Persona o entidad en nombre de la cual actúa un agente o un sistema de agentes.
- **Región o dominio.** Conjunto de sistemas de agentes que tienen la misma autoridad y que no tienen que ser del mismo tipo.

Pueden ocurrir tres circunstancias distintas en el proceso de comunicación entre dos agentes que se encuentran en distintos sistemas. Los sistemas comparten el mismo perfil (la misma norma) para la gestión de agentes, como se muestra en la figura 2.8, no existen problemas de interoperación y el agente puede viajar de un sistema a otro para hacer una comunicación local con el otro agente.

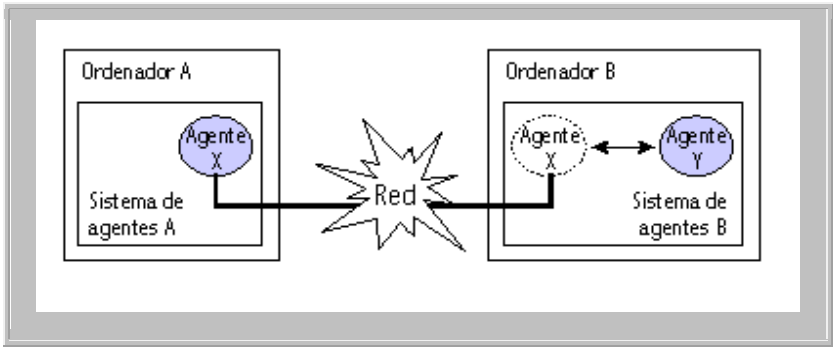


Figura 2.8 Sistemas compatibles

Los sistemas no siguen la misma norma, pero puede realizarse una comunicación local, como en el caso de la figura 2.9, en el computador destino existe otro sistema de agentes (C) compatible con el sistema origen (A), el agente se desplaza al sistema compatible y realiza la comunicación –RPC por ejemplo– con el otro agente.

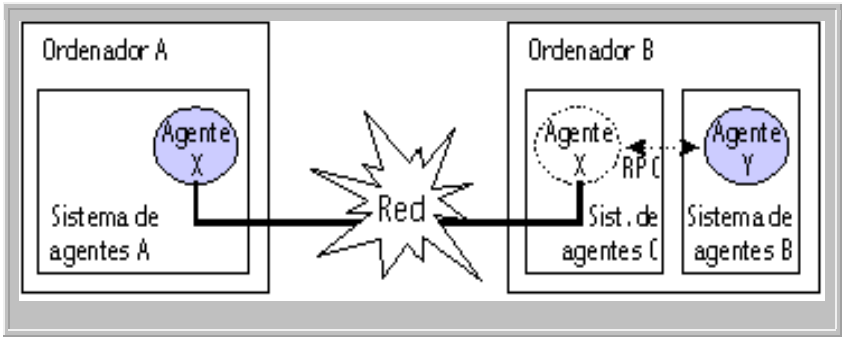


Figura 2.9 Sistemas Incompatibles con localidad

Los sistemas no son compatibles y no puede alcanzarse la propiedad de localidad, como se muestra en la figura 2.10, por lo tanto debe realizarse una comunicación normal entre los agentes.

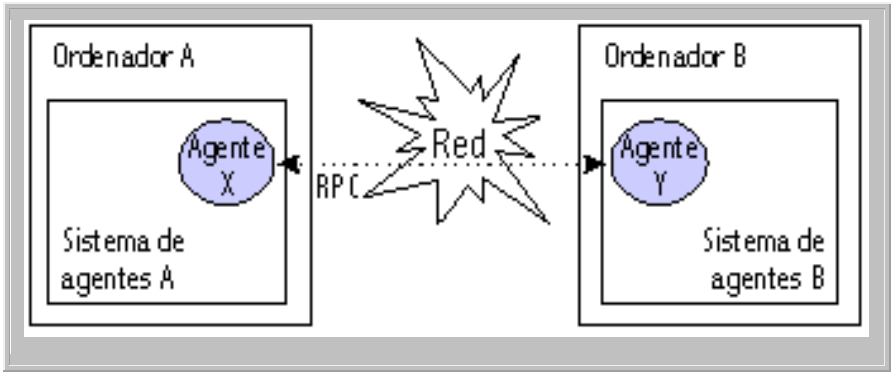


Figura 2.10 Sistemas Incompatibles

2.10 Aplicaciones de los Agentes Móviles

Los agentes móviles pueden ser útiles para muchas aplicaciones, entre ellas se tiene:

- *La recuperación de información* en la red puede ser soportada mucho más eficientemente si un agente puede moverse al lugar en donde los datos están almacenados, en lugar de tener que mover todos los datos a través de la red para revisarlos y posteriormente descartar la mayoría. Esta técnica ahorra un considerable ancho de banda.

- Otra área donde los agentes móviles pueden ser utilizados es en *la gestión de red.* En redes grandes, que contengan cientos o miles de computadores conectados, es muy difícil ejecutar operaciones de monitoreo y detección de fallas, ya que involucran grandes cantidades de datos. No es posible prefabricar programas de diagnóstico para cada eventualidad, pero será factible utilizar agentes móviles que observen detalladamente el sistema, enviando reportes sobre el estado de los computadores. [Goldszmidt y Yemini 1995] introducen un sistema basado en "delegación a agentes" los cuales están dinámicamente ligados a procesos remotos. Por este lado, el potencial de los agentes móviles para la gestión de red es de interés para las compañías de telecomunicaciones.

- *Comercio electrónico* es otro dominio en el cual pueden funcionar los agentes móviles: los negocios en Internet son una realidad y, como ya se cuenta con sistemas para pago electrónico, las premisas comerciales accesibles vía red crecerán rápidamente. Los agentes móviles pueden ayudar a localizar los lugares más baratos, negociar tratos o concluir transacciones de negocios en nombre de sus dueños.

- Una aplicación importante para los agentes móviles es la concerniente a *computación móvil.* Las computadoras portátiles son cada vez más pequeñas y más poderosas, pero el acceso a infraestructura de información fija es lenta debido a las restricciones en la transmisión. Para minimizar el poder de consumo y el costo de transmisión, los usuarios desearían no tener que permanecer en línea mientras alguna consulta complicada esta siendo ejecutada en su nombre por los recursos de computo fijo. Los agentes móviles ofrecen una manera prometedora para salir de este problema, los usuarios simplemente liberan un agente móvil que incorpore sus búsquedas y se desconectan, conectándose después para que los agentes devuelvan el resultado.

Para [Knabe 1995], los agentes móviles ofrecen solución a un amplio rango de problemas encontrados frecuentemente en aplicaciones distribuidas. Al mismo tiempo, hacen posibles nuevos tipos de aplicación con funcionalidades novedosas entre las que se encuentran:

- *Comunicación heterogénea.* Aunque las redes ofrecen muchos beneficios potenciales, todavía se tienen problemas de comunicación y distribución. Al tener dos sistemas juntos se revelarían los problemas de incompatibilidad en comandos y tipos de datos y a mayor número de sistemas mayor incompatibilidad. Los agentes móviles pueden resolver estos tipos de problemas sirviendo como un lenguaje que comparten muchos sistemas.

- *Protocolos especializados.* Los agente móviles permiten que los servidores utilicen protocolos de comunicación personalizada con los clientes. Para recibir un agente, el cliente y el servidor deben compartir algún protocolo estándar. Una vez que el agente esta corriendo, puede utilizar un protocolo especializado para la comunicación de regreso a su servidor de origen. Un agente en

ejecución puede comunicarse repetidamente con el servidor sin intervención del usuario, permitiendo la construcción de servicios dinámicos.

- *Reduce la carga del servidor.* Uno de los problemas con los servicios de Internet es que los componentes computacionales de un servicio típicamente deben residir en un servidor, porque los protocolos de aplicación utilizados como HTTP, Gopher, y Telnet se utilizan para el intercambio de datos no ejecutables, así que los servidores tienen la responsabilidad de ejecutar cualquier servicio relativo a computo para clientes. Esto lleva a transmisiones con requerimientos de gran ancho de banda y significa que el usuario debe esperar hasta que el servicio proporcione resultados. Estructurar un servicio con agentes puede resolver o reducir los problemas mencionados. La característica más importante de los agentes es que permiten trasladar computo de una máquina a otra. Un servidor puede descargar trabajo en un cliente enviándole un agente. El cliente está presumiblemente dispuesto a dedicar recursos tales como tiempo de la Unidad Central de Procesamiento (CPU: Central Processing Unit) para la interacción del servicio, y esos recursos pueden ser utilizados directamente por el agente. El usuario ahorra tiempo y la carga en el servidor y la red se aligera.

- *Datos inteligentes.* Agentes asociados con los datos pueden proporcionarle al dato una manera de "conocer" como procesarse a si mismo.

Obviamente ninguna de estas aplicaciones requiere del uso forzoso de agentes móviles, de hecho la mayoría podrían manejarse con programas estacionarios y algún paradigma de comunicación adecuado como RPC. Sin embargo, esto puede hacer que el sistema y la red se "carguen", con la consecuente incomodidad para el usuario.

2.11 Ventajas y Desventajas del uso de Agentes Móviles

Entre las ventajas de esta nueva tecnología se pueden mencionar las siguientes:

- *Reduce costos de comunicación.* Podría haber una gran cantidad de información que debe ser examinada para determinar su relevancia. Transferir esta información puede consumir tiempo y congestionar la red. Por ejemplo, el

tener que transferir muchas imágenes solo para elegir finalmente una. Es mucho más natural tener un agente que "vaya" a esa localidad, haga una búsqueda/elección y solamente transfiera la imagen elegida de regreso a través de la red. Esto evita la necesidad de hacer conexiones de red costosas entre computadores remotos tan requeridas en llamadas de procedimientos remotos (RPC). De igual forma se proporciona una alternativa mucho más económica en ancho de banda y en tiempo de acceso.

- *No se limita a recursos locales.* Si el poder de procesamiento y almacenaje en una máquina local es muy limitado, es necesario el uso de agentes móviles, de esta manera se puede migrar a una computador más poderoso y lograr ejecutar la aplicación deseada.

- *Coordinación más sencilla.* Puede ser más simple coordinar un número de solicitudes remotas e independientes y después solamente verificar los resultados de manera local.

- *Permite Computo Asíncrono.* El usuario puede activar sus agentes móviles y hacer alguna otra actividad mientras tanto y los resultados le llegarán por correo electrónico o algún otro medio, en algún tiempo posterior. Incluso puede operar aún cuando el usuario no este "conectado".

- *Proporciona* un *ambiente de desarrollo natural para implementar un libre mercado de servicios.* Nuevos servicios pueden ir y venir dinámicamente; y servicios mucho más flexibles pueden coexistir en unidades inferiores, proporcionando más opciones para los consumidores.

- *Proporciona una arquitectura flexible de computo distribuido.* Los agentes móviles proporcionan una arquitectura de computo distribuido única, la cual funciona de manera diferente de las arquitecturas estáticas. Esto proporciona una manera innovadora de hacer computo distribuido.

- *Presenta una oportunidad para hacer una reestructuración radical y atractiva del proceso de diseño en general.* Los agentes móviles transforman el proceso de diseño convencional, además de que algunos productos verdaderamente innovadores deberán emerger de esta nueva tecnología

.

- *Aprovechamiento de la asincronía.* Asincronía significa que dos actores de la comunicación no necesitan estar físicamente presentes al mismo tiempo (por ejemplo los usuarios del correo electrónico).

  Las ventajas de la asincronía son el mejoramiento en la utilización de las líneas de comunicación, la capacidad de realizar operaciones de recuperación de información más seguras y el hecho de que si el receptor esta ocupado cuando la comunicación se esta llevando a cabo, esta se procesara después. Esta última propiedad es muy interesante para equipos de computo móvil (PDA, LapTops) que no están permanentemente conectados. La estrategia estándar seria entonces: enviar el agente, desconectar y reconectar después. Con respecto a la utilización de las líneas de comunicación, se ha definido que las sesiones basadas en comunicaciones imponen una conexión permanentemente abierta entre el emisor y el receptor, esto requiere una conexión ocupada aunque nada este pasando actualmente.

  Para comunicaciones de bases de datos, esto puede empeorar si las transacciones imponen algunos bloqueos, este bloqueo se mantendrá hasta que la transacción sea abortada o reanudada. Pero si un agente es despachado de una manera asíncrona, una vez en un lugar remoto, el agente puede ejecutar un proceso síncrono y entonces esperar por una llamada de regreso de su computador de origen o decidir regresar por el mismo. Cuando el usuario se reconecta, recibe al agente de regreso.

  Por todo lo expuesto se dice que cuando la tarea a ser ejecutada no es en tiempo real, este esquema parece ser muy atractivo. Como se mencionó con anterioridad, la asincronía permite realizar operaciones de recuperación de datos más seguras. Cuando una transacción es comprometida, este es un proceso de todo o nada (¿quien no ha experimentado la frustración de ver su proceso de FTP interrumpido segundos antes de terminar y tener que comenzar todo otra vez?). En el caso de agentes, una vez que el agente ha sido transferido y exitosamente recibido ya no hay de que preocuparse, ya que el agente puede pedirle al servidor remoto ser activado o reactivado las veces necesarias hasta que el trabajo haya sido terminado.

- *Aprovechamiento de la autonomía.* Un agente debe mostrar algo de autonomía. Deben comportarse como "criaturas vivas" una vez que han sido convocadas. La autonomía realmente significa que no existe la necesidad de una conexión permanente entre el agente y su nodo de origen, ya que en el caso de agentes móviles el agente acarrea junto con él su propio código. El agente es todavía mas autónomo cuando tiene algún conocimiento de las preferencias del usuario. Esta propiedad de autonomía es muy importante ya que permite al agente trabajar por si mismo y no requiere de una conexión permanentemente abierta.

- *Aprovechamiento de las facilidades remotas. La* gran contribución de los agentes móviles es ser capaces de ejecutarse en máquinas remotas. Por lo tanto pueden aprovechar las capacidades remotas de determinadas máquinas, tales como:

  CPU. El agente es ejecutado en la máquina remota donde es más potente debido a la capacidad del CPU remoto. Esto es útil para dispositivos móviles (por ejemplo computadoras portátiles) con un CPU pobre o no disponible. Para máquinas cliente con CPU pobre, su debilidad puede ser resuelta a través de agentes.

  Memoria. Algunas operaciones pueden requerir una gran cantidad de memoria, por lo que puede ser útil tener acceso a memoria remota.

  Multiprocesamiento. Como una extensión de la CPU, si el nodo remoto tiene capacidades múltiples de procesamiento, estas pueden ser utilizadas por el agente.

  Multi- threacling. Los hilos pueden ser vistos como versiones "ligeras" de paralelización.

  Ancho de banda. *Si* el PC de un usuario tiene un modem de 28.8 baudios y la red de su oficina tiene un par de conexiones T1, el usuario puede enviar su agente a la red de la oficina donde puede aprovechar un ancho de banda mayor.

Otros recursos. Otros recursos que no pueden ser hallados localmente pueden ser utilizados por los agentes en el nodo remoto. Por ejemplo generadores de números aleatorios, coprocesadores matemáticos, hardware dedicado.

En teoría los agentes pueden ser capaces de aprovechar una gran variedad de recursos. Sin embargo los aspectos de seguridad y economía representan aún una gran barrera.

Considerando ahora las desventajas, la mayoría de los autores coinciden en que el punto más débil de los agentes móviles es precisamente la seguridad. Este tema será tratado con mas profundidad en la siguiente sección. Otras desventajas son las que se presentan en algunos de los lenguajes de programación para el diseño de agentes, entre las que podemos mencionar:

- La migración no puede ocurrir en puntos arbitrarios o requiere la captura explícita del estado de ejecución a nivel del agente.
- La comunicación entre agentes no existe o es difícil.
- Los agentes deben ser escritos en un lenguaje especifico y complejo.
- Las implementaciones solamente existen para hardware no estándar.
- Partes de la implementación solamente corren en plataformas especificas de Unix.
- El código fuente no esta disponible para la comunidad.

Como ejemplos de los lenguajes que presentan algunas de estas desventajas se podrían mencionar los siguientes: ***Telescript,*** el cual fue desarrollado en un lenguaje orientado a objetos muy complejo, requiere hardware poderoso de propósito especial, no esta abierto a los investigadores y limita al programador a un solo lenguaje. ***TACOMA*** requiere que el programador explícitamente capture el estado de ejecución antes de la migración. ***ARA*** no cuenta con niveles de seguridad adecuados [Gray 1995a; Gray 1996].

2.12 Aplicación de Agentes Móviles en Sistemas 3G

Los Sistemas de Tercera Generación impondrán un cambio radical en el campo de los sistemas inalámbricos tanto a nivel de los servicios prestados como de su estructura de funcionamiento. Por un lado el aumento en la demanda de aplicaciones cada vez más exigentes requiere procesos internos más complicados que garanticen la prestación eficiente de dichos servicios en el menor tiempo; adicionalmente a esto la tendencia a descentralizar el manejo de la información tanto de los usuarios como de los servicios y la posibilidad de recibir peticiones de conexión y acceso desde cualquier lugar del planeta conlleva a buscar mecanismos que sean capaces de recorrer de forma segura y ágil la red realizando las tareas necesarias para permitir la prestación de dichos servicios, apareciendo allí la tecnología de agentes móviles como una posible solución a estos nuevos requerimientos.

Dentro del ambiente en que se desenvuelven los Agentes móviles en esta nueva clase de sistemas podemos reconocer diferentes tipos de dominios con los que los Agentes deben interactuar, los cuales ya fueron estudiados en el capítulo 1, estos tipos de dominios son:

- *Dominio Administrativo.*
- *Dominio Local.*
- *Dominio Foráneo.*

Los clientes actualmente obtienen servicios de Internet negociando un punto de conexión a un “dominio propio”, generalmente a través de un Proveedor de Servicio de internet (ISP: Internet Service Provider), u otra organización desde la cual son establecidos y satisfechos los requerimientos del servicio. Con el incremento en la popularidad de los dispositivos móviles, se ha generado la necesidad de permitir a los usuarios conectarse a cualquier dominio conveniente para su localización actual. De este modo, un cliente necesita acceso a recursos que son provistos por un dominio administrativo (llamado “dominio foráneo”) diferente a su dominio propio. La necesidad de servicios de un “dominio foráneo” requiere, en muchos modelos, Autorización, la cual conduce directamente a la Autenticación, y por supuesto a la Tarificación (procesos AAA), garantizando así que la prestación del servicio se de a quien tenga derecho a él, cuando lo requiera y se le cobre la cantidad correcta por el mismo, independientemente de la ubicación en donde se encuentre el suscriptor.

Un agente en un dominio foráneo, puede ser llamado para proveer acceso a un recurso para un usuario móvil, siendo probable que sea necesario pedir o exigir al cliente que proporcione credenciales que puedan autenticarse antes de permitir el acceso al recurso. El recurso puede ser tan simple como un canal a Internet, o puede ser tan complejo como el acceso a recursos específicos de carácter privado, en el dominio foráneo, las credenciales pueden intercambiarse de muchas maneras diferentes utilizando la ayuda de los agentes móviles. Una vez autenticado, el usuario móvil puede ser autorizado para acceder los servicios dentro del dominio foráneo, iniciándose entonces la tarificación correspondiente al uso actual de los recursos. La figura 2.11 ilustra el concepto enunciado anteriormente.

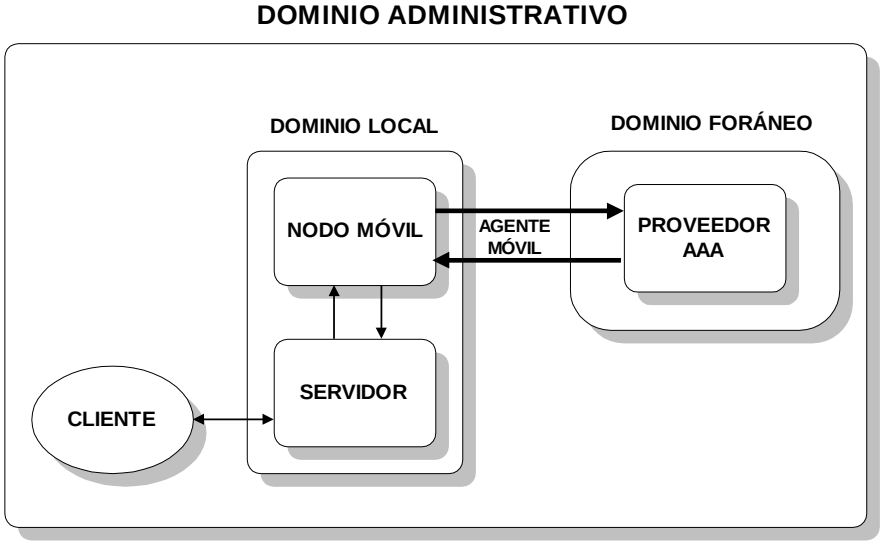


Figura 2.11 Agentes móviles en procesos AAA

IP móvil es una tecnología que permite a un nodo de la red (el nodo "móvil") migrar de su red "propia" a otras redes dentro del mismo dominio administrativo, o a otros dominios administrativos. La posibilidad de movimiento entre dominios que requieren servicios AAA ha creado la necesidad de diseñar y especificar los protocolos para dichos procesos, de tal forma que su infraestructura pueda aplicarse a las nacientes tecnologías en los sistemas inalámbricos.

2.13 Seguridad

El control de la seguridad es un grave problema, ya que un agente es un programa que viaja de un computador a otro, al igual que un virus. Los sistemas deben hacer

hincapié en la seguridad de los computadores y de la propia agencia. Los aspectos típicos de seguridad que deben ser controlados son:

- Protección de la máquina contra los agentes no autorizados.
- Protección contra otros agentes maliciosos.
- Protección de los agentes contra la máquina
- Protección de la red.

Los ataques más comunes que pueden realizarse a un sistema de agentes móviles son:

- Inundar el sistema con peticiones, tanto legales como ilegales.
- Escuchar la red para obtener información privada.
- Modificar, borrar o sustituir cualquier elemento transferido por la red.
- Grabar y retransmitir ilegalmente una comunicación.
- Falsificar la identidad, enmascaramiento de un agente o sistema de agentes para tener acceso a la información o a ciertos servicios.
- Utilización abusiva de algún recurso para que no pueda ser utilizado por otro usuario.
- Colocar un *Caballo de Troya* (agente o sistema de agentes) para recibir información confidencial o denegar acceso a los recursos.

Otros aspectos a tener en cuenta en lo referente a la seguridad son:

- La comunicación entre plataformas debe ser segura.
- Los agentes deben ser autenticados y autorizados con algunos derechos basándose en su identidad.
- Todas las interacciones entre la Plataforma de Ejecución de Agentes (AEP: Agent Ejecution Plataform) y el computador deben ser controladas y verificadas.
- La AEP debe ser protegida de agentes maliciosos.
- Los agentes deben estar protegidos unos de otros

2.13.1 Estrategias de Seguridad

Tanto los sistemas como los propios agentes móviles deben reforzar las tareas de seguridad para evitar, de un modo fiable, los ataques descritos anteriormente. De esta forma se pueden tener varias políticas de seguridad que permitan:

- Comprobar las credenciales de los participantes en cualquier comunicación.
- Restringir o garantizar las operaciones que puede ejecutar un agente.
- Gestionar privilegios de acceso a los recursos y establecer límites de consumo.

Los requisitos que se deben garantizar en cualquier comunicación son:

- **Confidencialidad:** evitar la escucha del canal.
- **Integridad:** comprobar que los datos no han sido modificados durante la transferencia.
- **Autenticación:** tanto el agente –o sistema– emisor como el receptor deben ser identificados para evitar accesos a información o a recursos reservados.
- **Detección de reproducción:** evitar la duplicación de un agente durante una comunicación.

Es importante resaltar que los agentes no deben incluir en su viaje ninguna clave criptográfica, sino que ha de utilizarse un algoritmo, denominado *autenticador,* en las MASIF que verifique la validez del agente y del sistema origen, las autoridades de los sistemas y agentes involucrados en la comunicación y cuales son las autoridades consideradas como seguras.

Aunque hay una gran variedad de políticas de seguridad que pueden utilizarse para evitar los ataques, un proceso de comprobación típico antes de iniciarse el viaje de un agente incluye los siguientes aspectos:

- El sistema debe verificar la autoridad propietaria del agente.
- Durante la creación de la petición, el propietario define las preferencias de seguridad para el agente.
- Al crearse la instancia del agente, se incluye información sobre su autoridad y la de su sistema.
- El sistema origen codifica la información.
- Los sistemas origen y destino crean un canal de comunicación seguro.

- El sistema destino decodifica la información y realiza las comprobaciones necesarias.

Por último recordar que, al contrario de un objeto normal, un agente tiene la potestad de restringir o permitir a otros agentes el acceso a sus métodos, a sus datos o a los recursos que controla, según su comportamiento o sus objetivos.

Otros posibles mecanismos de seguridad que pueden implementarse son:

- La utilización de un lenguaje de agentes "seguro" que no permita que otros tengan acceso a los datos "privados", tal como Java o el uso de espacios de direcciones aislados.
- Autenticación de los agentes, por ejemplo utilizando firmas digitales o técnicas de criptografía.
- El manejo de "cuentas" para el acceso a los recursos de la máquina.
- El uso de mecanismos de control de recursos tales como restricciones en tiempo de ejecución.
- Autenticación del origen del agente.
- Control de acceso/itinerario.
- Autenticación mutua entre los sistemas de agentes.

2.14 Retos a Superar

Dentro de los retos inmediatos que deben superar los Agentes Móviles se encuentran aspectos como los relacionados con el *transporte* de los mismos en un formato apropiado a través de las redes, y el *rendimiento* de estos en redes WAN donde se encuentran miles o millones de Agentes, siendo necesaria una mayor capacidad de control y procesamiento. Igualmente se hace indispensable establecer criterios de *tarificación* para la utilización de esta tecnología y estandarizar los servicios de i*nteroperabilidad-comunicación* en sistemas de arquitecturas diferentes y lenguajes de programación disímiles, de tal forma que las incompatibilidades sean reducidas al mínimo.

Finalmente en el campo de la seguridad se debe garantizar la protección a la privacidad de la información que estos transportan, la autenticidad de la misma y del

agente en sí, y finalmente el riesgo inminente que estos presentan en cuanto a la posibilidad de transportar virus ocultos que puedan ocasionar pérdida o daño en quien los recibe.

Los cuestionamientos planteados anteriormente muestran el gran camino que falta por recorrer en el desarrollo de Agentes Móviles. Esta es un área reciente que permite explorar y seguir una gran variedad de líneas de desarrollos en torno a ella.

3. PROCESOS AAA EN AMBIENTES 3G

3.1 Introducción

Dentro de la prestación de servicios hay diversos procesos que se deben llevar a cabo para que el usuario final reciba lo que requiere, en el momento en que lo desea y de manera apropiada, es así como por ejemplo se hace necesario verificar que quien solicita el servicio es quien realmente tiene derecho a utilizarlo, autorizarlo para utilizar dicho servicio y finalmente cobrar la tarifa apropiada por la prestación del mismo, todo esto lo más eficientemente posible y de forma transparente para el usuario.

Los clientes actualmente obtienen servicios de Internet negociando un punto de conexión a un "dominio local", generalmente a través de un ISP, u otra organización desde la cual son establecidos y satisfechos los requerimientos del servicio. Con el incremento en la popularidad de los dispositivos móviles, se ha generado la necesidad de permitir a los usuarios conectarse a cualquier dominio conveniente para su localización actual. De este modo, un cliente necesita acceso a recursos que son proveídos por un dominio administrativo (llamado "dominio foráneo") diferente a su propio dominio. La necesidad de servicios de un "dominio foráneo" requiere, en muchos modelos, Autorización, la cual conduce directamente a la Autenticación, y por supuesto a la Tarificación (procesos AAA).

Esta sección especifica los requerimientos para los procesos AAA en los sistemas inalámbricos de tercera generación (3G) los cuales soportan roaming sobre proveedores de servicio tradicionales y servicios IP Móviles. Esta arquitectura está diseñada para ser usada con una red celular como medio de acceso.

3.2 Definición de Procesos AAA

De acuerdo a la Fuerza de Tareas de Ingeniería de Internet (IETF: Internet Engieneering Task Force) los procesos de Autorización, Autenticación y Tarificación (AAA: Authorization, Authentication, Accounting) están definidos de la siguiente manera:

- **Autorización.** Proceso mediante el cual se determina si se posee un derecho específico. Por ejemplo, determinar si el acceso a algún recurso puede concederse al poseedor de una credencial particular.

- **Autenticación.** Proceso mediante el cual se verifica una identidad exigida, en la forma de una etiqueta pre-existente a partir de un campo “nombre”, el cual es mutuamente conocido. Por ejemplo, verificar el creador de un mensaje (autenticación de un mensaje) ó verificar el punto final de un canal de comunicación (autenticación de entidad).

- **Tarificación.** Proceso consistente en recolectar información sobre la utilización de un determinado recurso con el propósito de analizar tendencias, realizar auditorias, facturar, o asignar el costo por la utilización del servicio.

En lo referente a la prestación de los procesos AAA hay un concepto fundamental en cuanto a la relación entre los diferentes elementos involucrados y es el de *Asociación de Seguridad* (SA: Security Association). Una asociación de seguridad es un conjunto de información de seguridad relacionada con una conexión; entre esta información se encuentran, el Indice de Parámetros de Seguridad (SPI: Security Parameters Index), el cual especifica los algoritmos de autenticación y criptografía, las claves para dichos algoritmos y el tiempo de vida de las mismas, los vectores de inicialización y la dirección de origen de la asociación.

3.3 Arquitectura de Alto Nivel

La arquitectura de alto nivel está compuesta por siete entidades principales, estas entidades son:

- *Los Agentes Locales (HA: Home Agent)*
- *Los Agentes Foráneos (FA: Foreign Agent)*
- *Nodo Servidor de Paquetes de Datos (PDSN: Packet Data Serving Node)*
- *Los servidores AAA*
- *La Red Radio (RN: Radio Network)*
- *Los Registros de Localización Local y Visitante (HLR: Home Location Register/VLR: Visited Location Register)*
- *Los Nodos Móviles (MN: Mobile Node)*

En la figura 3.1 se pueden observar las diferentes entidades que componen la arquitectura de alto nivel y sus relaciones.

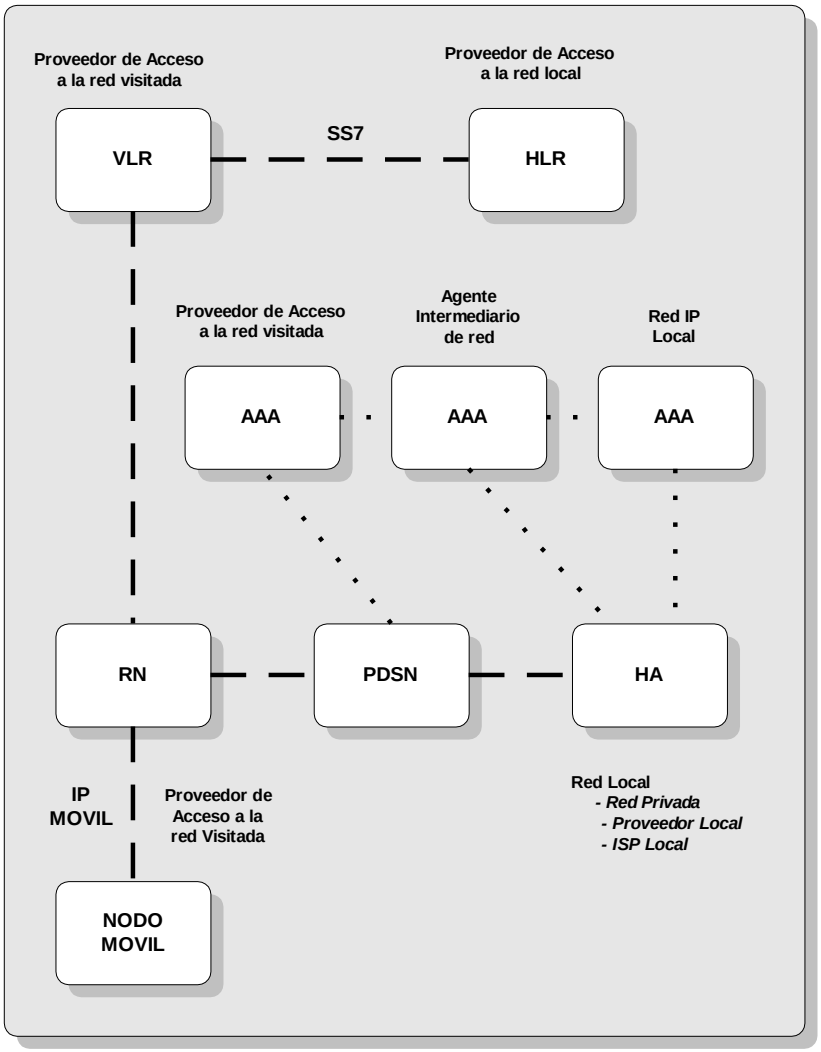


Figura 3.1 Arquitectura general AAA

A continuación se verán las diferentes funciones de los componentes de esta arquitectura.

3.3.1 PDSN

El Nodo Servidor de Paquetes de Datos establece, mantiene y termina el enlace con el cliente móvil, de la misma forma se encarga de iniciar la autenticación, autorización y tarificación para dicho cliente. Opcionalmente, asegura el enlace utilizando seguridad IP para el Agente local.

Otras de las funciones de este nodo es recepcionar los parámetros de servicio AAA para el cliente móvil, al igual que colectar los datos de uso para la tarificación; en caso de Tuneling debe enrutar los paquetes al HA o a redes de datos externas.

3.3.2 Servidor de Autorización, Autenticación y Tarificación

Esta entidad se encarga de interactuar con el Agente foráneo y otros servidores AAA para autorizar, autenticar y realizar la tarificación al cliente móvil, de igual forma provee mecanismos para soportar asociaciones de seguridad entre PDSN/FA y HA, y entre el MN y PDSN/FA.

El servidor AAA también puede realizar asignación dinámica de Agentes locales, identificando dinámicamente un HA y asignando un MN en dicho HA; de la misma forma proporciona la asociación de seguridad entre el MN y HA. Otras funciones que puede realizar estos servidores son:

- Provee información de Calidad de Servicio (QoS: Quality of Service) al PDSN.
- Opcionalmente puede asignar direcciones locales de forma dinámica.

3.3.3 La Red Radio

Es el encargado de validar la estación móvil para acceder al servicio y gestionar la conexión del Nodo Móvil con la capa física. Una vez hecho esto, mapea la referencia del identificador del Nodo Móvil a un único identificador de capa de enlace utilizado para comunicarse con el PDSN y mantiene el estado de accesibilidad para servicio de paquetes entre la red de acceso radio y la estación móvil.

Igualmente cumple funciones de almacenamiento de los paquetes provenientes del PDSN cuando los recursos radio no están disponibles o son insuficientes para soportar el flujo desde el PDSN. Adicionalmente transmite los paquetes entre la estación móvil y el PDSN.

3.3.4 Registros de localización (VLR/HLR)

La función principal de los registros de localización es almacenar la información de autenticación y autorización para la red radio.

3.3.5 Agente Local (HA)

El Agente Local almacena el registro de usuario y redirecciona los paquetes al PDSN, de ser necesario soporta asignación dinámica y Tuneling inverso. Opcionalmente, establece un túnel IP seguro con PDSN/FA y puede asignar direcciones locales de forma dinámica.

3.3.6 Nodo Móvil (MN)

Puede actuar como un Nodo IP Móvil y soportar Agentes foráneos de tipo Challenge y de Identificador de Acceso de Red (NAI: Network Access Identifier), de igual forma debe interactuar con la red radio para obtener los recursos apropiados para el intercambio de paquetes.

Cumple funciones de almacenamiento de información sobre el estado de los recursos radio (por ejemplo: activo, en estado de espera, inactivo); además sirve de buffer para los paquetes cuando los recursos radio no están disponibles o son insuficientes para soportar el flujo de la red.

3.4 Requerimientos AAA primordiales

A continuación se presenta un resumen de los requerimientos específicos AAA en los Sistemas 3G. En dichos requerimientos, la red proveedora de servicios y la red local pueden o no tener una relación comercial directa; en caso de que no exista una relación comercial directa, el servicio puede ser soportado indirectamente a través de Agentes

intermediarios. Estos requerimientos están relacionados específicamente con aspectos críticos de los procesos AAA, tales como la Autenticación y Autorización, los mecanismos de transporte y la Tarificación, entre otros.

Los requerimientos relacionados con el Transporte hacen referencia a la necesidad de proveer un mecanismo fiable de transporte capaz de indicar a una aplicación AAA que un mensaje se entregó a la próxima aplicación o que ocurrió un exceso en el tiempo de procesamiento, así como de controlar la retransmisión y no delegar esta labor a las capas bajas de los protocolos como ocurre con TCP. Las características del mecanismo de transporte deberán tener la capacidad para detectar fallos ocultos del receptor AAA o del enlace hacia dicho receptor, para manejar dichas fallas en una base proactiva.

Aún si el mensaje AAA es almacenado para enviarse posteriormente, las opciones del mensaje o su semántica no son acordes al protocolo AAA, el mecanismo de transporte reconocerá el mensaje AAA como recibido, sin embargo, si el mensaje no pasa el proceso de autenticación, no será reconocido. Igualmente, se deben transportar certificados digitales en mensajes AAA, tratando de minimizar el número de ciclos asociados con las transacciones AAA.

Se debe proveer retransmisión de protección y capacidad opcional de no rechazo para todos los mensajes de Autorización y Tarificación, el protocolo AAA debe proveer la capacidad de hacer coincidir los mensajes de tarificación con los mensajes previos de Autorización y transportar los atributos de los datos inalámbricos de la red local a la red de servicios en la forma de un perfil de usuario.

En lo referente a la Tarificación se debe soportar Tarificación a través de acuerdos bilaterales y servidores intermediarios AAA que proporcionen compensación de tarificación y acuerdos entre redes locales y prestadoras de servicios. Existe un acuerdo explícito donde se especifica que si la red privada o el ISP local autentican la estación móvil que solicita el servicio, entonces la red privada o el ISP local también están de acuerdo en reconocer la tarifa por parte del proveedor de servicio local o intermediario. La tarificación en tiempo real debe estar igualmente soportada.

Es necesario también proveer integridad del mensaje y autenticación de identidad en un enlace (nodo AAA) básico, así como seguridad entre los servidores AAA, y entre el servidor AAA y el PDSN o HA vía Seguridad IP.

Los requerimientos de interconexión indican que se deben soportar intermediarios tipo proxy y no-proxy, donde un intermediario tipo no-proxy implica que una vez el intermediario termina por completo con una demanda, inicia una nueva demanda. Los intermediarios AAA deben tener la capacidad para modificar ciertas partes de los mensajes AAA dependiendo del tipo de intermediario a utilizar.

3.5 Requerimientos específicos IP Móvil y AAA

El protocolo IP Móvil se utiliza para manejar movilidad de un host IP por subredes IP. A raíz de la creciente popularidad de los sistemas IP Móviles se ha definido la interacción entre estos y los procesos AAA buscando proporcionar:

- Escalabilidad mejorada de asociaciones de seguridad
- Movilidad fuera de las fronteras de los dominios administrativos
- La asignación dinámica de Agentes locales

El protocolo IP Móvil, como está definido, trabaja bien cuando todos los nodos móviles pertenecen al mismo dominio administrativo. En esta sección, se desarrolla un modelo multi-dominio para autorización IP Móvil y se presenta en términos de la infraestructura de red definida para este protocolo.

La figura 3.2 muestra el nuevo modelo AAA desarrollado para el protocolo IP Móvil. En este modelo cada red contiene los nodos móviles (MN) y un servidor AAA (AAA). Cada dispositivo móvil comparte una asociación de seguridad (SA) con el servidor AAA dentro de su propia red local. Esto significa que ninguno de los dispositivos móviles comparten inicialmente una asociación de seguridad. Los servidores AAA de dominios administrativos pueden compartir una asociación de seguridad, o pueden tener una asociación de seguridad mediante una agente intermediario.

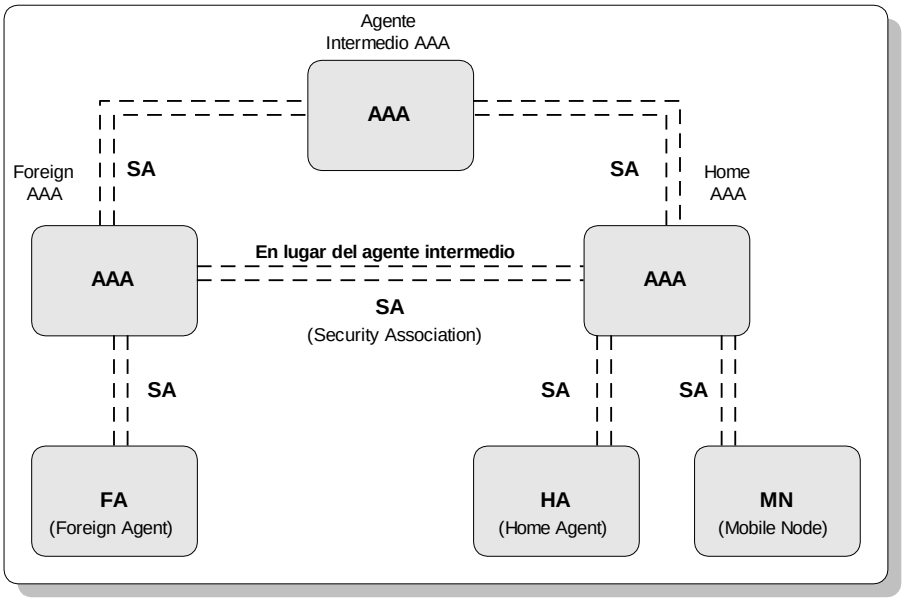


Figura 3.2 Modelo AAA para IP Móvil

La figura 3.3 proporciona un ejemplo de una red IP Móvil que incluye AAA. En la integración IP Móvil/AAA, se asume que cada Agente Móvil comparte una asociación de seguridad entre sí mismo y su servidor AAA local. Además, los servidores AAA locales y foráneos comparten una asociación de seguridad con el servidor AAA del agente intermediario. Por último, se asume que cada Nodo Móvil comparte una relación de confianza con su servidor AAA local.

En este ejemplo, un Nodo Móvil aparece dentro de una red foránea y emite una petición de registro al Agente Foráneo. Puesto que el Agente Foráneo no comparte ninguna asociación de seguridad con el Agente Local, envía una demanda de AAA a su servidor AAA local, el cual incluye la información de autenticación y la demanda de registro del Móvil IP. El Nodo Móvil no puede comunicarse directamente con el servidor AAA local por dos razones:

- No tiene acceso a la red. La petición de registro es enviada por el Nodo Móvil para pedir acceso a la red.
- El Nodo Móvil no puede tener una dirección IP, y puede estar pidiendo que le sea asignada una por su proveedor local.

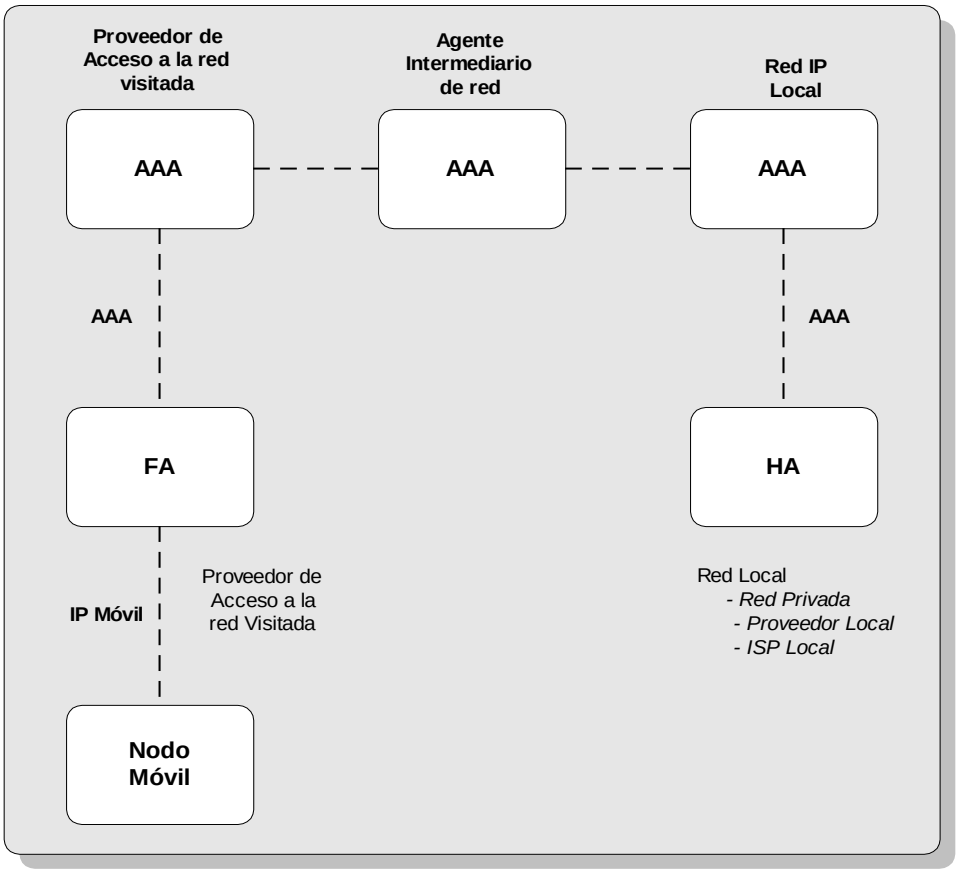


Figura 3.3 Arquitectura IP inalámbrica para AAA en IP Móvil

El Servidor AAA Foráneo determinará si la demanda puede ser satisfecha localmente a través del NAI proporcionado por el Nodo Móvil. El NAI tiene el formato *usuario@dominio* y el Servidor AAA utiliza la porción del dominio del NAI para identificar el Servidor AAA Local del Nodo Móvil. Si el Servidor AAA foráneo no comparte ninguna asociación de seguridad con el servidor local AAA del Nodo Móvil, puede remitir la demanda a su agente intermediario. Si el agente intermediario tiene una relación con la red local, puede gestionar la demanda, en otro caso una respuesta fallida se retorna al Servidor AAA Foráneo. Para llevar a cabo este proceso se hace necesario que en la interacción IP Móvil – AAA se cumplan los requerimientos tratados en las siguientes secciones.

3.5.1 Seguridad IP Móvil

Dentro de los requerimientos de seguridad se definen tres elementos principales:

- Seguridad HA – FA
- Seguridad MN – FA
- Seguridad HA – MN

A diferencia de otros modelos de seguridad como el del Protocolo de Internet (IPSec: IP Security), el modelo de seguridad IP Móvil proporciona sus propios mecanismos de autenticación calculados dentro de sus procedimientos de registro, mientras que IPsec utiliza IPsec AH.

Las llaves e Índices de Parámetros de Seguridad (SPI: Security Parameter Index) asociados con las extensiones MN-FA y HA-FA necesitan que se establezcan dinámicamente en un ambiente de roaming del portador inalámbrico. La extensión MN-FA es útil para permitir un nuevo FA que autentique rápidamente un móvil, utilizando la extensión previa del Agente Foráneo. La extensión HA-FA es útil para el HA, para asegurar que sólo FAs provenientes de portadores con acuerdos de roaming accedan al HA. La MN-HA es usualmente provisional, pero para la asignación dinámica de Agentes Locales, esta Asociación de Seguridad debe crearse dinámicamente.

3.5.2 Asignación dinámica de Agentes Locales

Un Servidor AAA Local o visitado opcionalmente puede ser capaz de realizar asignación dinámica de HA. Para la asignación dinámica de HA, el Servidor AAA visitado debe preguntar al servidor AAA local si soporta la asignación dinámica de HA en aquellos casos en que el nodo móvil requiera dicho tipo de asignación. En caso de soportarla, el Servidor Local AAA puede permitir al Servidor AAA visitado realizar la asignación de HA, de otra forma, el Servidor Local AAA asigna el HA.

3.5.3 Handoff rápido

Para lograr un handoff más rápido, el móvil puede intentar evitar una transacción AAA con el Servidor AAA local. Para lograr esto, el móvil puede enviarle al PDSN la dirección del FA previo, junto con la extensión de autenticación MN-FA. El PDSN entrega la dirección del FA previo y la extensión de autenticación de MN-FA al Servidor AAA visitado. Si el Servidor AAA visitado es capaz de autenticar la extensión de autenticación del MN-FA ara

el móvil, entonces el Servidor AAA visitado puede evitar una transacción con el Servidor AAA Local.

3.5.4 Autenticación HA-FA

Para lograr un registro rápido en el caso de una estación móvil con un Agente local, el PDSN y el HA pueden recibir de los mecanismos de AAA una llave HA-FA y SPI la cual es utilizada para que el PDSN y el HA puedan autenticarse el uno al otro.

3.5.5 Distribución de llaves

Estas funciones son principalmente útiles en ambientes inalámbricos donde los handoffs deben ocurrir rápidamente (lo que implica la necesidad de latencias bajas), o donde los dispositivos móviles tienen un limitado poder de procesamiento. Para llevar a cabo estas funciones el protocolo AAA será utilizado para pasar llaves y SPIs de forma segura entre la red de servicios y la red deseada de forma encriptada. Estas llaves son utilizadas entonces para las funciones específicas mencionadas a lo largo de este capítulo.

3.5.6 Interoperabilidad con Radio

Los usuarios con un Servidor AAA Local basado en Radio pueden tener en determinado momento la necesidad de estar en una red inalámbrica que utiliza los "nuevos" servidores AAA basados en la arquitectura presentada anteriormente, y viceversa. El protocolo AAA debe estar diseñado en cierto modo para hacer las conversiones para y de mensajes Radio directamente. Esto requerirá el desarrollo de procesos *gateway* para permitir dicha interoperabilidad.

> *Nota*: Las características de los nuevos protocolos AAA que están más allá del conjunto de características del protocolo Radio puede no estar disponibles para los usuarios sobre redes locales o de servicio basadas en radio.

3.6 Proceso de Autenticación

3.6.1 Introducción

Dadas las características de los Sistemas Móviles de Tercera Generación, el dominio local requiere la habilidad de interrogar a un usuario para proveer información de autenticación en cualquier momento durante una sesión, y así poder decidir si la sesión puede continuar o debe ser finalizada según el resultado de dicha autenticación. Adicionalmente, el dominio visitado también debe poder interrogar a un usuario para que proporcione la información de autenticación en cualquier momento de una sesión, así se permite que el dominio visitado tenga mayor control sobre el roaming. De la misma forma, el Nodo Móvil también debe poder autenticar la red cuando quiera. En esta sección se especificarán las extensiones de los mensajes IP Móvil para habilitar al dominio local y al dominio visitado en cualquier momento durante una sesión para pedir a un Nodo Móvil que proporcione las credenciales de autenticación. De igual forma también se definen las extensiones para habilitar al Nodo Móvil para realizar la autenticación de la red en cualquier momento de una sesión.

Este procedimiento de autenticación se hace necesario para limitar los fraudes, por ejemplo para evitar que un Nodo Móvil fraudulento suplante un Nodo Móvil legítimo y acceda a los recursos del dominio visitado. Las posibilidades de una red para iniciar el proceso de autenticación de un usuario incluyen por ejemplo, un temporizador periódico de tiempo de registro en el sistema, la presencia del Nodo Móvil en un área de alto riesgo de fraude, un Nodo Móvil “marcado” como posible fraudulento por el dominio local, o una demanda de autorización del Nodo Móvil para asegurar recursos que causen que la red requiera la re-autenticación del usuario, entre otros.

Los mecanismos de Autenticación basados en solicitud-respuesta proporcionan fuertes entidades de autenticación, así la red debe ser capaz en cualquier momento de desafiar al Nodo Móvil enviando una mensaje de requerimiento de Autenticación el cual lleva un número al azar (el challenge) y requiere que el Nodo Móvil lo autentique.

A diferencia de los mecanismos de desafío-respuesta actuales dónde el challenge utilizado para la autenticación es generado por los dominios visitados y transmitido en mensajes de aviso de enrutador, el mecanismo propuesto en este documento es de

usuario específico. De hecho, el challenge generado por la red se dirige a un MN particular (en lugar de a todos los MNs capaces de recibir la información transmitida, como está definido actualmente). Ya que el número aleatorio para el challenge se cambia para cada operación, los mecanismos de autenticación propuestos proveen una autenticación del usuario mucho más segura. Si el primer procedimiento de autenticación tuvo éxito o falló, el challenge de autenticación del usuario específico puede servir como un chequeo doble sobre la autenticidad del MN. De la misma forma, el Nodo Móvil debe poder también autenticar la red generando un challenge en cualquier momento durante una sesión y enviándolo a la red.

3.6.2 Requerimientos de Autenticación IP Móvil

La opción de requerimiento de Autenticación de destino se utiliza para requerir a un Nodo Móvil o a la red su Autenticación. Como una opción de destino, el requerimiento de Autenticación puede enviarse en un paquete solo o puede ser incluido en cualquier paquete existente a enviarse al Nodo Móvil cuando sea inicializado por la red o por el Nodo Móvil. Un paquete que contiene una opción de requerimiento de Autenticación es enviado de la misma forma en que se envía cualquier paquete al punto del extremo receptor. Cuando un Nodo Móvil o la red reciben un paquete que contiene una opción de requerimiento de autenticación, debe devolver una respuesta de Autenticación a la fuente del requerimiento de Autenticación. La opción de requerimiento de Autenticación se codifica en el siguiente formato:

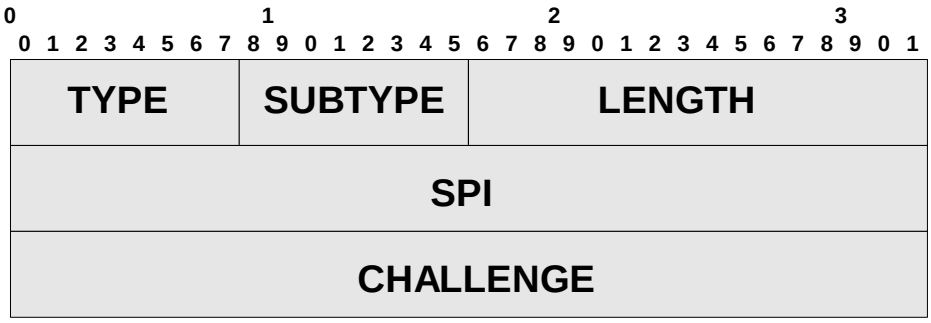


Figura 3.4 Formato de requerimiento de Autenticación

Type: Tipo de datos.

Subtype: Número asignado para identificar la forma en que el *Challenge* será utilizado.

Lenght: (Longitud) 4 más el número de bytes en el campo *subtype*; debe ser por lo menos 20.

SPI: Indice de Parámetro de Seguridad.

Challenge: Challenge a ser utilizado para procesar los datos de Autenticación.

3.6.3 Extensión IP Móvil para la respuesta de Autenticación

La opción de respuesta de Autenticación de destino se envía en respuesta a un requerimiento de Autenticación enviado por el Nodo Móvil o la red, a la red o al Nodo Móvil respectivamente, en cuanto se proporcionen los datos de autenticación.

La opción de repuesta de Autenticación de destino puede enviarse en un paquete, o puede ser incluido en cualquier paquete existente a enviarse al Nodo Móvil por la red o por el Nodo Móvil a la red. Un paquete que contiene una opción de repuesta de Autenticación se envía de la misma forma en que se envía cualquier paquete al extremo receptor.

La opción de respuesta de Autenticación es codificada en el siguiente formato:

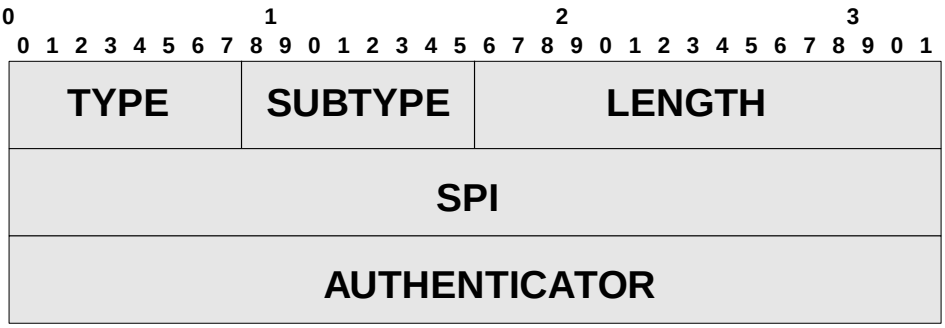


Figura 3.5 Formato de respuesta de Autenticación

Type: Tipo de datos.

Subtype: Un número asignado para identificar la forma en que el *challenge* va a ser utilizado.

Length: 4 más el número de bytes en el campo *Subtype*; debe ser por lo menos 20.

SPI: Indice de Parámetros de Seguridad.

Authenticator: Campo *Autenticador* de longitud variable.

3.6.4 Esquema requerimiento-respuesta

Es posible que las redes locales/visitadas o el MN envíen un requerimiento de autenticación al MN o a las redes Local/Visitada respectivamente, y, después de unos segundos, envíen otro requerimiento de autenticación con un challenge diferente codificado en él. De la misma forma se puede dar que el receptor final nunca reciba la primera demanda de autenticación (por ejemplo un mensaje se perdió en el acceso al enlace) y recibe solo la segunda demanda de autenticación. En esta situación, cuando una respuesta de autenticación se envía de vuelta a la red Local/Visitada o al MN (es decir a la entidad que inició el procedimiento de autenticación), la red Local/Visitada o el MN necesitan saber a qué demanda de autenticación corresponde la respuesta, es decir, que demanda de autenticación fue la que finalmente se recibió, para realizar la correcta validación de los datos de autenticación recibidos.

En esta situación se tienen dos posibles opciones:

- La entidad que recibe la demanda de autenticación incluye el challenge recibido en el mensaje de respuesta de autenticación.
- La entidad que comienza el procedimiento de autenticación incluye un identificador de Challenge (Challenge_Identifier) en la extensión de demanda de autenticación y la entidad que recibe dicha demanda de autenticación incluye dicho identificador en la respuesta de autenticación.

3.6.5 Esquema Básico Requerimiento-Respuesta

Dentro de la primera opción propuesta, la entidad que recibe la demanda de autenticación incluye el challenge recibido en la demanda de autenticación en el mensaje de respuesta de autenticación. De forma consistente con el esquema Requerimiento-Respuesta, la opción de destino adicional que contiene el challenge utilizado para la autenticación es adicionada al contenido del mensaje de respuesta de autenticación y tiene el formato siguiente.

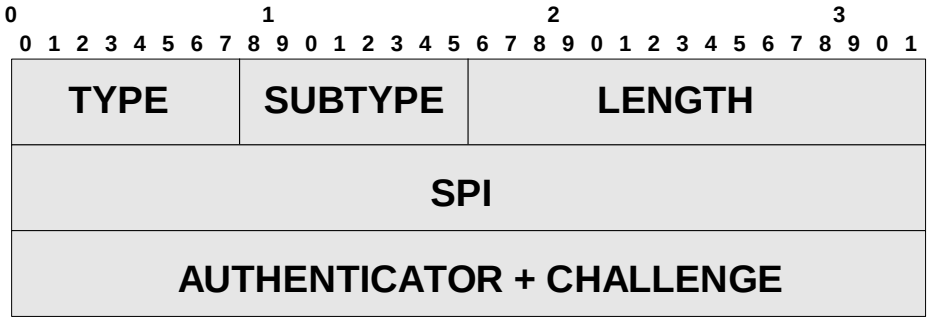


Figura 3.6 Formato de mensaje de respuesta. Esquema básico requerimiento-respuesta

3.6.6 Esquema optimizado Requerimiento-Respuesta

Pueden darse algunos casos dónde exista la necesidad de optimizar la información utilizada para la autenticación sobre el enlace de acceso, por ejemplo enlaces inalámbricos dónde los recursos radio están limitados. En dichos casos, incluso el Challenge en la respuesta de autenticación puede hacer que el encabezado sea demasiado grande. Una solución para esta situación es que la entidad que inicia el procedimiento de autenticación incluya un Challenge_Identifier en la extensión de requerimiento de Autenticación, por ejemplo en la forma de un *timestamp* o de un contador, y la entidad que recibe la demanda de autenticación incluya este Challenge_Identifier en la respuesta de autenticación para que la entidad autenticadora pueda saber a que Challenge corresponde dicha respuesta.

3.7 Proceso de Autorización

Una vez el Servidor AAA recibe la solicitud de AAA, autentica al usuario y empieza la fase de autorización. La fase de autorización incluye la generación de:

- Una sesión dinámica de llaves para ser distribuidas entre todos los Agentes Móviles.
- La asignación Dinámica optativa de un Agente local.
- La asignación Dinámica optativa de una dirección local (nótese que esto puede ser hecho por el Agente local).
- Asignación optativa de parámetros de QoS para el Nodo Móvil.

Una vez la autorización está completa, el Servidor AAA local emite un requerimiento AAA no solicitado al Agente local, que incluye la información sobre el requerimiento AAA original, así como la información de autorización generada por el servidor AAA local. El Agente local recupera el requerimiento de registro a partir del mensaje AAA enviado y sus procesos, entonces genera una respuesta sobre el proceso de registro que es enviada de vuelta al Servidor AAA en forma de una respuesta AAA. El mensaje se remite a través del Agente intermediario al Servidor AAA foráneo, y finalmente al Agente foráneo.

Los servidores AAA mantienen la información del estado de la sesión basados en la información de autorización. Si un Nodo Móvil se mueve a otro Agente foráneo dentro del dominio foráneo, una demanda al servidor AAA foráneo puede hacerse inmediatamente para retornar en ese momento las llaves que fueron emitidas para el Agente Foráneo anterior. Esto evita un proceso completo adicional a través de la red, y habilita el handoff.

3.7.1 Infraestructura de Red

IP Móvil utiliza un modelo de roaming estructurado de la siguiente manera (figura 3.7):

- El Nodo Móvil es el usuario
- La red foránea es el Proveedor de Servicio con el Agente Foráneo como el Equipo de Servicio.
- La red local es la organización local del usuario. Nótese que en la organización local de usuario no sólo opera un servidor AAA, sino que también opera el Agente local. De igual forma se ve que también, un agente intermediario se ha insertado entre el Proveedor de Servicio y la Organización local del usuario.

3.7.2 Latencias a través de la Red

Aunque habría sido posible que las interacciones AAA fuesen desarrolladas para la autenticación básica y la autorización, y enviar flujo de registro directamente al Agente Local desde el Agente Foráneo, uno de los requerimientos claves de IP Móvil es que se minimicen los viajes a través de la red. Incluso los requerimientos de registro y las respuestas en los mensajes AAA requieren un solo viaje para autenticar al usuario, realizar la autorización y procesar la demanda de registro.

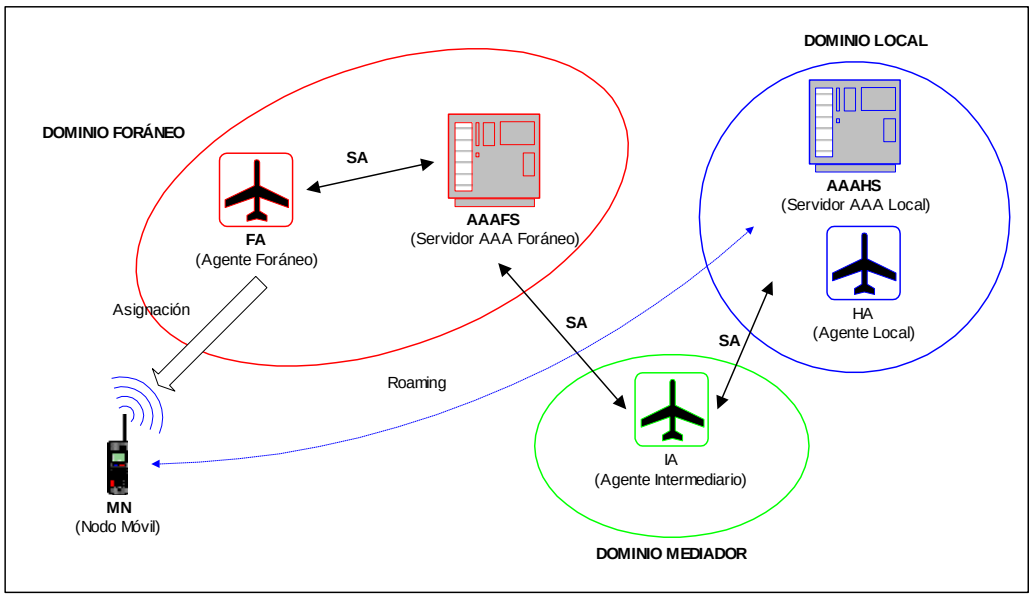


Figura 3.7 Arquitectura de red para IP Móvil

Esto se debe básicamente a la necesidad de minimizar la latencia de los dispositivos móviles que deseen acceder a la red. Los procesos de registro nuevos no deben aumentar el tiempo de conexión más allá del que proveen las redes celulares actuales.

3.7.3 Distribución de Llaves

Para permitir el acceso sobre dominios administrativos, es necesario minimizar las asociaciones de seguridad requeridas ya que de lo contrario esto se convertiría en un proceso engorroso. Esto significa que cada Agente Foráneo no debe compartir una asociación de seguridad con cada Agente local en la red. Los Agentes Móviles comparten una asociación de seguridad con su Servidor AAA local quien a su vez comparte una asociación de seguridad con otros servidores AAA. De nuevo, la utilización de Agentes intermediarios, se define para operaciones de roaming, esto permite escalar los servicios, logrando que el número de relaciones establecidas por los proveedores se reduzca.

Después de que un Nodo Móvil es autenticado, la fase de autorización incluye la generación de las llaves de sesión. Específicamente, tres llaves se generan:

- ***k1:*** Llave que se comparte entre el Nodo Móvil y el Agente Local
- ***k2:*** Llave compartida entre el Nodo Móvil y el Agente Foráneo

- ***k3:*** Llave compartida entre el Agente Foráneo y el Agente Local

Cada Llave es difundida a cada uno de los dispositivos móviles a través del protocolo AAA (para el Agente Foráneo y el Agente Local) y vía IP Móvil para el Nodo Móvil (siempre que el Nodo Móvil no se encuentre conectado directamente con los Servidores AAA).

La figura 3.8 muestra las nuevas asociaciones de seguridad utilizadas para mantener la integridad de los mensajes IP Móvil basados en las llaves generadas por el servidor AAA.

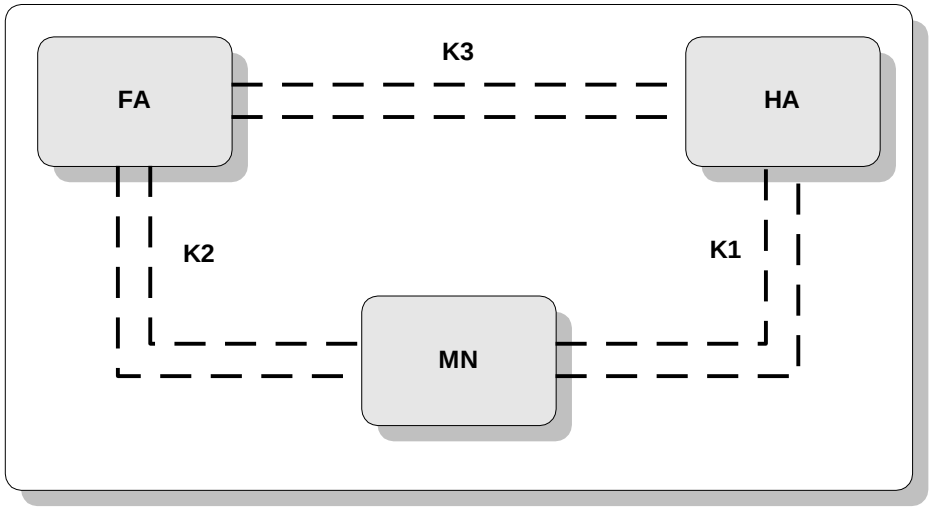


Figura 3.8 Asociaciones de seguridad después de la distribución de llaves

Una vez las llaves de sesión se han establecido y se han difundido, los dispositivos móviles pueden intercambiar la información de registro directamente sin necesidad de la infraestructura AAA. Sin embargo las llaves de sesión tienen cierto tiempo de vida, después del cual debe utilizarse la infraestructura AAA para adquirir nuevas llaves de sesión.

3.7.4 Requerimientos de Autorización para IP Móvil

IP Móvil requiere un protocolo AAA que utilice el modelo completo, de igual forma se requiere el apoyo del agente intermediario, y los objetos de datos deben incluir la integridad de los datos y la confidencialidad *extremo a extremo*. Esto significa que ni el Agente Intermediario ni cualquier otro nodo AAA intermedio debe ser capaz de descifrar los datos, pero deben poder verificar la validez de dichos objetos.

La autorización incluye la dirección del recurso. Esto permite al Servidor AAA mantener una instantánea de la localización actual de un Nodo Móvil, la información de codificación, entre otros. Debido a la naturaleza del servicio a ofrecerse, es indispensable que la transacción AAA agregue la latencia mínima al tiempo de conexión. Idealmente, el protocolo AAA debe permitir un solo ciclo para la autenticación y la autorización.

En cuanto al protocolo AAA a utilizarse, si éste permite mensajes de registro para el Móvil IP empotrados dentro de la solicitud de la autenticacion/autorizacion, esto reducirá el número de procesos requeridos y reducirá el tiempo de conexión, además debe ser posible pasar datos específicos sobre la gestión de llaves junto con los datos de autorización. Esto permite al Servidor AAA actuar como un Centro de Distribución de Llaves (KDC: Key Distribution Center). El protocolo AAA también debe permitir mensajes no solicitados para ser enviados a un "cliente", por ejemplo, el cliente AAA que está corriendo en el Agente Local.

Debe ser posible pasar otras unidades de datos de aplicación específica, como la selección del Agente Local y la asignación de la dirección para ser transportados con las unidades de datos de autorización. La respuesta de la autorización debe permitir diversos perfiles de QoS que puedan utilizarse por los Agentes Móviles que permitan proporcionar cierta QoS al Nodo Móvil.

3.8 Proceso de Tarificación

3.8.1 Introducción

El campo de la tarificación se ocupa de la recolección de datos de utilización de los recursos para propósitos de análisis de capacidad y tendencias, asignación de costos, auditorias, y cargo a cuentas.

Puesto que las aplicaciones de tarificación no tienen una seguridad uniforme y requerimientos de fiabilidad, no es posible diseñar un solo protocolo de tarificación y un conjunto de servicios de seguridad que cubran todas las necesidades. De esta forma, la finalidad de la gestión de tarificación es proporcionar un conjunto de herramientas que puedan utilizarse para reunir los requisitos de cada aplicación.

A continuación se describen algunos términos relacionados con el tema y que por su relevancia en el desarrollo de la sección es necesario especificarlos.

Auditoria. Es el acto de verificar la exactitud de un procedimiento. Para poder dirigir una auditoria es necesario ser capaz de determinar de forma definitiva qué procedimientos fueron llevados a cabo para poder comparar estos con el proceso recomendado. Para lograr esto pueden requerirse servicios de seguridad como la autenticación y la protección de la integridad.

Facturar. Acto de preparar una factura.

Facturación sensible. Un proceso de facturación que depende de la información de uso para preparar una factura puede decirse que es sensible. En contraste, un proceso que es independiente de la información de uso se dice que es no sensible.

Protocolo de tarifación. Protocolo encargado de transportar los datos para propósitos de tarificación.

Registro de sesión. Un registro de sesión representa un resumen del consumo del recurso por parte de un usuario sobre una sesión completa. Las entiades de tarificación que crean el registro de sesión lo pueden hacer procesando eventos de tarifación temporales o eventos de tarifación de varios dispositivos que sirven al mismo usuario.

Servidor de tarificación. El servidor de tarificación recibe los datos de tarificación de los dispositivos y los traduce en archivos de sesión. El servidor de tarificación también puede tomar la responsabilidad por la asignación del enrutamiento de los registros de sesión a las partes interesadas.

Tarificación Intra-dominio. La tarificación Intra-dominio involucra la colección de información sobre la utilización de los recursos dentro de un dominio administrativo, con el propósito de ser utilizada dentro de ese dominio. En la tarificación intra-dominio los paquetes de contabilidad y archivos de sesión generalmente no cruzan los límites administrativos.

Tarificación Inter-dominio. La tarificación Inter-dominio involucra la colección de información sobre la utilización de los recursos dentro de un dominio administrativo, con el fin de ser utilizada dentro de otro dominio administrativo. En la tarificación Inter-dominio, los paquetes de contabilidad y archivos de sesión generalmente traspasan las fronteras del dominio.

Tarificación en tiempo real. La tarificación en tiempo real involucra el procesamiento de información en la utilización del recurso dentro de una ventana de tiempo determinada. Las limitaciones de tiempo se imponen generalmente para limitar los riesgos financieros.

Tasar. Es el acto de determinar el precio a ser cobrado por la utilización de un recurso.

3.8.2 Arquitectura de tarificación

La arquitectura de tarificación involucra las interacciones entre los dispositivos de la red, los servidores de tarificación y los servidores de facturación. El dispositivo de red colecciona los datos de consumo de recursos en forma de medidas de tarificación. Esta información se transfiere entonces a un servidor de tarificación. Generalmente esta operación se realiza a través de un protocolo de tarificación, aunque también es posible que los dispositivos generen sus propios archivos de sesión.

El servidor de tarificación entonces procesa los datos de tarificación recibidos del dispositivo de red. Este proceso puede incluir la adición de información de tarificación provisional, eliminación de datos dobles, o generación de archivos de sesión. Los datos de tarificación procesados se envían entonces a un servidor de facturación, quien manejará la evaluación y generación de la factura, pero también puede llevar a cabo labores de auditoria, asignación de costos, análisis de tendencias o capacidad. Los archivos de sesión pueden ser organizados por lotes y comprimidos por el servidor de tarificación previo al envío al servidor de facturación, buscando de esta forma reducir el volumen de datos de tarificación y el ancho de banda requerido para su transmisión.

Una de las funciones del servidor de tarificación es distinguir entre eventos de tarificación inter e intra dominio para poder enrutarlos de forma apropiada. Para archivos de sesión que contienen un NAI, la distinción puede hacerse examinando la parte del dominio del NAI. Si la parte del dominio está ausente o corresponde al dominio local, entonces el

registro de la sesión es tratado como un evento de tarificación intra-dominio. De otro modo, es tratado como un evento de tarificación inter-dominio. Los eventos de tarificación intra-dominio son enrutados al servidor de facturación local, mientras que los eventos de tarificación inter-dominio serán enrutados a servidores de tarificación que operan dentro de otros dominios administrativos. Mientras no se requiera lo contrario, es deseable que los formatos de registro de sesión utilizados en tarificación inter e intra-dominio sean los mismos, puesto que de esta forma se eliminan posibles traducciones necesarias. La figura 3.9 muestra la arquitectura de tarificación.

Si se emplea un enrutador tipo proxy, el control de acceso basado en dominios puede ser empleado por este, en lugar de emplearse por los dispositivos. Los dispositivos de red se comunicarán con el proxy enrutador a través de un protocolo de tarificación, el cual puede convertir los paquetes de contabilidad en archivos de sesión, o paquetes de tarificación a ser enrutados a otro dominio. En cualquier caso, la separación de dominio la realiza el proxy clasificando los archivos de sesión o los mensajes de tarificación de acuerdo a su destino.

En el caso en que la tarificación no se delegue al proxy, puede ser difícil verificar que el proxy esté emitiendo los archivos de sesión correctos basado en los mensajes de tarificación que recibe, puesto que los mensajes de tarificación originales generalmente no se envían con los registros de sesión. Por consiguiente donde la confianza es un factor a considerar, el proxy mismo generalmente remite los paquetes de tarificación. Asumiendo que el protocolo de tarificación soporta seguridad en el transporte de los datos, esto permite que los puntos terminales puedan verificar que el proxy no haya modificado los datos en el transporte o haya curioseado el contenido de los paquetes.

3.9 Aplicabilidad a IPv4 Móvil

Las extensiones definidas en este documento son específicas a IPv6 Móvil pero pueden definirse extensiones similares para IPv4 Móvil habilitando a cualquier entidad para solicitar la autenticación en cualquier momento.

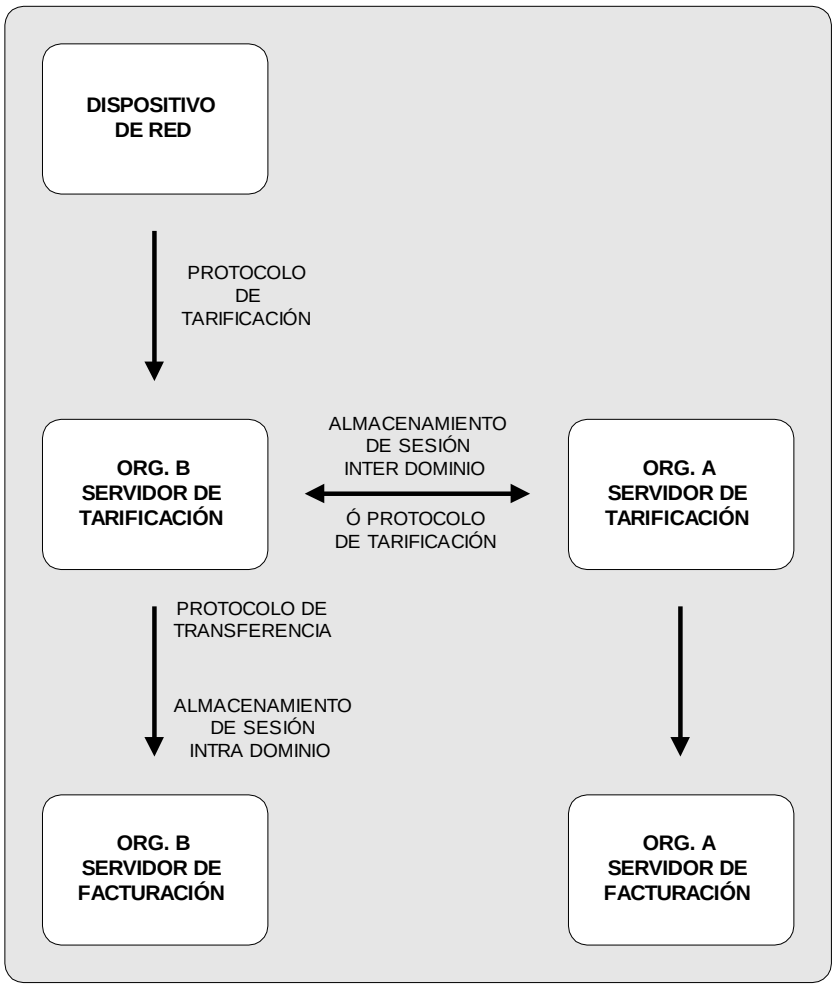


Figura 3.9 Arquitectura de tarificación

3.10 Consideraciones de Seguridad

Este capítulo en su mayoría se ha referido a consideraciones de seguridad. Sin embargo, de acuerdo a lo visto, las consideraciones de seguridad no requieren que la red local y de servicios estén en el mismo dominio ni que tengan una relación directa. La red de servicios requiere la autorización de la red local para poder cobrar por los servicios prestados al móvil, esto implica que la red local debe autenticar los usuarios. Las funciones AAA deben realizarse de una forma segura tal como se especificó en los requerimientos del servicio.

IP Móvil soporta mecanismos de autenticación aparte de IP Security. Estos mecanismos pueden reforzarse en un ambiente inalámbrico celular permitiendo al servidor AAA local distribuir las llaves a la red de servicios. Adicionalmente, el servidor AAA local debe poder enviar una llave pre-compartida para ser utilizada en el establecimiento de asociaciones de seguridad entre el FA y HA. Estas llaves previamente habrán sido enviadas encriptadas por la red local a la red de servicios, mediante criptografía pública y certificados de autenticidad.

4. MODELADO DE AGENTES IP MÓVILES PARA PROCESOS AAA EN AMBIENTES 3G

4.1 Introducción

Como se describió en el capítulo anterior, los procesos de Autenticación, Autorización y Tarificación (AAA) están directamente relacionados unos con otros y en términos generales el sistema basado en Agentes Móviles debe dar soporte a todos ellos para una adecuada prestación del servicio a los clientes y facilitar las labores al lado del proveedor.

Cuando un terminal móvil ingresa a una celda que corresponde a un dominio administrativo diferente al suyo, el primer proceso que se realiza es el de Autenticación del Nodo Móvil, y para el desarrollo de este capítulo se ha escogido este proceso como marco contextual con el fin de especificar (modelar) un par de agentes IP móviles que intervengan en esta tarea, utilizando para tal propósito la metodología del Proceso Unificado de Rational (RUP: Rational Unified Process) y consignando sus resultados más significativos para el proyecto.

4.2 Análisis de Requerimientos del Sistema

4.2.1 Definición y caracterización del sistema objetivo

Se tiene un Nodo Móvil (MN: Mobile Node) pide registro en una red distinta a la propia y solicita provisión de servicio por parte de dicha red. Entre el servidor de este dominio (dominio foráneo) y el servidor del dominio al cual pertenece el móvil (dominio local) no existe ninguna Asociación de Seguridad (SA: Security Association), por lo cual no es posible intercambiar información de AAA directamente.

Se requiere entonces, que sean especificados (modelados) dos agentes IP móviles: el Agente Foráneo (FA: Foreign Agent) y el Agente Intermediario (IA: Intermediary Agent), para que intervengan y hagan posible el proceso de Autenticación del MN por parte del Servidor AAA Foráneo (AAAFS: AAA Foreign Server), considerando que la arquitectura del sistema es de tercera generación (3G). En la Figura 4.1 se ilustra el caso descrito.

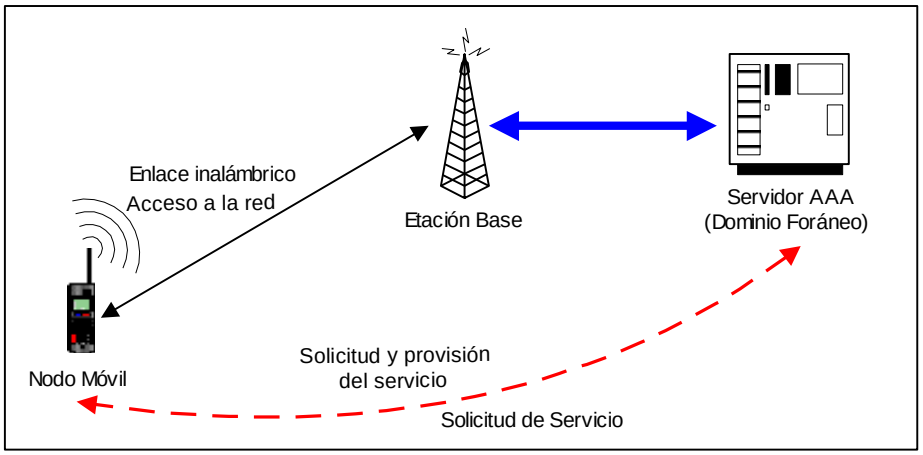


Figura 4.1 Caso de solicitud de registro

- El FA debe hacer posible la comunicación entre el MN y el AAAFS, permitir el registro del MN en dicha red y controlar la provisión del servicio a este móvil por parte del dominio foráneo.
- El IA debe permitir la comunicación entre el Servidor AAA Foráneo y el Servidor AAA Local (AAAHS: AAA Home Server) así como realizar el transporte de información de AAA entre los dos dominios (local y foráneo) para que los servicios sean provistos al MN en cuestión.

Tanto el FA como el IA deben proveer métodos para la asignación de MNs y Servidores AAA (AAAS: AAA Server) respectivamente. De igual forma los MNs y AAASs deben soportar la asignación dinámica de agentes. La Figura 4.2 muestra el diagrama que contiene todas las partes que intervienen en el proceso.

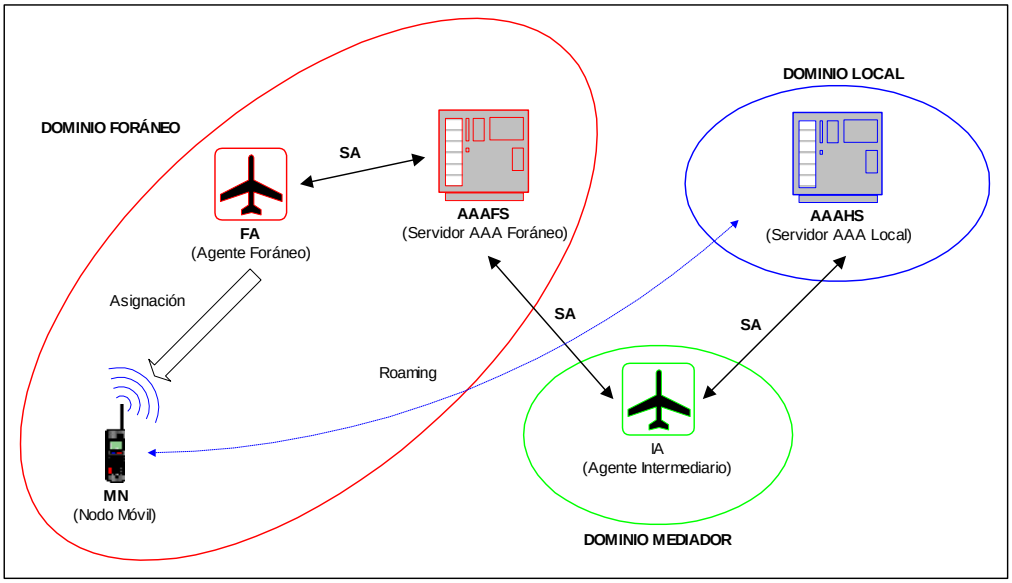


Figura 4.2 Entidades que intervienen en el proceso de Autenticación

4.2.2 Modelo del dominio del Sistema

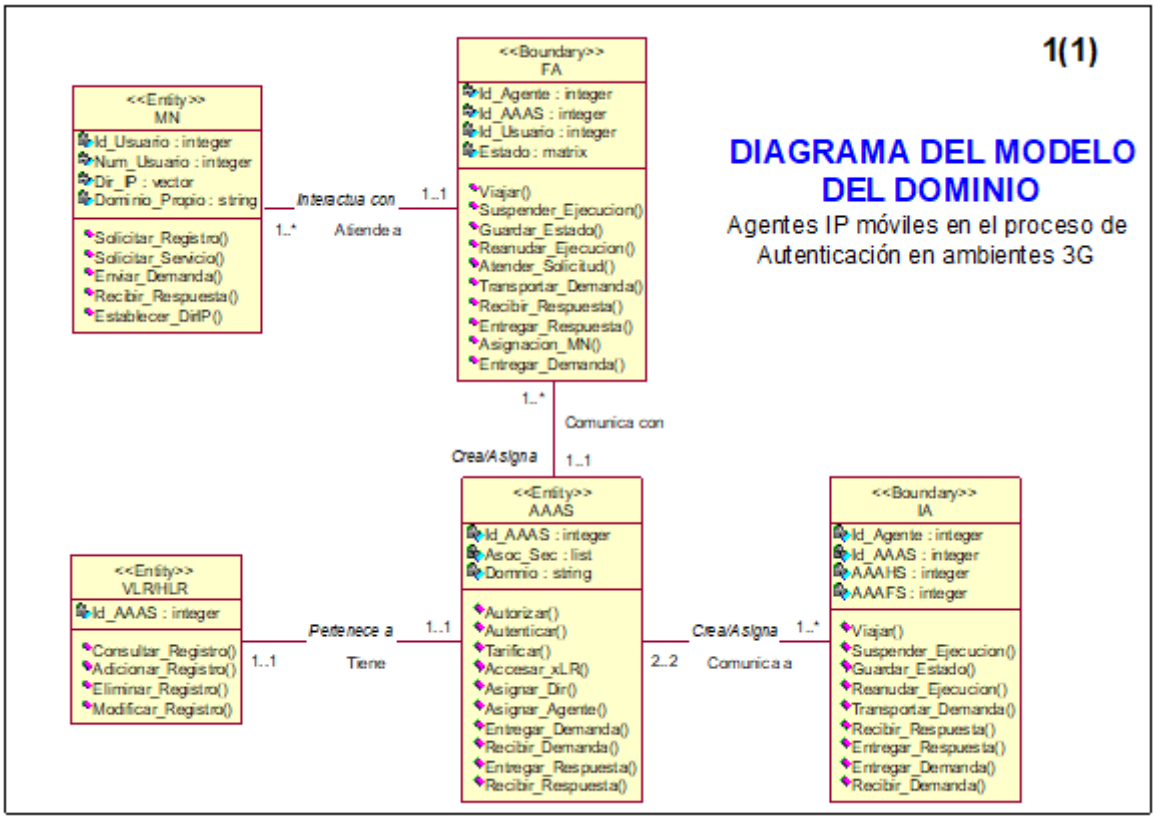


Figura 4.3 Modelo del dominio del sistema

4.2.3 Definición del modelo de desarrollo específico

4.2.3.1 Modelos que describirán el sistema

A partir del RUP se instanció el siguiente modelo de actividades para ser seguido durante el desarrollo del proyecto:

- *Captura de Requerimientos:* Realizar la identificación de los principales elementos que componen el problema a través del Modelo del Dominio, definir los principales términos utilizados en esta definición mediante un glosario, determinar las funciones que debe realizar el sistema en un árbol de funciones e identificar, priorizar y describir los casos de uso de alto nivel.
- *Análisis del software:* Realización del análisis de la arquitectura con el fin de encontrar los elementos del modelo (paquetes, clases, casos de uso ... etc.) que desempeñan actividades importantes dentro del sistema, además se estudiaran por separado cada uno de estos elementos realizando diagramas en los casos en que esto sea necesario, y se elaborarán los diagramas de interacción del sistema y de estados.

- *Diseño del software:* Se diseñarán los subsistemas con sus interfaces, las clases de diseño , descripción de los casos de uso reales y de la arquitectura del sistema, además del modelo de implantación.

4.2.3.2 Fundamentos metodológicos a utilizar

Como modelo para el desarrollo del sistema se seguirá el RUP para el desarrollo de programas, instanciado a nuestro caso particular según se ha descrito en el punto anterior.

4.2.3.3 Modelo del proceso de desarrollo

Este proceso se realizará basándose en el modelo en espiral planteado por el RUP y las fases que se seguirán serán las siguientes:

- C0: Análisis de requerimientos.
- C1: Análisis del software
- C2: Diseño del software

4.2.4 Árbol de funciones

De acuerdo a las entidades identificadas en el Modelo del Dominio, el árbol de funciones del sistema para el proceso de Autenticación es el siguiente:

ITEM	FUNCIÓN
1. Funciones del Servidor AAA:	
1.1.	Asignar Agente Local/Foráneo
1.1.1.	Localizar MN
1.1.2.	Asignar Agente
1.2.	Proveer Agente Intermediario
1.2.1.	Obtenet información sobre dominios
1.2.2.	Instancia Agente Intermediario
1.2.3.	Asignar Agente
1.3.	Asignar Dirección IP Local
1.4.	Accesar HLR/VLR
1.4.1.	Estructurar consulta
1.4.2.	Solicitar acceso
1.4.3.	Abrir registro
1.5.	Autenticar
1.5.1.	Atender demanda de AAA
1.5.2.	Comunicarse con Servidor AAA Local
1.5.2.1.	Establecer comunicación con el IA
1.5.2.2.	Recibir respuesta a demanda
1.5.3.	Enviar respuesta al FA
1.5.4.	Enviar respuesta al IA
1.6.	Autorizar
1.7.	Tarificar
2. Funciones del Nodo Móvil:	
2.1.	Solicitar Registro
2.1.1.	Enviar demanda de AAA
2.1.1.1.	Generar Challenge
2.1.1.2.	Presentar credenciales
2.1.2.	Recibir respuesta AAA
2.1.2.1.	Revisar Authenticator
2.2.	Establecer Dirección IP Local
2.3.	Solicitar Servicio
3. Funciones del Agente Foráneo:	
3.1.	Viajar
3.1.1.	Escoger destino
3.1.2.	Almacenar estado actual
3.1.3.	Transportarse
3.2.	Suspender Ejecución
3.3.	Reanudar Ejecución
3.4.	Apropiarse de MN
3.5.	Recibir Petición de Registro
3.6.	Transportar Demanda de AAA

3.7.	Recibir Respuesta de AAA
3.8.	Entregar Respuesta de AAA al MN
3.9.	Entregar Demanda de AAA
4. Funciones del Agente Intermediario:	
4.1.	Viajar
4.1.1.	Escoger destino
4.1.2.	Almacenar estado actual
4.1.3.	Transportarse
4.2.	Suspender Ejecución
4.3.	Reanudar Ejecución
4.4.	Identificar AAAHS y AAAFS
4.5.	Recibir Datos de AAA
4.6.	Transportar Datos de AAA
4.7.	Recibir Respuesta de AAA
4.8.	Entregar Demanda de AAA
4.9.	Entregar Respuesta de AAA
4.10.	Estableces SAs
5. Funciones del HLR/VLR:	
5.1.	Atender Solicitud de Acceso
5.1.1.	Validar usuario
5.2.	Ejecutar consulta
5.3.	Gestionar Base de Datos
5.3.1.	Almacenar registro
5.3.2.	Buscar registro
5.3.3.	Eliminar registro
5.3.4.	Modificar registro

4.2.5 Modelo de Casos de Uso (Alto nivel)

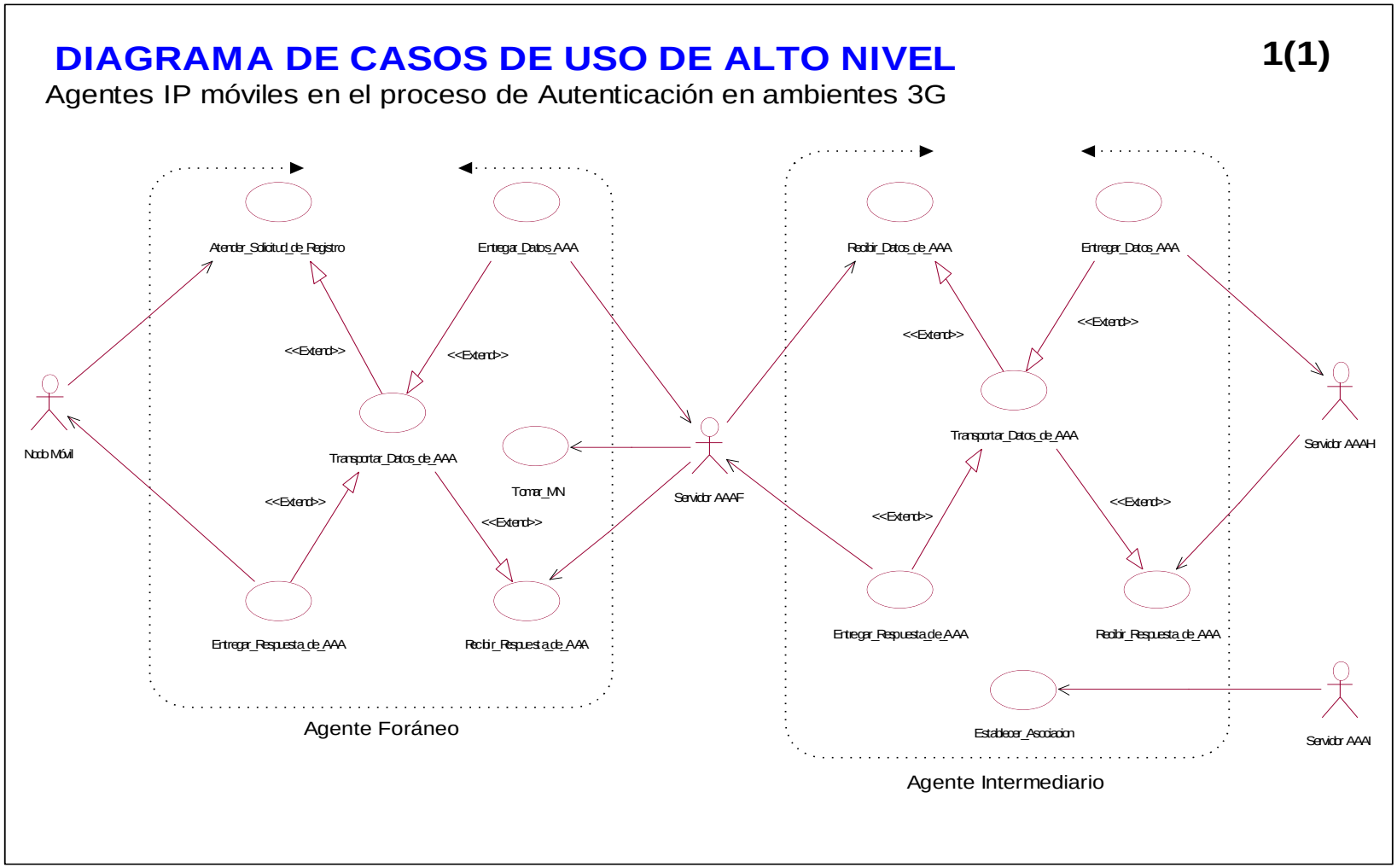


Figura 4.4 Diagrama de Casos de Uso de alto nivel

4.3 Análisis de los Agentes Móviles

4.3.1 Descripción de Casos de Uso Esenciales

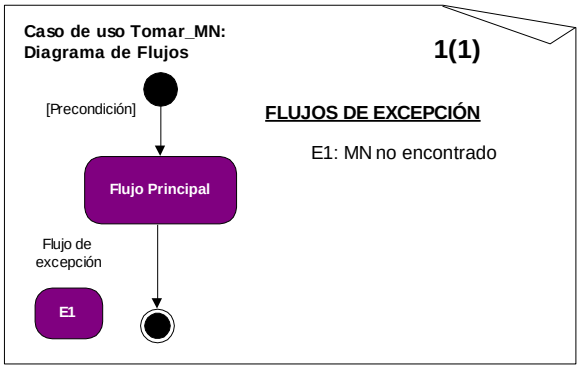
A continuación se hace la descripción de cada caso de uso de alto nivel, presente en el diagrama anterior que muestra los casos de uso que implementan a los dos agentes móviles (FA y IA).

4.3.1.1 Casos de Uso que implementan al Agente Foráneo (FA):

Caso de uso:	Tomar_MN.
Actores:	Servidor AAAF (Iniciador).
Propósito:	Permitir al Servidor AAA Foráneo asignar un Agente a un Nodo Móvil que acaba de entrar a su Dominio y que no pertenece al mismo.
Resumen:	El Servidor AAA Foráneo envía información a un Agente Foráneo sobre un Nodo Móvil que acaba de entrar a su área de cobertura y que no pertenece a su Dominio Administrativo, con el fin de asignarle la atención a dicho MN y que posibilite su registro en el sistema. Mediante el caso de uso Tomar_MN, el FA obtiene información sobre el MN al cual va a atender mientras éste se encuentre en dicho dominio (roaming), y se presenta a éste como su anfitrión.
Tipo:	Primario.
Referencias cruzadas	*Funciones:* R1.1, R1.1.1, R1.1.2 y R3.4.

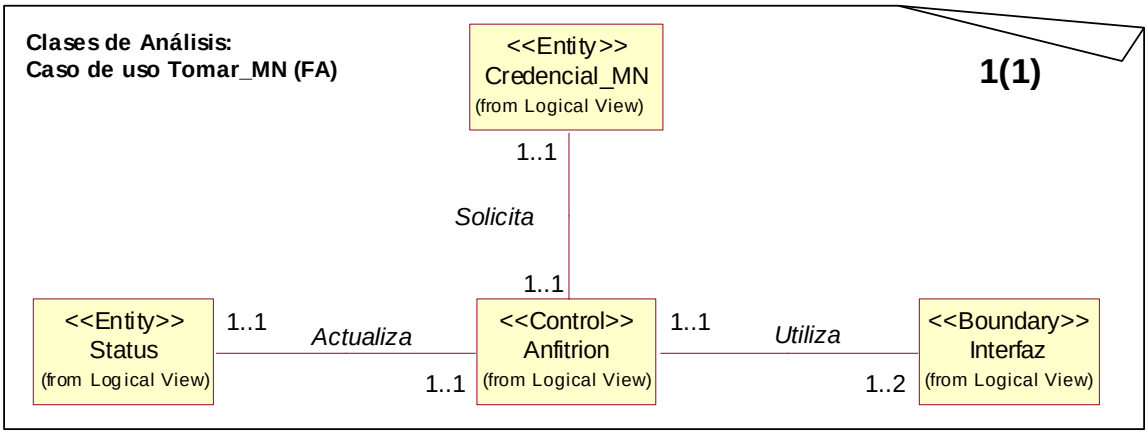
Pre-condiciones:	• El sistema debe contar con la siguiente información:
	  o Información proporcionada por la Red Radio sobre el Nodo Móvil.
	  o Información de disponibilidad de agentes.

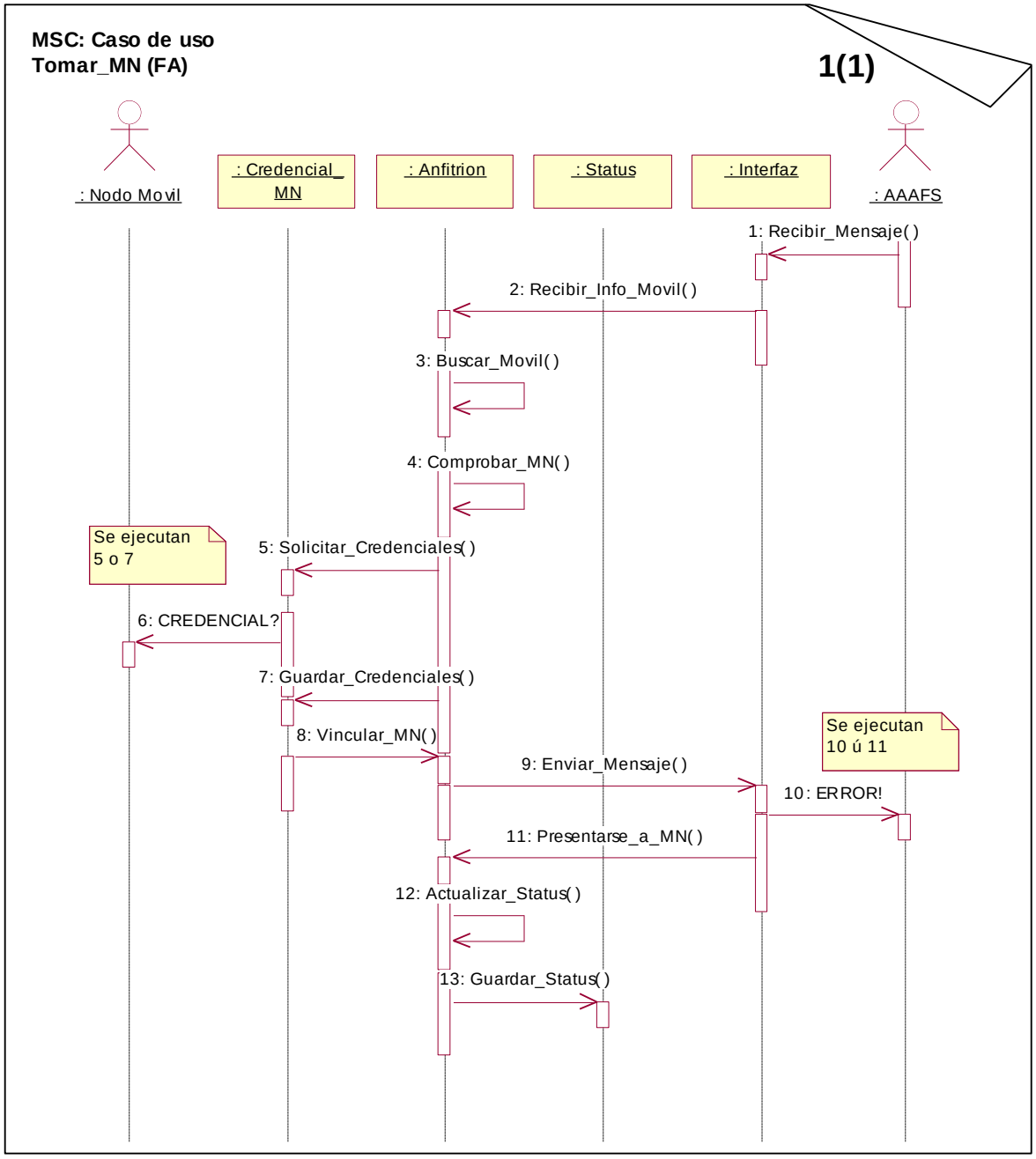
Flujo principal:	• Este caso de uso empieza cuando el Servidor AAA Foráneo instancia un agente y le entrega información sobre el MN que debe atender.
	• Con la información recibida, el Agente Foráneo viaja a buscar al MN y existen dos posibilidades:
	  o Una vez lo localiza, se continúa con la ejecución del flujo principal y se le "informa" al MN que será este agente quien lo atienda mientras se encuentre en *roaming*.
	  o No es posible localizar el MN, ***E1:*** MN no encontrado.



Flujos de excepción:

- E1: MN no encontrado
  - El FA retorna al servidor.
  - Entrega al AAAFS un mensaje de error indicando que el MN no fue encontrado para que éste haga lo propio.





Caso de uso: Atender_Solicitud_de_Registro.

Actores: Nodo_Movil (Iniciador).

Propósito: El propósito de este caso de uso es realizar las tareas necesarias para obtener del MN la información y credenciales requeridas para el registro del mismo.

Resumen: Una vez el MN está enterado de cual es el FA encargado de atenderlo, generar el *Challenge* y estructura la trama de *Requerimiento de Autenticación*. El caso de uso

comienza cuando esta información es recibida por el FA para ser transportada, para lo cual el FA solicita las credenciales al MN, recibe y atiende el requerimiento hecho para lograr el registro del móvil en la red. Finaliza cuando el caso de uso Transportar_Datos_de AAA es activado.

Tipo: Primario y esencial.

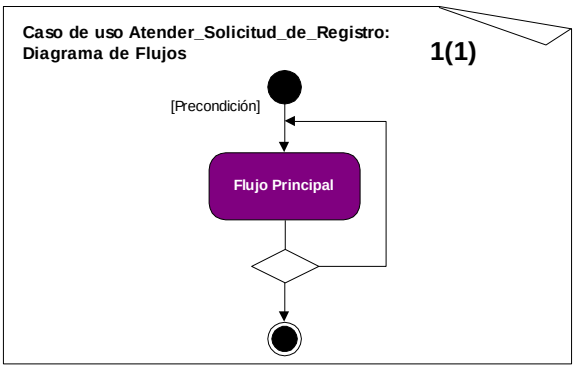
Referencias cruzadas *Funciones:* R2.1, R2.1.1, R2.1.1.1, R2.1.1.2, R3.5.

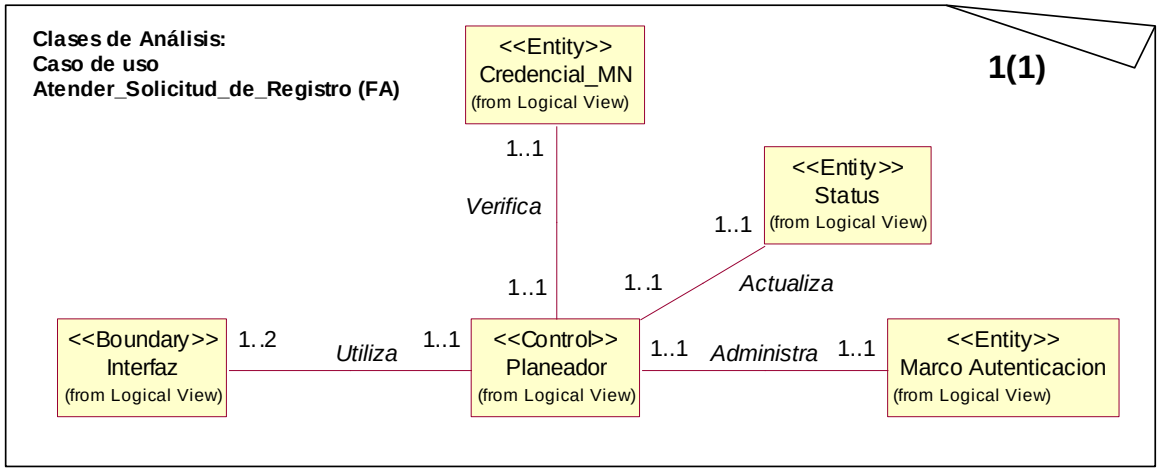
Pre-condiciones:

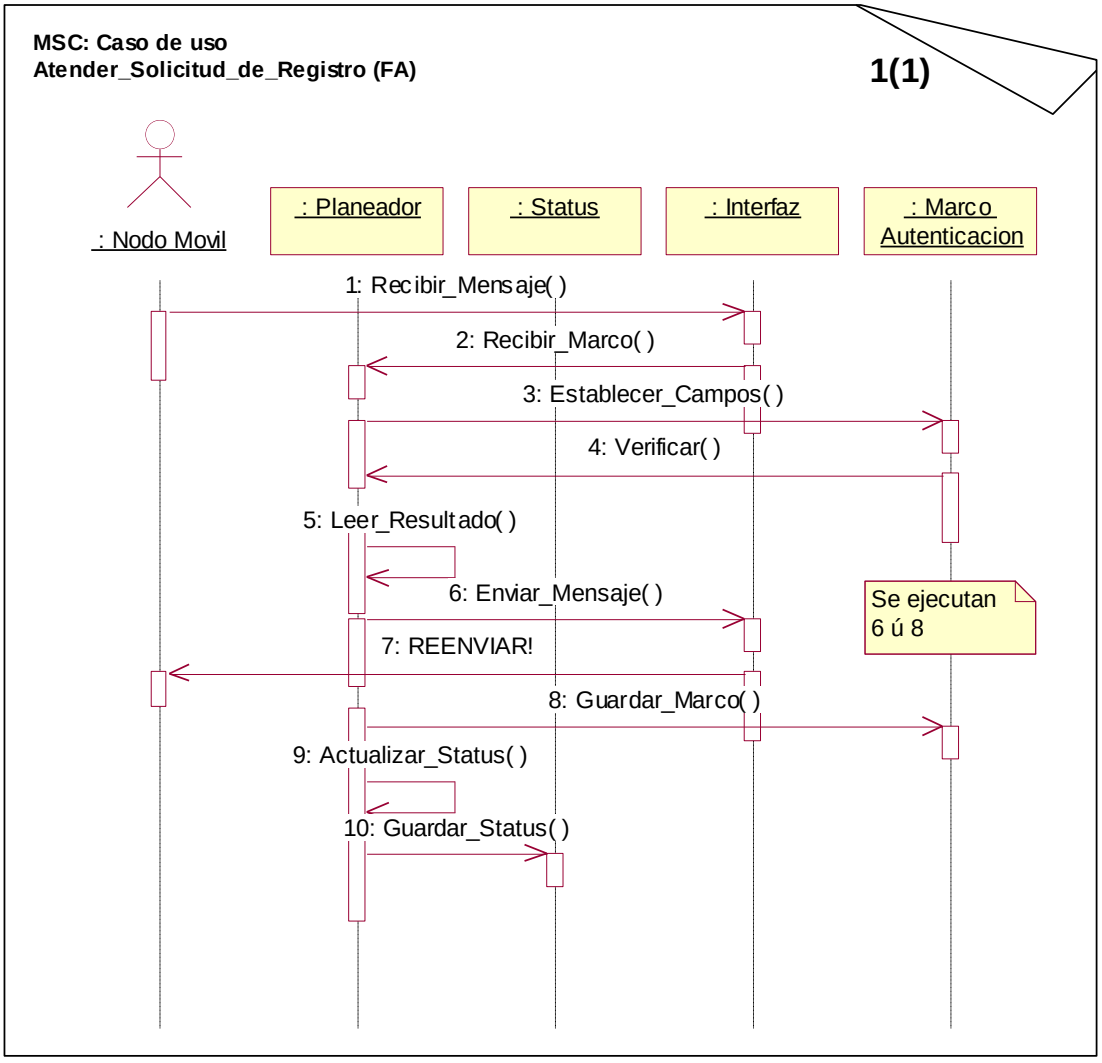
- El sistema debe contar con la siguiente información:
  - Tener ubicado el MN correspondiente.
  - Establecimiento total de la SA con el AAAFS.
- El caso de uso Tomar_MN debe haberse ejecutado previamente.

Flujo principal:

- El caso de uso comienza cuando el MN entrega al FA el *Requerimiento de Autenticación* y muestra sus credenciales para ser reconocido.
- El FA verifica esta información en cuanto a la estructura del requerimiento más no en cuanto a su validez.
- El FA verifica las credenciales entregadas por el MN.
- Dependiendo del resultado de las operaciones anteriores, se continúa con la ejecución del flujo principal o se solicita de nuevo la información requerida.
- Una vez validados correctamente los datos, esta información es guardada por el agente y se inicializa el transporte de los datos (*Requerimiento de Autenticación)* activando el caso de uso Transportar_Datos_de_AAA.



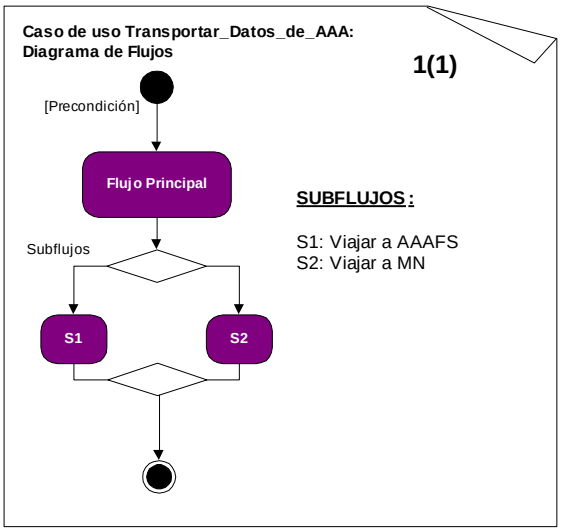

Clases de Análisis:
Caso de uso
Atender_Solicitud_de_Registro (FA)
1(1)
<<Entity>>
Credencial_MN
(from Logical View)
1..1
Verifica
1..1
<<Entity>>
Status
(from Logical View)
1..1
1..1
Actualiza
<<Boundary>>
Interfaz
(from Logical View)
1..2
Utiliza
1..1
<<Control>>
Planeador
(from Logical View)
1..1
Administra
1..1
<<Entity>>
Marco Autenticacion
(from Logical View)


MSC: Caso de uso
Atender_Solicitud_de_Registro (FA)
1(1)
: Nodo Movil
: Planeador
: Status
: Interfaz
: Marco Autenticacion
1: Recibir_Mensaje( )
2: Recibir_Marco( )
3: Establecer_Campos( )
4: Verificar( )
5: Leer_Resultado( )
6: Enviar_Mensaje( )
7: REENVIAR!
Se ejecutan
6 ú 8
8: Guardar_Marco( )
9: Actualizar_Status( )
10: Guardar_Status( )

Caso de uso:	Transportar_Datos_de_AAA.
Actores:	Ninguno. El caso de uso lo inicializan otros casos de uso con los cuales tiene una relación *Extend*.
Propósito:	El propósito de este caso de uso es realizar todas las operaciones necesarias para que el FA transporte adecuadamente la información entregada por una de las dos partes que le corresponden en el proceso de Autenticación (MN y AAAFS).
Resumen:	• En un sentido del proceso, una vez el FA tiene la información de credenciales y el *Requerimiento de Autenticación* generado por el MN, este caso de uso es inicializado por el caso de uso Atender_Solicitud_de_Registro, el FA suspende su ejecución, escoge el destino (AAAFS), guarda su estado actual e inicia su viaje a través de la red, después de lo cual vuelve a activarse en el destino, reinicia su ejecución y activa otro caso de uso para entregar los datos al AAAFS. • En el otro sentido del proceso, una vez el AAAFS tiene la *Respuesta de Autenticación*, este caso de uso es inicializado por el caso de uso Recibir_Respuesta_de_AAA, el FA suspende su ejecución, escoge el destino (MN), guarda su estado actual e inicia su viaje a través de la red, después de lo cual vuelve a activarse en el destino, reinicia su ejecución y activa otro caso de uso para entregar los datos al MN.
Tipo:	Primario y esencial.
Referencias cruzadas	*Funciones:* R3.1, R3.1.1, R3.1.2, R3.1.3, R3.2, R3.3, R3.6. *Casos de uso:* Atender_Solicitud_de_Registro, Recibir_Respuesta_de_AAA.

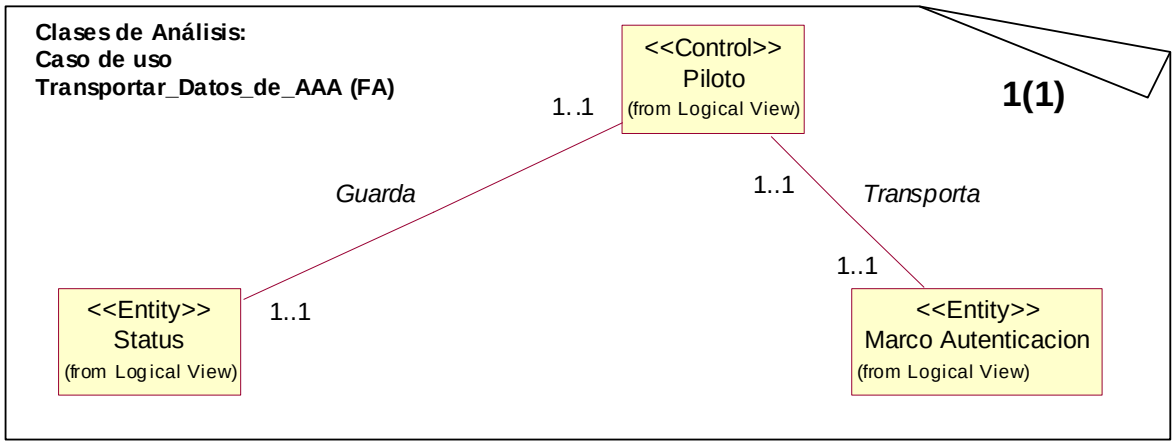
Pre-condiciones:	• El sistema debe contar con la siguiente información:
	  ○ Destino al cual va a desplazarse.
	  ○ Tipo de operación que debe realizar al llegar a su destino.
	• Según el caso, debe ejecutarse previamente el caso de uso Atender_Solicitud_de_Registro (en el lado del MN) ó el caso de uso Recibir_Respuesta_de_AAA (en el lado del AAAFS).

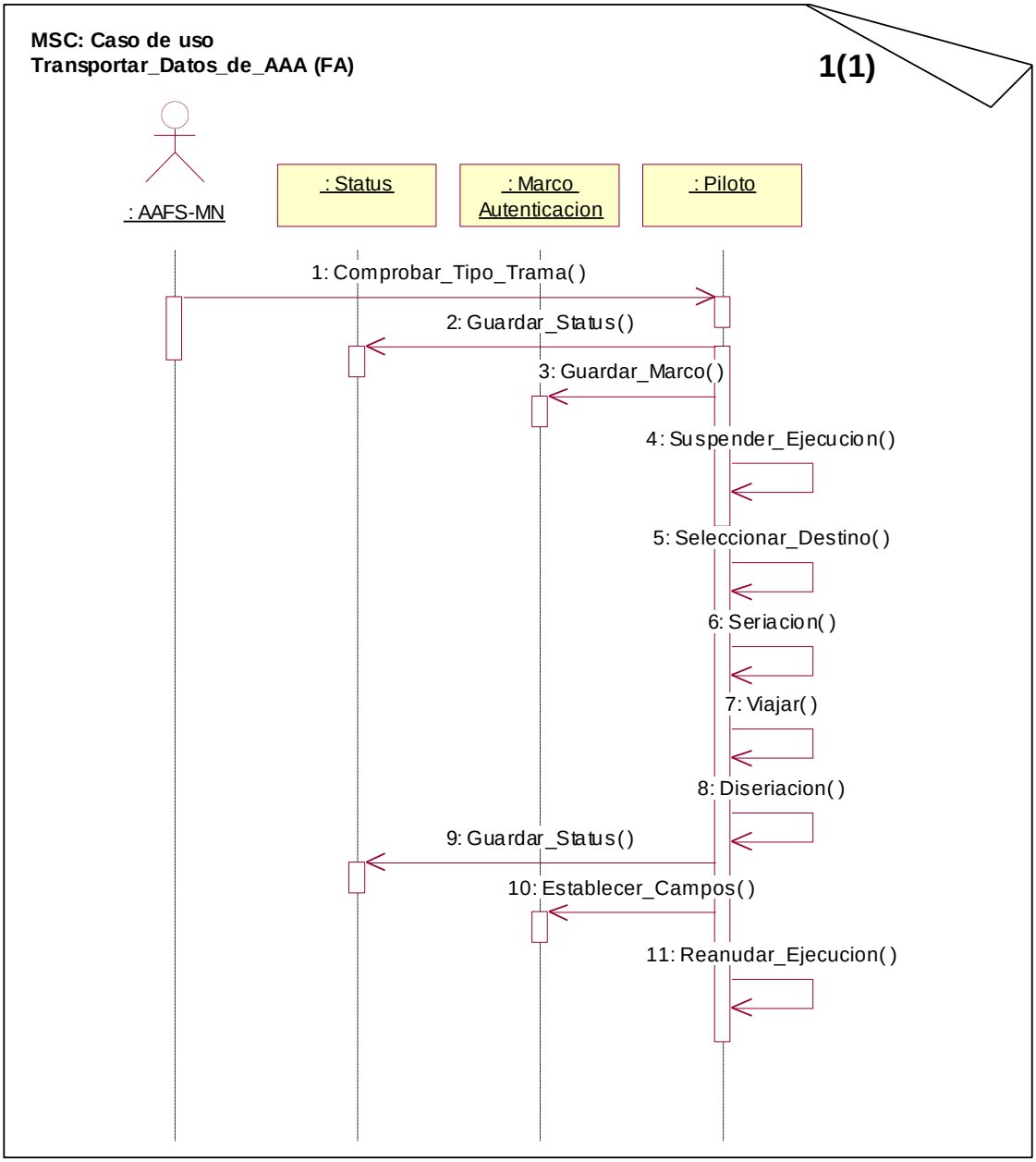
Flujo principal:	• El caso de uso empieza cuando el FA obtiene un resultado correcto en la revisión de los datos entregados por el MN o por el AAAFS según el caso.
	• El FA realiza un reconocimiento de quién le está entregando los datos, es decir, si lo que recibe es un *Requerimiento de Autenticación* o una *Respuesta de Autenticación*.
	• Una vez hecho esto, se tienen dos posibles caminos de ejecución:
	  ○ Se recibe un *Requerimiento de Autenticación,* ***S1:*** Viajar al AAAFS.
	  ○ Se recibe una *Respuesta de Autenticación,* ***S2:*** Viajar al MN.



SubFlujos:

- S1: Viajar al AAAFS
  - El FA suspende ejecución.
  - Se guarda estado del mismo.
  - Escoge destino (AAAFS).
  - Se transporta.
  - Una vez en su destino reanuda su ejecución.
  - El caso de uso finaliza inicializando el caso de uso Entregar_Datos_AAA.
- S2: Viajar al MN
  - El FA suspende ejecución.
  - Se guarda estado del mismo.
  - Escoge destino (MN).
  - Se transporta.
  - Una vez en su destino reanuda su ejecución.
  - El caso de uso finaliza inicializando el caso de uso Entregar_Respuesta_de_AAA.





Caso de uso: Entregar_Datos_AAA.

Actores: Ninguno. El caso de uso es inicializado por el caso de uso Transportar_Datos_de_AAA con el cual tiene una relación *Extend*.

Propósito: Permitir al FA entregar el *Requerimiento de Autenticación* generado por el MN al AAAFS y esperar a que éste responda.

Resumen: El FA ha llegado al AAAFS y ha reanudado su ejecución. Este caso de uso es activado por el caso de uso Transportar_Datos_de_AAA. El FA hace un reconocimiento de su

destino, pasa la información (*Requerimiento de Autenticación*) al AAAFS y queda en un estado de espera de la respuesta.

Tipo: Primario.

Referencias cruzadas *Funciones:* R1.5, R1.5.1, R3.9.

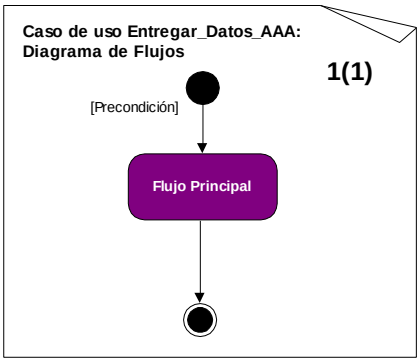
Casos de uso: Transportar_Datos_de_AAA.

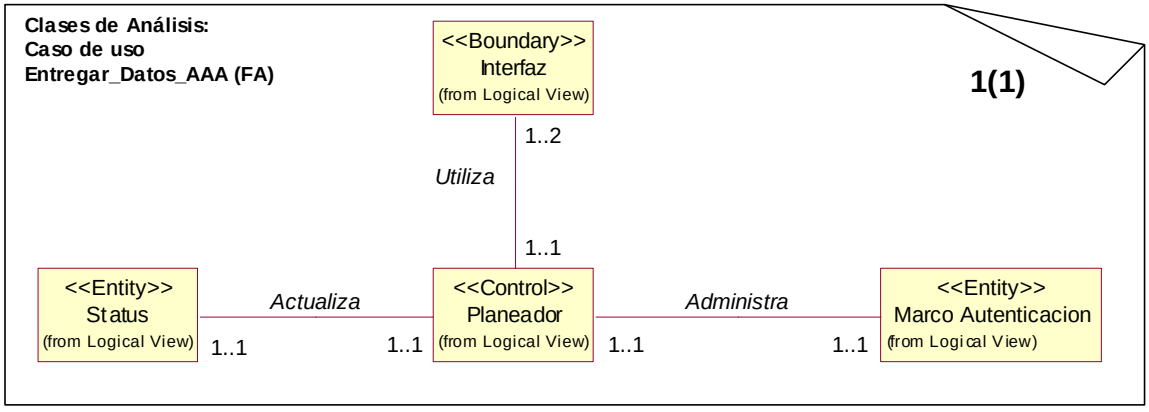
Pre-condiciones:

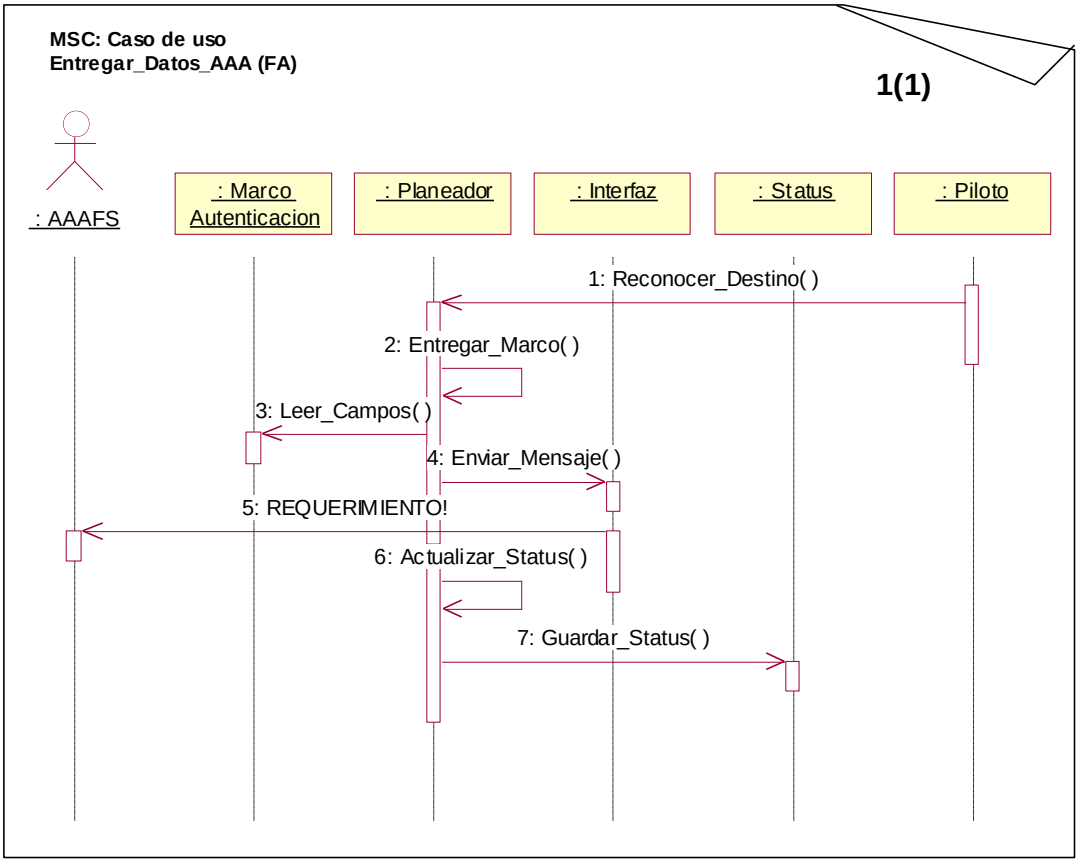
- El sistema debe haber ejecutado previamente el caso de uso Transportar_Datos_de_AAA.

Flujo principal:

- El caso de uso es inicializado por el caso de uso Transportar_Datos_de_AAA cuando el FA ha llegado al AAAFS.
- El FA pasa el *Requerimiento de Autenticación* al AAAFS (Demanda de AAA).
- El caso de uso termina cuando el FA es colocado en un estado de espera de la *Respuesta de Autenticación*.







Caso de uso: Recibir_Respuesta_de_AAA.

Actores: Servidor AAAF (Iniciador).

Propósito: La finalidad de este caso de uso es permitir que el FA reciba correctamente del AAAFS la respuesta al *Requerimiento de Autenticación* inicialmente entregado por el MN, para su posterior transporte.

Resumen: El FA se encuentra inicialmente en un estado de espera, y este caso de uso es activado cuando el AAAFS saca al FA de este estado entregándole la *Respuesta de Autenticación*. El FA recibe la respuesta y se finaliza este caso de uso cuando el caso de uso Transportar_Datos_de AAA es activado.

Tipo: Primario.

Referencias cruzadas *Funciones:* R1.5, R1.5.1, R1.5.3, R3.7.

Pre-condiciones:

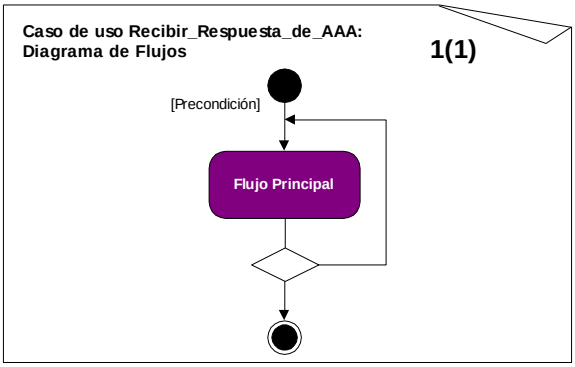
- El sistema debe contar con la siguiente información:
  - El AAAFS debe haber procesado el requerimiento hecho.
- El FA debe encontrarse en estado de espera de la respuesta.

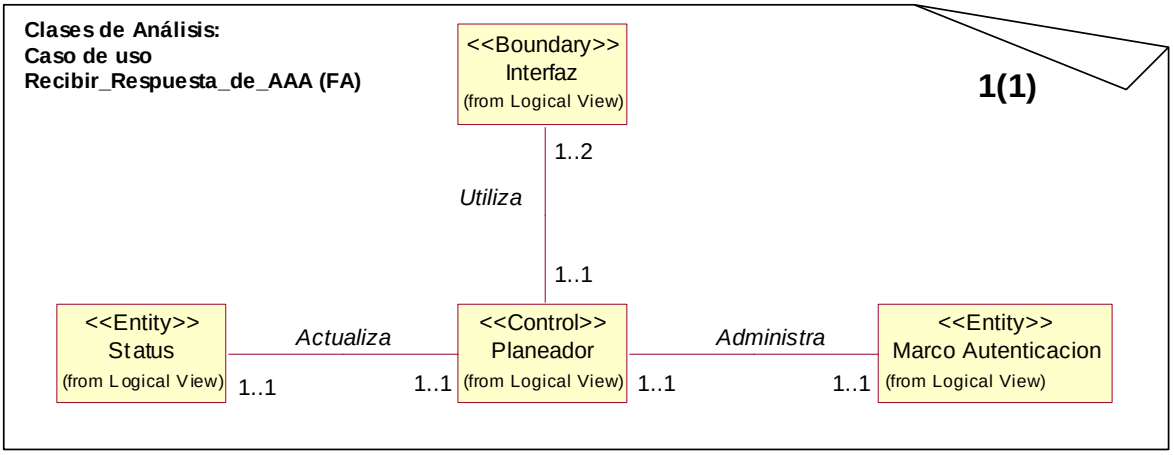
Flujo principal:

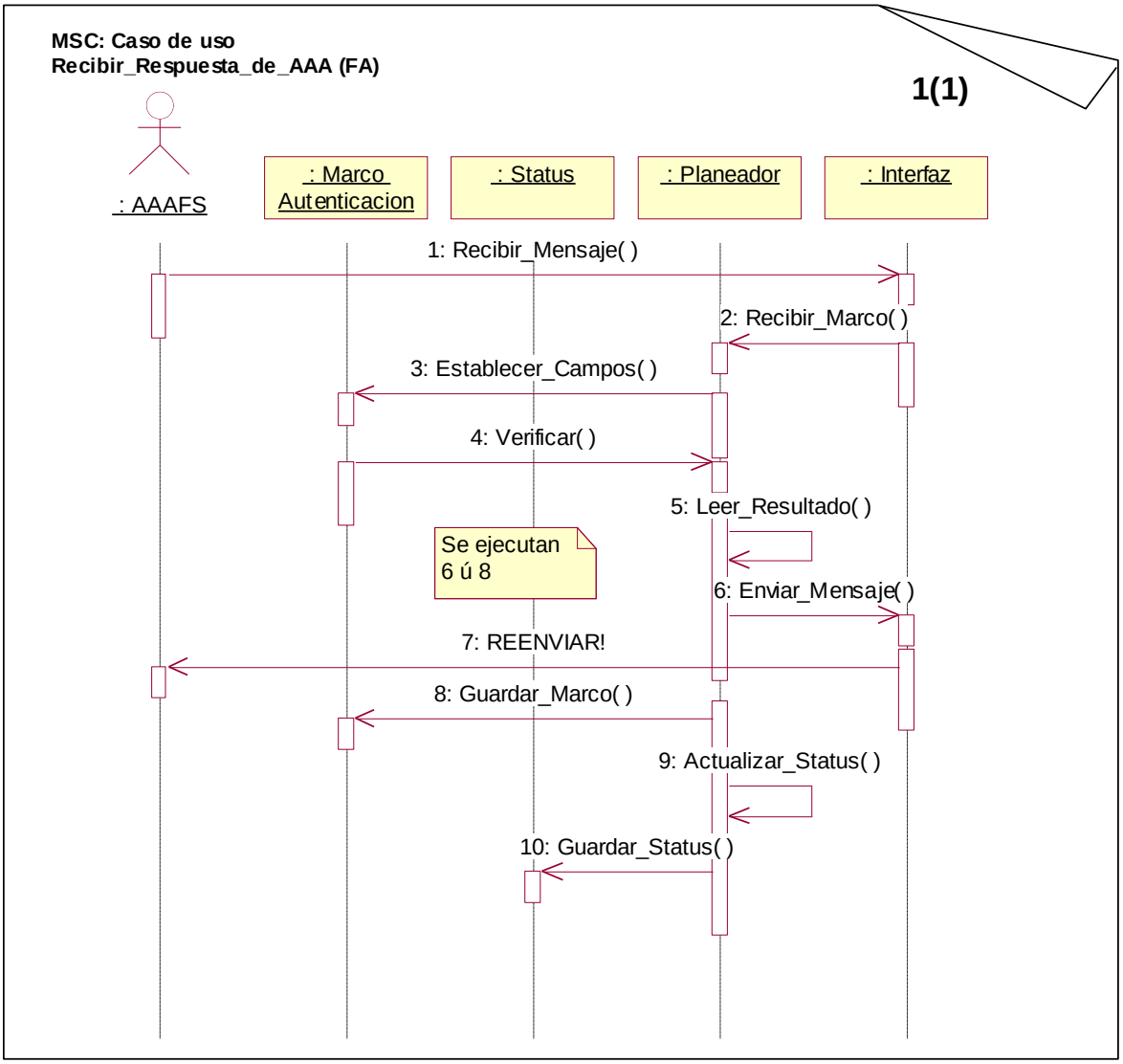
- El caso de uso comienza cuando el AAAFS entrega al FA la *Respuesta de Autenticación* para informar al MN su registro.
- El FA verifica esta información en cuanto a la estructura del requerimiento más no

en cuanto a su validez.

- Dependiendo del resultado de las operaciones anteriores, se continúa con la ejecución del flujo principal o se solicita de nuevo la información requerida.
- Una vez validados correctamente los datos, esta información es guardada por el agente y se inicializa el transporte de los datos (*Respuesta de Autenticación)* activando el caso de uso Transportar_Datos_de_AAA.







Caso de uso: Entregar_Respuesta_de_AAA.

Actores: Ninguno. El caso de uso es inicializado por el caso de uso Transportar_Datos_de_AAA con el cual tiene una relación *Extend*.

Propósito: Permitir al FA entregar la *Respuesta de Autenticación* generada por el AAAFS al MN.

Resumen: El FA ha llegado al MN y ha reanudado su ejecución. Este caso de uso es activado por el caso de uso Transportar_Datos_de_AAA. El FA hace un reconocimiento de su destino, pasa la información (*Respuesta de Autenticación*) al MN y queda en un estado de espera de cualquier otra solicitud hecha bien sea por el MN o por el AAAFS.

Tipo: Primario.

Referencias cruzadas *Funciones:* R2.1.2, R2.1.2.1, R3.8.

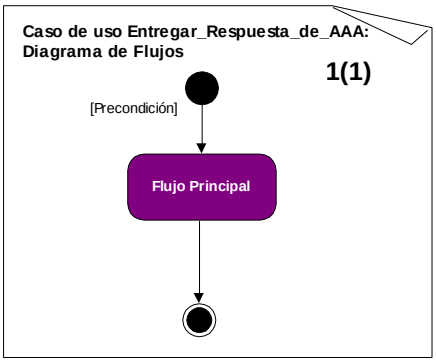
Casos de uso: Transportar_Datos_de_AAA.

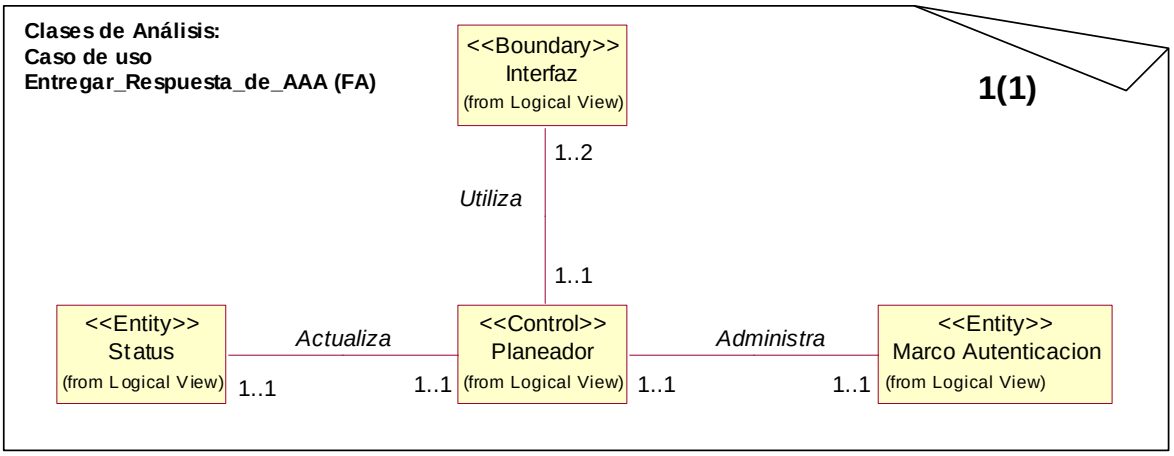
Pre-condiciones:

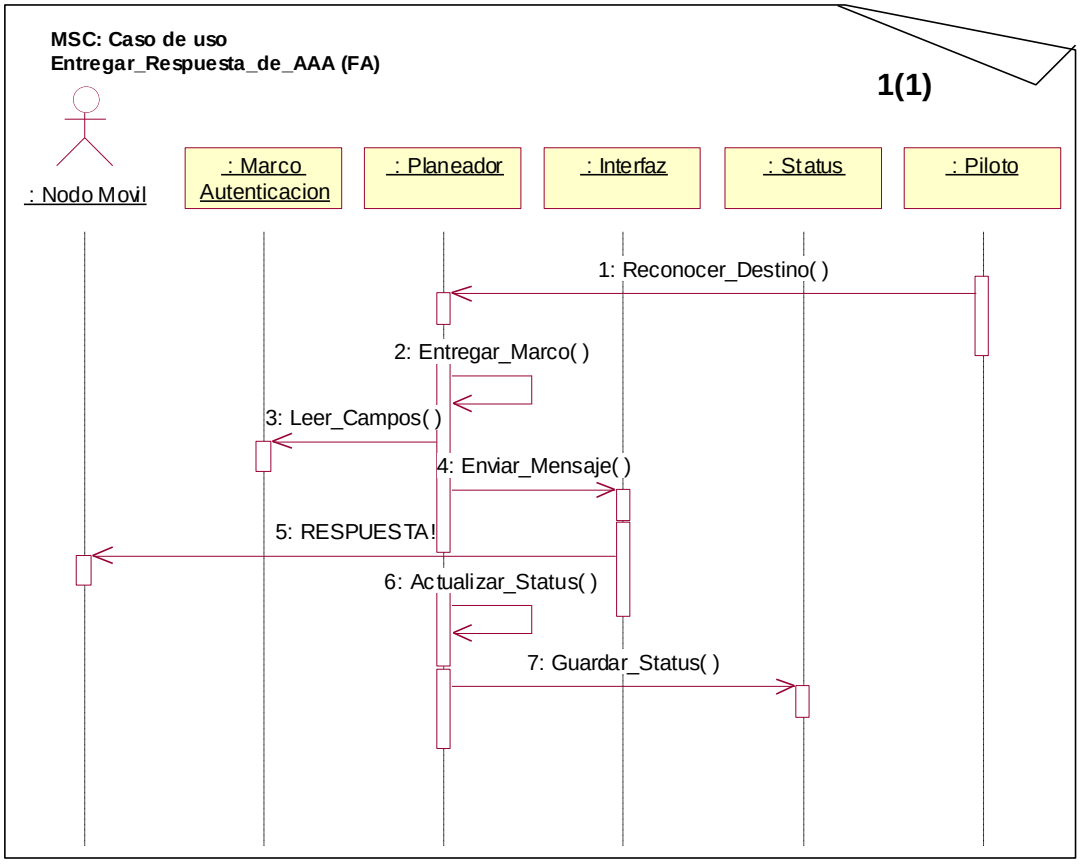
- El sistema debe haber ejecutado previamente el caso de uso Transportar_Datos_de_AAA.

Flujo principal:

- El caso de uso es inicializado por el caso de uso Transportar_Datos_de_AAA cuando el FA ha llegado al MN.
- El FA pasa la *Respuesta de Autenticación* al MN.
- El caso de uso termina cuando el FA es colocado en un estado de espera de cualquier otra solicitud por parte del MN o del AAAFS.







4.3.1.2 Casos de Uso que implementan al Agente Intermediario (IA):

Caso de uso: Establecer_Asociación.

Actores: Servidor AAAI (Iniciador).

Propósito: Permitir al Servidor AAA Mediador asignar un Agente Intermediario (IA) para que se encargue de manejar las Asociaciones de Seguridad (SA) correspondientes y posibilitar la comunicación entre el AAAFS y el AAAHS para efectos de prestar el servicio al MN que se encuentra en roaming.

Resumen: Debido a que el AAAFS y el AAAHS no comparten una SA, la comunicación debe hacerse utilizando un IA.

El AAAFS solicita la provisión de un IA a un Servidor AAA Mediador (AAAIS: AAA Intermediary Server) con el cual sí comparte una SA. Este AAAIS obtiene información sobre los dominios y servidores Local y Foráneo, y activa este caso de uso cuando instancia un Agente Intermediario (IA) y le pasa dicha información para que él haga un reconocimiento de los dos dominios y gestione en adelante las SA posibilitando su comunicación.

Tipo: Primario.

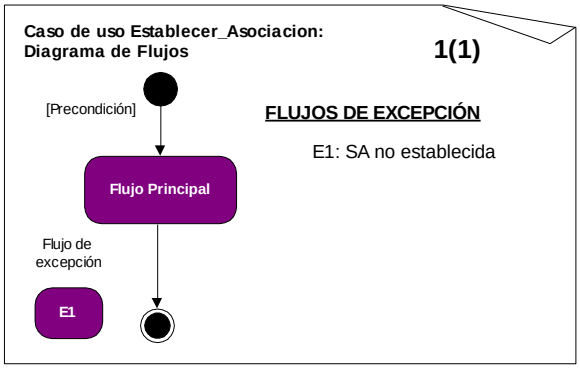
Referencias cruzadas *Funciones:* R1.2, R1.2.1, R1.2.2, R1.2.3, R4.4, R4.10.

Pre-condiciones:

- El sistema debe contar con la siguiente información:
  - Información sobre los dominios Local y Foráneo.
  - Información sobre las SA correspondientes.
  - Información de disponibilidad de agentes.

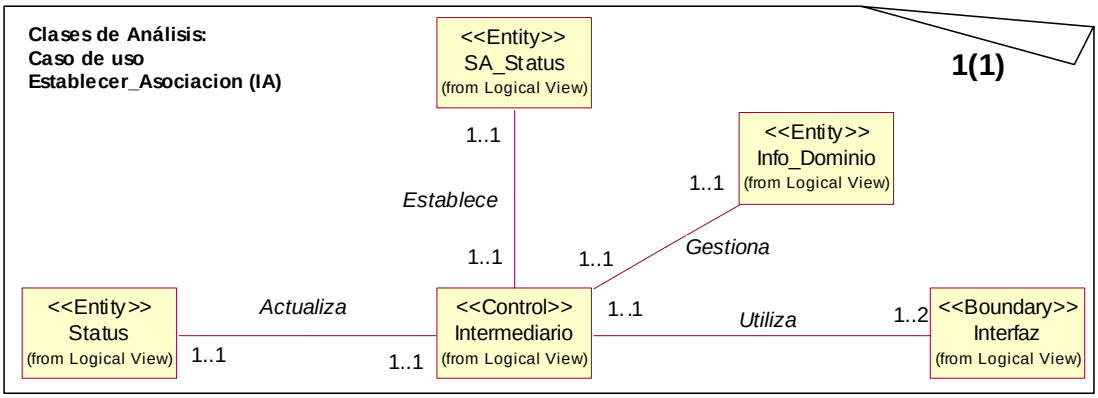
Flujo principal:

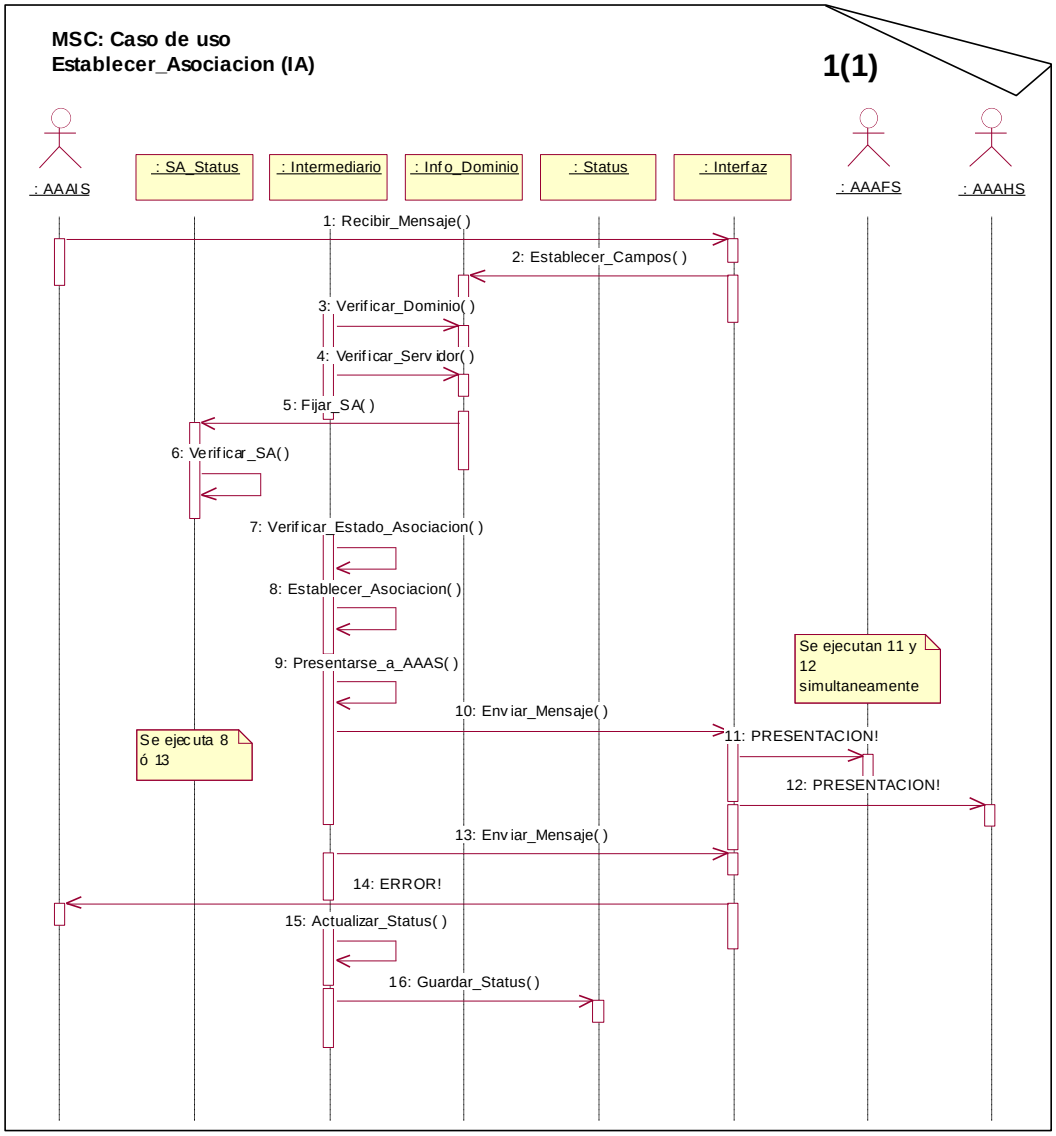
- Este caso de uso empieza cuando el Servidor AAA Mediador (AAAIS) instancia un agente y le entrega información sobre los dominios Local y Foráneo, y sobre las SAs involucradas.
- Con la información recibida, el Agente Intermediario verifica las SAs y la información entregada con el fin de posibilitar la comunicación entre el AAAFS y el AAAHS.
- Una vez hecho esto se tienen dos posibilidades:
  - SAs válidas, se continúa con la ejecución del flujo principal y el Agente Intermediario se identifica ante los dos servidores AAA.
  - SAs no válidas, ***E1:*** SA no establecida.



Flujos de excepción:

- E1: SA no establecida
  - El IA retorna al Servidor AAA Mediador.
  - Entrega al AAAIS un mensaje de error indicando que no existe una SA entre éste y el AAAHS para que él haga lo propio.





Caso de uso: Recibir_Datos_de_AAA.

Actores: Servidor AAAF (Iniciador).

Propósito: El propósito de este caso de uso es realizar las tareas necesarias para obtener del AAAFS la información requerida para el registro del MN (Demanda de AAA) y que será entregada al Agente Intermediario (IA).

Resumen: Una vez el IA está enterado de cuales son los servidores AAA que atenderá, se queda en un estado de espera de información del requerimiento (*Demanda de AAA*) generado inicialmente por el MN.

Este caso de uso comienza cuando el IA es sacado del estado de espera y la información (Demanda de AAA) le es entregada por parte del AAAFS para ser

transportada. Finaliza cuando el caso de uso Transportar_Datos_de AAA es activado.

Tipo: Primario.

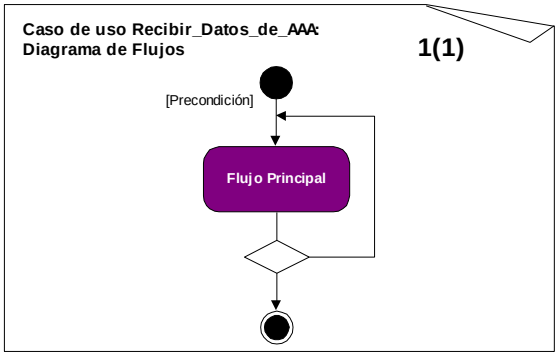
Referencias cruzadas *Funciones:* R1.5, R1.5.2, 1.5.2.1, 4.5.

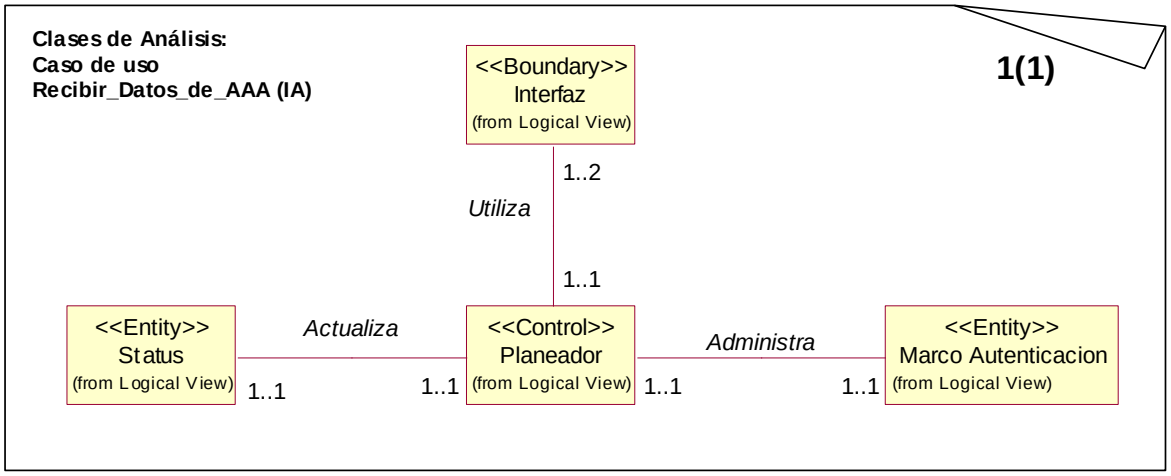
Pre-condiciones:

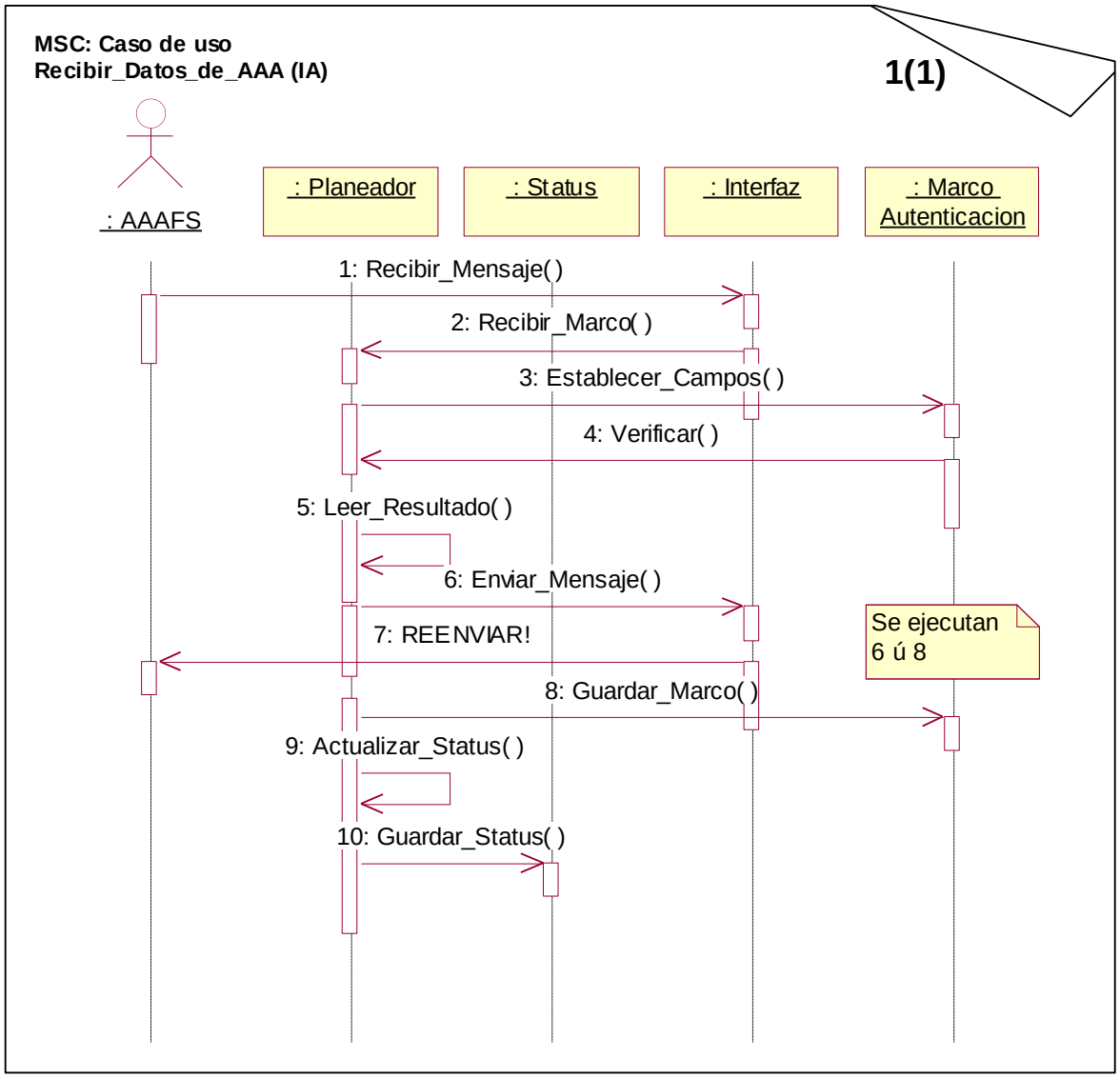
- El sistema debe contar con la siguiente información:
  - Tener identificados los servidores AAA Foráneo y Local a los cuales va a atender.
  - Establecimiento total de las SAs con dichos servidores.
- El caso de uso Establecer_Asociación debe haberse ejecutado previamente.

Flujo principal:

- El caso de uso comienza cuando el AAAFS entrega al IA la *Demanda de AAA*.
- El IA verifica esta información en cuanto a la estructura del requerimiento más no en cuanto a su validez.
- Dependiendo del resultado de las operaciones anteriores, se continúa con la ejecución del flujo principal o se solicita de nuevo la información requerida.
- Una vez validados correctamente los datos, esta información es guardada por el agente y se inicializa el transporte de los datos (*Demanda de AAA)* activando el caso de uso Transportar_Datos_de_AAA.







Caso de uso: Transportar_Datos_de_AAA.

Actores: Ninguno. El caso de uso lo inicializan otros casos de uso con los cuales tiene una relación *Extend*.

Propósito: El propósito de este caso de uso es realizar todas las operaciones necesarias para que el IA transporte adecuadamente la información entregada por una de las dos partes que le corresponden en el proceso de Autenticación (AAAFS y AAAHS).

Resumen:

- En un sentido del proceso, una vez el IA tiene la información y la *Demanda de AAA* generada inicialmente por el MN, este caso de uso es inicializado por el caso de uso Recibir_Datos_de_AAA, el IA suspende su ejecución, escoge el destino (AAAHA), guarda su estado actual e inicia su viaje a través de la red, después de lo cual vuelve a activarse en el destino, reinicia su ejecución y activa otro caso de uso para

entregar los datos al AAAHS.

- En el otro sentido del proceso, una vez el AAAHS ha validado al usuario (MN) y tiene la *Respuesta de Autenticación*, este caso de uso es inicializado por el caso de uso Recibir_Respuesta_de_AAA, el IA suspende su ejecución, escoge el destino (AAAFS), guarda su estado actual e inicia su viaje a través de la red, después de lo cual vuelve a activarse en el destino, reinicia su ejecución y activa otro caso de uso para entregar los datos al AAAFS.

Tipo: Primario y esencial.

Referencias cruzadas *Funciones:* R4.1, R4.1.1, R4.1.2, R4.1.3, R4.2, R4.3, R4.6.

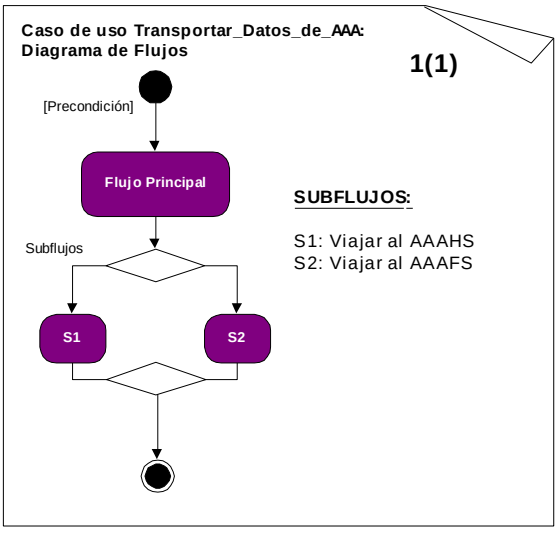
Casos de uso: Recibir_Datos_de_AAA, Recibir_Respuesta_de_AAA.

Pre-condiciones:

- El sistema debe contar con la siguiente información:
  - Destino al cual va a desplazarse.
  - Tipo de operación que debe realizar al llegar a su destino.
- Según el caso, debe ejecutarse previamente el caso de uso Recibir_Datos_de_AAA (en el lado del AAAFS) ó el caso de uso Recibir_Respuesta_de_AAA (en el lado del AAAHS).

Flujo principal:

- El caso de uso empieza cuando el IA obtiene un resultado correcto en la revisión de los datos entregados por el AAAFS o por el AAAHS según el caso.
- El IA realiza un reconocimiento de quién le está entregando los datos, es decir, si lo que recibe es una *Demanda de AAA* o una *Respuesta de Autenticación*.
- Una vez hecho esto, se tienen dos posibles caminos de ejecución:
  - Se recibe un *Demanda de AAA,* ***S1:*** Viajar al AAAHS.
  - Se recibe una *Respuesta de Autenticación,* ***S2:*** Viajar al AAAFS.

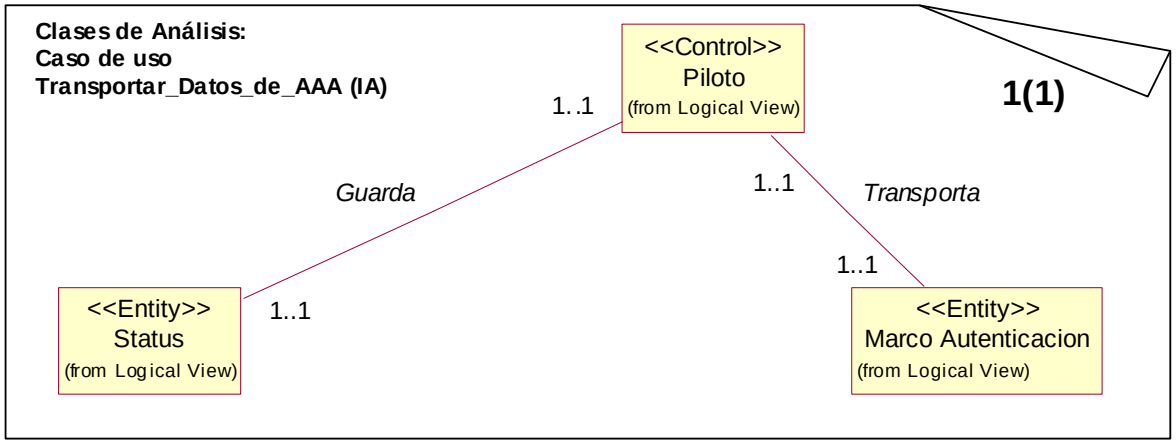


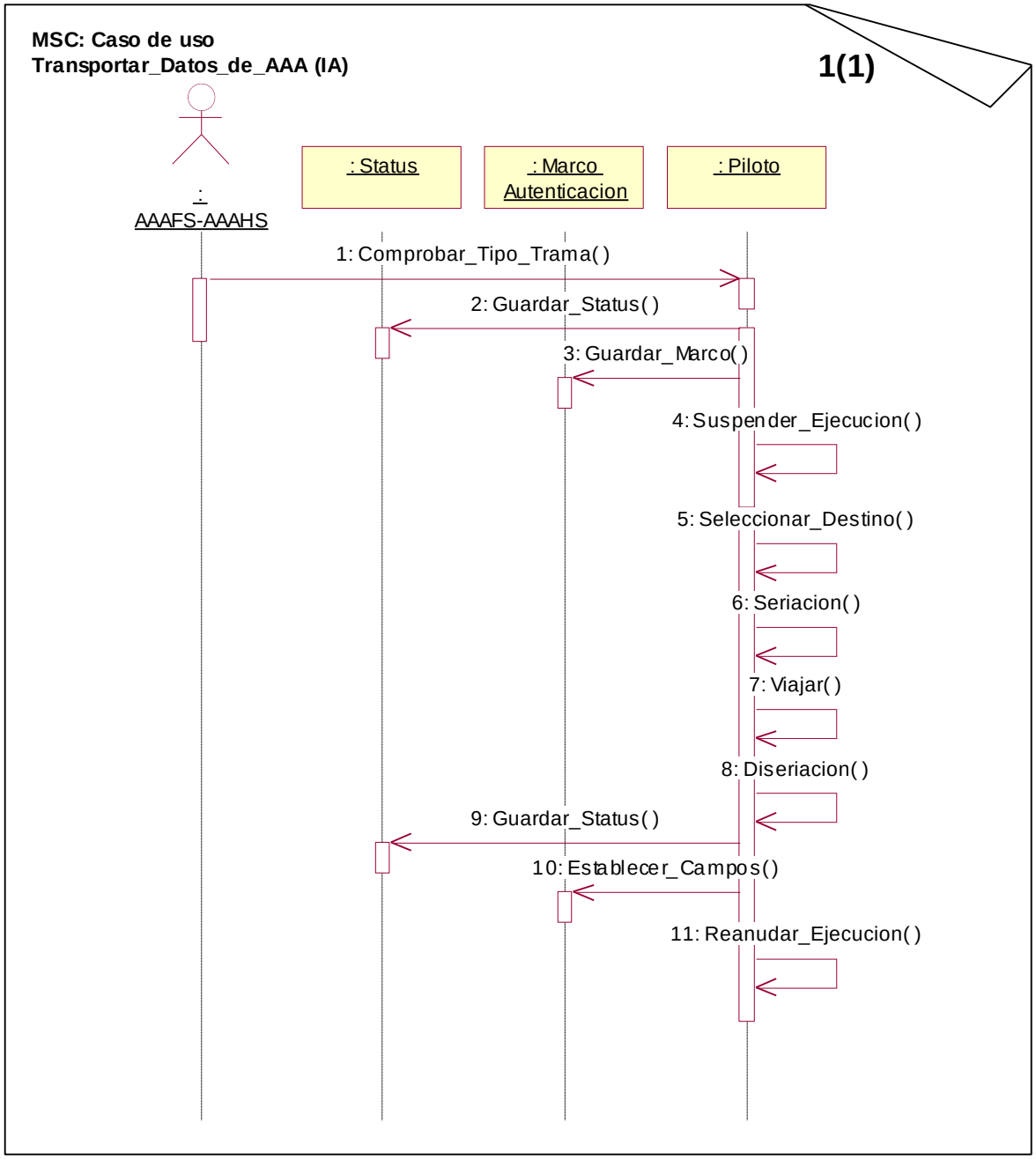
SubFlujos:

- S1: Viajar al AAAHS
  - El IA suspende ejecución.
  - Se guarda estado del mismo.

- Escoge destino (AAAHS).
- Se transporta.
- Una vez en su destino reanuda su ejecución.
- El caso de uso finaliza inicializando el caso de uso Entregar_Datos_AAA.

- S2: Viajar al AAAFS
  - El IA suspende ejecución.
  - Se guarda estado del mismo.
  - Escoge destino (AAAFS).
  - Se transporta.
  - Una vez en su destino reanuda su ejecución.
  - El caso de uso finaliza inicializando el caso de uso Entregar_Respuesta_de_AAA.





Caso de uso: Entregar_Datos_AAA.

Actores: Ninguno. El caso de uso es inicializado por el caso de uso Transportar_Datos_de_AAA con el cual tiene una relación *Extend*.

Propósito: Permitir al IA entregar el *Requerimiento de Autenticación (Demanda de AAA)* generado inicialmente por el MN y enviado por el AAAFS al AAAHS y esperar a que éste responda.

Resumen: El IA ha llegado al AAAHS y ha reanudado su ejecución. Este caso de uso es activado

por el caso de uso Transportar_Datos_de_AAA. El IA hace un reconocimiento de su destino, pasa la información (*Requerimiento de Autenticación o Demanda de AAA*) al AAAHS y queda en un estado de espera de la respuesta.

Tipo: Primario.

Referencias cruzadas *Funciones:* R1.5, R1.5.1, R4.8.

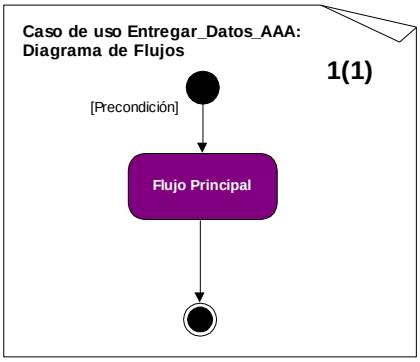
Casos de uso: Transportar_Datos_de_AAA.

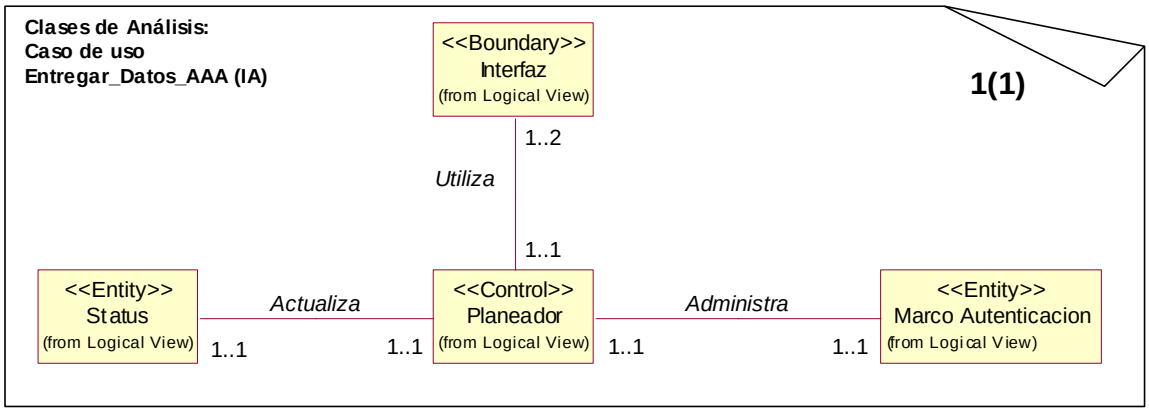
Pre-condiciones:

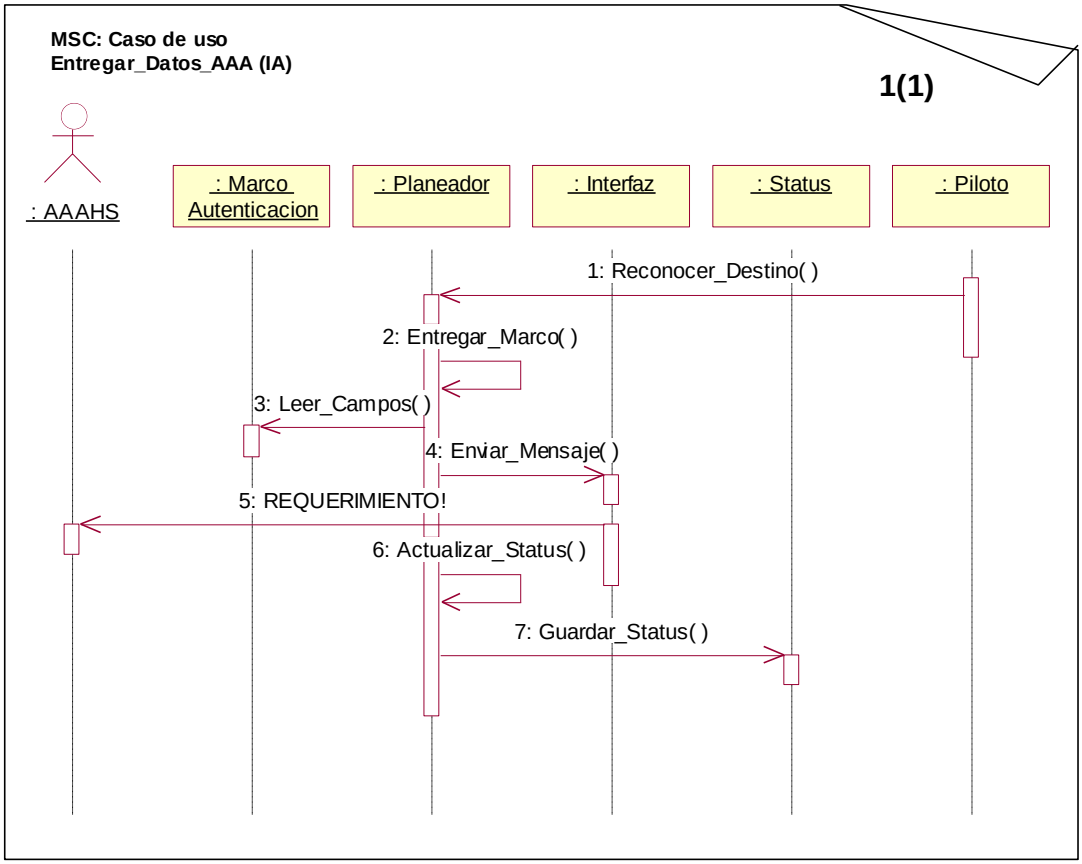
- El sistema debe haber ejecutado previamente el caso de uso Transportar_Datos_de_AAA.

Flujo principal:

- El caso de uso es inicializado por el caso de uso Transportar_Datos_de_AAA cuando el IA ha llegado al AAAHS.
- El IA pasa el *Requerimiento de Autenticación* (*Demanda de AAA*) al AAAHS.
- El caso de uso termina cuando el IA es colocado en un estado de espera de la *Respuesta de Autenticación*.







Caso de uso: Recibir_Respuesta_de_AAA.

Actores: Servidor AAAH (Iniciador).

Propósito: La finalidad de este caso de uso es permitir que el IA reciba correctamente del AAAHS la respuesta al *Requerimiento de Autenticación* entregado inicialmente por el MN, para su posterior transporte.

Resumen: El IA se encuentra inicialmente en un estado de espera, y este caso de uso es activado cuando el AAAHS saca al IA de este estado entregándole la *Respuesta de Autenticación*. El IA recibe la respuesta y este caso de uso finaliza cuando el caso de uso Transportar_Datos_de AAA es activado.

Tipo: Primario.

Referencias cruzadas *Funciones:* R1.5, R1.5.1, R1.5.4, R4.7.

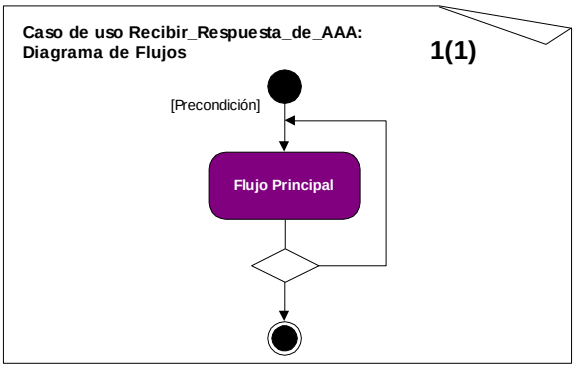
Pre-condiciones:

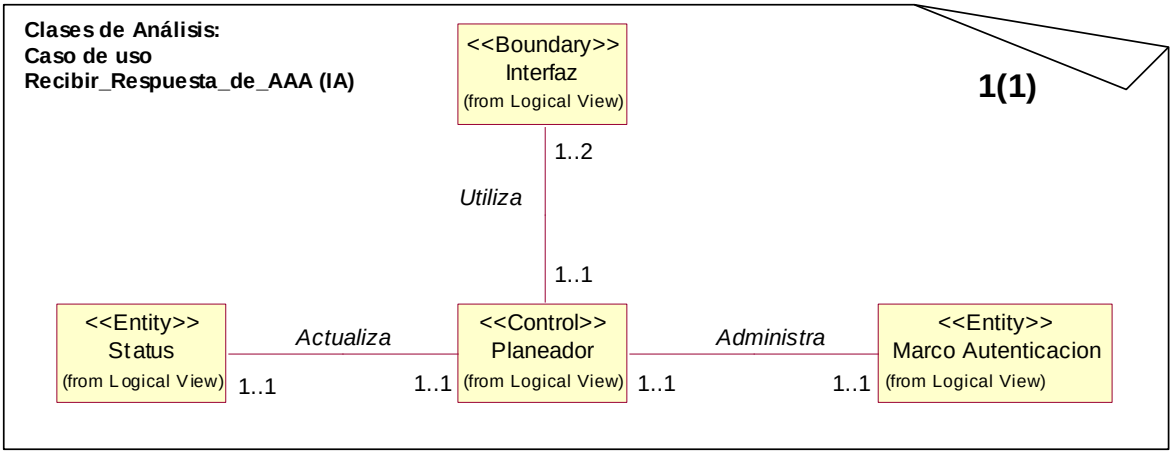
- El sistema debe contar con la siguiente información:
  - El AAAHS debe haber procesado el requerimiento hecho.
- El IA debe encontrarse en estado de espera de la respuesta.

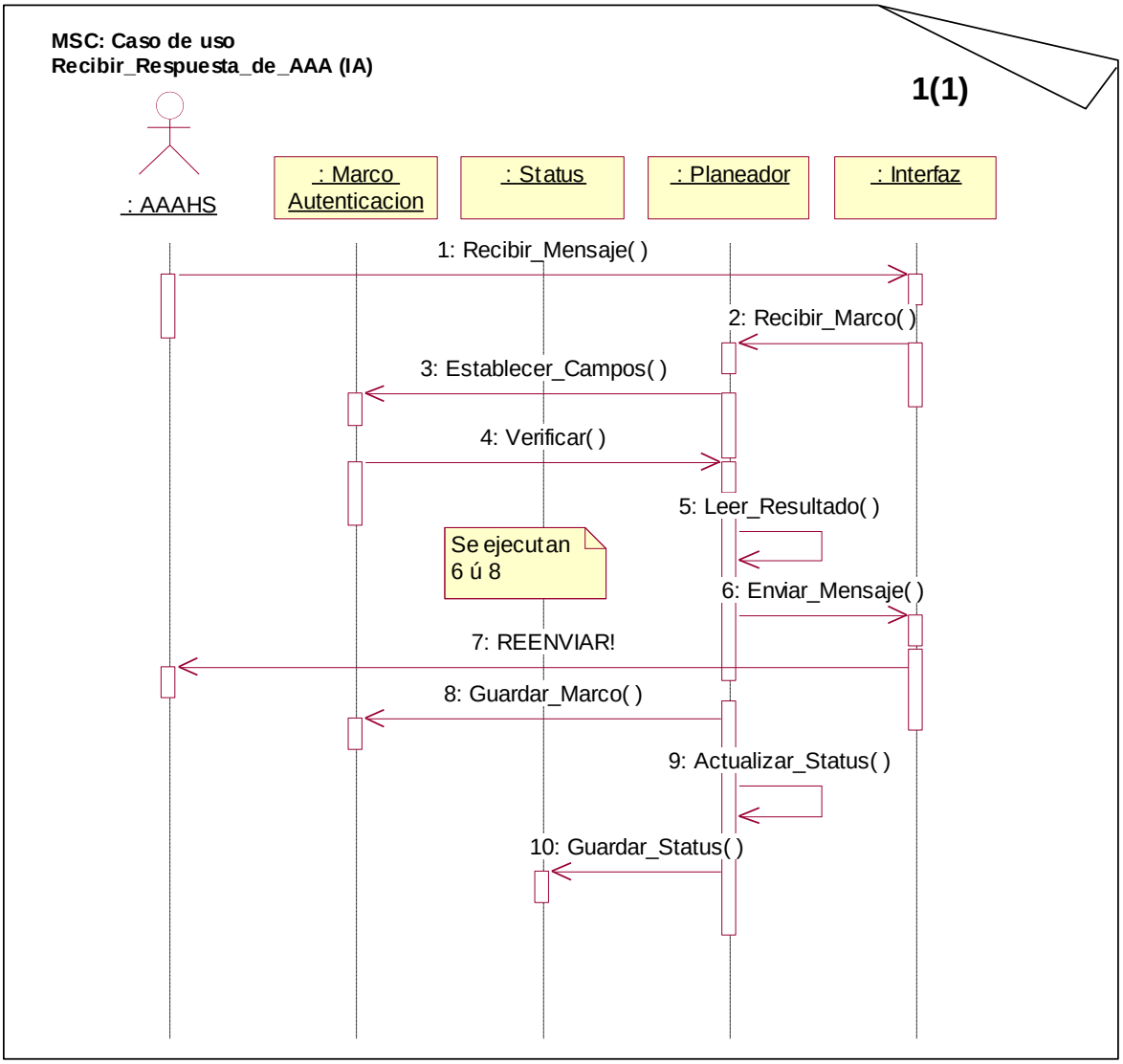
Flujo principal:

- El caso de uso comienza cuando el AAAHS entrega al IA la *Respuesta de Autenticación* para informar al AAAFS el registro del MN.

- El IA verifica esta información en cuanto a la estructura del requerimiento más no en cuanto a su validez.
- Dependiendo del resultado de las operaciones anteriores, se continúa con la ejecución del flujo principal o se solicita de nuevo la información requerida.
- Una vez validados correctamente los datos, esta información es guardada por el agente y se inicializa el transporte de los datos (*Respuesta de Autenticación)* activando el caso de uso Transportar_Datos_de_AAA.







Caso de uso: Entregar_Respuesta_de_AAA.

Actores: Ninguno. El caso de uso es inicializado por el caso de uso Transportar_Datos_de_AAA con el cual tiene una relación *Extend*.

Propósito: Permitir al IA entregar la *Respuesta de Autenticación* generada por el AAAHS al AAAFS.

Resumen: El IA ha llegado al AAAFS y ha reanudado su ejecución. Este caso de uso es activado por el caso de uso Transportar_Datos_de_AAA. El IA hace un reconocimiento de su destino, pasa la información (*Respuesta de Autenticación*) al AAAFS y queda en un estado de espera de cualquier otra solicitud hecha bien sea por el AAAFS o por el AAAHS.

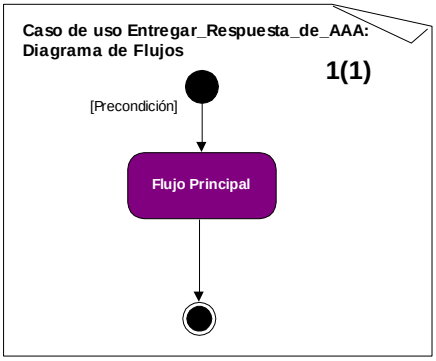
Tipo: Primario.

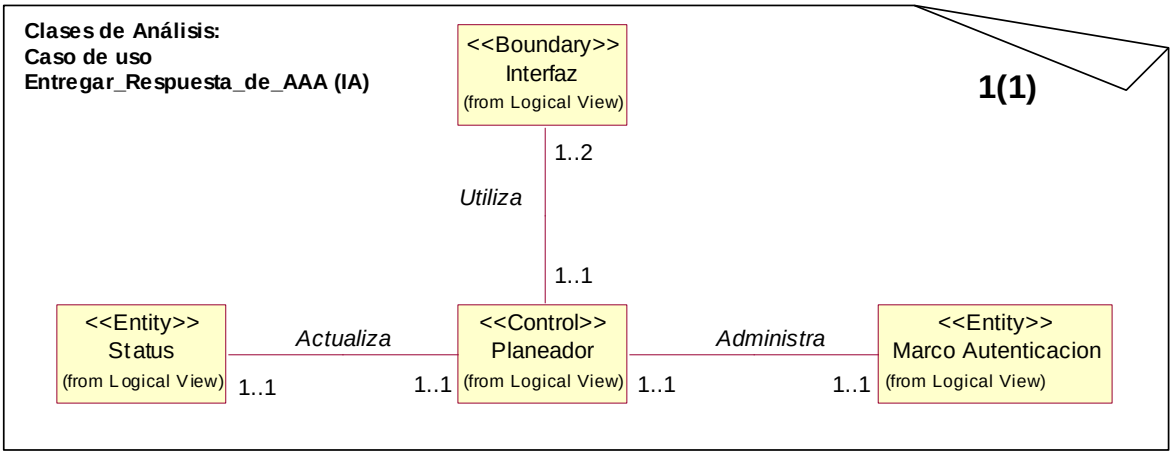
Referencias *Funciones:* R1.5.2.1, R1.5.2.2, R4.9.

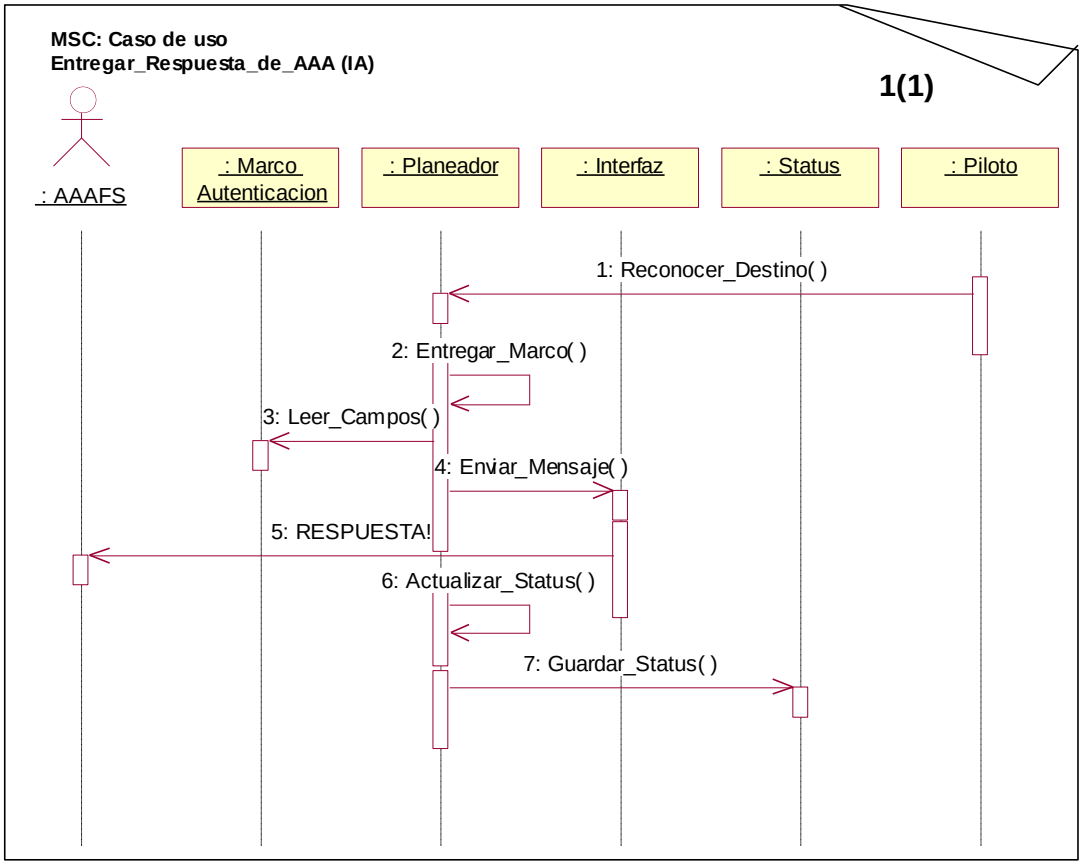
cruzadas *Casos de uso:* Transportar_Datos_de_AAA.

Pre-condiciones:
- El sistema debe haber ejecutado previamente el caso de uso Transportar_Datos_de_AAA.

Flujo principal:
- El caso de uso es inicializado por el caso de uso Transportar_Datos_de_AAA cuando el IA ha llegado al AAAFS.
- El IA pasa la *Respuesta de Autenticación* al AAAFS.
- El caso de uso termina cuando el IA es colocado en un estado de espera de cualquier otra solicitud por parte del AAAFS o del AAAHS.







4.4 Diseño de los Agentes Móviles

4.4.1 Clases de diseño

A continuación se muestran los diagramas de las clases que implementan los dos agentes y sus relaciones (asociaciones). El código y las estructuras de datos que implementan cada operación y atributo respectivamente se encuentra en el Anexo A.

4.4.1.1 Clases de diseño para el Foreign Agent (FA):

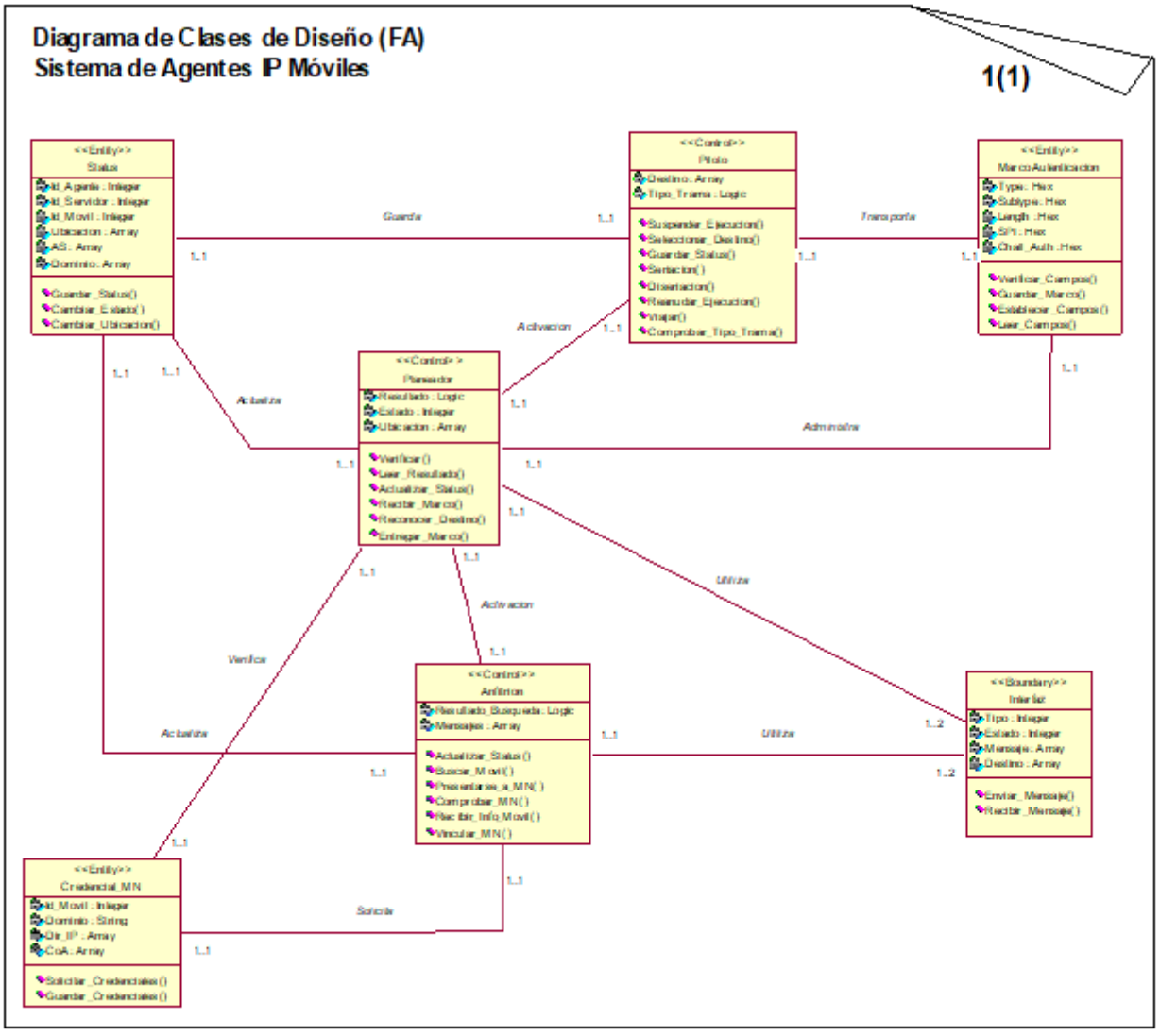


Figura 4.5 Diagrama de clases de Diseño (FA)

4.4.1.2 Clases de diseño para el Intermediary Agent (IA):

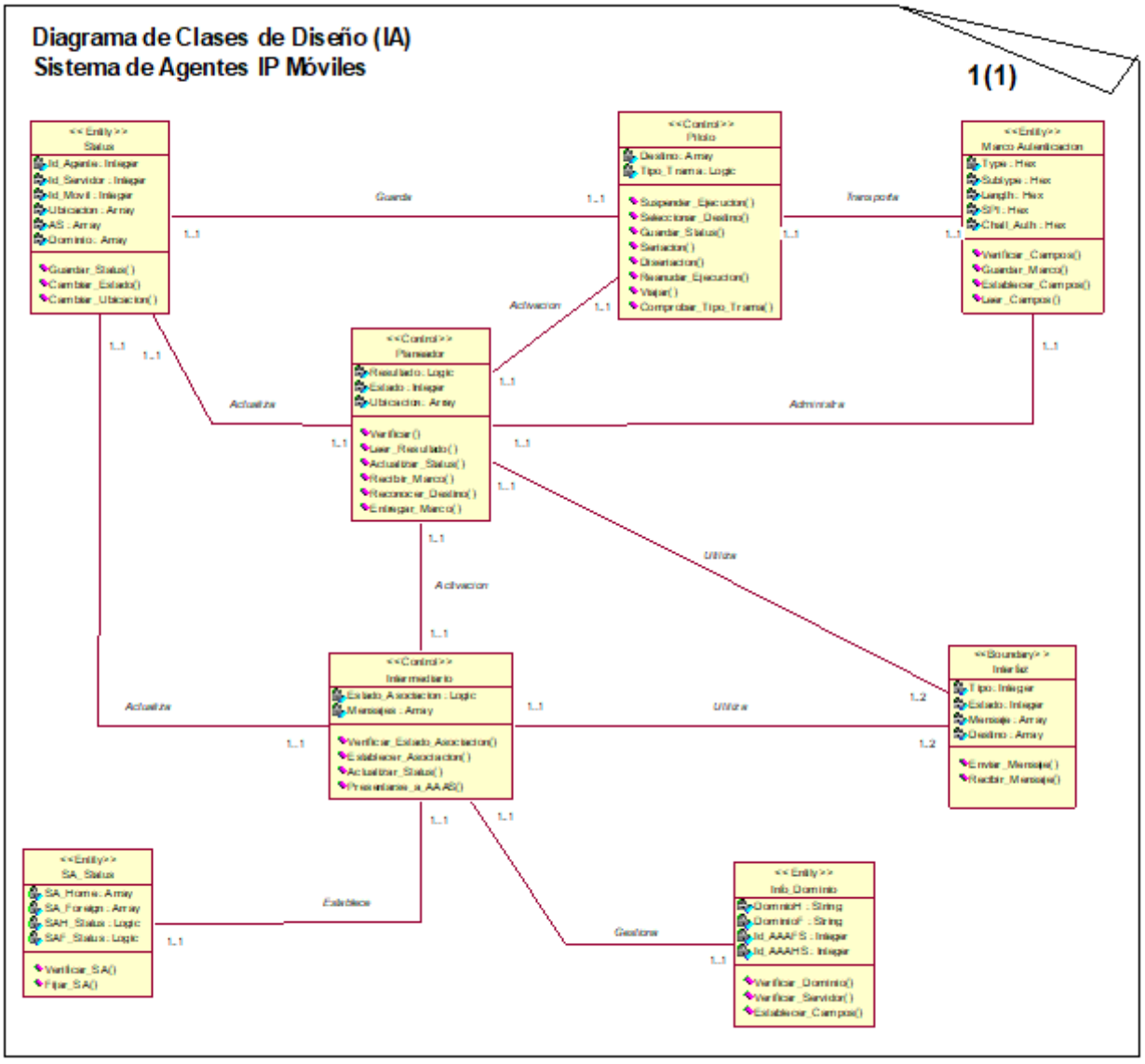


Figura 4.6 Diagrama de Clases de Diseño (IA)

4.4.2 Diagrama subsistemas e interfaces

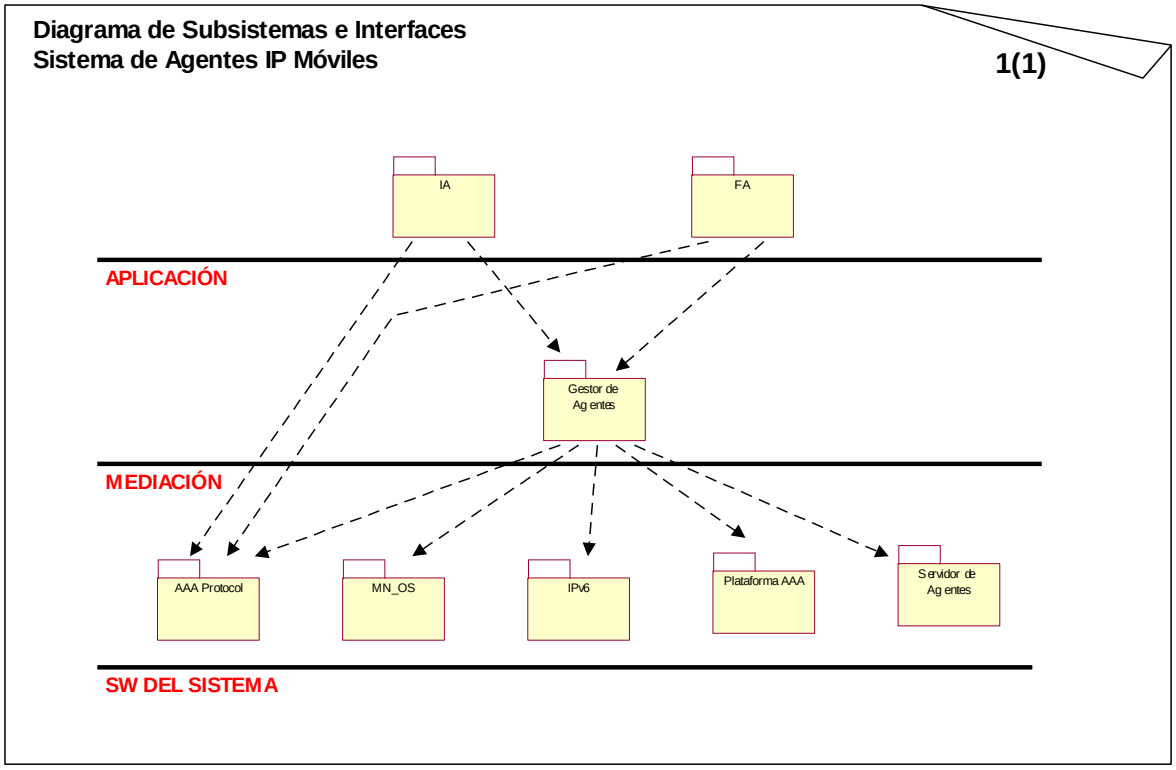


Figura 4.7 Diagrama de Subsistemas e Interfaces

4.4.3 Diagrama de implantación

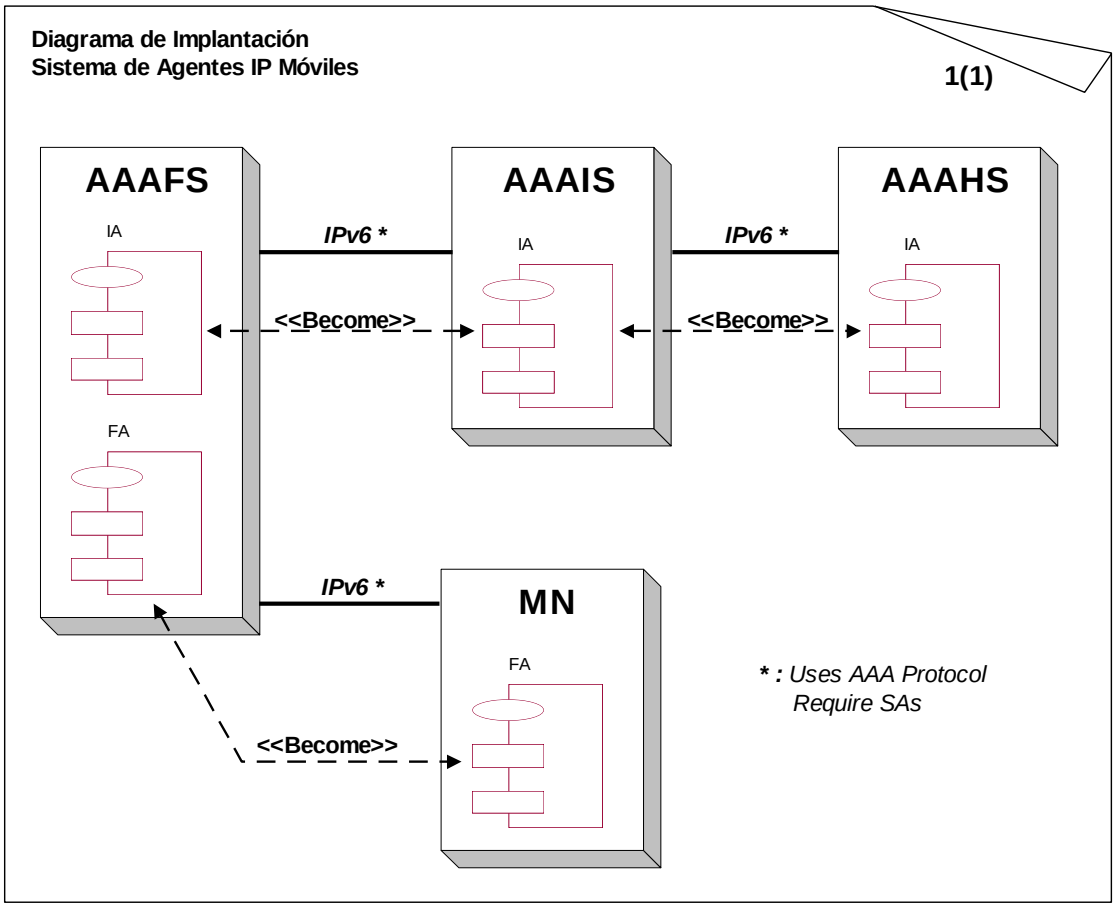


Figura 4.8 Diagrama de Implantación

CONCLUSIONES Y RECOMENDACIONES

- Las especificaciones para la aplicación de esta tecnología abarcan los procesos desde un alto nivel de abstracción haciendo compleja la formulación de modelos significativamente aplicables considerando que estamos en un entorno académico.

- Parte de la dificultad de llevar el modelo propuesto a las fases de implementación y prueba, radica en que la manera como se llevan a cabo dichas fases depende significativamente de tecnologías propietarias. Estas fases tienen elevados requerimientos a nivel de infraestructura e información técnica a las cuales no se tiene acceso en este momento, lo cual hace que dichos desarrollos correspondan más a actividades a nivel de empresa que a nivel de academia.

- Desde el punto de vista del usuario los requerimientos para 3G van mucho más allá del tipo de servicios y la velocidad con que se prestan, siendo indispensable proveer sistemas seguros y confiables que garanticen la integridad de la información, ya que al ser mayor el número de usuarios y la importancia de los datos a transportar, aumenta el peligro de intromisiones y merodeadores que puedan poner en riesgo la correcta prestación de los servicios. Por consiguiente, a pesar de que se exige como mínimo un nivel de seguridad igual al brindado por las redes celulares actuales es evidente la necesidad de que esta sea mucho mayor, ya que son bien conocidos los inconvenientes que existen en este tipo de redes, inconvenientes que serian mucho más críticos en la nueva generación de sistemas móviles.

- Para lograr el ambiente de movilidad y compatibilidad deseado para los Sistemas de Tercera Generación se hace necesario que conjuntamente con los esfuerzos tecnológicos se realicen grandes esfuerzos cooperativos por parte de los

diferentes actores en dicho campo, los cuales deben estar encaminados hacia la consecución de los objetivos planteados para esta nueva tecnología.

- A partir de la investigación realizada se puede concluir que la tecnología de Agentes Móviles se convierte en una buena opción para descargar trabajo de los equipos servidores y relegar inteligencia fuera de ellos, gracias a las capacidades de procesamiento que poseen y a sus características de movilidad y capacidad de decisión podrán llevar a cabo labores medianamente complejas sin que exista la necesidad de que los clientes móviles tengan que dialogar directamente con los servidores encargados de prestar el servicio, sino que simplemente se entenderán con el Agente delegado para atenderlos, el cual servirá de puente entre éste y el correspondiente servidor, disminuyendo en forma considerable la congestión en los equipos principales.

- La utilización de Agentes Móviles en procesos relacionados con la prestación de servicios en los Sistemas de Tercera Generación brinda ventajas adicionales tales como:

    - Gran tolerancia a fallas puesto que los agentes reaccionan a situaciones desfavorables.
    - Reducción en el tiempo de utilización de la red ya que los Agentes actúan solo en los momentos en que es indispensable hacerlos y sus características les permite cambiar de su estado de ejecución a un estado de espera activa.
    - Posibilidad de utilizar los ambientes en diferentes ambientes.

- Las características de movilidad y la implementación de los procesos AAA se ven ampliamente beneficiados por las ventajas que traerá consigo la nueva versión del Protocolo de Internet (IPv6), especialmente en lo que a la movilidad se refiere (IPv6 Móvil), ya que gran parte del desarrollo planteado a lo largo de este proyecto tiene como sustento este protocolo el cual ha sido diseñado para cubrir las deficiencias que tenia la versión anterior en el área de la movilidad, adicionalmente a esto dicho protocolo permite un nivel de mayor seguridad.

- El modelado presentado se realizó teniendo en cuenta los parámetros y la regulación establecida hasta ahora para los Sistemas de Tercera Generación, sin embargo, es bueno recordar que en el campo de las Telecomunicaciones los cambios en la normatividad se dan de forma paralela con el desarrollo tecnológico y fácilmente se pueden presentar grandes diferencias en la forma en que se conciben los procesos, por lo tanto es sumamente importante que en el momento de desarrollar una implementación basada en el contenido de esta monografía se revise el estado de dicha normatividad de tal forma que el trabajo a realizarse esté lo más acorde posible con las necesidades y requerimientos tecnológicos del momento.

- Se recomienda que las futuras implementaciones sean realizadas en un lenguaje de programación compatible con las diferentes arquitecturas en las cuales tendrán que interactuar los sistemas, teniendo presente siempre que son redes de carácter global y con un alto grado de movilidad.

ACRÓNIMOS

3GPP: 3G Partnership Project – Proyecto de Asociación para 3G

AAA: Authentication, Authorization and Accounting - Autenticación, Autorización y Tarificación

AEP: Agent Ejecution Plataform - Plataforma de Ejecución de Agentes

AAAFS: AAA Foreign Server - Servidor AAA Foráneo

AAAIS: AAA Intermediary Server - Servidor AAA Mediador

AAAHS: AAA Home Server - Servidor AAA Local

AMP: Agent Meeting Places - Lugares de Reunión de Agentes

AMPS: Advanced Mobile Phone System – Sistema Avanzado de Telefonía Móvil

API: Application Program Interface - Interfaz de Programa de Aplicación

AAAS: AAA Server - Servidores AAA

B2B: Business to Business - Negocio a Negocio

B2C: Business to Consumer - Negocio a Consumidor

CDMA: Code Division Multiple Access - Acceso Múltiple por División de Código

CDPD: Cellular Digital Packet Data - Transmisión Digital de Paquetes en Redes Móviles

CI: Communication Infrastructure - Infraestructura de Comunicación

CN: Central Network - Red Central

CORBA: Common Object Request Broker Architecture - Arquitectura Genérica para Mediación de Requerimientos de Objetos

CPU: Central Processing Unit - Unidad Central de Procesamiento

DoS: Denial of Service - Negación de Servicio

FA: Foreign Agent - Agente Foráneo

GSM: Global System for Mobile Communications - Sistema Global para Comunicaciones Móviles

HA: Home Agent - Agente Local

***HLR**: Home Location Register - Registro de Localización Local*

http:: HiperText Transfer Protocol - Protocolo de Transferencia de Hypertexto

IA: Intermediary Agent - Agente Intermediario

IETF: Internet Engieneering Task Force - Fuerza de Tareas de Ingeniería de Internet

IKE: Internet Key Exchange - Intercambio de Llaves en Internet

InA: Intelligent Agent - Agente Inteligente

IP: Internet Protocol - Protocolo de Internet

IPSec: IP Security - Seguridad IP

ISDN: Integrated Services Digital Network - Red Digital de Servicios Integrados

ISP: Internet Service Provider - Proveedor de Servicio de Internet

ITU: International Telecommunications Union - Unión Internacional de Telecomunicaciones

KDC: Key Distribution Center - Centro de Distribución de Llaves

MASIF: Mobile Agent System Interoperability Facility - Facilidades para la Interoperabilidad entre Sistemas de Agentes Móviles

MN: Mobile Node - Nodo Móvil

MT: Mobile Terminal - Terminal Móvil

NAI: Network Access Identifier - Identificador de Acceso de Red

NMT: Nordic Mobile Telephone Network - Red Nórdica de Teléfonos Móviles

OMG: Object Management Group - Grupo para la Gestión de Objetos

PCS: Personal Communicatios Services - Servicios de Comunicaciones Personales

PDC: Personal Digital Cellular - Móvil Digital Personal

PDSN: Packet Data Serving Node - Nodo Servidor de Paquetes de Datos

PLMN: Public Land Mobile Network - Redes Móviles de Carácter Público

PSTN: Public Switching Telephone Network - Red Telefónica Pública Conmutada

QoS: Quality of Service - Calidad de Servicio

RAN: Radioelectric Access Network - Red de Acceso Radioeléctrico

RFC: Request for Coments - Petición de comentarios

RMI: Remote Method Invocation - Método de Invocación Remota

RN: Radio Network - Red Radio

RNC: Radio Network Controller - Controlador de la Red Radio

RP: Remote Programming - Programación Remota

RPC: Remote Procedure Call - Llamadas a Procedimientos Remotos

RUP: Rational Unified Process - Proceso Unificado de Rational

SA: Security Association - Asociación de Seguridad

SIM: Subscriber Identity Module - Módulo de Identificación de Abonado

SIP: Session Initiation Protocol - Protocolo de Iniciación de Sesión

SIP NE: SIP Network Entity – Entidad de Red SIP

SPI: Security Parameters Index - Indice de Parámetros de Seguridad

TACS: Total Access Communication System - Sistema de Comunicación de Acceso Total

TCP/IP: Transmission Control Protocol/Internet Protocol - Protocolo de Control de Transmisión/Protocolo de Internet

TDMA: Time Division Multiple Access - Acceso Múltiple por División de Tiempo

UE: User Equipment - Equipo de Usuario

UIM: User Indentity Module - Módulo de Identidad de Usuario

UML: Unified Modeling Language - Lenguaje de Modelamiento Unificado

UMTS: Universal Mobile Telecommunications System - Sistema Universal de Telecomunicaciones Móviles

UMTS-AKA: UMTS Authentication and Key Agreement - Protocolo de Autenticación y Acuerdo de Llaves en UMTS

UWC: Universal Wireless Comunications – Comunicaciones Inalámbricas Universales

VLR: Visited Location Register - Registro de Localización Visitante

WAN: Wide Area Network - Redes de Area Amplia

WAP: Wireless Application Protocol - Protocolo de Aplicaciones Inalámbricas.

GLOSARIO

3GPP: *(3G Partnership Project)*. Proyecto de Asociación para 3G. Organización conformada por fabricantes y entidades reguladoras del sector de las telecomunicaciones para la evolución y estandarización de los Sistemas 3G.

Agente Inteligente: Es un programa que puede actuar en nombre de un usuario o de otro programa y puede hacer esto con cierto grado de independencia.

Agente Móvil: Es un Agente que no está limitado al sistema donde se inició su ejecución, siendo capaz de transportarse de una máquina a otra a través de la red. Esta posibilidad le permite interactuar con el objeto deseado de forma directa sobre el sistema de agentes donde se halla dicho objeto.

Amenaza. Una amenaza es toda acción, operación o hecho no autorizado que podría afectar adversamente al sistema. Involucra la determinación de cualquier tipo desautorizado de acceso, cambio, destrucción, revelación, interrupción, bloqueo o hurto de los medios que constituyen el sistema.

AMPS: *(Advanced Mobile Phone System)* Sistema Avanzado de Telefonía Móvil. Estándar americano para servicios móviles de carácter analógico.

Analógico: Método de transmisión de señales en el cual la información se transmite alterando de manera continua la forma de ondas electromagnéticas. Utilizado en radio AM, FM y la mayoría de circuitos de voz.

Ancho de banda: Medida de la capacidad de una conexión troncal de una red o de un canal de radio. Es la anchura o diferencia entre las frecuencias de transmisión más alta y baja de una banda. Cuanto mayor es el ancho de banda, más información se puede transmitir de forma simultánea.

Asociación de Seguridad (SA: Security Association): Una asociación de seguridad es un conjunto de información de seguridad relacionada con una conexión.

Autenticación: Proceso mediante el cual se verifica una identidad exigida, en la forma de una etiqueta pre-existente a partir de un campo "nombre", el cual es mutuamente conocido. Por ejemplo, verificar el creador de un mensaje (autenticación de un mensaje) ó verificar el punto final de un canal de comunicación (autenticación de entidad).

Autorización: Proceso mediante el cual se determina si se posee un derecho específico. Por ejemplo, determinar si el acceso a algún recurso puede concederse al ponente de una credencial particular.

Banda ancha: Este término tiene varios significados, aunque originalmente se utilizó para describir un canal con un ancho de banda mayor que el de un canal con calidad de audio, que normalmente es un circuito de 48 KHz.

Bps: Bits (transmitidos) por Segundo. Unidad que sirve para medir la velocidad a la que se están transmitiendo los datos de una señal por un circuito o sistema.

Caballo de Troya: Un "Caballo de Troya" es un programa o archivo que suplanta a otro cumpliendo, además de la función que el programa original cumple, otras que son invisibles para el usuario, y que pueden comprometer la seguridad del servidor.

CDMA: *(Code Division Multiple Access)* Acceso Múltiple por División de Código. Tecnología celular que no asigna una frecuencia específica a cada usuario, sino que cada canal utiliza un espectro completamente disponible. Las conversaciones individuales se codifican usando códigos ortogonales.

CDPD: *(Cellular Digital Packet Data)* Transmisión Digital de Paquetes en Redes Móviles. Servicio digital de datos de alta velocidad que permite la transmisión de éstos sobre la capacidad desaprovechada de una red celular analógica.

Comunicaciones Celulares: Las comunicaciones celulares son una tecnología de comunicaciones inalámbricas en donde las áreas de comunicación se dividen en pequeñas secciones llamadas celdas y en las que las transmisiones pasan de celda a

celda hasta que llegan a los destinatarios. Cada celda contiene una antena y dispositivos que permiten recoger información y pasarla de una celda o de un emisor a otro.

Challenge: Número al azar generado por un Nodo Móvil, el cual será utilizado para computar los datos de Autenticación.

Cliente/servidor: Modelo de trabajo en una red en el que el procesamiento se reparte entre muchos computadores (clientes) y un computador central (servidor), que almacena los ficheros y datos que se pueden compartir entre todos los "clientes".

Comunicaciones fijas: Comunicaciones en las cuales los usuarios de los terminales no disponen de movilidad.

Comunicaciones inalámbricas: Comunicaciones que no requieren hilos de conexión, cables o fibra. Los sistemas emplean radiofrecuencias para transmitir voz, datos o vídeo.

Comunicaciones móviles: Son un tipo de comunicaciones inalámbricas o por radio que permiten a los usuarios acceder a los servicios sin tener que encontrarse en una ubicación determinada, brindando de esta manera una gran movilidad.

CORBA: *(Common Object Request Broker Architeture)* CORBA es una arquitectura y especificación para crear, distribuir y gestionar programas de objetos distribuidos en una red. Esto permite que programas en diferentes entornos y desarrollados por diferentes vendedores se comuniquen en una red a través de una interfaz “broker”.

Criptografía: Es la técnica de convertir un texto inteligible, texto en claro (plaintext), en otro llamado criptograma (ciphertext) cuyo contenido de información es igual al anterior pero sólo lo pueden entender las personas autorizadas.

DECT: *(Digital Enhanced Cordless Telecommunications)* Norma de comunicaciones por medio de terminales sin cables y que mejora la calidad de transmisión de voz.

Digitalización: Conversión de la información en bits de datos para que se transmitan a través de cables, fibra óptica, cable de fibra óptica, o de manera inalámbrica.

Dominio Administrativo: Es una intranet o una colección de redes, computadores y bases de datos bajo una administración común. Se pude asumir que las entidades computacionales operan en una administración común y comparten las asociaciones de seguridad creadas administrativamente.

Dominio Local: Es un dominio administrativo que contiene la infraestructura de Autenticación, Autorización y Tarificación (AAA: Authentication, Authorization and Accounting) de interés inmediato para un cliente IP móvil cuando está fuera de casa.

Dominio Foráneo: Es un dominio administrativo visitado por un cliente móvil IP, y contiene la infraestructura necesaria para soportar las operaciones que conlleven a habilitar el registro del móvil IP.

Encriptación: Conversión de una comunicación en un mensaje codificado por razones de seguridad y privacidad.

GSM: *(Global System for Mobile Communications)* Sistema Global para Comunicaciones Móviles. Estándar paneuropeo para redes de telefonía móvil digital que permite itinerancia a través de las fronteras de los países.

HandOff: Proceso mediante el cual se le sigue proveyendo servicio a un móvil que cambia de celda, pero que permanece dentro del dominio del mismo operador.

Host: En Internet, el término “host” hace referencia a cualquier computador que tenga acceso total bidireccional a otros computadores en la red. Un host tiene un número local específico, que junto con el número de red forman una dirección IP única.

IPSec: Mecanismos de seguridad definidos dentro del protocolo IP.

ITU: *(International Telecommunications Union)* Organización con sede en Ginebra responsable de la estandarización en el campo de las telecomunicaciones.

Mbps: Megabits por segundo. Estándar de medida de la velocidad de transmisión de datos equivalente a un millón de bits por segundo.

NMT: *(Nordic Mobile Telephone Network)* Red Nórdica de Teléfonos Móviles. El primer sistema celular en el mundo que entró en servicio.

Nodo Móvil: *(MN)* Dispositivo que se desplaza a través de los diferentes dominios de la red.

OMG: *(Object Management Group)* Organización fundada en 1989 por un grupo de vendedores con el propósito de crear una arquitectura estándar para objetos distribuidos en redes. La arquitectura resultante es CORBA:

PCS: *(Personal Communicatios Services)* Servicios de Comunicaciones Personales. Es un paquete de servicios avanzados que incorpora el concepto de teléfono único global, y que ofrece la característica de diferenciar servicios y facturación.

PDC: *(Personal Digital Cellular)* Móvil Digital Personal. Estándar japonés para telefonía móvil digital. Hasta el momento, este estándar es utilizado sólo en Japón, pero se podría difundir a otros países.

Prestación de seguridad: Es un proceso que brinda cierto grado de protección contra una o varias posibles amenazas a la seguridad.

Procesos AAA: Procesos de Autenticación, Autorización y Tarificación (Authorization, Authentication and Accounting), indispensables para la prestación de un servicio.

Red: Diferentes puntos interconectados por medio de canales de telecomunicaciones.

RDSI: *(Red Digital de Servicios Integrados)* Tecnología que ofrece transmisión de múltiples servicios (voz, datos, imágenes y vídeo) a alta velocidad, a través de una infraestructura de líneas fijas.

RFC: *(Request for Coments)* Petición de comentarios. Son una serie de informes técnicos los cuales son almacenados en línea y pueden ser recuperados por cualquier interesado.

Roaming: Situación en la cual un Nodo Móvil se encuentra dentro de una celda que corresponde al dominio administrativo de un operador distinto a su proveedor de servicios original.

SIM: *(Subscriber Identity Module card)* Módulo de Identificación de Abonado. Un SIM es un pequeño circuito impreso que se debe insertar en cualquier teléfono móvil basado en GSM cuando se enciende el teléfono. Se utiliza para personalizar las características del terminal; contiene información relativa al abonado y de seguridad, así como la memoria que albergará una lista de teléfonos personal; todo ello debidamente encriptado dentro del sistema GSM. La tarjeta puede tener formato de circuito para insertar en reducidas dimensiones, o de tamaño de tarjeta de crédito, pero en ambos casos posee la misma funcionalidad.

TACS: *(Total Access Communication System)* Sistema de Comunicación de Acceso Total. Estándar de telefonía móvil analógica en el rango de frecuencia de 900 Mhz.

Tarificación: Proceso consistente en recolectar información sobre el uso de un determinado recurso con el propósito de analizar tendencias, realizar auditorias, facturar, o asignar el costo por el uso del servicio.

TCP/IP: *(Transmission Control Protocol/Internet Protocol)* Protocolo de Control de Transmisión/Protocolo de Internet. TCP/IP, desarrollado en 1974, es el principal protocolo empleado para la transmisión de información en Internet en la actualidad.

Tercera generación (3G): Es el término genérico utilizado para la próxima generación de sistemas de comunicaciones móviles. Los Sistemas 3G proporcionarán servicios que aumentarán las capacidades de aquellos disponibles hoy en día (voz, texto y datos), al igual que un sinnúmero de servicios multimedia que no estaban disponibles anteriormente para los usuarios móviles.

TimeStamp: Etiqueta de tiempo impuesta a determinada información para indicar su tiempo de vida o validez.

Tunelling: El tunelling o entunelamiento proporciona un mecanismo para utilizar la infraestructura de una tecnología para transmitir otra diferente. Por ejemplo, utilizar la infraestructura de X.25 para transmitir información IP.

WAP: *(Wireless Application Protocol)* Protocolo de Aplicaciones Inalámbricas. La finalidad de esta nueva tecnología, es ofrecer servicios y contenidos de Internet a través de conexiones inalámbricas, siendo concebida para pantallas pequeñas y navegación sin teclado.

REFERENCIAS

Publicaciones

1. [Crystaliz 1997] Crystaliz. 1997. Mobile agent facility specification. *Propuesfo* (UTILIZA, Junio)

2. [Ghezzi y Vigna 1994] Ghezzi, C. y Vigna, G. 1994. Mobile code paradigms and technologies: a case study. Reporte Tecnico. Depto. De Electrónica e Información, Politécnico de Milano.

3. [Goldszmidt y Yemini 1995] Goldszmidt, G. y Yemini, Y. 1995. Distributed management by delegation. *En Procedimientos de la 15ª Conferencia Internacional sobre Sistemas de Computación Distribuida* (Los Alamitos. CA., IEEE Computer Society), 333-340.

4. [Gray 1995a] Gray, R., Kotz, D., Nog, S., Rus, D. y Cybenko, G. 1995. Mobile agents for mobiling computing. Reporte técnico PCS-TR96-285, Departamento de Ciencias de la Computación, Dartmouth College, Hanover, New Hampshire 03755, Mayo.
ftp://ftp.cs.darthmouth.edu/TR/TR96-285.ps.Z.

5. [Hylton et al. 1996] Hylton, J, Manheimer, K., Warsaw, B., Masse, R. y Rossum, G. - 1996. Knowbo1 programming: system support for mobile agents. Procedimientos del 5º Taller Internacional sobre Orientación a Objetos en Sistemas Operativos (IWOOOS 96, Oct.), 8-13.

6. [Johansen et al.1995] Johansen, D., Renesse, R. y Schneider, F. 1995a. Operating system support for mobile agents. Procedimientos del 5º Taller de la IEEE sobre Tópicos Importantes en Sistemas Operativos (HOTOS-V, Mayo), 42-45.

7. [Kato et al. 1997] Kato, K., Toumura, K., Matsubara, K., Aikawa, S., Joshida, J., Kono, K., Taura, K. y Sekiguchi, T. 1997. Protected and secure mobile object computing in Planet. Reporte Tecnico. Ciencias de la Información y Electrónicas, Universidad de Tsukuba, Tsukuba, Japon.

8. [Knabe 1995] Knabe, F. C. 1995. Language support for mobile agents. Disertación Doctoral. CMUCS-95-223. Escuela de Ciencias de la Computación, Universidad Carnegie Mellon, Pittsburgh, PA 15213, Diciembre.

9. [Kotay y Kotz 1994] Kotay, K. y Kotz, D. 1994. Transportable Agents. Procedentes del Taller del CIKM sobre Agentes de Información Inteligentes, Tercera Conferencia Internacional sobre Información y Gestión del Conocimiento (CIKM 94, Diciembre).

10. [Lange 1997] Lange, D. 1997. Java aglet application programming interface (J-AAPI) White paper. 2da. Propuesta. Laboratorio IBM de Desarrollo. Tokyo, Japón. http://www.trl.ibm.co.jp/aglets.

11. [Lingnau et al. 1995] Lingnau, A., Drobnik, O. y Domel, P 1995. An HTTP-based infrastructure for mobile agents Procedentes de la 4a Conferencia Internacional sobre WWW (December), 1995. Publicación electrónica disponible en http://www.w3.org/pub/Conferences/WVVVV4/Papers/150/

12. [Nwana 1996] Nwana, H.S., *The Potential Benefits of Software Agent Technology to BT*. Reporte Técnico Interno, Proyecto NOMADS, Desarrollo de Sistemas Inteligentes, AT&T, BT Labs, UK. 1996

13. [Reza et al. 1996] Reza, A., Tabatabai A., Langdale, G., Lucco, S. y Wahbe R. 1996. Efficient and language independet mobile programs. Conferencia sobre Lenguajes de Programación, Diseño e Implementación (PLDF '96 ACM SIGPLAN'96, Philadelphia. PA., Mayo).

14. [Sanchez 1997]Sánchez, J. A. 1997. A taxonomy of agents. Reporte técnico. ICT-97-1. Laboratorio de Tecnologías Interactivas y Cooperativas. Universidad de las Américas Puebla, Cholula, Pue. 72820.

15. [Stone et al. 1996] Stone, S., Zyda, M., Brutzman, D. y Falby, J. 1996. Mobile agents and smart networks for distributed simulations. Reporte Tecnico. Departamento de Ciencias de la Computación, Escuela Naval de Postgraduados, Monterey, California 93943-5118.

16. [Straber et al. 1996] Straber, M., Baumann, J. y Hohl, F. 1996 . Mole- A Java based mobile agent system. Reporte Tecnico. Instituto para Sistemas de Computación Paralela y Distribuida, Universidad de Sttutgart, Breitwiesenstrabe 20-22, D-70565 Stuttgart, Octubre. (publicacion electronica disponible en http://www. inforrnatik.uni-sttutgart. de/ipvr/vs/projecte/mole.html

17. [Vitek 1996] Vitek, J. 1996. Secure object spaces. Reporte Tecnico. Grupo de Sistemas Objeto, Universidad de Geneva. Geneva, Switzerland

18. [White 1996] White, J. 1996. Mobjle Agents W~ire Paper. Reporte Tecnico. AAA1 Press. The MlT Press., General Magic, Menlo Park. California.

Recomendaciones, drafts y RFCs

1. Recomendación UIT-R M.1078. Principios de Seguridad para las Telecomunicaciones Móviles Internacionales – 2000 (IMT-2000)
2. Recomendación UIT-R M.1223. Evaluación de los Mecanismos de Seguridad para las IMT-2000

3. AAA Solutions
4. Authentication_ Authorization_ and Accounting (Protocol Evaluation)
5. draft-le-mobileip-authreq-00
6. draft-hiller-cdma2000-aaa-02
7. draft-ietf-aaa-proto-eval-02
8. draft-ietf-mobileip-3gwireless-ext-05
9. draft-ietf-mobileip-aaa-reqs-04
10. draft-ietf-mobileip-ipv6-13

11. draft-kroeselberg-sip-3g-security-req-00
12. draft-mkhalil-mobileip-ipv6-handoff-00
13. rfc1752 - The Recommendation for the IP Next Generation Protocol
14. rfc2002 - IP Mobility Support
15. rfc2543 - SIP Session Initiation Protocol
16. rfc2903 - Generic AAA Architecture
17. rfc2905 - AAA Authorization Application Examples
18. rfc2906 - AAA Authorization Requirements
19. rfc2977 - Mobile IP Authentication, Authorization, and Accounting Requirements

Direcciones de Internet

Internet Engineering Task Force (IETF): http://www.ietf.org
Unión Internacional de Telecomunicaciones: http://itu.org
Foro IPv6 (Ipv6 Forum): http://www.ipv6forum.com
Sociedad de Agentes (The Agent Society): http://www.agent.org
3GPP: http://www.3gpp.org
Grupo de Gestión de Objetos (Object Management Group): http://www.omg.org
IEEE: http://www.ieee.org
Foundation for Intelligent Agents: http://drogo.cselt.stet.it/fipa/
Ericsson: http://www.ericsson.com
Nokia: http://www.nokia.com
Rational: http://www.rational.com
Universidad de Puebla (Mexico): http://ict.pue.udlap.mx
Wapeton: http://www.wapeton.com
Canal TI: http://www.canalti.com
Google: http://www.google.com