ESCUELA SUPERIOR POLITECNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

‘‘NORMAS DE SEGURIDAD EN REDES UMTS’’

INFORME DE SEMINARIO DE GRADUACION

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTORES:

ROBERTH OSWALDO CAMPOVERDE HIDALGO

JOHN AGUSTIN SUCRE VELIZ

GUAYAQUIL – ECUADOR

AÑO 2010

AGRADECIMIENTO

A mi padre celestial, porque gracias a ÉL he llegado a culminar mis estudios sin problema alguno, gracias Dios mío por iluminar mi vida, que siempre me llenaste de fuerza para seguir adelante.

A mis padres, que siempre me inculcaron lo mejor, por ser siempre mis guías, mi apoyo constante y por brindarme lo mejor para poder superarme.

A mis familiares, por brindarme su cariño, y por darme consejos que me ayudan a crecer como persona, gracias por ser la mejor familia del mundo.

A mis maestros, por transmitirme todos sus conocimientos que me ayudaron a formar profesionalmente.

***Roberth Oswaldo Campoverde Hidalgo**.*

Antes que a todos quiero agradecer a Dios por darme la fuerza necesaria en los momentos que mas la necesite y bendecirme con la posibilidad de caminar a su lado durante toda mi vida.

También quiero agradecer a los Profesores por brindarme su apoyo y conocimiento para lograr ser un profesional.

A mi profesor del seminario de Graduación Ing. Washington Adolfo Medina Moreira ya que sin su ayuda esto no hubiera sido posible.

John Agustín Sucre Veliz.

DEDICATORIA

Este Trabajo va dedicado a mis padres y hermanos, por ser la mejor familia que en las buenas y en las malas siempre nos hemos mantenido unidos, gracias a ustedes estoy en esta etapa importante de mi vida lleno de felicidad y listo para empezar nuevas metas.

Roberth Oswaldo Campoverde Hidalgo.

Quiero dedicar este trabajo a mis padres, por acompañarme en cada uno de los momentos difíciles a los que me enfrente para lograr este objetivo, apoyándome en todo momento sin nunca darme la espalda.

A mis hermanos que me han ayudado a cumplir este objetivo mostrándome su amistad en todos los momentos.

A mi familia por brindarme su comprensión y en especial por sus sabios consejos que me ayudaron a tomar el camino correcto.

John Agustín Sucre Veliz.

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Trabajo Final de Graduación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

_____ _____

Roberth Campoverde Hidalgo **John Agustín Sucre Véliz**

TRIBUNAL DE SUSTENTACION

_____

Ing. Juan Carlos Avilés

PROFESOR DELEGADO POR EL DECANO FIEC

_____

Ing. Washington Medina

PROFESOR DEL SEMINARIO DE GRADUACIÓN

Resumen

Las Normas de Seguridad en UMTS fueron diseñadas con la finalidad de que los usuarios que adoptan esta tecnología no sufran de amenazas en la confidencialidad de envió 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 una manera grafica al lector interesado, de las arquitecturas tratadas en las normas de la serie 33 mencionadas, y conocer la importancia de las normas de seguridad para la prevención de los diferentes tipos de amenazas que se puede presentar en dichas arquitecturas.

Por esta razón se ha implementado los procedimientos de seguridad en las arquitecturas citadas en cada una de estas normas mediante una presentación de Microsoft Office PowerPoint 2007 para que sea más factible su comprensión, y así de una manera dinámica detallar en qué puntos se realiza un control de

seguridad ante cualquier situación que pueda atentar con la confidencialidad de los datos.

También se elaboró un diagrama de bloques sobre el funcionamiento de la Arquitectura de Seguridad del Sistema UMTS, en el cual detallaremos los procedimientos que son necesarios para la transmisión y recepción de información de forma segura entre el Equipo Usuario (UE) y la Red Central (CN).

Para el cumplimiento de este objetivo se ha dividido el trabajo de investigación en 3 capítulos los cuales se detallan a continuación:

En el Capitulo 1 se revisa todo lo relacionado con el sistema de tercera generación de telefonía celular, con la finalidad de que el lector, conozca el origen del sistema UMTS, su evolución desde GSM, los objetivos que se plantearon para una red UMTS y la configuración de la estructura.

En el Capitulo 2 se hace referencia de una manera general a la normalización del sistema 3G, que Organizaciones son las encargadas de implementar estas normas, cuales son los organismos claves en la normalización de los sistemas móviles, como también del alto nivel de la arquitectura del sistema UMTS

En el Capitulo 3, que representa el capitulo central de investigación, se detalla la Normativa Q (Conmutación y Señalización en el sistema 3G), con las diferentes

recomendaciones técnicas de seguridad y la implementación de gráficos en los cuales se da a conocer:

- El funcionamiento de cada una de las Arquitecturas definidas en las normas citadas.
- El Funcionamiento del Registro del Equipo Móvil (Registro ME)

Las Arquitecturas mencionadas son:

- Arquitectura de Seguridad 3G.
- Arquitectura IMS.
- Arquitectura NDS (protocolos basados en IP)

Nota: La presentación mediante diapositiva será adjuntada al final del proyecto en manera digital

INDICE GENERAL

CAPITULO 1
DESCRIPCION DE UMTS

CAPITULO 2
NORMALIZACION DE LOS SISTEMAS MOVILES 3G

CAPITULO3
NORMALIZACION Q (Conmutacion y Señalizacion)

INDICE DE FIGURAS

INDICE DE TABLAS

Apéndice

Lista de Acrónimos

2G	Segunda generación (second generation)
3G	Tercera generación (third generation)
3GMS	Sistema de comunicaciones móviles de tercera generación (third generation mobile communication system)
3GPP	Proyecto asociado de tercera generación (third generation partnership project)
ACTS	Servicios y Tecnología de comunicaciones avanzada
AMNT	Asamblea Mundial de Normalización de las Telecomunicaciones.
ANSI	American National Standards Institute
ARIB	Association of Radio Industries and Business
ASK	Modulación por desplazamiento de amplitud
ATDMA	Acceso múltiple con división de tiempo avanzada
AuC	Centro de autenticación (authentication centre)
BS	Estación de base (base station)
BSC	Control de estación de base (base station control)
BSS	Sistema de estación de base (base station system)
BTS	Estación transceptora de base (base transceiver station)
CDMA	Acceso Múltiple por División de Código
CN	Red medular; red central (core network)
CS	Conmutación de circuitos (circuit switched))
CSCF	Control de funciones en Estado de llamadas
CWTS	China Wireless Telecommunications Standards Group

DECT	Telecomunicaciones Inalámbricas Mejoradas Digitalmente (Digital Enhanced Cordless Telecommunications)
DTE	Equipo terminal de datos (data terminal equipment)
EGPRS	GPRS mejorado (enhanced GPRS)
EIR	Registro de identidad de equipo (equipment identity register)
EN	Norma europea (european norm)
ETSI	Instituto Europeo de Normas de Telecomunicación (European Telecommunications Standards Institute)
FDD	Doble división de frecuencia.
FDMA	Acceso multiple por división de frecuencia.
FPLMTS	Sistema de comunicaciones móviles de tercera generación, actualmente denominado IMT-2000
FRAMES	Futuro sistema de radio acceso multiple de banda ancha.
FSK	Modulación por desplazamiento de frecuencia
GERAN	Red de acceso radioeléctrico GSM EDGE (GSM EDGE radio access network)
GGSN	Nodo de pasarela GPRS (gateway GPRS support node)
GLR	Registro de posición de pasarela (gateway location register)
GMSC	MSC de pasarela (gateway MSC)
GPRS	Servicio general de radiocomunicaciones por paquetes (general packet radio service)
gprsSSF	Función de conmutación de servicio GPRS (GPRS service switching function)
GSM	Sistema global para comunicaciones móviles (global system for mobile communications)
GSM-EFR	Códec vocal de velocidad completa mejorada GSM (GSM enhanced full rate speech codec)
GSN	Nodos de soporte de GPRS (GPRS support nodes)

HLR	Registro de posiciones propio (home location register)
HSS	Home Subscriber Server
ID	Identificador
IETF	Grupo de Trabajo en Ingeniería de Internet
IKE	Intercambio de clave de Internet
IMEI	Identidad del equipo móvil internacional (international mobile equipment identity)
IM-GSN	Nodo servidor GPRS intermedio (intermediate GPRS serving node)
IM-MSC	Centro intermedio de conmutación de servicios móviles (intermediate mobileservices switching centre)
IMS	Subsistema Multimedia IP de red Central (IP Multimedia Core Network Subsystem).
IMT-SC	Single carrier(UWC-136/EDGE)
IMSI	Identidad internacional de estación móvil (international mobile station identity)
INAP	Protocolo de aplicación de red inteligente (intelligent network application protocol)
IP	Protocolo Internet (Internet protocol)
IRP	Punto de referencia de integración (integration reference point)
ISO	Organización Internacional de Normalización (International Organization for Standardization)
Itf-N	Interfaz N (interface N)
Iu-b	Interfaz entre los Nodos B y el RNC
LAN	Red de área local (local area network)
LI	Intersección Legal
LMSI	Identidad de la estación móvil local (local mobile station identity)
MAP	Parte aplicación móvil (mobile application part)

ME	Equipo móvil (mobile equipment)
MIC	Modulación por impulsos codificados
MIM	Modelo de información de gestión (management information model)
MIME	Ampliaciones multifunción del correo Internet (multipurpose Internet mail extensions)
MLC	Centro de posición del servicio móvil (mobile location centre)
MM	Gestión de la movilidad (mobility management)
MMI	Interfaz hombre-máquina (man-machine interface)
MMS	Servicio de mensajería multimedios (multimedia messaging service)
MNC	Indicativo de red para el servicio móvil (mobile network code)
MNP	Portabilidad de número móvil (mobile number portability)
MO	Originado en móvil (mobile originated)
MO-LR	Petición de localización originada en móvil (mobile originated location request)
MPTY	Multipartitos (multiparty)
MS	Estación móvil (mobile station)
MSC	Centro de conmutación de servicios móviles (mobile switching centre)
MSISDN	Número RDSI internacional de estación móvil (mobile station international ISDN number)
MSP	Perfil de abonado múltiple (multiple subscriber profile)
MSRN	Número itinerante de estación móvil (mobile station roaming number)
MT	Terminal móvil (mobile terminal)
MT	Terminación móvil (mobile termination)
MRP	Socios representantes del mercado.
MWIF	Foro móvil de internet inalámbrico (Mobile Wireless Internet Forum)

NDS	Seguridad en el dominio de red
NE	Network Entity
OHG	Grupo de armonización de operadores (Operator Harmonization Group)
OSI	Interconexión de sistemas abiertos (open system interconnection)
PS	Conmutación de paquetes (packet switched)
PSE	Entorno de servicio personal (personal service environment)
PSK	Modulación por desplazamiento de fase.
QPSK	Modulación de desplazamiento de fase- 4 símbolos (Quadrature Phase-Shift Keying)
16-QAM	(Modulación de amplitud en cuadratura de 16 estados)
RLC/MAC	Control de radioenlace/control de acceso al medio (radio link control/médium access control)
RMTP	Red móvil terrestre pública
RNC	Controlador de red radioeléctrica (radio network controller)
RNS	Sistema de red radioeléctrica (radio network system)
SCR	Velocidad controlada por la fuente (source controlled rate)
SCS	Servidores de capacidades de servicio (service capability servers)
SDO	Organización de Desarrollo de Normas (Standards Development Organization)
SEG	Entrada de Seguridad (Security Gateways)
SGSN	Nodo servidor soporte del servicio GPRS (serving GPRS support node)
SIM	Módulo de identidad del usuario GSM (GSM subscriber identity module)
SIP	Protocolo de Inicio de Sesión .
SM	Gestión de sesión (session management)

SMG	Grupo Especial de móviles.
SMS	Servicio de mensajes cortos (short message service)
SMSC	Centro de servicio de mensajes cortos (short message service center)
SMTP	Protocolo de transferencia de correo simple (simple mail transfer protocol)
SRNS	RNS servidor (serving RNS)
SSG	Grupo de estudio especial
TDD	Doble división de tiempo(Time division duplexing)
T1 T1	Standardization Committee (parte de ANSI)
T1P1	Technical Subcommittee for wireless/Mobile Services and Systems
TDMA	Acceso múltiple por división en el tiempo (time division multiple access)
TE	Equipo terminal (terminal equipment)
TIA	Asociación de industrias de telecomunicaciones
TS	Especificación técnica (technical specification)
TSG	Grupo de especificaciones técnicas (Technical Specification Group)
TTA	Telecommunication Technology Association (Corea)
TTC	Telecommunication Technology Committee (Japón)
TDD	Doble división de tiempo (Time Division Duplex).
TDCDMA	División de Tiempo CDMA
UA	Agente de usuario (User agent)
UDP	Protocolo de datagrama de usuario (user datagram protocol)
UE	Equipo de usuario (user equipment)
UICC	Tarjeta IC universal (universal IC card)
UIM	Módulo de identidad de usuario (user identity module)

UIT	Unión Internacional de Telecomunicaciones
UIT-R	Unión Internacional de telecomunicaciones - Radio
UIT-T	Sector de Normalización de las Telecomunicaciones de la UIT.
UMTS	Sistema de telecomunicaciones móviles universales (universal mobile telecommunication system)
USAT	Juego de herramientas de aplicación de USIM (USIM application toolkit)
USIM	Módulo de identidad de abonado universal (universal subscriber identity module)
UTRA	Acceso radioeléctrico terrenal universal (universal terrestrial radio access)
UTRAN	Red terrenal de acceso radioeléctrico universal (universal terrestrial radio Access network)
Uu	Interfaz de usuario se encuentra entre equipo de usuario y la red UTRAN
UUS	Señalización de usuario a usuario (user-to-user signalling)
UWC136	Universal Wireless Communications based on IS-136
UWCC	Consorcio de comunicaciones inalámbricas universal
VHE	Entorno propio virtual (virtual home environment)
VLR	Registro de posición de visitantes (visitor location register)
WCDMA	Acceso múltiple por división de código de banda ancha

CAPITULO 1

DESCRIPCION DE UMTS

1.1 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).

Como punto importante se puede decir que la ITU creó IMT-2000, y a su vez de ésta salió UMTS, cdma2000 y UWC-136. De éstas, UWC-136 se decidió dejar de usar y las otras 2, especialmente UMTS el cual cada vez se usa en más partes del mundo.

UMTS es la propuesta de la ETSI para tercera generación de telefonía celular, siendo éste el sucesor de GSM. UMTS ha sido planeado para funcionar en Europa y los países que deseen adoptarlo.

ETSI/Special Mobile Group (SMG) ha sido el responsable para la estandarización de UMTS desde los 90's. [3]

Desde el comienzo de la discusión de UMTS, la intención ha sido proveer un estándar para un mundo de telefonía móvil personal, dando calidad equivalente a servicios inalámbricos y acceso a una amplia gama de servicios.

Nuevas capacidades de servicios específicos UMTS serán ofrecidas, de acuerdo a las necesidades del mercado y sus limitaciones inherentes. Uno de los más

importantes aspectos para el éxito de UMTS es que sus servicios no deben ser más caros que los de las redes actuales.

UMTS busca extender las actuales tecnologías móviles, inalámbricas y satelitales proporcionando mayor capacidad, posibilidades de transmisión de datos y una gama de servicios mucho más extensa, usando un innovador programa de acceso radioeléctrico y una red principal mejorada. La cobertura será hecha por una combinación de tamaños de células en un rango que va de pico células a células globales (provistas por satélite), las cuales inclusive darán servicio a regiones remotas del mundo.

UMTS ha sido concebido como un sistema global, que incluye tanto componentes terrestres como satelitales. Terminales multimodales capaces de funcionar también por sistemas de Segunda Generación (2G), tales como las bandas de frecuencias GSM 900, 1800 y 1900 extenderán aún más el alcance de muchos servicios UMTS.

UMTS soportará ambas operaciones, tanto FDD como TDD. El primer tipo, típicamente será usado por licencias, redes públicas que ofrecen servicio. El segundo tipo será para aplicaciones indoor, donde la radio base es puesta en lugares cercanos al móvil.

Estas redes TDD pueden estar funcionando por licencias, pero pueden además involucrar redes privadas operando en bandas de frecuencia que no las necesiten.

Un requerimiento clave para UMTS es la alta eficiencia espectral para la mezcla de servicios de las diferentes portadoras, en donde la eficiencia espectral se ha propuesto que sea al menos tan buena como la de GSM para la baja velocidad de transmisión. El sistema además debe ser flexible para soportar una variedad de capacidad de cobertura y facilitar la evolución de ésta; en donde debe haber uso y relación entre varios tipos de célula dentro de un área geográfica, incluyendo la habilidad para soportar cobertura en áreas rurales.

UMTS soportará el sistema dual GSM/UMTS, en donde por ejemplo, la selección de célula y el procedimiento de voceo será diseñado para acomodar que la red pueda consistir de células GSM, células UTRAN ó combinación de ambas.

1.2 Evolución desde GSM

En el mismo año que GSM fue lanzado comercialmente, la ETSI (European Telecommunication Standard Institute) comenzó a trabajar en UMTS. El trabajo fue realizado por el comité SMG. [2]

Los sistemas de telecomunicaciones de tercera generación, tal como GSM, habilitaron el tráfico de voz para que fuera inalámbrico: el número de teléfonos móviles excedió el número de líneas fijas y la penetración del teléfono móvil excedió el 70 % en países con el más avanzado mercado inalámbrico. [6]

En sí se podría decir que GSM cumple para algunos objetivos de UMTS, tal como se mencionan en la tabla 1.1

Objetivo de UMTS	GSM cumple o No
Móvil barato	Sí
Penetración profunda	Sí, en algunos mercados
Movilidad (anywhere, anytime)	Sí
Capacidad de Hot Spot	Sí
Calidad de voz	Sí
Roaming global	Sí (mediante tarjeta SIM)
Servicios IM	Sí
Multimedia, entretenimiento	Sí
Flexibilidad de mezclar diferentes Tipo de portadoras	No
Servicios de alta velocidad de bit (>200 kbps)	No

Tabla 1.1. Comparación entre objetivos de UMTS y GSM [2]

La evolución se considera un proceso de cambios y desarrollo del sistema GSM hacia las capacidades y funcionalidades de UMTS. La visión de UMTS está basada en la evolución de GSM. Inevitablemente significa que la red GSM envuelve la red UMTS.

La forma de la evolución será fuertemente influenciada por las consideraciones del mercado. UMTS será estandarizado por un proceso de evolución comenzado principalmente desde GSM e ISDN, usando una parte de acceso.

Con el sistema GSM de 2.5G las redes GSM se están volviendo en una transición muy suave hacia UMTS. Es decir que están relacionadas para los procedimientos y requerimientos para los cuales fueron creadas. Por ejemplo en GSM el llamado BTS en UTRAN es llamado Nodo B, el BSC de GSM es nombrado como RNC en UTRAN. [4]

Para servicios de conmutación de circuitos, las redes de UMTS pueden usar existentes elementos de GSM tal como el MSC (Mobile Switching Center) y HLR (Home Location Register).

También UMTS fue creado para que pueda existir un eficiente Handover entre éste y GSM. Lo anterior hace posible la movilidad del usuario y el cambio de sistema, lo que aún reafirma más la relación entre estos dos sistemas.

El sistema GSM/EDGE hereda las especificaciones GSM/GPRS/EDGE del grupo SMG de ETSI. Actualmente su trabajo se centra en la interconexión de estas redes con UMTS y, en la medida de lo posible, proporcionar los servicios especificados para UMTS.

A continuación se muestra en la tabla 1.2 las frecuencias identificadas para diversos sistemas, especialmente lo que es acerca de UMTS y GSM.

	Uplink	Downlink	Total
GSM1800	1710-1785	1805-1880	2 x 75 MHz
UMTS-FDD	1920-1980	2110-2170	2 x 60 MHz
UMTS-TDD	1900-1920	2010-2025	20 + 15 MHz
Americas PCS	1850-1910	1930-1990	2 x 60 MHz

Tabla 1.2. Bandas de frecuencias en diversos sistemas [4]

La misma situación que ha ocurrido con la evolución de UMTS a través de GSM probablemente ocurrirá cuando los sistemas de cuarta generación sean introducidos, Inter-trabajo con los sistemas UMTS y compatibilidad, será deseable para los sistemas de cuarta generación. [9]

Compatibilidad y trabajo entre sistemas son dos diferentes estrategias de componentes para operar juntos. Los sistemas pueden hacerse compatibles, pero a medida que se logre compatibilidad, los protocolos de red tienen que ser similares y permitir que los sistemas trabajen juntos.

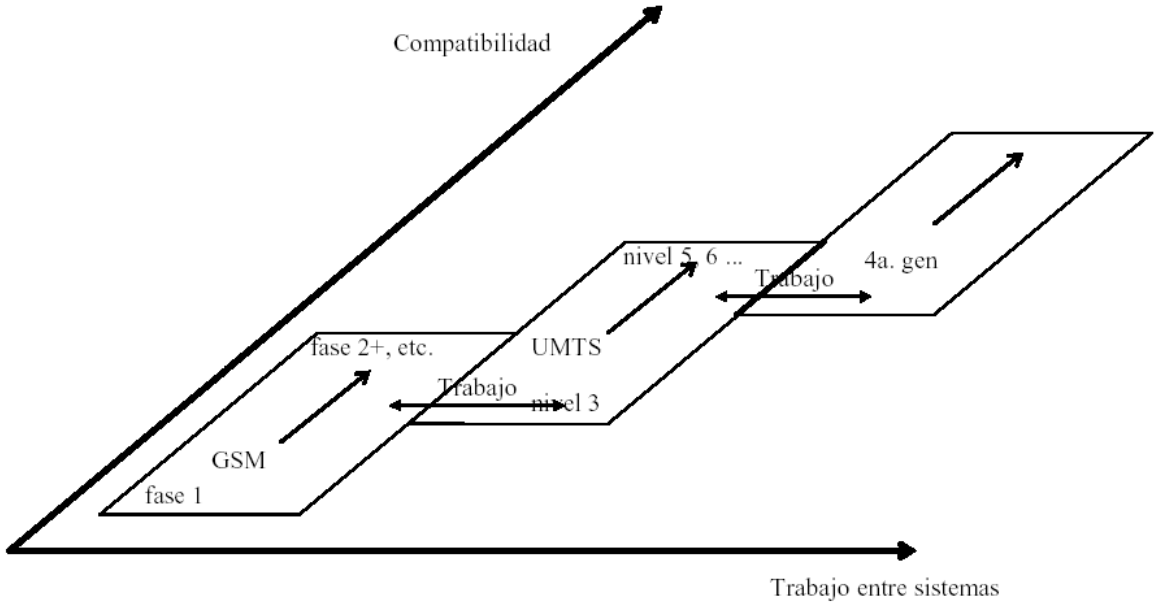


Figura 1.1. Trabajo y compatibilidad con respecto a evolución [9]

La figura 1.1 ilustra la relación entre compatibilidad y trabajo dentro y entre sistemas desde segunda generación, y hasta lo que será la cuarta generación.

1.3 Objetivos de UMTS

Algunos de los objetivos de UMTS son:

- Equipos de usuarios pequeños y económicos
- Servicio todo el tiempo
- Servicio en cualquier lugar (ambientes de espacios cerrados)
- Interoperabilidad con un sistema satelital
- Capacidad en los sitios con alta demanda
- Roaming global
- Calidad de voz como si existiera una conexión física

- Velocidad alta de transmisión de datos
- Múltiples servicios multimedia

El objetivo será facilitar bajo costo de las terminales, lograr compatibilidad con GSM, facilitar el modo dual FDD/TDD.

Los servicios UMTS se basan en capacidades comunes en todos los entornos de usuarios y radioeléctricos de UMTS. Al hacer uso de la capacidad de roaming desde su red hacia la de otros operadores UMTS, un abonado particular experimentará así un conjunto consistente de sensaciones como si estuviera en su propia red local (Entorno de Hogar Virtual o VHE). Asimismo, VHE permitirá a las terminales gestionar funcionalidades con la red visitada, posiblemente mediante una descarga de software, y se proveerán servicios del tipo como en casa con absoluta seguridad y transparencia a través de una mezcla de accesos y redes principales.

La tecnología satelital puede fácilmente proveer cobertura y servicio globales y se estima que tendrá un importante papel en la cobertura de UMTS a nivel mundial. UMTS está atravesando el proceso de normalización con el fin de asegurar una capacidad de roaming y eficiencia entre redes satelitales y terrestres.

Debido a la alta velocidad de comunicación, el requerido ancho de banda para una red comercial de tercera generación es grande, lo cual resulta en una ocupación del espectro de 20 Mhz. La actual necesidad para el espectro además

dependerá en el desarrollo de mayor eficiencia, lo cual se podría lograr con mejores antenas.

El más importante criterio para la propuesta terrestre son la eficiencia espectral y la eficiencia en la cobertura.

Una mejor caracterización de UMTS será la integración de servicios fijos y móviles, en donde habrá una flexible provisión de servicios. [5]

1.4 Estructura de la red UMTS

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:

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

1.4.1 Red Central (CN)

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).

Algunos requerimientos para UMTS con respecto al CN son los siguientes: [14]

- CN soportará servicios de datos por conmutación de paquetes con capacidad de al menos 2 Mbit/s.

- El establecimiento de portadora no va a prevenir la conexión de una nueva portadora. Esta portadora puede ser de tipo PS o CS.

- UMTS CN proveerá una solución efectiva de tráfico entre redes.

- UMTS CN proveerá facilidad de soporte para monitorear y medir flujo de tráfico y características dentro de la red (ejm.: control de congestión)

El CN está dividido en un dominio de servicios de conmutación de paquetes y un dominio de servicios de conmutación de circuitos. Redes y terminales pueden tener sólo el dominio PS, sólo el dominio CS ó ambos dominios implementados. [10]

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. Elementos: HLR, VLR, AuC, EIR y centros de SMS.

1.4.2 Red de Acceso de Radio (RAN o UTRAN)

El equivalente a la BTS de GSM se denomina Nodo B y el equivalente a la BSC se denomina RNC. Las radio bases (Nodo B) de UMTS podrán ser colocadas con las existentes radio bases de GSM.

Los dos sistemas que abarca UMTS, los llamados modos FDD y TDD, se distinguen por la forma de conseguir la transmisión dúplex: mientras en FDD se emplean distintas portadoras para el enlace ascendente y el descendente, en TDD se emplea una única portadora para todos los usuarios y ambos enlaces, pero dividiéndolas en pedazos de tiempo temporales para ambos enlaces.

El modo TDD puede sólo ser usado para pequeñas distancias, pero esto permite más altas velocidades de transmisión y serviría tal como para comunicaciones de Internet.

1.4.3 Terminales móviles (UE)

Se denomina equipo de usuario o también llamado móvil, al equipo que trae el suscriptor para lograr la comunicación.

En la figura 1.2 se observa claramente cómo están interconectados los tres bloques antes mencionados.

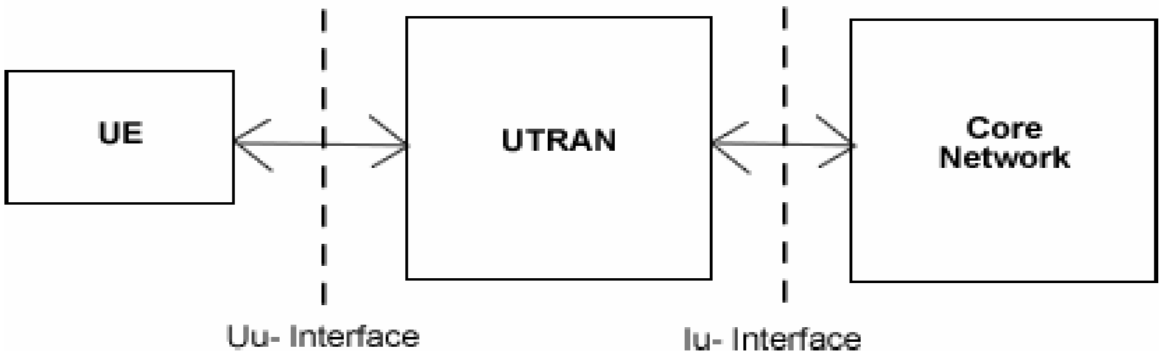


Figura 1.2. Bloques del sistema UMTS [2]

La velocidad de transferencia de datos va desde los 144 kbit/s sobre vehículos a gran velocidad hasta los 2 Mbit/s sobre terminales en interiores de edificios pasando por los 384 kbit/s para usuarios móviles, o vehículos a baja velocidad.

La figura 1.3 da un mejor detalle en la descripción de la arquitectura UMTS.

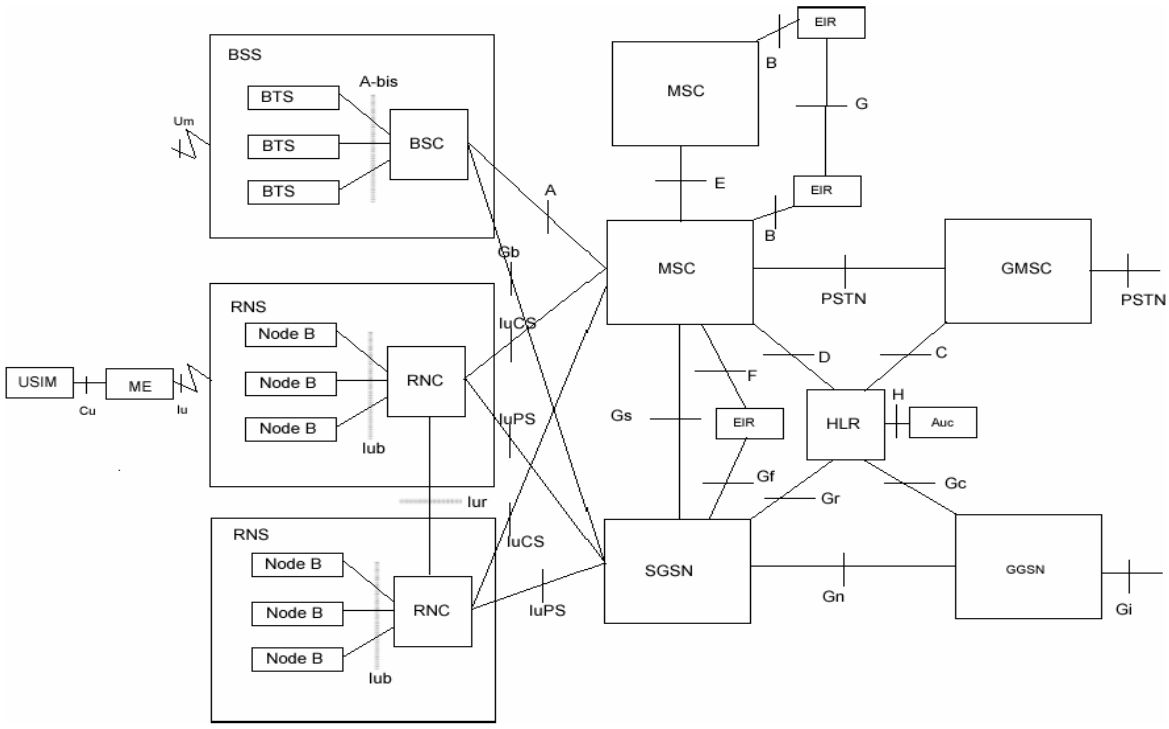


Figura 1.3. Arquitectura de UMTS [2]

En la imagen se incluye también la entidad de acceso a la red GSM (el BSS) para clarificar la relación de estas dos tecnologías.

1.5 Elementos de CN

La red central (CN) se encuentra formada por varios elementos como el MSC, el SGSN, GMSC, GGSN, HLR, etc. Los cuales se explicarán a continuación.

1.5.1 MSC (Mobile Switching Center)

El MSC es la pieza central en una red basada en conmutación de circuitos. El mismo MSC es usado tanto por el sistema GSM como por UMTS, es decir la BSS de GSM y el RNS de UTRAN se pueden conectar con el mismo MSC. Varios BSSs pueden ser conectados a un MSC.[2]

La función de un MSC incluye las siguientes cosas:

- Voceo o Paging
- Coordinación de llamadas
- Función de trabajo con otros tipos de redes
- Control del Handover
- Intercambio de señales entre diferentes interfaces
- Asignación de frecuencia

El MSC constituye la interfaz entre el sistema de radio y la red fija. El MSC ejecuta todas las funciones necesarias para el manejo de servicios de conmutación de circuitos hacia y desde la radio base. [10]

En disposición para obtener cobertura de radio de un área geográfica dada, un número de BSS o RNS son normalmente requeridos; aquí cada MSC debe tener interfaz a una o más BSSs o RNSs. Para la cobertura en un país, varios MSC pueden ser requeridos. [10]

1.5.2 HLR (Home Location Register)

El Home Location Register contiene los datos permanentes de registro de suscriptor. La información del suscriptor entra en un HLR cuando el usuario hace una suscripción. Hay 2 tipos de información en un HLR, el registro de entrada permanente y temporal.[2]

Los datos permanentes incluyen:

- Identidad internacional de suscriptor (IMSI), el cual identifica al suscriptor.
- Posibles restricciones de Roaming
- Clave de autentificación
- Parámetros de servicios suplementarios

Los datos temporales incluyen:

- Identidad local de la estación móvil(LMSI)
- Número de MSC
- Número de VLR

1.5.3 VLR (Visitor Location Register)

El VLR contiene información acerca del roaming en ésta área del MSC. Un VLR contiene información de todos los suscriptores activos en esta área, aún de quien esa red sea su red local. El VLR contiene mucha de la misma información que el HLR, la diferencia es que la información en el VLR está allí temporalmente, mientras que el HLR es un lugar que contiene información permanente.[2]

El VLR contiene toda la información necesaria para manejar las llamadas enviadas o recibidas por el móvil registrado en la base de datos. [10]

Un VLR contiene la siguiente información del usuario:

- Identidad internacional de suscriptor (IMSI)
- Número ISDN de la estación móvil internacional (MSISDN)
- Identidad temporal de la estación móvil (TMSI)
- Identidad local de la estación móvil (LMSI)
- Lugar del área donde la estación móvil ha sido registrada.

1.5.4 EIR (Equipment Identity Register)

El EIR almacena la identidad internacional del equipo móvil (IMEIs) usado en el sistema. [2]

Un EIR puede contener tres listas separadas:

- lista blanca: Los IMEIs del equipo que está en buen orden
- lista negra: Los IMEIs de algún equipo reportado perdido.
- Lista gris: Los IMEIs del equipo sabido que contiene problemas(tal como software defectuoso)

1.5.5 AuC (Authentication Center)

El centro de autentificación se asocia con un HLR. El AuC almacena la clave de autentificación del suscriptor (ki), así como su correspondiente IMSI (International

Mobil Suscriber Identity). Estos son datos permanentes que entran en el momento de la suscripción.[2]

El AuC es asociado con un HLR y almacena una clave de identidad (KI) para cada subscriptor móvil registrado con el HLR. Esta clave es utilizada para generar datos de seguridad para cada subscriptor móvil: [10]

- Datos, los cuales son usados para autentificación del IMSI (International Mobile Subscriber Identity) y la red.
- Una clave usada para verificar la integridad de la comunicación sobre la ruta de radio entre el móvil y la red.

1.5.6 SGSN (Serving GPRS Support Node)

El SGSN es el elemento central en la conmutación de paquetes dentro de la red. El SGSN se conecta con UTRAN mediante la interfaz lu-PS y con el GSM-BSS mediante la interfaz GB.[2]

1.5.7 Gateway MSC (GMSC)

GMSC es un MSC que está localizado entre la PSTN y los otros MSCs en la red. Su función es rutear llamadas entrantes al apropiado MSC. [2]

La elección de cual MSC puede actuar como GMSC lo decide el operador. [10]

1.6 Elementos de UTRAN

El UMTS Radio Access Network (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)

La otra posible implementación en el futuro puede incluir, por ejemplo, el Broadband Radio Access Network (BRAN) y el UMTS Satellite Radio Access Network (USRAN).

UTRAN consiste de RNCs (Radio Network Controllers) y Nodo Bs(Base Stations). Ambos elementos forman un RNS(Radio Network Subsystem).

La tecnología básica para UMTS Terrestrial Radio Access Network (UTRAN) tiene diversos elementos, los cuales se muestran en la figura 1.4, y se describirán posteriormente.

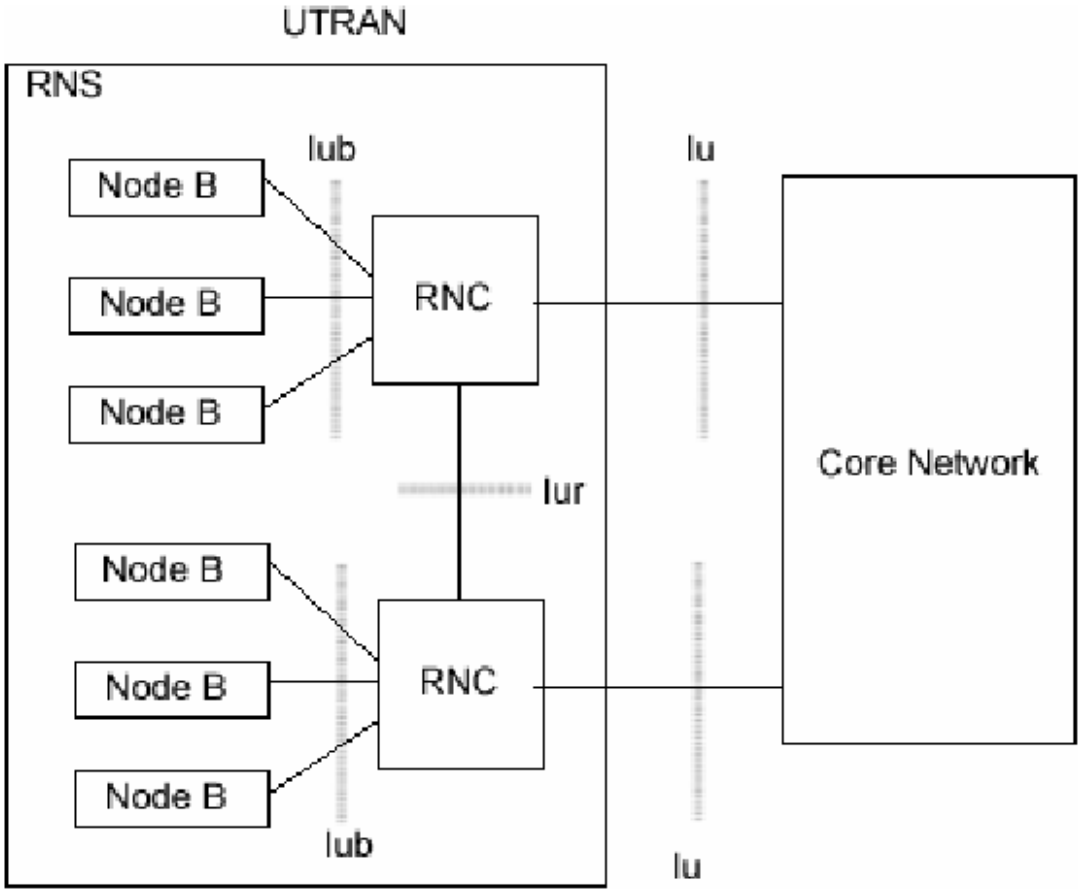


Figura 1.4. Arquitectura de UTRAN [2]

1.6.1 RNC (Radio Network Controller)

RNC controla uno o más nodos Bs. Este puede ser conectado a un MSC mediante la interfaz IuCS, o a un SGSN mediante la interfaz IuPS. Un RNC es comparable a un BSC (Base Station Controller) en redes GSM.

El área RNC es un área de cobertura de radio que consiste de una o más células controladas por un RNC. [10]

Un RNC es un componente en la red, el cual tiene la función de controlar uno o más nodos B. [10]

1.6.2 NODO B

En UMTS el nodo B es equivalente a una radio base. Éste puede soportar una o más células, aunque en general las especificaciones solo hablan acerca de una célula por Nodo B.

El nodo B es equivalente en UMTS al BTS (Base Transceiver Station) de GSM. El nodo B puede dar servicio a una o más células, sin embargo es recomendable que sólo a una. En éste se encuentra la capa física de la interfaz aérea.

Uno de los principios ha sido conservar el manejo de la movilidad y el manejo de la conexión independientes de la tecnología de radio en las interfaces aéreas. Esta idea se puede llevar a cabo por la realización de los conceptos AS (Access Stratum) y NAS (Non Access Stratum).El AS es una entidad funcional que incluye los protocolos de acceso de radio entre el UE y UTRAN. Dichos protocolos terminan en UTRAN. El NAS incluye la red central, y los protocolos entre el UE y la misma CN. Dichos protocolos no terminan en UTRAN, sino en la red Central (CN) en donde UTRAN es transparente para el NAS. [1]

La interfaz de radio puede ser definida como el conjunto de parámetros físicos de radio (radio frecuencia, espaciamiento de canal, modulación, etc.) y

protocolos para formar el enlace de comunicación entre un móvil y una radio base dentro de la combinación del ambiente operado de radio y ambiente de servicio.

1.7 Equipo de usuario (UE)

Un UE en UMTS puede operar en uno de los tres modos de operación: CS, PS/CS o PS. Para UMTS, las capacidades de acceso de radio del UE han sido fijadas para soportar un gran monto de diferentes parámetros. [1]

El UE incluye parámetros multimodo, lo cual significa que el móvil está hecho para soportar tanto UTRA FDD, como UTRA TDD. Además que está hecho para soportar tanto UMTS, como GSM.

Las siguientes son vistas como aumentos de las perspectivas del equipo de usuario: [9]

- Incremento de la vida de la batería del móvil
- Un más fácil entendimiento de las interfaces usadas.
- Incremento del tiempo de actividad
- Soporte de descarga de seguridad de aplicaciones al UE.

Dos modos de conexión son definidos para el UE, modo desocupado (idle) y modo conectado.

El modo conectado se realiza cuando la conexión RRC es establecida, la cual se realiza entre el UE y un RNC llamado SRNC.

El UE deja el modo conectado, y regresa al modo desocupado cuando la conexión RRC es liberada o falla la conexión RRC.

En la figura 1.5 se muestra el principio de conexión del UE cuando CN consiste de dos separados nodos de servicio (CS o PS) o un combinado nodo de servicio (CS y PS).

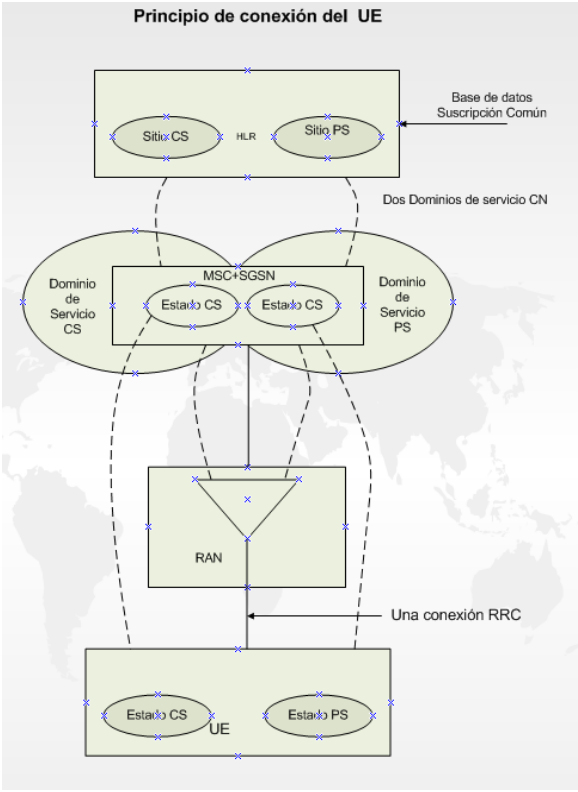


Figura 1.5. Principio de conexión del UE

En el caso de una arquitectura integrada CN, el CN consiste de ambos dominios, tanto CS como PS con un combinado MSC y SGSN en el nodo principal. Dentro de UE se encuentra USIM (UMTS Subscriber Identity Module). Un requerimiento de UMTS USIM, es que proveerá nuevas y aumentadas características de seguridad. [14]

USIM tendrán una única identidad y serán asociadas con uno y sólo un ambiente. En una zona será posible identificar únicamente a un usuario por el USIM. El USIM será usado para proveer características de seguridad, también es posible actualizar información específica de USIM a través de la interfaz aérea, en una manera segura. [14]

USIM es una evolución de las SIMs utilizadas en GSM, y en el sistema UMTS estas tarjetas son de mayor memoria, capacidad y permiten un mejor desempeño. Esto debido a que el comercio electrónico y las transacciones financieras usando las USIM's se convertirá en una de las aplicaciones más importantes y los usuarios podrán utilizar su misma tarjeta en cualquier unidad móvil sobre cualquier red.

1.8 Modulación de los datos

Al hablar de un sistema de tercera generación de telefonía celular, dentro de una gama de posibilidades de técnicas, las más utilizadas pueden ser FSK, ASK, PSK.

El sistema UTRAN utiliza la modulación QPSK (Quadrature Phase Shift Keying) en el enlace de bajada. Por su parte en el enlace de subida, UTRAN utiliza un esquema de combinaciones complejas en donde UTRAN utiliza generalmente el nombre de QPSK de canal dual y 16QAM.

En la tabla 1.3 se muestran algunos parámetros básicos de modulación, en los cuales también se muestran algunas características de spreading.

Velocidad	La misma como la básica velocidad en FDD: 3.84 Mchip/s	Baja velocidad: 1.28 Mchip/s
Modulación de datos	QPSK,16QAM (solo HS- PDSCH)	QPSK, 8PSK,16QAM (solo HS-PDSCH)
Características de Spreading	Ortogonal Q chips/symbol, donde $Q = 2^p$, $0 <= p <= 4$	Ortogonal Q chips/symbol, donde $Q = 2p$, $0 <= p <= 4$

Tabla 1.3. Parámetros de modulación básica [15]

1.9 Interfaces

Las interfaces en el sistema UMTS siguen la convención GSM/GPRS. UTRAN contiene algunas nuevas interfaces, y por lo tanto algunos nuevos nombres. [2] Desde el punto de vista de las especificaciones, hay tres tipos de interfaces en la red UMTS/ GSM.

La primera categoría contiene las interfaces que son verdaderamente abiertas. Esto significa que ellas son especificadas, y la especificación hace que se pueda adquirir equipos de diferentes fabricantes. En la vieja red GSM, sólo la interfaz A y la interfaz aérea son verdaderamente abiertas. [2]

La segunda categoría incluye las interfaces que son especificadas en algunos niveles, pero la interfaz tiene silenciosamente propietario. El equipo para

el cual la interfaz podría venir del mismo fabricante. Un buen ejemplo de ello es la interfaz A-bis. [2]

La tercera categoría contiene las interfaces para las cuales no hay especificación. Un ejemplo de ellos es la interfaz A e I en la red GSM. [2]

1.9.1 Interfaz Iu

Esta interfaz conecta el núcleo de red y el UMTS Radio Acces Network(URAN). Ésta es considerada como un punto de referencia. URAN puede tener varios tipos de implementaciones físicas. La primera en ser implementada es UTRAN. La segunda que puede ser implementada es Broadband Radio Access Network (BRAN).

El UMTS Satellite Radio Access Network (USRAN) conecta una red satelital al Core Network, pero esto se tiene pensado implementar en el futuro.

Dentro de Iu, se encuentra Iu-CS e Iu-PS. Iu-CS es la instancia física de Iu hacia el dominio de servicio de conmutación de circuitos del CN. Iu-PS es la instancia física de Iu hacia el dominio de servicio de conmutación de paquetes del CN.

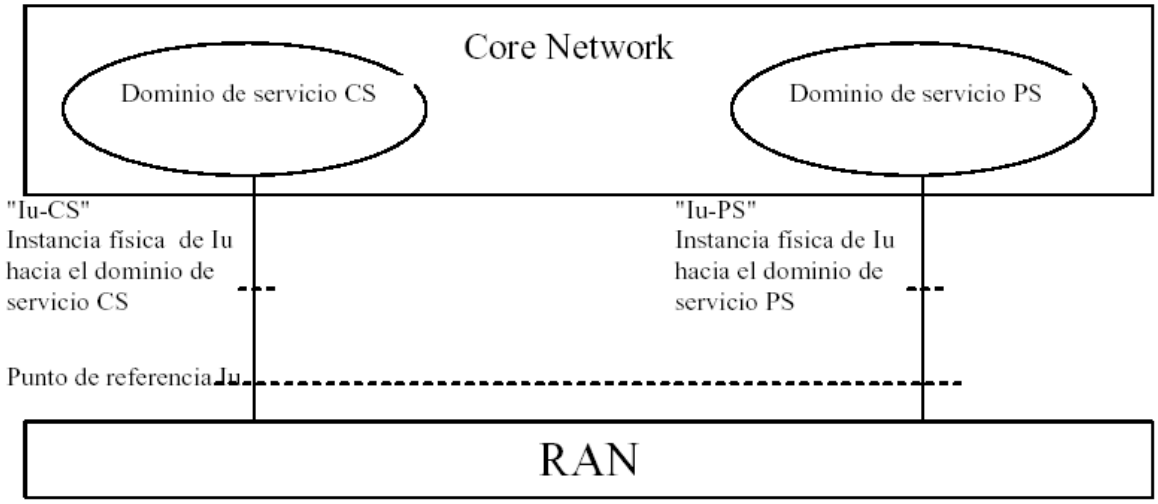


Figura 1.6. Punto de referencia Iu

En la Figura 1.6 se muestra la interfaz Iu, ya sea si se requiere conmutación de circuitos o conmutación de paquetes, en donde RAN representa UTRAN, ya que actualmente la red de acceso satelital se está implementando.

1.9.2 Interfaz Iub

Esta interfaz está situada entre el RNC y el nodo B en el UTRAN. En términos de GSM ésta corresponde a la interfaz A-bis, la cual está entre el BTS y el BSC. Cuando el RNS consiste de un RNC y uno o más nodos B, esta interfaz es usada entre el RNC y Nodo B para soportar servicios ofrecidos al usuario y suscriptor UMTS. La interfaz además permite control del equipo de radio y asignación de radio frecuencias en el nodo B. [10]

1.9.3 Interfaz Iur

La interfaz Iur conecta dos RNC. Ésta interfaz puede soportar el intercambio de información y datos de usuarios.

1.9.4 Interfaz Uu

Esta interfaz se encuentra entre el equipo de usuario y la red UTRAN.

1.9.5 Interfaz Iu

Esta interfaz conecta a la red central con la red de acceso de radio de UMTS (URAN).

1.9.6 Interfaz MAP

Las interfaces que hay entre algunos elementos del Core Network son llamadas interfaces MAP, ya que ellas generalmente usan el protocolo Mobile Application

Part (MAP) como protocolo de señalización.

La introducción de GPRS en GSM trajo nuevas interfaces, las cuales fueron nombradas usando la letra G con una pequeña letra. A continuación se muestra una lista del significado de las diferentes interfaces "Gx", de acuerdo al nombre proveniente en inglés de la segunda letra.

Gf = "fraud" interface

Gi = "Internet" interface

Gp = "PLMN" interface

Gc = "context" interface

Gn = "node" interface

Gb = "base" interface

Gn y Gp son las interfaces entre SGSN y GGSN. Estas interfaces son usadas para soportar movilidad entre el SGSN y GGSN. La interfaz Gn es usada cuando GGSN y SGSN son localizados dentro de un PLMN. La interfaz Gp es usada si GGSN y SGSN son localizados en diferentes PLMNs. La interfaz Gn/Gp además incluye una parte en la cual permite a SGSNs para comunicar suscriptores y datos de usuario, cuando se cambia SGSN.[10]

La interfaz **Gc** es la ruta entre GGSN y HLR. Esta opcional ruta de señalización puede ser usada por el GGSN para recuperar información acerca de la localización y soporte de servicios para el suscriptor, para ser capaz de activar una dirección de red de paquetes de datos. [10]

La interfaz **Gf** es la interfaz usada entre SGSN y EIR para intercambiar datos, en función que EIR pueda verificar el estado de IMEI recuperado del móvil.[10]

La interfaz entre MSC/VLR y SGSN se denomina interfaz **Gs**. El SGSN puede enviar información de localización hacia el MSC/VLR a través de la opcional interfaz Gs.

El SGSN puede recibir solicitud de voceo del MSC/VLR a través de la interfaz GS. El MSC/VLR puede indicar a un SGSN, a través de la interfaz Gs, que un móvil está comprometido en un servicio manejado por el MSC. [10]

1.9.7 Interfaz B

La interfaz que hay entre el MSC y su asociado VLR se denomina interfaz B. El VLR es la base de datos de control para el roaming del suscriptor móvil en el área controlada por el asociado MSC. Cuando sea que el MSC necesite datos relacionados al móvil en esta área, éste interroga al VLR. Cuando un móvil inicia actualización de lugar con un MSC, el MSC informa al VLR, el cual almacena la información relevante. Cuando un usuario activa un servicio suplementario específico, o modifica algunos datos atribuidos a un servicio, el MSC informa(a través del VLR) al HLR, el cual almacena esta información y actualiza el VLR, si lo requiere.

1.9.8 Interfaz C

La interfaz que hay entre el MSC y su asociado HLR se denomina interfaz C. El MSC puede interrogar al HLR del requerido suscriptor para obtener información para una llamada o mensaje corto dirigido a ese suscriptor. [10]

1.9.9 Interfaz D

La interfaz que hay entre el HLR y el VLR se denomina interfaz D. Esta interfaz es usada para intercambiar datos relacionados a la localización del móvil y a la administración del suscriptor. El principal servicio que se provee al móvil es la capacidad para establecer o recibir llamadas dentro de dicha área de servicio. El VLR informa al HLR de la localización de un móvil controlado con su número de equipo. El HLR envía hacia el VLR todos los datos necesarios para soportar el

servicio del móvil. El HLR entonces instruye al previo VLR para cancelar el registro de localización del suscriptor. Intercambio de datos puede ocurrir cuando el suscriptor requiere un servicio particular, cuando él requiere cambiar algunos datos asignados a su suscripción, o cuando algunos parámetros de suscripción son modificados. [10]

1.9.10 Interfaz F

La interfaz que hay entre el MSC y EIR se denomina interfaz F. Esta interfaz es usada entre MSC y EIR para intercambiar datos, en orden que EIR pueda verificar el estado IMEI recuperado del móvil. [10]

1.10 Direccionamiento IP

Con la introducción de la tercera generación (UMTS/IMT-2000) en donde las capacidades de segunda generación serán extendidas, añadiendo capacidades multimedia a las plataformas de segunda generación, tal como el soporte para altas velocidades de bit y la introducción de acceso a paquetes de datos mediante IP.[10]

La arquitectura UMTS/GSM soportará IPv4 / IPv6, basados en los siguientes puntos:

- Transporte IP entre elementos de la red de la conectividad de servicios IP (entre RNC, SGSN y GGSN) y transporte IP para el dominio CS: Ambos IPv4 e IPv6 son opciones para conectividad IP.

- Elementos del subsistema IM CN:
    - La arquitectura hará un óptimo uso de IPv6
    - Las especificaciones 3GPP diseñan el subsistema IM CN, en donde elementos e interfaces exclusivamente soportan IPv6. Sin embargo algunas implementaciones IM anteriores pueden usar IPv4.
    - Las especificaciones 3GPP diseñan el UE exclusivamente para soportar IPv6 par la conexión al subsistema IM CN. Sin embargo UE pueden en adición soportar IPv4. El cual permite para la conexión a los primeros subsistemas IM CN que sólo usen IPv4.
- Acceso a existentes servicios de datos (Intranet, Internet)
- El UE puede accesar servicios basados en IPv4 e IPv6.

En la figura 1.7 se muestra una instalación en donde el UE tiene tanto IPv4 como IPv6:

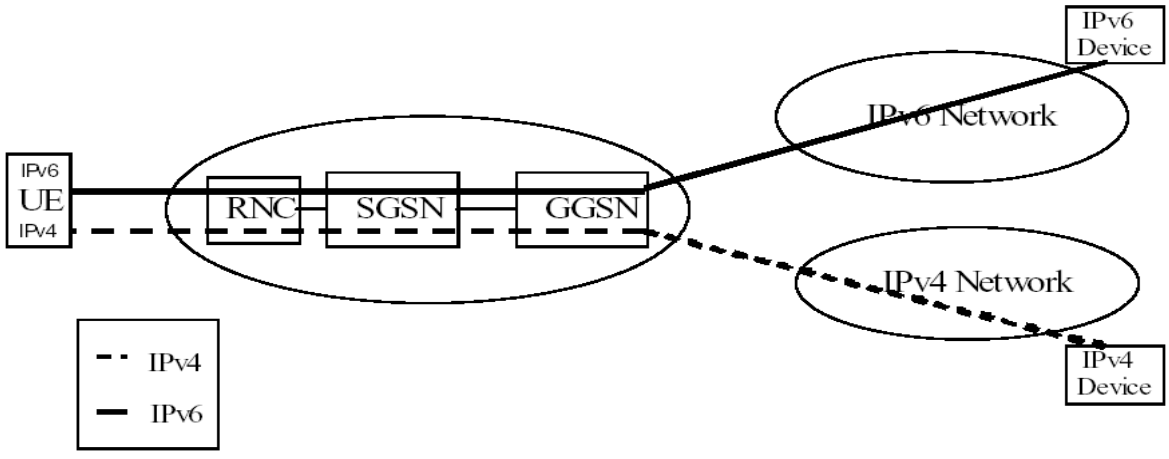


Figura 1.7. UE conectado a redes IPv4 e IPv6 [16]

Este escenario no necesita algún soporte de transición específica de la red. Sin embargo éste requiere ambas versiones de IP en el UE. El GGSN en este escenario puede ser diferente para la conexión IPv4 e IPv6.

También puede existir otro escenario en donde el móvil usando IPv6 se conecta a un diseño IPv6 a través de una red IPv4, lo cual se muestra en la figura 1.8.

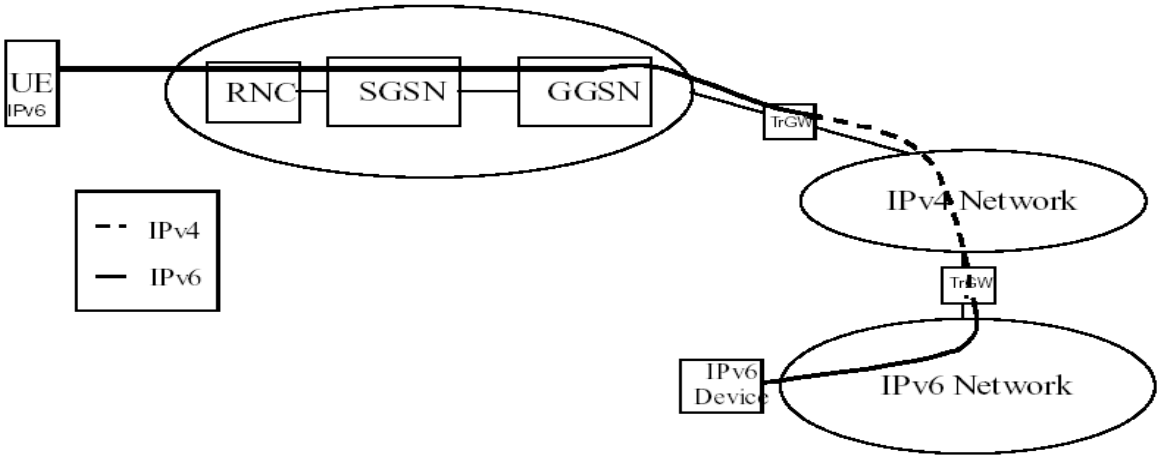


Figura 1.8. UE IPv6 conectado a un diseño IPv6 vía una red IPv4

Los dominios IPv6 pueden ser interconectados como un automático o configurado tunneling de IPv6 sobre IPv4.

1.11 Relación entre UMTS y WCDMA

UMTS es un sistema muy generalizado en donde se encuentra el estándar WCDMA. Se podría decir que sólo WCDMA es una parte del sistema UMTS, es decir es sólo la interfaz aérea de UMTS. Por lo tanto UTRAN, que también se puede llamar WCDMA, es una parte de la interfaz de radio de UMTS.

La interfaz aérea en UMTS tiene un soporte flexible de servicios mezclados, servicios de velocidad variable, y un eficiente modo de paquetes. Cabe destacar que la interfaz entre el UE y la red UTRAN es la tecnología WCDMA, es decir, la conexión entre el equipo de usuario y la red de acceso de radio para UMTS es mediante la tecnología WCDMA. [8]

UTRAN es la red de radio acceso diseñada especialmente para UMTS. Sus fronteras son la interfaz Iu al núcleo de red y la interfaz Uu (interfaz de radio) al equipo de usuario (UE).

La clave de las propiedades enfatizadas en WCDMA es mejorar funciones en sistemas de segunda generación incluyendo:

- Mejora de capacidad.- Donde la principal razón para la mejora es la frecuencia extra debido al alto ancho de banda
- Mejora de cobertura
- Un alto grado de servicios flexibles, incluyendo:
    - Soporte de un rango ancho de servicios con máxima velocidad de bit acerca de los 2 Mbps y la posibilidad para múltiples servicios en una sola conexión.
- Un alto grado de flexibilidad de operación
- El rápido control de potencia en el downlink dará mejoras en las funciones
- Soporte flexible de nuevos servicios multimedia.- Esto se logra con servicios de velocidad variable

El principal parámetro de WCDMA es la capa física. WCDMA soporta dos nodos básicos de operación: FDD (Doble división de frecuencia) y TDD (doble división de tiempo). En el modo FDD, la frecuencia portadora es 5 Mhz ya sea para el Uplink o para el downlink. En TDD sólo los 5 Mhz se comparten en tiempo entre el uplink y el downlink.

UTRAN consiste de RNCs (Radio Network Controllers) y Nodo Bs (Base Stations). Ambos elementos forman un RNS (Radio Network Subsystem).

CAPITULO 2

NORMALIZACION DE LOS SISTEMAS MOVILES 3G

2.1 Introducción a la normalización

Hoy en día la normalización es una disciplina esencial para todos los actores 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.

Hoy, las numerosas compañías que han hecho de la normalización un elemento técnico y comercial esencial de sus actividades saben, que si ellas no participan corren el riesgo de tener que sufrir unas normas que difícilmente tendrán en cuenta sus intereses. 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).

2.2 Evolución Histórica de la Normalización

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). En Europa, el programa RACE I, lanzado en 1988, comenzó el trabajo básico de investigación. Este fue seguido por el programa RACE II, durante los años 1992-95, que condujo al desarrollo de los prototipos del CDMA (Acceso Múltiple por División de Código) y del ATDMA (Acceso

múltiple con división de tiempo avanzado). Conjuntamente, otras interfaces aire de banda ancha estaban siendo estudiadas en Europa, Japón y otros países. Este trabajo continuó dentro del programa ACTS (Servicios y Tecnología de comunicaciones avanzadas) del proyecto FRAMES (Futuro sistema de radio acceso múltiple de banda ancha).

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. Se hizo evidente que sería muy difícil alcanzar especificaciones idénticas para asegurar una compatibilidad global de los equipos que era un requisito crucial con todo este trabajo realizándose en paralelo. Sin embargo, hubo iniciativas para crear

un foro único para la normalización de una especificación común del UTRA. El proyecto 3GPP fue establecido en 1998 con este objetivo en mente. En él participan los siguientes socios: TTC/ARIB por Japón, ETSI por Europa, TTA por Corea, T1P1 por EE.UU. y, más recientemente (1999), CWTS por China. Casi al mismo tiempo, el mercado celular norteamericano creó el grupo 3GPP2 para trabajar sobre la tecnología de radio rival cdma2000, y el UWCC (Universal Wireless Communication Consortium) fue ampliado para cubrir la tecnología

UWC136 ó IMT-SC (Single Carrier). Estos dos grupos industriales se apoyan en los 41 protocolos de movilidad del ANSI (Institutito Nacional de Estándares Americanos) definidos en el comité TIA TR45.2.

Los dos consorcios, junto con el UWCC y el proyecto ETSI que trabajan sobre el sistema DECT de 2 Mbit/s (Telecomunicación Inalámbrica mejorada digitalmente), están trabajando a través de sus propios organismos de normalización para completar el marco UIT para las tecnologías radio para el IMT2000, como se muestra en la Figura 2.1

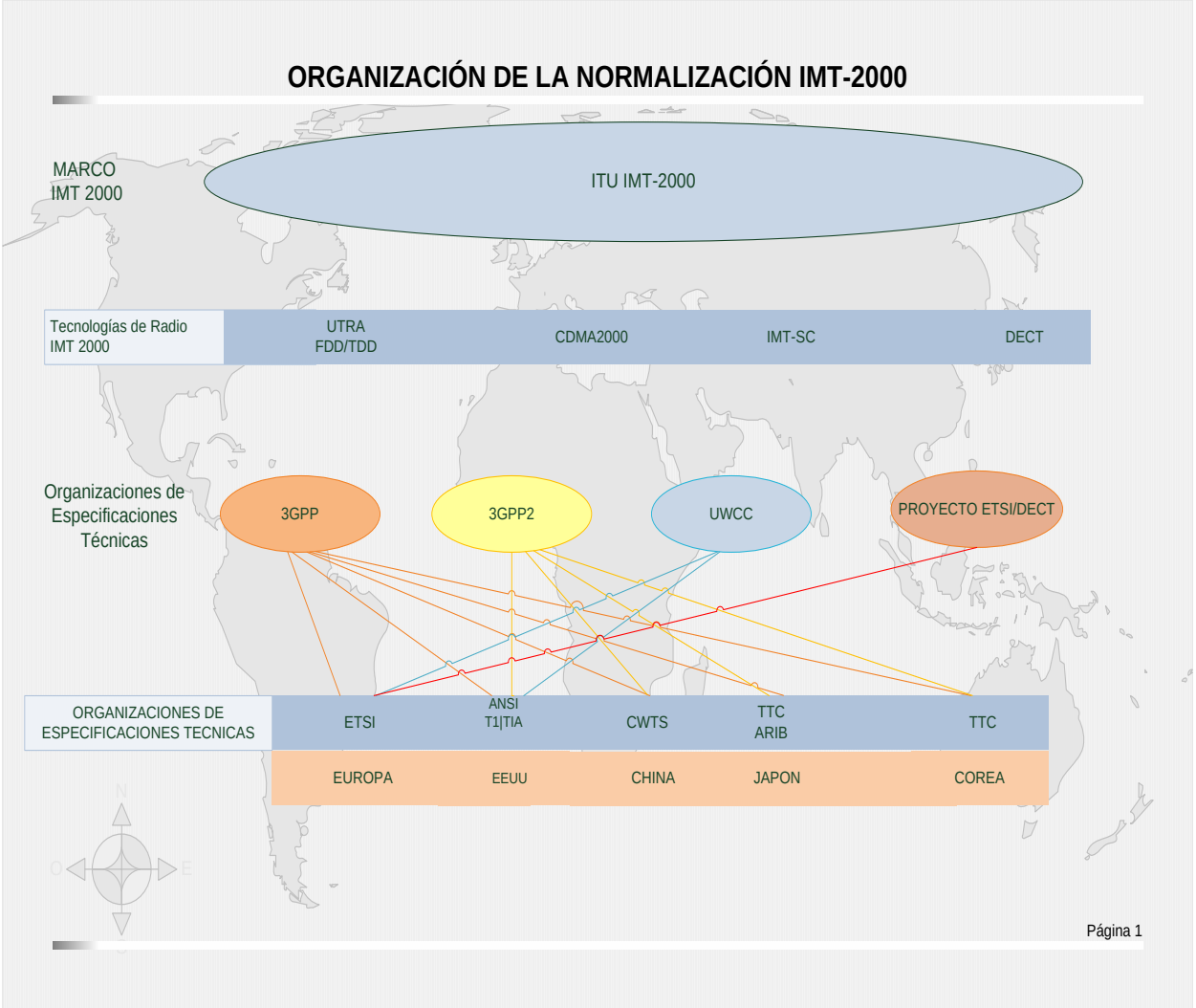


Figura 2.1. Organización de la normalización IMT-2000

2.3 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).

• El OHG (Grupo de armonización de operadores) ha jugado un papel esencial “en la trastienda” para poner de acuerdo a los competidores en el mercado de la movilidad (GSM, CDMA, TDMA) y desactivar la situación explosiva que se produjo durante 1999

acerca de la armonización de las normas de radio 3G. El grupo continúa reuniéndose, junto a representantes de la industria, para discutir sobre la evolución de las normas de los móviles 3G.

Las relaciones entre todos estos organismos puede parecer muy compleja, pero en la práctica la situación está más clara si uno considera el flujo de ideas y la jerarquía de la influencia técnica que existe. 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”.

Estas son, a su vez, referenciadas y/o resumidas por la UIT en sus “recomendaciones” oficiales. En paralelo algunos de esos mismos expertos están involucrados en los organismos que “establecen los requisitos”, tales como OHG, MWIF y 3G.IP, donde pueden discutir acerca de la problemática del funcionamiento de los distintos sistemas y sobre la armonización.

2.4 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.

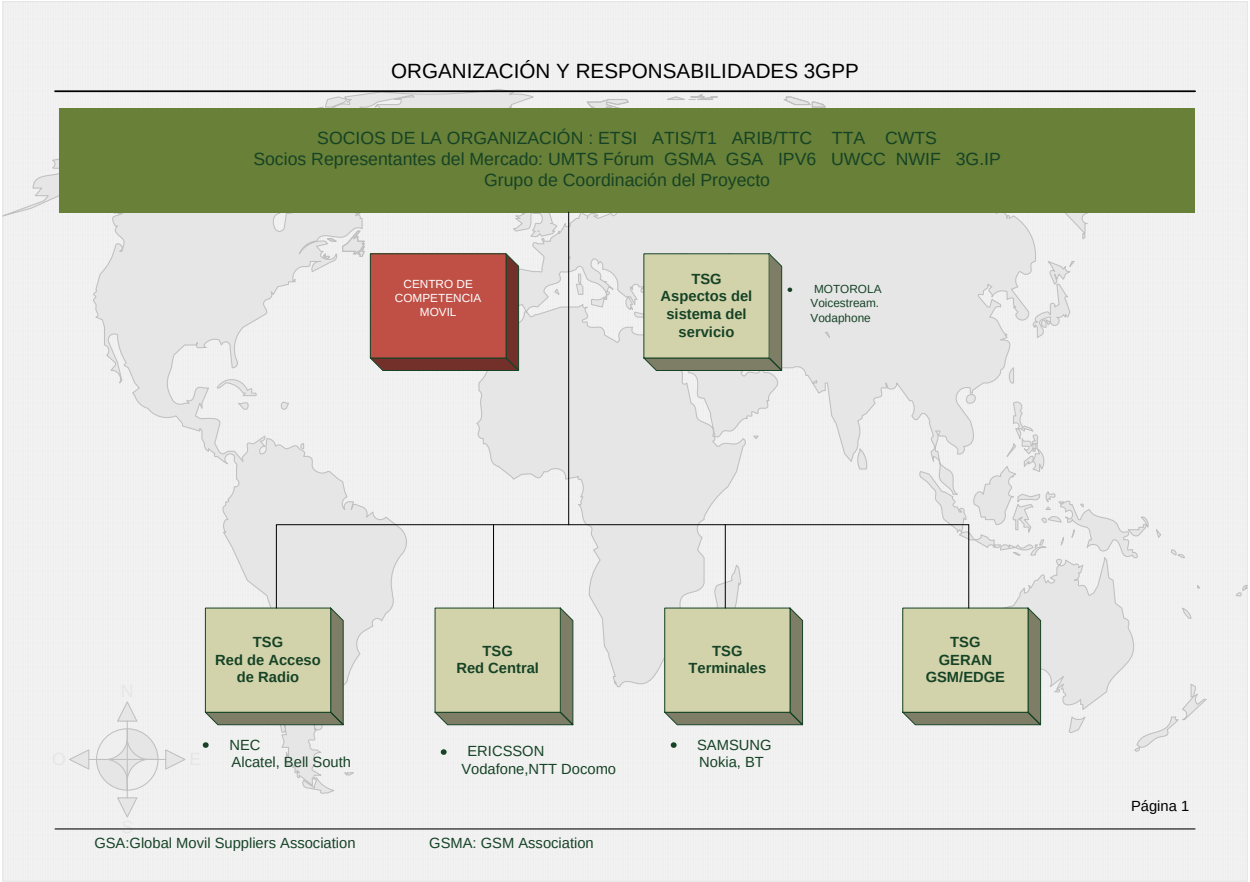


Figura 2.2 Organización y Responsabilidades 3GPP

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, que incluye:

• *Socios de la Organización (OP):* Estos son organismos de normas abiertas que están oficialmente reconocidos en sus propios países y que tienen la capacidad y autoridad para definir, publicar y establecer normas a nivel nacional o regional, y que han firmado el acuerdo de participación en el proyecto.

• *Socios Representantes del Mercado (MRP):* Estos socios son responsables de la identificación de los requisitos de mercado. Su papel en el 3GPP es el de llegar a un consenso sobre los requisitos de mercado (por ejemplo, servicios, facilidades y funcionalidad). Un MRP es invitado por los Socios de la Organización.

• *Miembros Individuales (IM):* Los IMs contribuyen técnicamente o de otra manera a los Grupos de Especificaciones Técnicas. Tienen que ser miembros de una OP.

• *Observadores:* La categoría de "Observador" puede ser concedida por los Socios de la Organización a una entidad que tiene las cualificaciones para llegar a ser en el futuro un Socio de la Organización. El trabajo técnico detallado se lleva a cabo en los Grupos de Especificaciones Técnicas (TSG). Las tareas de estos grupos son las de especificar, aprobar y mantener las especificaciones técnicas y los informes. El grupo de Aspectos de los Sistemas y Servicios es responsable de la coordinación técnica del trabajo emprendido dentro del 3GPP, así como de la integridad de la arquitectura total del sistema.

Como se indica en la Figura 2.2, existen cinco TSGs, cada uno de ellos dividido en subgrupos:

• *El TSG de los Aspectos del Sistema y del Servicio:* Responsable de la definición y el desarrollo de la capacidad del servicio, fase uno, así como de la descripción de la tarificación y de la contabilidad, aspectos de la gestión de red y de seguridad, definición

de la arquitectura total, evolución y mantenimiento, principios para la definición de la transmisión extremo a extremo (aspectos del codec), y coordinación del proyecto.

• *El TSG de la Red de Acceso Radio:* Este TSG es el más relacionado con la tecnología CDMA. Es el responsable de las especificaciones de las capas 1 a 3, especificación de las interfaces Iu-b, Iu-r y Iu, requisitos de operación y mantenimiento de la UMTS Terrestrial Radio Access Network (UTRAN), rendimiento de la estación base de la radio, y especificaciones de las pruebas de homologación de los productos.

• *El TSG de la Red Central:* Este TSG es responsable de la gestión de la movilidad, señalización de control de las conexiones de las llamadas entre el equipo del usuario y la red central, definición de las características de interfuncionamiento, cuestiones relacionadas con paquetes tales como mapa de la calidad de servicio, aspectos de la interfaz Iu relacionados con la red central, y requisitos de operación y mantenimiento de la red central.

• *El TSG del Terminal:* Este TSG está encargado de los protocolos de capacidad del servicio, mensajería, interfuncionamiento extremo a extremo de los servicios, interfaz del terminal móvil con el módulo UMTS, modelo e infraestructura de las interfaces de los terminales y ejecución de los servicios, y especificaciones de las pruebas de homologación de los terminales, incluyendo los aspectos radio.

• *El TSG GERAN:* Creado a mediados del año 2000 para asegurar la cohesión entre las especificaciones del GSM y del 3G. El TSG GSM/EDGE Radio Access Network (GERAN) es responsable del mantenimiento y desarrollo de las especificaciones y los

informes técnicos del GSM, incluyendo las tecnologías evolucionadas del acceso radio GSM tales como el GPRS y el EDGE.

Además, existe un Centro de Competencia Móvil (MCC), cuyo papel es el de proporcionar soporte administrativo y técnico para los temas de gestión de red y las peticiones de cambios.

La toma de decisiones dentro del Grupo de Coordinación del Proyecto (PCG) y los TSGs está basada en el consenso entre los Socios de la Organización en el PCG, o entre los Miembros Individuales en el TSG, o por votación cuando esta es inevitable.
El 3GPP define con gran precisión las reglas para la toma de decisiones en cada uno de los niveles de la organización.

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.

2.5 Tecnología de radio IMT2000

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.

Aunque definidas dentro de un marco global, varias interfaces de radio han sido adoptadas para el móvil 3G. Esto fue necesario ya que, incluso después de largas discusiones, no todo el mundo involucrado pudo llegar a un acuerdo sobre una única interfaz radio debido a diferentes razones de tipo político, histórico y técnico.

La elección de la interfaz radio es crucial ya que determina no sólo la capacidad de la red de radio móvil, sino que también tiene relación con aspectos tales como las interferencias, la propagación de camino múltiple, y la entrega de las llamadas de una estación base a otra, cuando los abonados se mueven entre ellas. Consecuentemente, la elección de la interfaz radio afecta en gran medida a la complejidad y al costo del sistema.

Para entender qué es lo que se está desarrollando y el porqué, comencemos por uno de los requisitos establecidos para los sistemas 3G como es el de soportar tasas de datos de usuario variables tan altas como 2 Mbit/s. De una forma o de otra, todas las tecnologías de radio adoptadas hacen posible la adaptación de la anchura de banda bajo demanda.

Algunos sistemas utilizan el WCDMA para la interfaz radio, mientras que otros usan distintas variedades del TDMA.

En el caso del CDMA, los bits de información del usuario están distribuidos sobre una anchura de banda ampliada artificialmente, multiplexándolos con un flujo de

bits con una tasa de bits pseudoaleatoria más alta. Los bits en el flujo de bits pseudoalatorio, normalmente llamado código disperso, son referenciados como chips.

Esta operación aumenta la anchura de banda que ocupaba la información original. La relación de la tasa del chip con la tasa de información original se llama ganancia de dispersión.

Por sí misma, la dispersión del espectro no aporta ningún beneficio. Es la combinación de dispersión con la ausencia de ésta, incluyendo todas las técnicas avanzadas de proceso de la señal implantadas en el receptor, lo que hace que el CDMA sea atractivo. Una de las principales razones es que los mismos juegos de frecuencias pueden ser usados por cada una de las estaciones base de una red, debido a que cada conexión está asignada a un código de dispersión diferente. Una segunda razón tiene que ver con su capacidad para resolver caminos de propagación diferentes, convirtiendo la distorsión del camino múltiple en una buena aliada en vez de ser una molestia destructiva. Para ayudar a entender esta idea, conviene recordar que el FDMA evita que las conexiones de usuario puedan interferir unas con otras asignándoles distintas bandas de frecuencia. Mientras que los sistemas TDMA hacen esto por medio de la asignación de distintas ranuras de tiempo. Cuando se usa CDMA, las conexiones de usuario usan las mismas ranuras de tiempo y bandas de frecuencia, pero se distinguen unas de otras por los diferentes códigos de dispersión.

En la operación de agrupamiento (no dispersión) se extraen todas las señales de interés. Las otras señales multiplexadas con códigos de dispersión diferentes simplemente se añaden al ruido de fondo, lo cual limita el número de usuarios que pueden compartir un canal. Para que el sistema funcione, las potencias transmitidas

deben controlarse estrictamente de tal manera que las señales desde todos los terminales móviles lleguen a la estación base con, aproximadamente, la misma fuerza (igualmente para el enlace descendente) a pesar de sus distintas distancias a la estación base y a las diferentes condiciones de propagación. El bucle de control de potencia realiza medidas en el móvil y en la estación base. Los canales de control usados para informar de las medidas operan entre 800 Hz y 1,5 KHz. En el caso del WCDMA, se utilizan dos modos básicos (FDD y TDD) para el funcionamiento con bandas apareadas y con bandas no apareadas, respectivamente. Los modos FDD y TDD están definidos de la siguiente forma:

• *FDD:* Las transmisiones de los enlaces ascendentes y descendentes usan dos portadoras diferentes localizadas en bandas de frecuencia específicas. Los usuarios que usan el mismo juego de portadoras se distinguen por distintos códigos de dispersión.

• *TDD:* Las transmisiones de los enlaces ascendentes y descendentes se transportan sobre las mismas portadoras usando intervalos de tiempo sincronizados. Las ranuras de tiempo están divididas en partes emisoras y receptoras.

La información se transmite alternativamente sobre el enlace ascendente y el enlace descendente. Además, los usuarios que comparten las mismas ranuras de tiempo y portadora están multiplexados en modo CDMA.

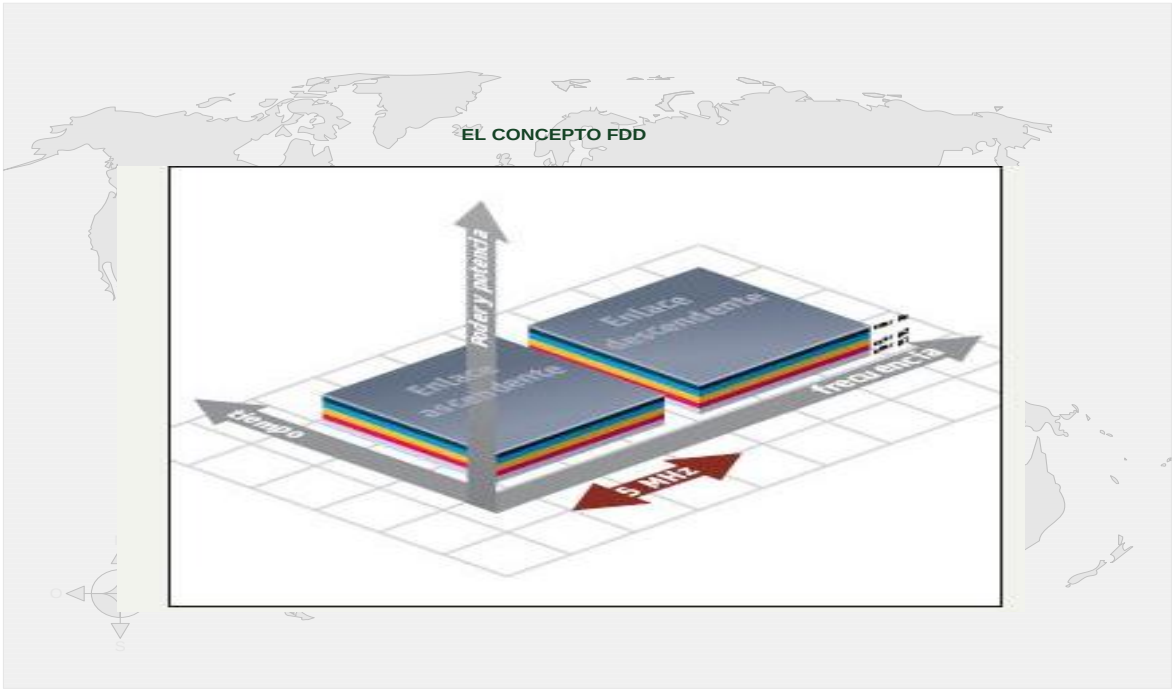


Figura 2.3. El concepto FDD

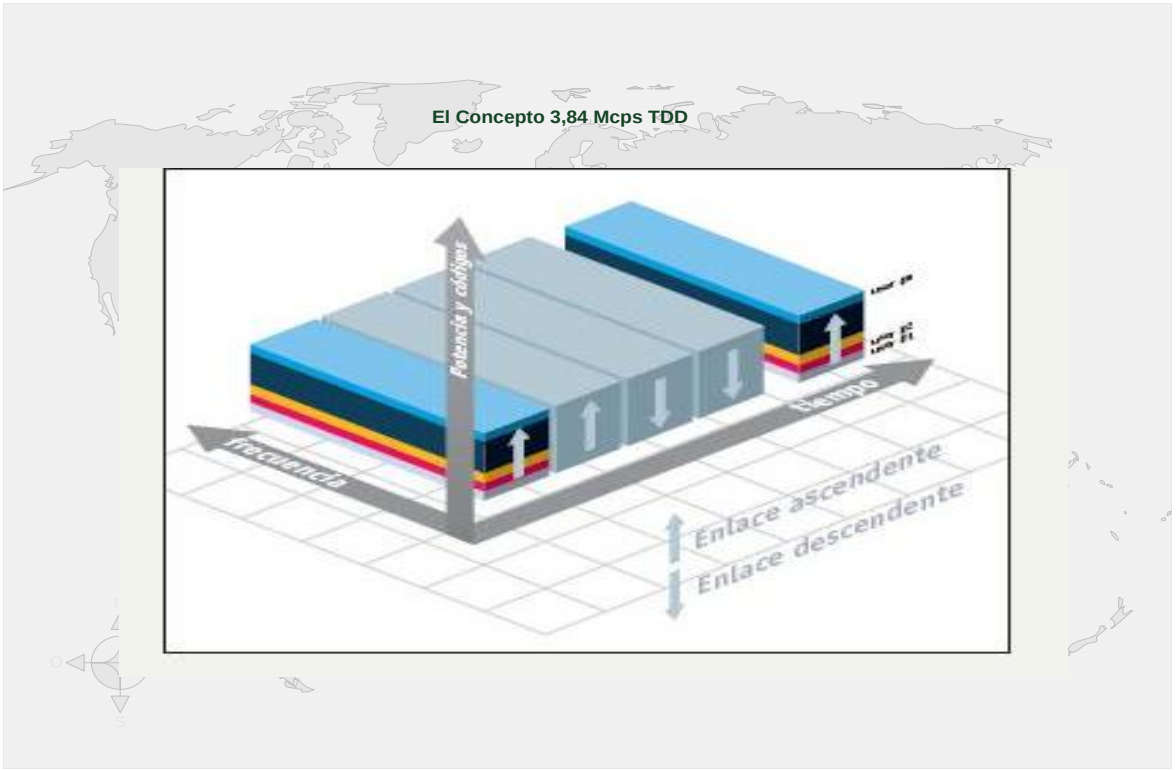


Figura 2.4 El Concepto 3.84 Mcps TDD

Las Figura 2.3 y 2.4 son representaciones conceptuales de las técnicas FDD y TDD, respectivamente. El TDD incluye dos modos:

• TDD a 3,84 Mcps1 (también llamado TDD de alta tasa de chip).

• TDD a 1,28 Mcps (también llamado TDD de baja tasa de chip, y también TD-SCDMA por el organismo de normalización chino CWTS).

Las diferencias entre los TDDs de alta y baja tasa de chip no están limitadas a la frecuencia del chip. Las estructuras de las tramas son también diferentes, lo que afecta a los rendimientos del sistema de varias maneras.

Está generalmente aceptado que el modo TDD a 3,84 Mcps es el más adecuado para la cobertura de las pico y micro-celdas en áreas densamente pobladas, mientras que el modo FDD es el más adecuado para un área de cobertura más extensa. El TDD hace un mejor uso de los recursos de radio que el FDD para tráfico asimétrico y tasa alta de datos.

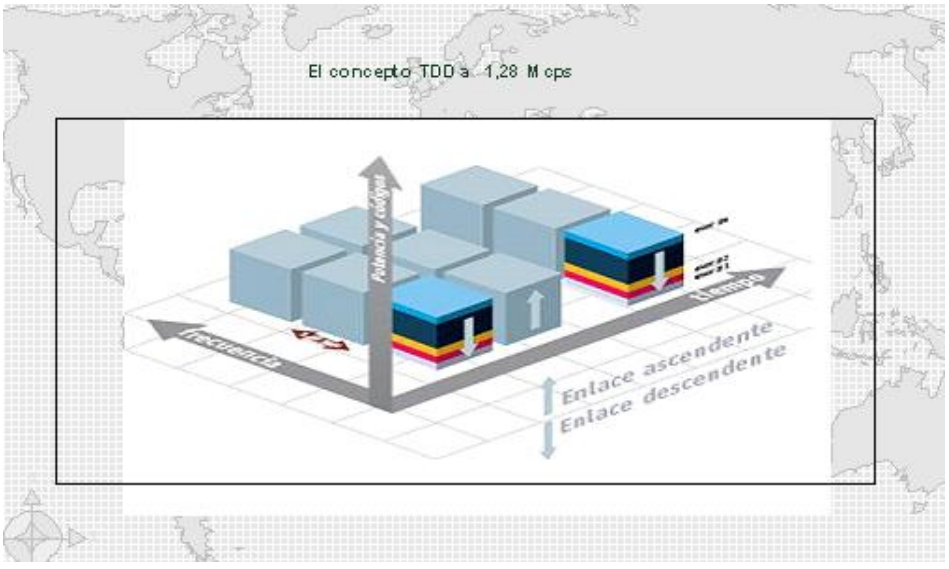


Figura 2.5 El concepto TDD a 1.28 M cps

El modo TDD a 1,28 Mcps (ver Figura 2.5) hereda algunas características del TDD a 3.84 Mcps. Además, se considera que tiene algunas ventajas comparado con el FDD y el modo TDD de tasa de chip alta:

• Capacidad más alta que el FDD y el TDD de tasa de chip alta.

• Adecuado para la cobertura de pico a macro-celdas (los rangos máximos de cobertura son comparables a los del FDD).

• Mejora de la flexibilidad de planificación de frecuencia.

Este es un aspecto muy importante desde el punto de vista de los operadores, ya que a cada operador se le ha asignado únicamente una banda de 5 MHz en el espectro no apareado.

• Soporte de la movilidad a alta velocidad (hasta 250 Km/h).

• Costes del equipo más bajos, principalmente para el Nodo B.

La definición de la forma de onda del TDD a 1,28 Mcps facilita el uso de antenas inteligentes y la detección multiusuario, siendo estas las principales razones detrás de las ventajas expuestas más arriba. Las antenas inteligentes reducen las interferencias del sistema, dando lugar a una capacidad más alta y a un incremento de la sensibilidad, lo que a su vez conduce a un área de cobertura más amplia.

Sin embargo, existen todavía un número de serios inconvenientes y preguntas sin respuesta que podrían limitar el despliegue de las normas TDD. Los principales problemas están relacionados con aspectos de la sincronización, coexistencia entre el FDD y el TDD, problemas de interferencias, y la viabilidad de los terminales multimodo.

Los anteriores problemas pueden dar lugar a severas restricciones en el funcionamiento real de la red.

La introducción oficial de las dos normas TDD en el IMT2000 no impide el éxito comercial y el despliegue de cada tecnología. En China, parece probable que sólo una de las normas TDD sobrevivirá. Del resto del mundo aún no se tienen referencias. Desde luego que la tecnología de baja tasa de chip está despertando cierto interés entre la mayoría de los operadores europeos. Debido a la existencia de un mercado altamente competitivo, las elecciones tecnológicas vendrán determinadas principalmente por las disponibilidades de los equipos. La disponibilidad de terminales multimodo será el principal factor determinante en la elección que realicen los operadores. Otro resultado posible es que sólo la versión TDD de baja tasa de chip sea desplegada, y que la tecnología original UTRA/TDD acabe abandonándose.

Un escenario alternativo sería que diferentes regiones desplegaran distintas tecnologías, requiriendo el desarrollo de terminales del modo multi–TDD para permitir la movilidad global.

2.6 Alto nivel de la Arquitectura del Sistema UMTS

Las principales directrices que han gobernado la definición de la arquitectura son las siguientes:

• La señalización y la red de transporte de datos están separadas lógicamente.

• Las funciones del UTRAN y las de la red central están totalmente separadas de las funciones de transporte.

• La macro–diversidad (sólo FDD) está soportada totalmente en el UTRAN.

• La movilidad para la conexión del Control de los Recursos Radio (RRC) está totalmente soportada en el UTRAN.

• La división funcional a través de las interfaces tiene pocas opciones, aunque sea posible.

• Las interfaces deben basarse en un modelo lógico de la entidad controlada a través de esta interfaz.

Estos principios generales, que son muy diferentes de los del GSM, se han establecido para solucionar las limitaciones del GSM.

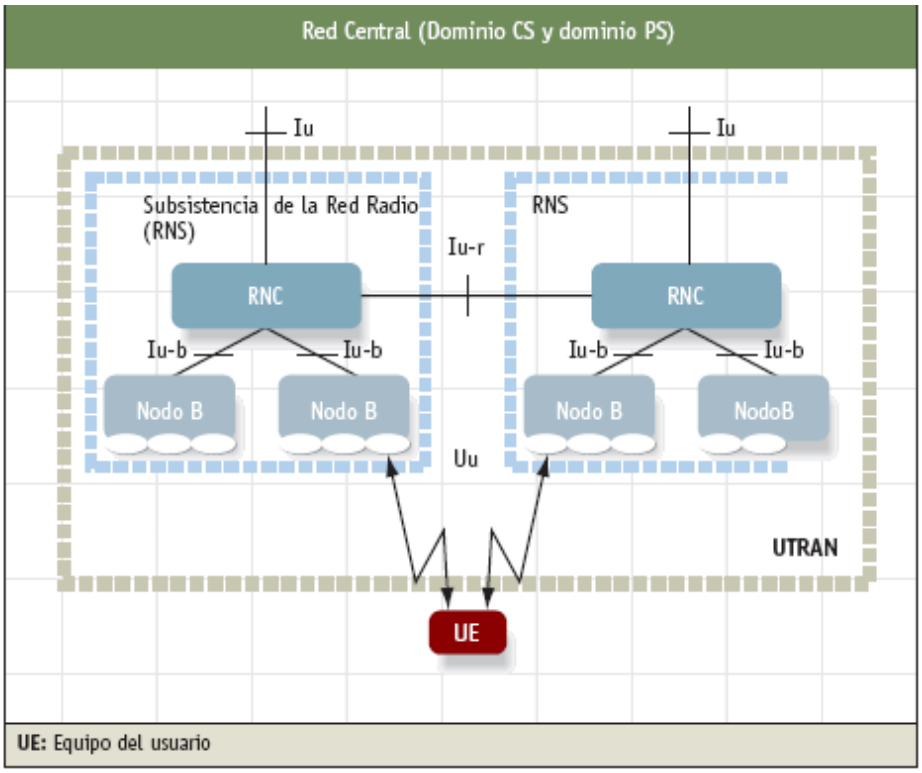


Figura 2.6 Red Central (Dominio CS y Dominio PS)

La arquitectura de referencia del UTRAN se ilustra en la Figura 2.6.

El equipo del usuario consta de dos partes:

• El equipo móvil (ME): es el equipo usado para la comunicación radio a través de la interfaz aire.

• El módulo de la identidad del abonado UMTS (USIM): Es una tarjeta inteligente que contiene la identidad del abonado y que realiza varias funciones de seguridad.

El UTRAN también consta de dos elementos distintos:

• El nodo B: Convierte el flujo de datos entre las interfaces lu-b y Uu, y participa en la gestión de los recursos radio.

• El Controlador de la Red de Radio (RNC): Contiene y controla los recursos radio de los Nodos B a los cuales está conectado.

El RNC es el punto de acceso al servicio para todos los servicios que UTRAN proporciona a la red central.

La red central trata la conmutación y el encaminamiento de las llamadas hacia las redes externas.

CAPITULO 3

RECOMENDACIONES UIT-T Q.1741.3

3.1.1 Resumen

En esta Recomendación se presenta una versión del miembro de la familia de los sistemas de telecomunicaciones móviles internacionales-2000 (IMT-2000), "Red medular del sistema de telecomunicaciones móviles universales (UMTS) derivada del sistema global para comunicaciones móviles (GSM)".

Las organizaciones de normalización (es decir, ARIB, CWTS, ETSI, T1, TTA, TTC) conocen esta versión del miembro de la familia IMT-2000 como la "Versión 5 del proyecto asociado de tercera generación (3GPP)". En las Recomendaciones UIT-T Q.1741.1 y UITT Q.1741.2 se especifican versiones anteriores de este miembro de la familia, en tanto que otros miembros de la familia IMT-2000 se especifican en otras Recomendaciones de la serie Q.174x.

En esta Recomendación se combinan y asocian las normas pertinentes de varias organizaciones de normalización para la red medular, o núcleo de red, de este miembro de la familia IMT-2000 en una única Recomendación a nivel mundial.

3.1.2 Prefacio

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias.

3.2 Estructura de las Especificaciones técnicas

Esta cláusula proporciona una visión general de las especificaciones para este miembro de la familia IMT-2000 basado en una red medular UMTS que ha evolucionado de GSM.

El texto siguiente describe el esquema de numeración utilizado para las especificaciones e informes del sistema móvil de tercera generación 3GPP,

Los siguientes títulos y descripciones de las series se indican sólo con fines orientativos y pueden ser re-elaborados de acuerdo con la experiencia.

Las series de especificaciones son:

Serie 21 Especificaciones de requisitos.

Serie 22 Aspectos relativos al servicio.

Serie 23 Realización técnica.

Serie 24 Protocolos de señalización (red entre UE y CN).

Serie 25 Aspectos relativos a UTRA (nota)

Serie 26 Códecs (vocales, de vídeo, etc.).

Serie 27 Datos.

Serie 28 Protocolos de señalización (RSS-CN).

Serie 29 Protocolos de señalización.

Serie 30 Gestión de programas (nota).

Serie 31 Módulo de identidad de usuario (UIM, *user identity module*).

Serie 32 Operación y mantenimiento.

Serie 33 Aspectos relativos a la seguridad.

Serie 34 Especificaciones de prueba (nota).

Serie 35 Especificaciones de algoritmos.

Serie 48 Aspectos relativos a GERAN (nota).

NOTA – Las especificaciones técnicas de esta serie no se incluyen en el ámbito de esta Recomendación.

3.3 Especificación técnica basada en la serie 33 (Aspectos relativos a la Seguridad)

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. En este contexto, se recomienda al lector que busque la versión más reciente de las normas/especificaciones SDO.

3.3.1 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.

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.

Esta especificación define procedimientos de seguridad 3G aplicados en las redes con capacidades 3G, es decir, en UMTS y entre UMTS y GSM. A título de

ejemplo, la autenticación UMTS es aplicable al acceso radioeléctrico UMTS así como al acceso radioeléctrico GSM, a condición de que el nodo de red servidor y la MS tengan capacidades UMTS. También se trata la interoperabilidad con las redes sin capacidad UMTS.

Se coloco un grafico donde podemos apreciar la Arquitectura de Seguridad 3G para lograr comprender el objetivo de la norma y hacia donde se orienta

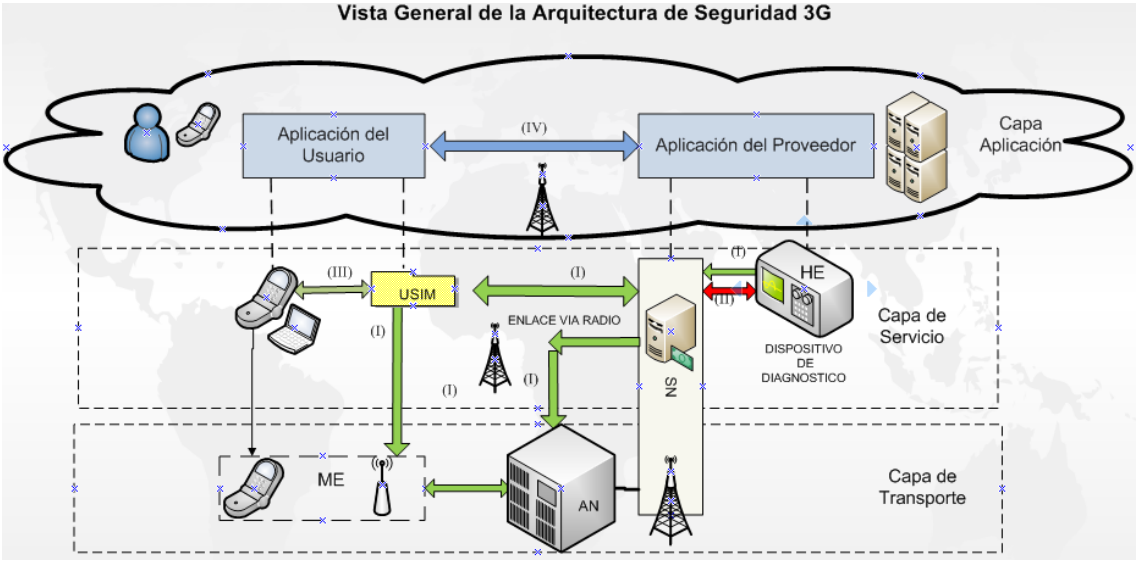


Figura 3.1 Arquitectura de Seguridad 3G

Donde:

(I) Seguridad en la Red de Acceso

(II) Seguridad en el Dominio de Red

(III) Seguridad en el Dominio de Usuario

(IV) Seguridad en el Dominio de Aplicación

(V) Seguridad en Visibilidad y capacidad de Configuración

Como podemos observar en este gráfico donde ilustramos las tres capas principales de la arquitectura de seguridad UMTS:

- Capa de aplicación: Es la superior y contiene las aplicaciones del usuario y las aplicaciones del proveedor.
- Capa de servicios: Es la intermedia y contiene el USIM (User Services Identity Module), SN (Serving Network) y HE (Home Environment), en esta capa también se encuentra el TE (Terminal Equipment) que forma parte del dominio ME (Mobile Equipment).
- Capa de transporte: Es la capa inferior y contiene MT (Mobile Termination) que también forma parte del dominio ME, AN (Access Network) y SN (Serving Network).

CAPA DE APLICACION

En la capa de aplicación se debe tomar en cuenta el enlace que permita la relación de una manera segura entre el bloque aplicación del proveedor y el bloque aplicación de usuario, esta caracterización de seguridad es el enlace entre los dos bloques mencionados para tener una transferencia de información de forma segura y bidireccional, es conocida como seguridad del dominio de aplicación y lo detallaremos a continuación:

(IV)SEGURIDAD DEL 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. El toolkit de aplicación SIM es un interfaz estandarizado que soporta varios servicios de seguridad (autenticación de entidad, autenticación de mensajes, detección de repeticiones, garantía de integridad de secuencia, confidencialidad y prueba de recepción).

CAPA DE SERVICIO

Como anteriormente la detallamos se encuentra conformada por la USIM, HE, SN y TE, la importancia de cada uno de estos dominios los detallaremos a continuación:

- El bloque USIM es una aplicación, que puede alojarse en una tarjeta inteligente removible que puede contener otras aplicaciones. También puede no ser removible y estar integrada en el equipo móvil. El USIM contiene datos y procedimientos que le identifican de forma segura y sin ambigüedad y están normalmente incluidos en una tarjeta inteligente.
- El HE (entorno doméstico) UMTS, tiene la opción de proteger a sus usuarios contra cualquier ataque implementando un mecanismo para mejorar la confidencialidad de la identidad de usuario. Es el que tiene responsabilidad global de proporcionar un servicio a los usuarios con el que tiene una asociación. Esto incluye la provisión, asignación y gestión de cuentas de usuario y los mecanismos necesarios para facturar a los

usuarios por sus cargos y para pagar a las redes SNs por los cargos de los usuarios.

- La SN (Serving Network). Es el que proporciona recursos de radio, gestión de la movilidad y capacidades fijas para conmutar, enca minar y manipular los servicios ofrecidos a los usuarios. Las capacidades de SN se proporcionan en nombre de los HEs con los que la SN tiene un acuerdo apropiado. Las responsabilidades de la SN son: recoger los datos de contabilidad y transferirlos a los HEs, así como la interacción y la provisión de facilidades a los HEs para identificar, autenticar, autorizar y localizar a los usuarios.
- El TE (Terminal Equipment), es un sub-dominio de ME que contiene la funcionalidad relativa a las aplicaciones extremo a extremo (por ejemplo, micrófono, altavoz, pantalla de un laptop-computer).

El dominio USIM contiene la funcionalidad utilizada para acceder a los servicios UMTS de una red doméstica, a la vez sirve como una interfaz con el equipo terminal TE, para poder acceder a los servicios de la red.

En la capa de servicio hay que tomar en cuenta la seguridad que hay entre la relación interna de la capa de aplicación con la capa de servicio, en este caso la relación que tiene el bloque de dominio del proveedor con los bloques de dominio SN y HE, es un enlace caracterizado como Seguridad del dominio del Proveedor, a continuación detallamos lo mencionado.

(II)SEGURIDAD DEL DOMINIO DEL PROVEEDOR

Esta clase de características de seguridad contiene las que proporciona a los operadores de red SN y entornos domésticos HE con la capacidad de comunicaciones seguras a través de los enlaces de la red central y monitorizar la utilización de su sistema, detectando y contrarrestando comportamientos fraudulentos. Abarca las siguientes características de seguridad:

1) Autenticación de entidad (entre las entidades de red central)
2) Negociación de claves (entre las entidades de la red central)
3) Distribución de claves (entre las entidades de la red central)
4) Confidencialidad de datos (de señalización sobre los enlaces de la red central)
5) Integridad de datos (de señalización sobre los enlaces de la red central)
6) Detección de fraudes. Esta característica recoge información de posibles fraudes para permitir a los operadores detectar y combatir posibles comportamientos fraudulentos.

Las cinco primeras características de seguridad permiten a los nodos del dominio del proveedor autenticar de forma segura y negociar las claves de sesión y a continuación intercambiar de forma segura datos de señalización.

En la capa de servicio tenemos tres clases de características de seguridad que relacionan a cada dominio como podemos observar en la figura 3.1, estas se encuentran enumeradas y son las siguientes:

(I) Seguridad de Acceso a la Red.

(II) Seguridad en el Dominio de Red

(III) Seguridad en el Dominio de Usuario

Cada uno de estos enlaces tienen su dependencia en el envío o recepción de información entre dominios, esta puede ser direccional o bidireccional, es decir que un dominio puede depender del otro o necesitan de si para poder funcionar eficientemente y de forma segura, a continuación detallamos los tres enlaces que son las características de seguridad que intervienen en la capa de servicio y a la vez en la capa de transporte.

(I)SEGURIDAD DE ACCESO A LA RED

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. Sin embargo, el mecanismo de GSM permite a la SN pedir que el usuario envíe su identidad de usuario en texto sin cifrar a través del enlace de acceso vía radio. El hecho de que este procedimiento no puede eliminarse posibilita a un atacante activo utilizar un capturador de identidad que revela la identidad del usuario. Un entorno doméstico HE UMTS tiene la opción de proteger a sus usuarios contra dicho ataque implementando un mecanismo para mejorar la confidencialidad de la identidad de usuario (denominado EUIC, Enhanced User Identity Confidentiality), colocado entre las USIM del usuario y una entidad de red

HE denominada UIC (User Identification Centre). Para realizar esto, la SN soportará un mecanismo de transporte para mejorar la confidencialidad de la identidad del usuario. La implementación del mecanismo para la EUIC entre el USIM y el UIC es opcional y el propio mecanismo puede ser de propiedad del HE.

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). Así mismo, el mecanismo genera una clave de cifrado para confidencialidad de datos y una clave de integridad para implantar la integridad de los datos transmitidos a través del enlace de acceso aéreo. El mecanismo usa números de secuencia y contadores ubicados en el AuC y el USIM asegura lo fresco (actual/vigente/no repetido) de los datos de autenticación. De acuerdo al estándar ISO/IEC 9798-4, el mecanismo proporciona «autenticación mutua» entre el usuario y la red.

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. Para proporcionar esto implementaron una función de autenticación de mensajes en cada extremo del enlace de acceso. Esta característica protege contra el «hijacking» («secuestro») de servicios para autenticar al usuario y red durante y antes de la provisión del servicio y para permitir que ambas partes establezcan de forma segura conexiones sin ejecutar un protocolo AKA (Autenticación y acuerdo de clave).

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: La segunda característica nueva de acceso a red de UMTS/3G es el 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. Esta característica se incluye en la categoría de características de seguridad del nivel de aplicación. Sin embargo el mecanismo reutiliza el cifrado para la seguridad de acceso a la red y debería considerarse una característica de seguridad de acceso a red, aunque su objetivo con respecto a la

confidencialidad de los datos (enlace de acceso) sea primariamente proteger los datos de usuario cuando se transmiten a través de las conexiones de la red 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.

Específicamente es la misma caracterización de seguridad en el dominio del proveedor, esto ya lo detallamos anteriormente.

(III)SEGURIDAD DEL 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), las detallamos a continuación:

1) Autenticación usuario-USIM: Restringe el acceso al USIM a un usuario autorizado o a un conjunto de usuarios autorizados. Para realizar esto, los usuarios y el USIM deben compartir un secreto (un PIN o incluso información biométrica: reconocimiento del patrón de voz, reconocimiento del iris, retina, huellas dactilares, distribución de los poros de la piel, geometría de la mano, patrón de colocación de venas de la mano/muñeca, caracterización grafológica de la firma manuscrita, composición química del olor corporal, características de la cara y emisión térmica, composición genética basada en RNA/DNA, etc.) que se almacena de forma segura en el USIM.

2) Autenticación USIM-UE: Restringe el acceso al UE a un USIM particular o a un conjunto de USIMs. En este caso el USIM y el UE deben compartir un secreto que se almacena de forma segura en el USIM y en el UE.

CAPA DE TRANSPORTE

La capa de transporte proporciona transferencia transparente de datos entre los dominios, proporcionando servicios confiables de la transferencia de datos a las capas superiores. Anteriormente detallamos los dominios que en esta capa se involucran, así como las caracterizaciones de seguridad que actúan en la misma. A continuación vamos a describir cada uno de los dominios que se indican en la capa de transporte de la figura 3.1

- El MT (Mobile Termination) contiene la funcionalidad relativa a la transmisión de radio, forma parte del dominio ME, es decir MT e un sub-dominio de ME, de esta manera nos podemos dar cuenta que tanto TE y el MT conforman el dominio ME.
- AN (Access Network): La red de acceso se caracteriza por estar en contacto directo con el UE y el dominio CN (Núcleo de red). El dominio AN comprende las funciones específicas para la técnica de acceso, mientras las funciones del dominio CN se pueden utilizar con flujos de información que utilizan cualquier técnica de acceso. Esta división permite diferentes enfoques para la red CN, cada enfoque especifica distintos tipos de CNs conectables al dominio AN, así como diferentes técnicas de acceso, cada tipo de AN conectable al dominio CN

- SN (Serving Network): El dominio SN es la parte del dominio CN al que está conectada la AN que proporciona el acceso de usuario. Representa las funciones de CN que son locales al punto de acceso del usuario y por tanto su localización cambia cuando el usuario se mueve. La red SN es la responsable de encaminar llamadas y transportar la información del usuario desde la fuente al destino. Tiene la capacidad de interactuar con la HN para atender los servicios/datos específicos del usuario y con la red TN para propósitos de servicios/datos específicos que no son de usuario.

La CN se sub-divide en el dominio SN (Serving Network), el dominio HN (Home Network) y el dominio TN (Transit Network). SN, TN y HN se interpretan como los roles que pueden desempeñar ciertas redes en relación a una cierta llamada. Las redes pueden tener la capacidad de desempeñar más de un «rol» y para una única llamada no son necesariamente diferentes.

Hemos descrito de una manera más didáctica esta recomendación en lo que se refiere a la Arquitectura de Seguridad.

A continuación presentaremos un grafico donde se ofrece una visión general del registro ME y conexiones principales dentro de UMTS con un servicio de dominio CS y un dominio de servicio PS.

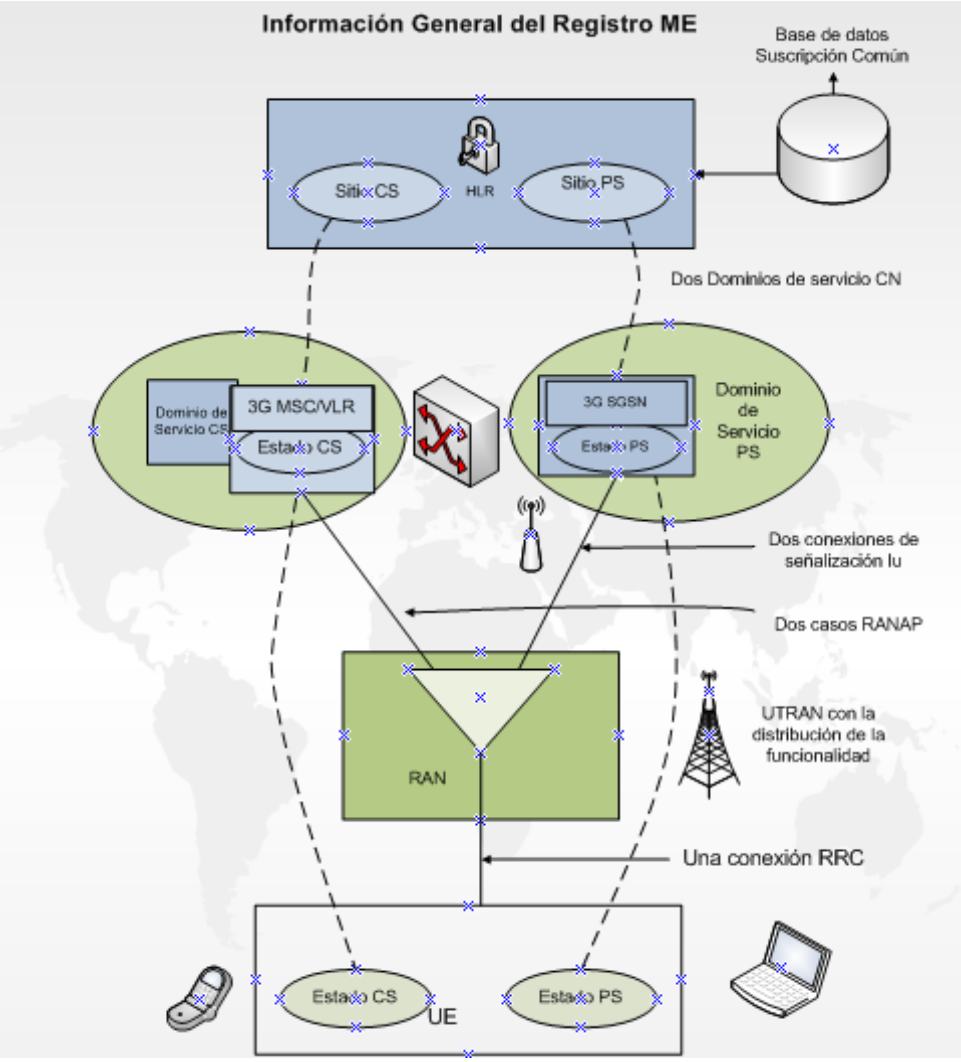


Figura 3.2 Registro ME

Como podemos observar en la figura 3.2 es la manera más fácil de indicar el proceso de registro del EU, ya sea por Conmutación de paquetes (PS) , por conmutación de circuitos (CS) o PS/CS, hay que tomar en consideración que intervienen los tres bloques importantes del sistema UMTS véase (fig1.2).

Primeramente vamos a distinguir qué elementos intervienen en cada bloque de la fig. 1.2:

- En el UE intervienen la CS, PS.

- La UTRAN o RAN consiste de RNCs (Radio Network Controllers) y Nodo Bs (Base Stations). Ambos elementos forman un RNS (Radio Network Subsystem). Sus fronteras son la interfaz Iu al CN y la interfaz Uu al equipo de usuario (UE),

  La movilidad para la conexión del Control de los Recursos Radio (RRC) está totalmente soportada en el UTRAN.

- La red central (CN) se encuentra formada por varios elementos como el MSC, el SGSN, GMSC, GGSN, HLR, VLR.

Para el registro UE debe existir el modo conectado, este ocurre cuando la conexión RRC es establecida, la cual se ejecuta entre el UE y un RNC llamado SRNC, una vez realizada la conexión, necesitamos la habilitación para que la UTRAN se enlace con la CN, esto se logra con un protocolo llamado RANAP (Radio Access Network Aplication Part) es un protocolo considerable, comparable al protocolo BSSAP en el sistema GSM. RANAP provee los servicios de señalización entre UTRAN y CN. Este se caracteriza por controlar la conexión entre RNC y SGSN. Además controla la conexión de conmutación de circuitos entre RNC y MSC sobre la interfaz Iu. Este reside entre UTRAN y CN, además maneja señalización entre RNC y SGSN en la interfaz Iu – PS y entre RNC y MSC en la interfaz Iu-CS.

Los servicios de RANAP son divididos en tres grupos:

- Servicio de control general. Estos se refieren a toda interfaz Iu.

- Servicio de notificación. estos se refieren a un específico UE o a todos loa UE en un área específica.
- Servicios de control dedicado. Estos son referidos a solo un UE.

Una vez que se realizó la activación de la señalización entramos al dominio de servicios CS o PS.

Estos dominios se enlazan para enviar la información a la base de datos de suscripción de la HLR que es la que contiene los datos permanentes de registro de suscriptor, ahí los identifica si es por conmutación de circuito o de paquete, cabe recalcar que todos estos términos están especificados en el capítulo 1 de esta investigación.

Esta es el procedimiento que normalmente se debe seguir en este sistema de tercera generación para empezar la conexión del EU y que lo detallamos gráficamente en la figura 3.2

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

El ámbito de esta especificación técnica son las funcionalidades y mecanismos de seguridad para el acceso seguro al subsistema multimedios IP (IMS) del sistema de telecomunicaciones móviles 3G.

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.

Se coloco un grafico donde podemos apreciar la Arquitectura de Seguridad de IMS en el cual podremos comprender su funcionamiento y así lograr entender el objetivo de la norma

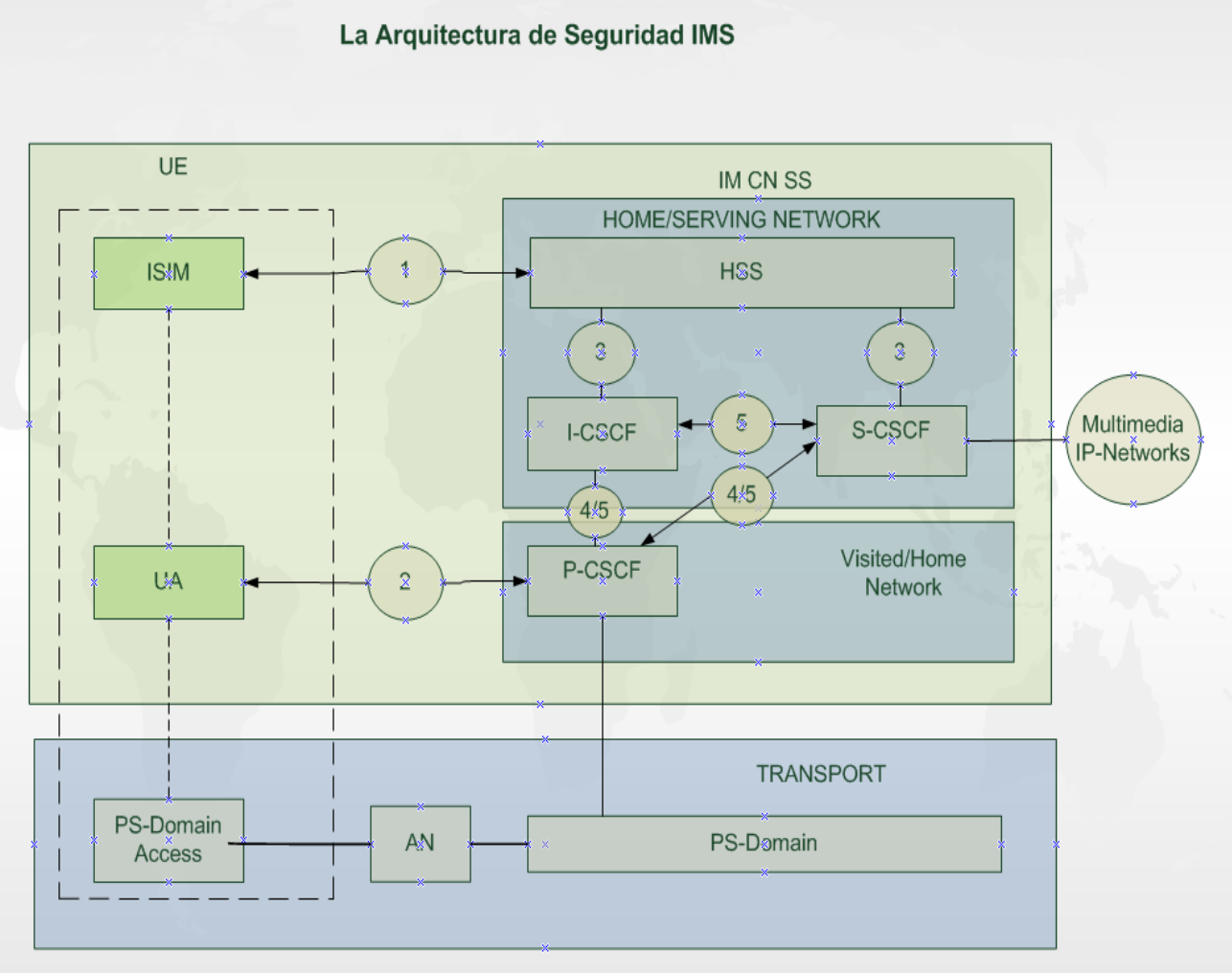


Figura 3.3 Arquitectura de Seguridad IMS

Donde:

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 3.3, 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.

En el equipo de usuario usamos el ISIM (Modulo de Identidad IM del Subscritor), que para propósitos de esta investigación el USIM es un término que indica la colección de datos de seguridad IMS y funciones en una UICC (Universal IC card),

y el UA (user agent) es un nombre técnico para programas que ejecutan tareas para un usuario en la red por ejemplo este es el medio de acceder cuando un usuario intenta desde en equipo móvil procesar datos o compartir información en la red.

3.3.3 TS 33.210 Seguridad en 3G, Seguridad del dominio de red (NDS); Seguridad de la capa de red IP

Este documento 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.

Se coloco un grafico donde podemos apreciar la Arquitectura NDS para Protocolos Basados en IP en el cual podremos comprender su funcionamiento

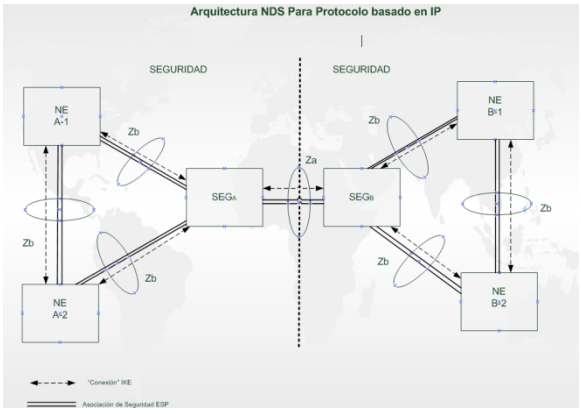


Figura 3.4 Arquitectura NDS para protocolo basado en IP

Donde:

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.

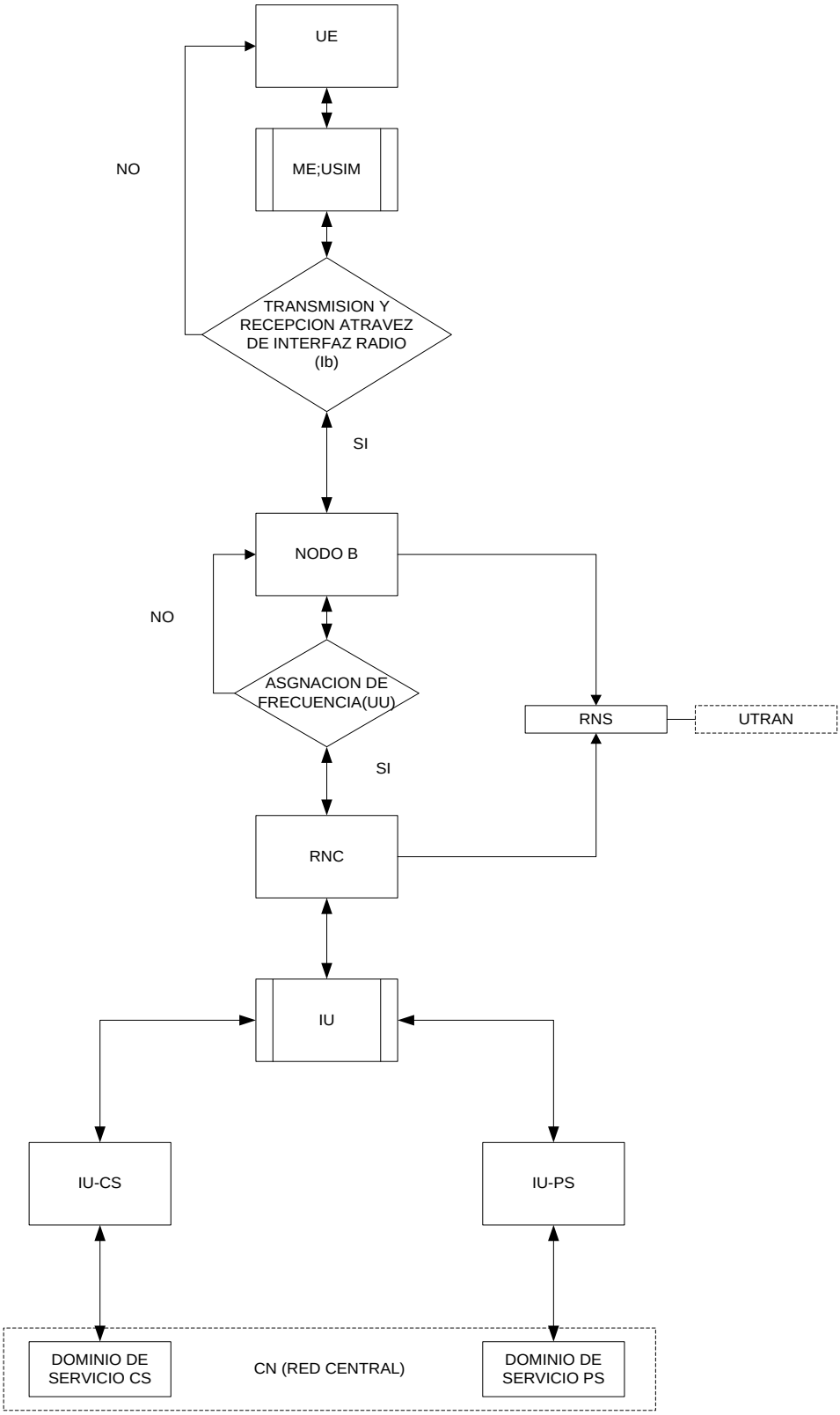
Interfaz Zb (NE – SEG / NE - NE)

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.

FUNCIONAMIENTO DE LA ARQUITECTURA DE SEGURIDAD DE UMTS



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.

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 grafica 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.

BIBLIOGRAFIA

[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

[7]. Harri Holma and Antti Toskala, ‘‘WCDMA for UMTS: radio access for third generation mobile communications’’, John Wiley & Sons, 2002.

[8]. 3GPP TS 21.902, V6.0.0, Evolution of 3GPP System, http://www.3gpp.org/ftp/Specs/archive/21_series/21.902/ , 2005

[9]. Alan Clapton, ‘‘ Future mobile networks: 3G and beyond’’, BT exact Technologies, 2001.

[10]. 3GPP TS 23.002, V6.6.0, Network architecture,

http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/ , 2005

[11]. Gert Bostelmann, Rudolf Zarits, ‘‘ UMTS design details and system engineering’’,2002.

[12]. 3GPP TS 23.221, V6.3.0,Architectural requirements,

http://www.3gpp.org/ftp/Specs/archive/23_series/23.221/ , 2005

[13]. 3GPP TS 25.213, V6.1.0, Spreading and modulation (FDD),

http://www.3gpp.org/ftp/Specs/archive/25_series/25.213/ , 2005

[14]. 3GPP TS 22.105, V6.2.0, Services and service capabilities,

http://www.3gpp.org/ftp/Specs/archive/22_series/22.105/ , 2005

[15]. Erick Dahiman, Bjorn Gudmundson, Mats Nilsson and Johan Skold, ‘‘UMTS/IMT-2000 Based on Wideband CDMA’’, IEEE Communications Magazine, September 1998.