NORMAS DE SEGURIDAD EN REDES UMTS

John Agustín Sucre Veliz (1), Roberth Oswaldo Campoverde Hidalgo (2)
Facultad de Ingeniería en Electricidad y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo, Km 30.5 Vía Perimetral
Apartado 09-01-5863. Guayaquil, Ecuador
jsucre@fiec.espol.edu.ec (1), rcampove@fiec.espol.edu.ec (2)
Ing. Washington Medina
wmedina@espol.edu.ec

Resumen

Las Normas de Seguridad en Redes UMTS (Sistema Universal de Telecomunicaciones Móviles) fueron diseñadas con la finalidad de que los usuarios que adoptan esta tecnología no sufran de amenazas en la confidencialidad de envío y recepción de información, estas normas han sido perfeccionadas desde 1986 mediante numerosos países por medios de organizaciones que son encargadas de regularlas. Algunas veces las normas de seguridad no son muy explicativas y requieren de una dedicación y experiencia para su comprensión. Por esta razón se considera conveniente disponer de un documento que facilite su lectura para un rápido entendimiento. El objetivo de nuestra investigación es facilitar la comprensión de forma gráfica al lector interesado, acerca de las arquitecturas tratadas en las normas de la serie 33"Aspectos Relativos a la Seguridad en el Sistema UMTS", donde detallamos los procedimientos de seguridad en cada una de arquitecturas de esta Tecnología móvil 3G.

Palabras Claves: *Seguridad en Redes UMTS, características de Seguridad en el Sistema UMTS,*

Abstract

The Standards of Security in Networks UMTS (Universal Mobile Telecommunication System) were designed with the finality of which the users who adopt this technology do not suffer from threats in the confidentiality of sent and receive information, these procedure have been perfected from 1986 through numerous countries by means of organizations that are entrusted to regulate. Often the safety procedure are not very explanatory and need of a dedication and experience for his comprehension. For this reason it is considered suitable to have a document that facilitates his reading for a rapid understanding. The objective of our investigation is to facilitate the comprehension of graphical form at the interested reader, about the architectures discussed in the Standards of the series 33 " Aspects Relative to the Security in the System UMTS ", where we detail the safety procedures in each of architectures of this mobile Technology 3G.

1. Introducción

UMTS (Universal Mobile Telecommunication System) es un estándar europeo desarrollado para redes móviles de tercera generación. UMTS, siglas que en inglés hace referencia a los Servicios Universales de Telecomunicaciones Móviles, es miembro de la familia global IMT-2000 del sistema de comunicaciones móviles de tercera generación de la ITU (Unión Internacional de Telecomunicaciones).

2. Fundamentos teóricos.

UMTS aparece para integrar todos los servicios ofrecidos por las distintas tecnologías y redes actuales, incluyendo Internet.

El sistema UMTS se compone de 3 grandes bloques:

- Terminales móviles (User Equipment, UE).
- Red de acceso de radio (Radio Access Network, RAN o UTRAN).
- Red central (Core Network, CN).

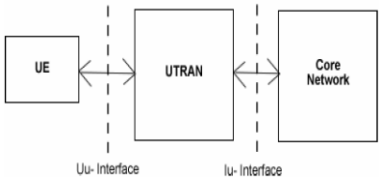

Figura 2.1 Bloques de la Arquitectura del sistema UMTS

2.1. Equipo de usuario (UE). Se denomina equipo de usuario o también llamado móvil, al equipo que trae el suscriptor para lograr la comunicación, con el bloque de la Red de acceso de Radio (UTRAN) específicamente con la estación base llamado nodo B, siempre y cuando exista cobertura en cierta área.

2.2. Red de acceso de radio (UTRAN). La UTRAN se encuentra formada por varios elementos, entre los que se encuentran los RNC (Radio Network Controller) y los Nodo B (en UTRAN las estaciones base tienen el nombre de Nodo B). Ambos elementos mencionados forman el RNS (Radio Network Subsystem)

La (UTRAN) es la red de acceso de radio diseñada especialmente para UMTS. Sus fronteras son la interfaz Iu al CN y la interfaz Uu al equipo de usuario (UE).Las interfaces internas de UTRAN incluyen la interfaz Iub la cual se encuentra entre el Nodo B y el RNC y la interfaz Iur que conecta a los RNC entre sí.

La figura 2.2 muestra los elementos UTRAN y las interfaces.

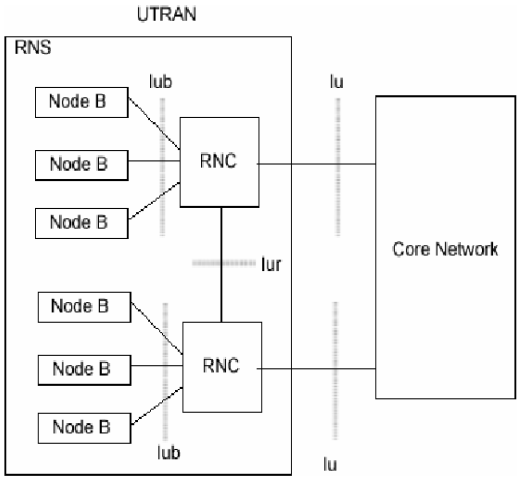

Figura 2.2 Arquitectura de UTRAN.

2.3. Red Central (CORE NETWORK). La red central también es llamada Core Network (CN) y se encuentra formada por varios elementos como el MSC (pieza central en una red basada en conmutación de circuito) y el SGSN (pieza central en una red basada en conmutación de paquetes). Realiza labores de transporte de información, tanto para tráfico como de señalización y contiene la inteligencia del sistema. A través de esta UMTS se conecta a otras redes de comunicaciones. Los elementos que conforman a la CN: HLR, VLR, AuC, EIR y centros de SMS.

Está formada por tres dominios: el de Red Servidora (Serving Network), el de Red Base (Home Network o Home Environment) y el de Red de Transporte (Transit Network).

La figura 2.3 da un mejor detalle en la descripción del sistema UMTS, donde se detalla las interfaces y los elementos que conforman a cada bloque del Sistema, incluye también la entidad de acceso a la red GSM (BSS) para clarificar la relación de estas dos tecnologías, ya que UMTS es compatible con GSM.

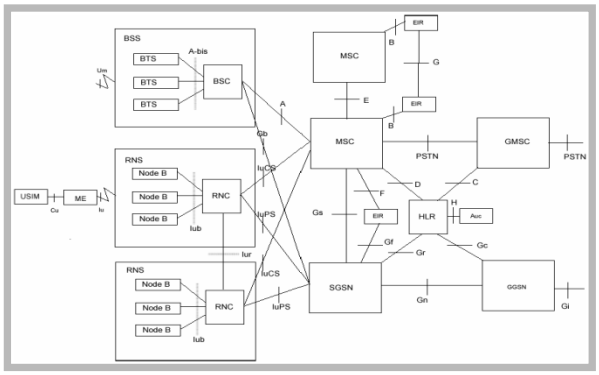

Figura 2.3 Arquitectura de UMTS.

3. Normalización de los Sistemas Móviles 3G

En la actualidad la normalización es una disciplina esencial para todos los sectores de la economía que deben esforzarse por dominar sus motivaciones e implicaciones. Hace una veintena de años, este era un área reservado a algunos especialistas. En este capítulo se describe la historia de los trabajos de normalización que conllevan a las recomendaciones para la tercera generación de los sistemas móviles terrestres, se presentan los principales organismos de normalización y describe las interfaces terrestres de radio adoptadas para los sistemas móviles de tercera generación (3G).

El estado actual de la normalización de los sistemas móviles 3G es el resultado de los trabajos llevados a cabo en numerosos países desde 1986, fecha en la que comenzaron las tareas de normalización del FPLMTS (Sistema de comunicaciones móviles de tercera generación actualmente denominado IMT-2000) iniciadas por la Unión Internacional de telecomunicaciones - Radio (UIT-R).

3.1 Organización de la Normalización IMT-200

La normalización Europea de la radio 3G alcanzó su "fase caliente" durante 1997, cuando cinco sistemas candidatos fueron considerados por el comité SMG (Grupo Especial de Móviles) del ETSI. Después de un largo debate, en enero de 1998 el ETSI SMG acordó usar finalmente la tecnología WCDMA para la interfaz aire del UTRA (Radio acceso terrestre UMTS) sobre bandas de frecuencias apareadas para el funcionamiento de las tecnologías FDD y TDCDMA (División de tiempo CDMA) y asignaciones del espectro no emparejadas para el funcionamiento del TDD. Esta decisión fue la base para la propuesta del UTRA presentada por el ETSI a la UIT como una candidata a la tecnología de transmisión radio IMT2000. Al mismo tiempo, otros países como Japón, Estados Unidos y Corea, fueron eligiendo independientemente sus propias tecnologías de acceso radio 3G, con Corea, Japón, Europa y uno de los comités norteamericanos (T1P1) seleccionando soluciones similares.

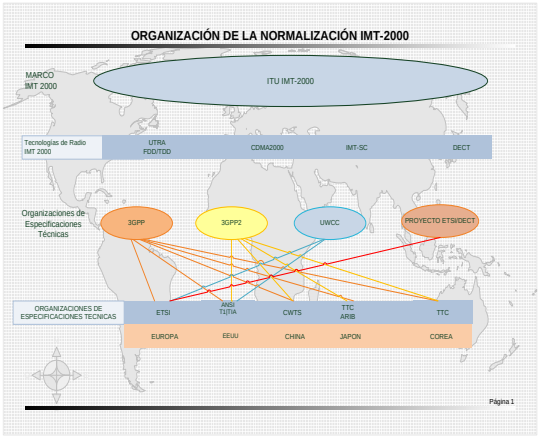

Figura 3.1 Organización de la Normalización IMT-2000.

3.2 Organismos claves en la Normalización de móviles 3G.

Aunque los organismos 3GPP, 3GPP2, UWCC y ETSI EP DECT son los líderes en la normalización de los móviles 3G, no son los únicos grupos que están trabajando en este campo. Existen otras organizaciones importantes como:

- La UIT tiene varios grupos trabajando en el IMT2000 (el término genérico oficial para los móviles 3G). Dentro del UIT-T, el principal grupo es el nuevo SSG (Special Study Group) IMT2000, mientras que el liderazgo en UIT-R está ahora asignado al Working Party WP8F, que sustituye a los antiguos grupos TG8/1 y WP8/13.

- El Mobile Wireless Internet Forum (MWIF), que tiene la misión de ''impulsar la aceptación y la adopción de una única arquitectura para la radio móvil e Internet, independiente de la tecnología de acceso". El objetivo principal del foro es la búsqueda de la asociación entre los mercados GSM/UMTS y CDMA/cdma2000.

- 3G Mobile Internet (3G.IP), que tiene la responsabilidad de "promover activamente un sistema radio común basado en IP para la tecnología de comunicación móvil de tercera generación, con el fin

de asegurar un rápido desarrollo de las normas y su recepción por parte de los operadores, vendedores y diseñadores de aplicaciones". El objetivo principal es la búsqueda de la asociación entre los mercados GSM/UMTS y TDMA/UWC136, para de esta forma promover el uso común de un paquete de datos troncal basado en el servicio GPRS.

• El IETF (Grupo de trabajo e ingeniería de Internet) está cada vez más involucrado en los aspectos de las normas móviles conforme se introduce la tecnología IP en las redes móviles. Los grupos de trabajo principales para la movilidad 3G son MOBILEIP (para la movilidad), SIP (Protocolo de inicio de sección) y SIGTRAN (para la transmisión de señalización).

La mayoría de los principales expertos en normalización de los organismos regionales más importantes trabajan a través de los proyectos conjuntos del 3GPP/3GPP2 y UWCC para acordar las "especificaciones" que luego serán publicadas oficialmente por sus organizaciones como "normas".

3.3 Organización de 3GPP

El 3GPP es grande, con una organización inspirada en la establecida por el ETSI para el GSM. Se estima que más de mil personas están contribuyendo de una manera u otra. Esto significa un número de expertos sin precedentes trabajando para el mismo proyecto. Tal organización, con sus procedimientos bien definidos, es crucial para el éxito de la normalización de la tercera generación, Sorprendentemente, ¡funciona! En sólo dos años, esta inmensa organización ha suministrado especificaciones casi estables, aceptadas por la mayoría de las industrias más importantes involucradas. Naturalmente, esto no hubiera sido posible sin la experiencia adquirida en los trabajos anteriores realizados por el 3GPP participando en proyectos de investigación llevados a cabo en todos los países involucrados.

Las responsabilidades del 3GPP son las de preparar, aprobar y mantener las especificaciones técnicas globales para la tercera generación de sistemas móviles. La Figura 2.2 muestra la organización general del 3GPP.

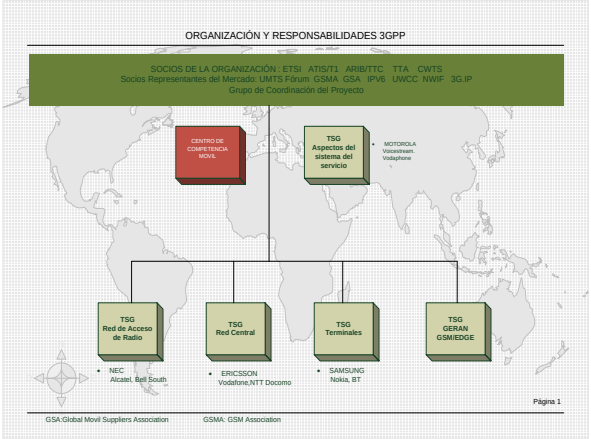

Figura 3.2 Organización y Responsabilidades 3GPP

Los Miembros Individuales del 3GPP están ligados por las normas de los Derechos de Propiedad Intelectual (IPR) de sus respectivos Socios de la Organización. Los Miembros Individuales son alentados para declarar, lo antes posible cualquier IPR que piensen que pudiera ser esencial, o potencialmente esencial, para cualquier trabajo en curso dentro del 3GPP. Después de comparar sus políticas sobre el IPR, ARIB, ETSI, T1, TTA y TTC acordaron que esas políticas compartieran principios comunes bastante similares para maximizar el éxito del 3GPP.

3.4 Tecnología de radio IMT-2000.

La tercera generación de sistemas móviles celulares (IMT-2000) nació con el objetivo de superar las limitaciones de los sistemas móviles de segunda generación. Inicialmente se le llamó FPLMTS, posteriormente cambio al nombre de IMT-2000 (Telecomunicación Móvil Internacional 2000). IMT-2000 es el término que la ITU adoptó para referirse a los estándares de interfaces radioeléctricas que forman parte de la tercera generación de los sistemas de comunicaciones móviles.

4. Recomendaciones UIT-T Q.1741.3

4.1 Especificaciones técnicas basadas en las serie 33

Los procedimientos de trabajo del 3GPP permiten la mejora continua de sus especificaciones mediante un procedimiento de petición de cambio. Las peticiones de cambio son examinadas por cada

Grupo de Trabajo 3GPP y presentadas para aprobación en las reuniones plenarias trimestrales del TSG de 3GPP. Por consiguiente, las normas/especificaciones SDO pueden ser actualizadas después de cada reunión plenaria del TSG de 3GPP.

4.2 TS 33.102 Seguridad en 3G, Arquitectura de seguridad

Esta especificación define la arquitectura de seguridad, es decir, las funcionalidades y mecanismos de seguridad para el sistema de telecomunicaciones móviles de tercera generación, donde una funcionalidad de seguridad es una capacidad de servicio que satisface uno o varios requisitos de seguridad, y un mecanismo de seguridad es un elemento que se utiliza para realizar una funcionalidad de seguridad. El conjunto de todas las funcionalidades y mecanismos de seguridad forma la arquitectura de seguridad.

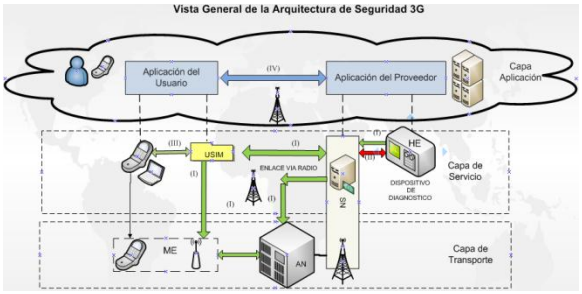

Figura 4.2 Arquitectura de Seguridad 3G

Dónde:

(I) Seguridad en la Red de Acceso

Este primer enlace opera entre el HE-SN y entre la SN- USIM, también opera en la capa de transporte como podemos observar en el grafico arriba detallado, este enlace tiene algunas características de seguridad y las describimos a continuación:
a) Confidencialidad de la identidad del usuario: Para llevar a cabo la confidencialidad de la identidad de usuario, el mecanismo de GSM (telefonía 2G) utiliza identidades temporales acordadas entre la red SN y el usuario/abonado mantenido
b) Autenticación de entidad (enlace de acceso): La autenticación de entidad para el usuario y red se realiza a través del mecanismo de autenticación UMTS y del mecanismo de acuerdo/gestión de clave (AKA). Las partes que se autentican son el USIM expedido por el HE y el AuC (Authentication Centre) del dominio HE. Además de las características de seguridad proporcionadas por el mecanismo GSM, el mecanismo AKA de UMTS asegura que el usuario sólo acepte datos de autenticación frescos (desafío aleatorio y las claves derivadas)
c) Confidencialidad de los datos (enlace de acceso): En UMTS la confidencialidad de los datos se aplica a los datos de usuario y a los datos de señalización transmitidos a través del enlace de acceso por radio.
d) Integridad de datos (enlace de acceso): La primera característica nueva de seguridad de acceso de red en UMTS es la integridad de los datos que se aplicará a los mensajes de señalización seleccionados transmitidos a través del enlace de radio
e) Identificación del equipo de usuario: GSM implementa un mecanismo para la identificación del equipo de usuario pero dicho mecanismo no es seguro. Para disuadir de posibles robos, una característica de personalización entre el USIM y el UE puede proporcionar un mecanismo alternativo, sin implicar las entidades de red. Otra alternativa es ubicar esta característica de seguridad debajo del nivel de aplicación.
f) Cifrado de red: Es una extensión de esta característica de seguridad que proporciona un modo protegido de transmisión a los canales de tráfico de usuario a través de toda la red. De este modo proporciona a los usuarios garantía de que sus datos de usuario se encuentren protegidos contra escuchas clandestinas en todos los enlaces de la red, es decir no sólo en los enlaces de radio particularmente vulnerables de la red de acceso, sino también en los enlaces fijos dentro de la red troncal central

(II) Seguridad en el Dominio de Red

Este segundo enlace opera con la SN y el HE, por medio de un conjunto de características de seguridad que permiten a los nodos del dominio del proveedor intercambiar de forma segura datos de señalización y de esta manera protejan contra ataques en la red fija de naturaleza alámbrica.

(III) Seguridad en el Dominio de Usuario

Contiene aquellas características de seguridad que controlan el acceso al USIM o al terminal y que se encuentran completamente implementadas en el dominio de usuario (UE+USIM).

(IV) Seguridad en el Dominio de Aplicación

Esta clase de características de seguridad proporciona interfaces y subniveles de seguridad que permiten a las aplicaciones establecer comunicaciones de forma segura a través de enlaces vía radio y alambico; así, por ejemplo proporciona seguridad de aplicaciones

seguras entre las aplicaciones en el dominio del usuario y en el dominio del proveedor.

4.2.1 Registro ME

El proceso de registro del EU se realiza ya sea por Conmutación de paquetes (PS), o por conmutación de circuitos (CS), hay que tomar en consideración que en el proceso de registro ME intervienen los tres bloques importantes del sistema UMTS como son la UTRAN, CN(red central) y el UE(equipo usuario).

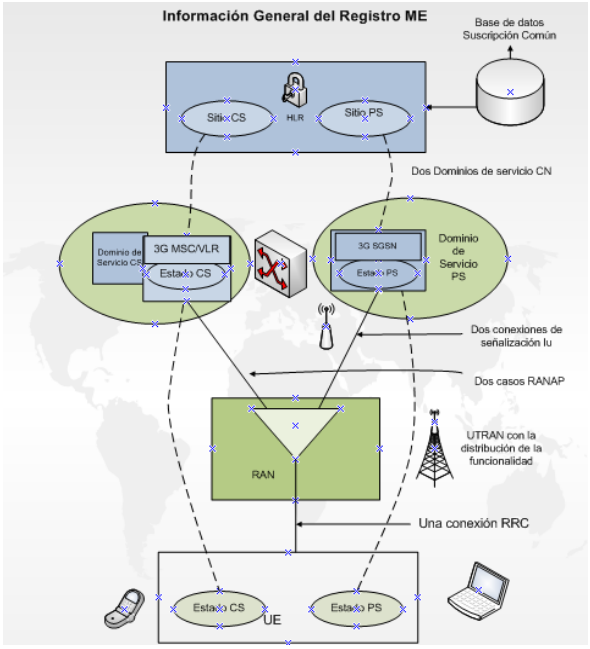

Figura 4.2.1 Registro ME

4.3 TS 33.203 Seguridad en 3G, Seguridad de acceso para servicios basados en IP

El IMS de UMTS soportará aplicaciones multimedios IP tales como video, audio y conferencias multimedia. El protocolo de inicio de sesión (SIP) se ha elegido como protocolo de señalización para crear y terminar sesiones multimedios. Esta especificación sólo se ocupa de cómo se protege la señalización SIP entre el abonado y el IMS, cómo se autentica el abonado y cómo el abonado autentica al IMS.

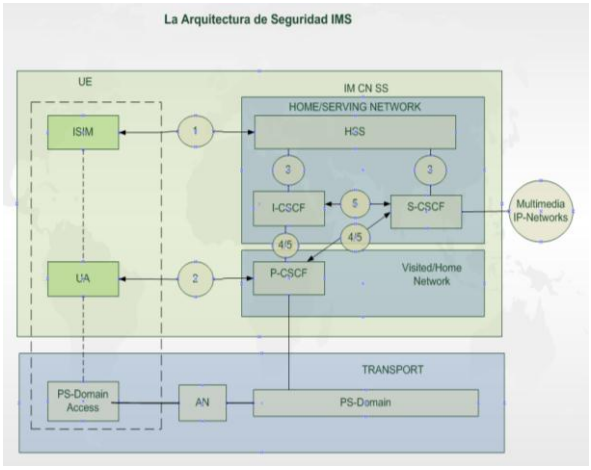

Figura 4.3 Arquitectura de Seguridad IMS

Dónde:

1) Proporciona autenticación mutua, donde el suscriptor tendrá una identidad de usuario privada (IMPI) y por lo menos una identidad de usuario pública (IMPU).
2) Proporciona un enlace seguro y una asociación de seguridad entre la UE y un P-CSCF
3) Proporciona seguridad en el dominio de red interna entre HSS con I-CSCF y S-CSCF
4) Proporciona seguridad entre redes diferentes para los nodos de protocolos de inicio de sección (SIP)
5) Proporciona seguridad dentro de la red interna entre los nodos SIP.

Como muestra la figura 4.3, la arquitectura IMS consta en la parte central de los servidores CSCF (Control de funciones en estado de llamadas) lo cuales usan el protocolo SIP. Estos se dividen en: P-CSCF (Proxy CSCF), S-CSCF (Serving CSCF) e I-CSCF (Interrogating CSCF).

- El P-CSCF es un servidor proxy SIP y es el primer contacto de un equipo terminal con la plataforma IMS. Este acepta todos los requerimientos SIP que se originan en el equipo terminal o van hacia él, los procesa internamente o los reenvía a otro servidor. También posee funciones de control y administración de recursos.

- El S-CSCF es un servidor SIP que siempre reside en la red local del suscriptor y provee servicios de control de sesión, el S-CSCF constituye el elemento central de la red IMS en el plano de la señalización, el cual crea un enlace entre la identidad pública del usuario (dirección SIP) y la

dirección IP del terminal. El S-CSCF interactuar con el HSS (Home Subscriber Server) extrayendo desde ahí la dirección IP o perfil de usuario y vectores de autentificación que permiten la creación del enlace, todos los mensajes SIP originados por el terminal o destinados hacia él pasan por el S-CSCF, aquí se procesan los mensajes y se determinan las tareas subsiguientes a partir del contenido de estos.

- El I-CSCF es un servidor proxy SIP que constituye el enlace de la plataforma IMS con redes externas, este selecciona un S-CSCF para un usuario y traspasa los mensajes SIP entre ellos. La selección del S-CSCF se basa en las capacidades requeridas, las disponibles y la topología de la red. También puede ser usado para esconder información sobre la estructura interna de la red, a través de la encriptación de parte de los mensajes SIP.

La plataforma IMS incluye muchas otras entidades funcionales como es HSS el cual contiene la principal base de datos, con los datos de todos los usuarios (incluyendo servicios autorizados), al cual varias entidades lógicas de control (CSCF) acceden, el HSS contiene los datos del usuario, que son pasados al S-CSCF, y almacena la información temporaria con la localización del S-CSCF donde el usuario está registrado en un momento dado.

4.4 TS 33.210 Seguridad en 3G, Seguridad del dominio de red (NDS)

Esta especificación define la arquitectura de seguridad del plano de control basado en IP del dominio de red UMTS. El alcance de la seguridad del plano de control del dominio de red UMTS abarca la señalización de control en interfaces seleccionadas entre elementos de red UMTS.

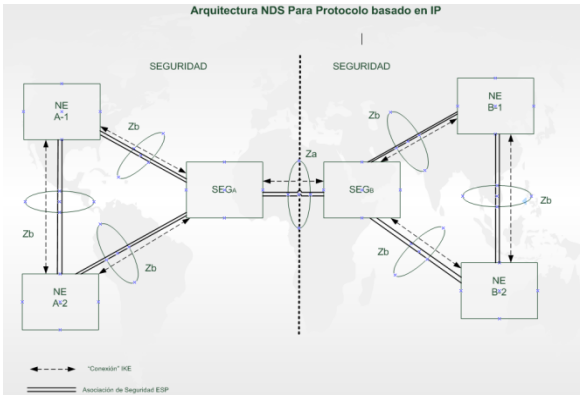

Figura 4.4 Arquitectura NDS para protocolo basado en IP

Dónde:

Interfaz Za (SEG - SEG)

La interfaz de Za cubre todo lo relacionado con el trafico NDS/IP entre dominios de seguridad, SEG usa IKE (intercambio de clave de internet) para negociar, establecer y mantener un túnel seguro entre ellos, Los túneles se ven sujetos a cambios de roaming, en el cual los túneles entre SEG estarían normalmente disponible en cualquier momento, pero también estos podrían estar disponibles según sea necesario. ESP (asociación de seguridad) podrá utilizarse para el cifrado y la autenticación, pero un solo modo de autenticación es permitido, el túnel es utilizado para NDS/tráfico IP entre dos dominios de seguridad.
Una SEG puede dedicarse a servir únicamente un cierto subconjunto de todos los socios de roaming, lo cual limitará el número de asociaciones de seguridad y túneles que hay que mantener.

Interfaz Zb (NE – SEG / NE - NE)

La interfaz Zb es localizada entre SEG y NE, y entre NE con el mismo dominio de seguridad, la interface Zb es opcional para la implementación pero en caso de ser implementada esta debería implementarse con ESP+IKE
En la interfaz ZB, ESP siempre se utiliza con la autenticación y protección de integridad y el uso de cifrado es opcional. La Asociación de Seguridad ESP se utilizará para todo el tráfico de plano de control que se necesita con la protección de seguridad

5 Conclusiones

1) La comprensión de las Arquitecturas tratadas en las normas citadas es la base principal para cualquier estudio de las normas de seguridad, porque de esta manera llegamos a tener un mejor enfoque de las recomendaciones de seguridad que son necesarias para la confidencialidad de datos entre el Equipo de Usuario y la Red Central.

2) Los mecanismos de seguridad son de vital importancia para lograr proveer de conectividad IP a las redes de telefonía móvil de tercera generación de una manera segura, sin que esta tenga la posibilidad de sufrir algún tipo de amenaza y de esta manera otorgar a los usuarios una amplia gama de servicios IP disponibles con la seguridad deseada.

3) El envió de información tanto del Equipo Usuario (UE) hacia la Red Central (CN) o viceversa, se realiza de una manera segura gracias a los procedimientos de comprobación que realizan las interfaces de seguridad del Sistema UMTS, debido a que si no cumple con los requerimientos necesarios no se le permite el paso de información al siguiente bloque de comunicación del Sistema.

6 Recomendaciones

1) En el análisis del registro del equipo móvil (ME), se debe entender todos los elementos que intervienen en el grafico como son los tres bloques principales en este sistema UMTS, EU (Equipo de Usuario), la UTRAN (Red de Radio ceso Terrestre UMTS) y la CN (Red Central), debido a que existe entre cada uno de estos bloques una interfaz que se encarga de la seguridad entre su comunicación ante posibles amenazas.

2) Tomar en consideración que la normativa no detalla de forma gráfica que el EU (Equipo de usuario) se subdivide en dos dominios que son el ME (Equipo Movil) y el USIM , y que a su vez él ME se subdivide en MT(Mobile Termination) y TE(Terminal Equipment), por lo que se cree conveniente que las personas interesadas lo puedan desglosar para lograr tener una mejor descripción y comprensión del funcionamiento entre el equipo de usuario con el equipo de infraestructura IE, el cual está conformado por el AN (Access Network) y CN (Core Network).

3) Se debe tener en cuenta el Protocolo ‘‘Diameter’’ el cual no se detalla en las especificaciones de seguridad en la arquitectura IMS, pero consideramos importante mencionarlo debido a que por medio de este se logra interactuar el S-CSCF con el HSS (Home subscriber server), para proveer servicios de autorización y auditoria de aplicaciones como el acceso de red o movilidad IP.

4) En el futuro la normalización crearía las condiciones necesarias para el interfuncionamiento de los sistemas 3G a nivel mundial, sin embargo todas las tecnologías IMT2000 de radio terrestre competirán en el mercado. Indudablemente, no todas las normas de radio 3G disfrutarán del mismo éxito. Es por eso que nuestra recomendación a las empresas que aun no han adoptado el Sistema UMTS es que empiecen a tener funcionamiento con este sistema ya que si no lo hacen de una manera muy eficaz y con el cuidado ante las amenazas y a la seguridad como lo hemos explicado en el capítulo 3 quedaran de una manera u otra retrasadas en la actualización del Sistema Universal de Telecomunicación móvil.

7 Referencias

[1]. The Mobile broadband Standard, 3GPP Specifications, http://www.3gpp.org, 2005
[2]. Timo Halonen, Javier Romero and Juan Melero, ‘‘GSM, GPRS and EDGE performance: evolution toward 3G/UMTS’’, John Wiley & Sons, 2002.
[3]. Promoting Mobile Broadband Evolution, UMTS Descriptions, http://www.umts-forum.org, 2005
[4]. Rudi Bekkers, ‘‘Mobile Telecommunications standards: GSM, UMTS, TETRA, and ERMES’’.2001
[5]. 3GPP TS 22.101 V7.0.0, Service principles, http://www.3gpp.org/ftp/Specs/archive/22_series/22.101/ , 2005
[6]. Juha Korhonen, ‘‘Introduction to 3G mobile comminications’’, Artech House, 2001.