MODELOS DE SEGURIDAD PARA MÓVILES

AUTOR : Almudena González

DIRECTOR : Manel Medina i Llinàs

Indice

Índice de Figuras

1Referencias

[1] Universal Mobile Telecommunications System (UMTS). General UMTS Architecture
3GPP (UMTS 23.101)

[2] Universal Mobile Telecommunications System (UMTS). UMTS Access Stratum; Services and Functions (Release 1999)
3GPP (UMTS 23.110)

[3] Universal Mobile Telecommunications System (UMTS). Virtual Home Environment; Open Service Architecture
3GPP (UMTS 23.127)

[4] Universal Mobile Telecommunications System (UMTS). UMTS Core Network based on ATM Transport
3GPP (UMTS 23.25)

[5] Evolution of the GSM platform towards UMTS
3GPP (UMTS 23.20)

[6] Universal Mobile Telecommunications System (UMTS).
Security Mechanism and Architecture
3GPP (UMTS 33.23)

[7] Universal Mobile Telecommunications System (UMTS).Security Features
3GPP (UMTS 33.22)

[8] Universal Mobile Telecommunications System (UMTS).Security Requirements
3GPP (UMTS 33.21)

[9] 3rd Generation Partnership Project. Integration Guidelines
3GPP (3G TS 33.103)

[10] 3rd Generation Partnership Project.Security Architecture
3GPP (3G TS 33.102)

[11] Combined GSM and Mobility IP Handling in UMTS IP CN
3GPP (3G TS 13.923)

[12] 3rd Generation Partnership Project. 3G Security; Security Principles and Objectives
3GPP (3G TS 33.120)

[13] Security Architecture for the Internet Protocol
Kent S., R. Atkinson (RFC 2401)

[14] IP Authentication Header
Kent S., R. Atkinson (RFC 2402)

[15] IP Encapsulating Security Payload (ESP)
R. Atkinson. (RFC 2406)

[16] The Internet Key Exchange (IKE)
Harkins D, D. Carrel (RFC 2409)

[17] Internet Security Association and Key Management Protocol
D. Maughan, D.Schertler (RFC 2408)

[18] Mobile radio interface layer 3 specification; Core Network Protocols Stage 3
3GPP (TS 24.008)

[19] Mobile radio interface signalling layer 3. General aspects (Release 1999)
3GPP (TS 24.007)

[20] Universal Mobile Telecommunications System (UMTS). Security Threats and Requirements
3GPP (UMTS 21.133)

[21] Combined GSM and Mobile IP Handling in UMTS IP CN.
3GPP (3G TR 23.923)

[22] Network Architecture (Release 99)
3GPP (3G TS 23.002)

[23] General Packet Radio Service (GPRS). Service description
3GPP (3G TS 23.060)

[24] Architectural Requirements for Release 1999.
3GPP (3G TS 23.121)

[25] Functional stage 2 description of location services in UMTS
3GPP (3G TS 23.171)

[26] Architectural for an All IP network
3GPP (3G TR 23.922)

[27] UMTS Core Network based on ATM Transport UMTS
3GPP (3G TS 23.925)

[28] Iu Principles
3GPP (3G TR 23.930)

[29] Radio Interface Protocol Architecture (Release 99)

3GPP (3G TS 25.301)

[30] RRC Protocol Specification
3GPP (3G TS 25.331)

[31] UTRAN Overall Description
3GPP (3G TS 25.401)

[32] UTRAN Iu Interface: General Aspects and Principles
3GPP (3G TS 25.410)

[33] UTRAN Iu Interface Signalling Transport
3GPP (3G TS 25.412)

[34] UTRAN Iu Interface RANAP Signalling
3GPP (3G TS 25.413)

[35] UTRAN Iu Interface Data Transport and Transport Signalling
3GPP (3G TS 25.414)

[36] UTRAN Iu Interface User Plane Protocols
3GPP (3G TS 25.415)

[37] UTRAN Iur Interface General Aspects and Principles
3GPP (3G TS 25.420)

[38] UTRAN Iur Interface Signalling Transport
3GPP (3G TS 25.422)

[39] UTRAN Iur Interface RNSAP Signalling
3GPP (3G TS 25.423)

[40] Cryptographic Algorithm Requirements
3GPP (3G TS 33.105)

[41] Lawful Interception Requirements
3GPP (3G TS 33.106)

[42] Lawful Interception Architecture and Functions
3GPP (3G TS 33.107)

[43] A Guide to 3rd. Generation Security
3GPP (3G TR 33.900)

[44] Universal Mobile Telecommunications System (UMTS).
Security Principles
3GPP (UMTS 33.20)

[45] Security Aspects
ETSI (GSM 02.09)

[46] Network Architecture
ETSI (GSM 03.02)

[47] Security Related Network Functions
ETSI (GSM 03.20)

[48] GPRS Service Description
ETSI (GSM 03.60)

[49] Identificación de Cuestiones de Seguridad
J. Areito, M.T. Areito
Eurofach Electrónica

[50] The Wireless Application Protocol. Wireless Internet Today

[51] The Wireless Application Protocol. Identity Module Specification

[52] The Wireless Application Protocol. Architecture Specification

[53] The Wireless Application Protocol. Wireless Transport Layer Security Specification

[54] Security Architecture in the Third Generation Networds
A. Barba, J.L. Melús, F. Recacha
IEEE

[55] Security in Third Generation Mobile Systems
Nigel Jefferies
IEEE

[56] Security Provision of UMTS Services over Diverse Access Networks
John Charles Francis, Holger Herbrig, Nigel Jefferies
IEEE

[57] Security Aspects of Third Generation Mobile Telecommunications Systems
Michael Walker, Ray Forbes, Dieter Gollman
IEEE

[58] The Internet Security Domain of Interpretation for ISAKMP
D. Piper (RFC 2407)

[59] The OAKLEY Key Determination Protocol
H. Orman (RFC 2412)

[60] Classical IP and ARP over ATM
M. Laubach (RFC 2225)

[61] Directory Services for UMTS. Security Aspects
A. Barba, J.L. Melús
IEEE

[62] IP Mobility Support
D. Perkins (RFC 2002)

[63] Internet protocol
Information Sciences Institute. University of Southern California (RFC 791)

[64] Compressing TCP/IP headers for low-speed serial links
V. Jacobson (RFC 1144)

[65] The Recommendation for the IP Next Generation Protocol
S. Bradner (RFC 1752)

[66] IP in IP Tunneling
W. Simpson (RFC 1853)

[67] Path MTU Discovery
J.Mogul, S. Deering (RFC 1191)

[68] Path MTU Discovery for IP Version 6
J.McCann, S. Deering, J. Mogul (RFC 1981)

[69] Generic Packet Tunneling in IPv6 Specification
A. Conta, S. Deering (RFC 2473)

[70] Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
B. Carpenter, C. Jung (RFC 2529)

[71] Transition Mechanisms for IPv6 Hosts and Routers
R. Gilligan, E. Nordmark (RFC 2893)

[72] IPng Mobility Considerations
W. Simpson (RFC 1688)

[73] IP Encapsulation within IP
C. Perkins (RFC 2003)

[74] Minimal Encapsulation within IP
C. Perkins (RFC 2004)

[75] Reverse Tunneling for Mobile IP

G. Montenegro (RFC 2344)

[76] RADIUS Attributes for Tunnel Protocol Support
G. Zorn, D. Leifer, A. Rubens, J. Shriver, M. Holdrege, I. Goyret (RFC 2868)

[77] Mobile IP Authentication, Authorization, and Accounting Requirements
S. Glass, T. Hiller, S. Jacobs, C. Perkins (RFC 2977)

[78] Internet Protocol, Version 6 (IPv6) Specification
S. Deering, R. Hinden (RFC 2460)

[79] Mobility Support in IPv6 (Borrador)
D. Johnson, C. Perkins

[80] GRE Extensions (Borrador)
P. Calhoun, T. Hiller, P.McCann, Y. Xu

[81] Wireless Extensions to TLS
S. Blake-Wilson, M. Nystrom

1.1 Referencias a páginas web

http://www.ietf.org
http://www.3gpp.org
http://www.wapforum.org

Acceso a documentos RFC (por ejemplo RFC1688):
http://www.ietf.org/rfc/rfc1688.txt

Acceso a borradores de internet (por ejemplo draft-calhoun-mobileip-gre-ext-00.txt)
http://www.ietf.org/internet-drafts/draft-calhoun-mobileip-gre-ext-00.txt

2Definiciones

Acceso no autorizado a datos
Acceso a datos almacenados en el sistema o intento de obtención de información del sistema bien mediante escucha del tráfico de usuario o del sistema, bien, suplantando a un elemento de la red a fin de interceptar datos.

Acceso no autorizado a servicios
Tentativa de obtención de un servicio no autorizado para esa entidad.

Asociación de Movilidad
Asociación de la dirección particular con su care-of-address correspondiente incluyendo el tiempo de vida restante de la asociación.

Autenticación del origen de datos
Corroboración de que la fuente de los datos recibidos es la proclamada.

Autenticación de Entidad
Corroboración de la identidad de una entidad.

Autorización Legal
Permiso otorgado por una LEA bajo ciertas condiciones para interceptar determinadas telecomunicaciones requiriendo la cooperación con un operador de red o proveedor de servicios.

Care-of-Address
Extremo de un túnel hacia un nodo móvil, utilizado por datagramas dirigidos hacia el nodo móvil mientras está fuera de su entorno particular.

Care-of-Address de agente externo
Dirección perteneciente a un agente externo a la red con la cual el nodo móvil ha sido registrado.

Care-of-Address Ubicada
Dirección, obtenida de forma externa a la red, con la cual el nodo móvil se ha asociado mediante una de sus interfaces de red.

Clonación
Proceso de cambio de la identidad de una entidad por otra entidad del mismo tipo, de forma que existan dos entidades del mismo tipo con la misma identidad.

Control de Acceso
Prevenir el uso no autorizado de un recurso, incluyendo el uso de un recurso de forma no autorizada.

Confidencialidad
Propiedad de aquella información no accedida por usuarios/entidades no autorizados/as.

Contexto de Seguridad UMTS

Estado establecido entre un usuario y un dominio de red de servicios que define como mínimo una clave de integridad/cifrado y un identificador de conjunto de claves.

DIAMETER
Protocolo base que ofrece un entorno para los servicios que necesitan soporte de un AAA.

Dirección particular
Dirección IP asignado por un período de tiempo largo a un nodo móvil. Esta dirección permanece inalterable independientemente de lugar donde el móvil se conecte a Internet.

Dominio
Nivel superior de grupos de entidades físicas. Se definen puntos de referencia entre dominios.

Dominio de Interpretación (DOI)
Entorno donde se definen la Situación del DOI, el conjunto de políticas de seguridad que deben y/o pueden ser soportados, la sintaxis de la especificación de los servicios de seguridad propuestos, un esquema de nombres asociados a la información de seguridad relevante, incluyendo algoritmos de encriptación, algoritmos de intercambio de claves, atributos de política de seguridad y autoridades de certificación.

El dominio de interpretación incluye también el formato de los mensajes así como, cualquier tipo de Intercambio de Información requerido.

Estado de Conexión
Entorno operativo del protocolo de registro.

Estrato
Grupo de protocolos relacionados con un aspecto de los servicios ofrecidos por uno o varios dominios.

Evidencia
Información que por sí misma o en relación con otros datos, se utiliza para establecer pruebas sobre un evento o acción.

Gestión de Claves
Administración y uso de la generación, registro, certificación, deregistro, distribución, instalación, almacenamiento, archivo, revocación, derivación y destrucción de claves de acuerdo con una política de seguridad.

Índice de Parámetro de Seguridad
Índice identificativo de un contexto de seguridad, de los definidos en una Asociación de Seguridad, entre dos nodos.

Integridad
Manipulación de la información transmitida, o almacenada, en el sistema o de la información de usuario. Alteración del comportamiento del terminal o USIM fingiendo la identidad de la fuente de aplicaciones y / o datos.

Law Enforcement Agency (LEA)
Organización autorizada por una autorización legal, basada en una ley nacional, que recibe los resultados de las intercepciones de telecomunicaciones.

Módulo de acceso de usuario
Bien un USIM o un SIM.

Negación de servicio
Impedir el acceso a servicios de la red a otra entidad.

Nodo Móvil
Parte del equipamiento móvil que contiene la funcionalidad de MIP.

Procedimiento Elemental
Unidad de interacción entre RNS y CN. El protocolo de RANAP consiste en Procedimientos elementales.

Protocolo de Registro
Protocolo de gestión de PDUs.

Red Externa
Cualquier red diferente de la Red Particular del nodo móvil.

Repudio
Negación del uso de un servicio, de una recepción o transmisión de datos.

Sincronización
Procedimiento de establecimiento de opciones de protocolo entre cliente y servidor.

Sincronización Abreviada
Creación de un nuevo estado de conexión basado en una sesión segura existente.

Sincronización Completa
Creación de una nueva sesión segura entre dos entidades basándose en la negociación de parámetros y en el intercambio de información de clave pública entre cliente y servidor.

Sincronización Optimizada

Creación de una nueva sesión segura entre dos entidades basándose en el certificado del cliente en posesión del servidor.

Situación de Dominio de Interpretación
Conjunto de información que se utiliza para determinar los servicios de seguridad requeridos.

Suscriptor UMTS
Estación móvil consistente en un equipamiento de usuario con un USIM.

Transporte de Datagrama
Servicio de transporte que no garantiza que no se pierda el SDU enviado.

Túnel
Camino asignado a un datagrama mientras está encapsulado.

USIM
En un contexto de seguridad, este módulo es responsable de efectuar la autenticación de la red y del suscriptor, así como de fijar las claves.

3Abreviaturas

Se han considerado las abreviaturas de los términos en inglés a fin de utilizar los términos más conocidos.

AAL2 ATM Adaptation Layer 2. *Nivel 2 de Adaptación a ATM.*
AAL5 ATM Adaptation Layer 5. *Nivel 5 de Adaptación a ATM.*
AC Access Network. *Red de Acceso.*
AK Anonymity Key. *Clave de Anonimato.*
AKA Authentication and Key Agreement. *Autenticación y Acuerdo de Claves.*
AMF Authentication Management Field. *Campo de Gestión de Autenticación.*
AN Access Network. *Red de Acceso.*
APN Access Point Name. *Nombre de Punto de Acceso.*
ARP Address Resolution Protocol. *Protocolo de Resolución de Direcciones.*
AS Access Stratum. *Estrato de Acceso.*
ATM Asynchronous Transfer Mode. *Modo de Transmisión Asíncrono.*
AuC Authentication Centre. *Centro de Autenticación.*
AUTN Authentication Token. *Valor de Autenticación.*
AUTS Synchronisation Authentication Token. *Valor de Autenticación de Sincronización.*
AV Authentication Vector. *Vector de Authenticación.*
BG Border Gateway. *Pasarela Límite.*
BSSAP+ Base Station System Application Part+.
Sistema de Estación Base de Parte + de Aplicación.
BSSGP Base Station System GPRS Protocol.
Sistema de Estación Base del Protocolo GPRS.
CA Certification Authority.
Autoridad de Certificación.
CAMEL Customized Application for Mobile Network Enhanced Logic.
Aplicaciones Customizadas para Redes Móviles de Lógica Enhanced.
CC Call Control.*Control de Llamadas.*
CGF Charging Gateway Funtionality.*Funcionalidad de Puerta de Cargo.*
CK Cipher Key.*Clave de Cifrado.*
CM Connection Management. *Gestión de Conexión.*
CN Core Network. *Red Troncal.*
CS Circuit Switched.*Conmutación de Circuitos.*
DC Dedicated Control SAP. *SAP de Control Dedicado.*
DCH Dedicated Transport Channel. *Canal de Transporte Dedicado.*
DCK Derived Cipher Key. *Clave de Cifrado Derivada.*
DHCP Dynamic Host Configuration Protocol.
Protocolo de Configuración de Host Dinámico.
DIK Derived Integrity Key. *Clave de Integridad Derivada.*
DL Down-link. *Conexión Descendente.*
DRNC Drift Radio Network Controller. *Controlador de Red de Radio.*
$D_{SK(X)}$(data) Decryption of "data" with Secret Key of X used for signing.
Desencriptación de datos con Clave Secreta de X utilizada para firmar.
EMSI Encrypted Mobile Subscriber Identity.*Identidad de Suscriptor Móvil Encriptada.*

$E_{KSXY(i)}$(data)	Encryption of "data" with Symmetric Session Key #i for sending data from X to Y. *Encriptación de datos con Clave de Sesión Simétrica #i para enviar datos de X a Y.*
$E_{PK(X)}$(data)	Encryption of "data" with Public Key of X used for encryption. *Encriptación de datos con Clave Pública de X.*
ESP	Encapsulating Security Payload. *Seguridad de Encapsulamiento de Carga Útil.*
FA	Foreign Agent. *Agente Externo.*
GC	General Control SAP. *SAP de Control General.*
GGSN	Gateway GPRS Support Node. *Nodo de Soporte de Entrada a GPRS.*
GMM	GPRS Mobility Management for packet switched traffic. *Gestión de Movilidad GPRS para tráfico de paquetes conmutados.*
GPRS	General Packet Radio Service. *Servicios de Radio Generales de Paquetes.*
GSN	GPRS Support Node. *Nodo de Soporte a GPRS.*
GTP	GPRS Tunneling Protocol. *Protocolo de Túnel de GPRS.*
GTP-C	GTP Control Plane. *Plano de Control de GTP.*
GTP-U	GTP User Plane.*Plano de Usuario de GTP.*
HA	Home Agent. *Agente Particular.*
HE	Home environment. *Entorno origen.*
HLR	Home Location Register. *Registro de Ubicación Particular.*
IF	Infrastructure. *Infraestructura.*
IK	Integrity Key. *Clave de Integridad.*
IMEI	International Mobile Equipment Identity. *Identidad Internacional del Equipamiento Móvil.*
IMSI	International Mobile Subscriber Identity. *Identidad Internacional del Suscriptor Móvil.*
IMUI	International Mobile User Identity. *Identidad Internacional del Usuario Móvil.*
IP	Internet Protocol. *Protocolo de Internet.*
IPv4	Internet Protocol version 4. *Protocolo de Internet versión 4.*
IPv6	Internet Protocol version 6. *Protocolo de Internet versión 6.*
IV	Initialisation Vector. *Vector de Inicialización.*
KSI	Key Set Identifier. *Identificador de Conjunto de Claves.*
LAC	Logical Access Control. *Control de Acceso Lógico.*
LAI	Location Area Identity. *Identidad de Área de Ubicación.*
LEA	Law Enforcement Agency. *Agencia de Seguridad.*
LIS	Logical IP Subnet. *Subred IP Lógica.*
LLC	Logical Link Control. *Control de Conexión Lógica.*
L1	Layer 1. *Nivel 1.*
L2	Layer 2. *Nivel 2.*
L3	Layer 3. *Nivel 3.*
MAC	Media Access Control. *Control de Acceso al Medio.*
MAP	Mobile Application Part. *Parte de Aplicación Móvil.*
ME	Mobile Equipment. *Equipo móvil.*
MIP	Mobile IP. *Movilidad IP.*
MM	Mobility Management for circuit switched traffic. *Gestión de Movilidad para tráfico de circuito conmutado.*
MS	Mobile Station. *Estación Móvil.*
MSC	Mobile Switching Center. *Centro de Conmutación Móvil.*
MT	Mobile Termination. *Terminación Móvil.*

MTP3b Message Transfer Part. *Parte de Transferencia de Mensaje*.

MExE	Mobile Station Application Execution Environment. *Entorno de Ejecución de Aplicaciones de Estaciones Móviles.*
NAS	Non Access Stratum. *No Estrato de Acceso.*
NS	Network Service. *Red de Servicios.*
NSAPI	Network layer Service Access Point Identifier. *Identificador de Punto de Acceso a Servicios de nivel de Red.*
Nt	Notification SAP. *SAP de Notificación.*
PAK	Permanent Authentication Key. *Clave de Autenticación Permanente.*
PD	Protocol Discriminator. *Identificador de Protocolo.*
PDU	Packet Data Unit. *Unidad de Paquete de Datos.*
PDP	Packet Data Protocol *Protocolo de Paquete de Datos.*
PLMN	Public Land Mobile Network. *Red Terrestre Móvil Pública.*
PPP	Point to Point Protocol. *Protocolo Punto a Punto.*
PS	Packet Switched. *Paquetes Conmutados.*
P-TMSI	Packet-TMSI. *TMSI de Paquetes.*
PVC	Permanent Virtual Circuit. *Camino Virtual Permanente.*
QoS	Quality of Service. *Calidad de Servicio.*
RA	Routing Area. *Área de Direccionamiento.*
RAB	Radio Access Bearer. *Identificador de Canal Lógico de Acceso a Radio.*
RAI	Routing Area Identifier. *Identificador de Área de Direccionamiento.*
RANAP	Radio Access Network Adaptation Protocol *Protocolo de Adaptación a Red del Acceso de Radio.*
RAND	Random challenge. *Número Aleatorio.*
RLC	Radio Link Control. *Control de Conexión de Radio.*
RNC	Radio Network Controller. *Controlador de la Red de Radio.*
RRM	Radio Resource Management.*Gestión de Recursos de Radio.*
SAAL-NNI	Signalling ATM Adaptation Layer. *Nivel de Adaptación a ATM de Señalización.*
SAP	Service Access Point. *Punto de Acceso a Servicio.*
SAPI	Service Access Point Identifier. *Identificador de Punto de Acceso a Servicio.*
SCP	Service Control Point. *Punto de Control de Servicio.*
SCCP	Signalling Connection Control Part. *Parte de Control de Conexión de Señalización.*
SCTP	Simple Control Transmission Protocol. *Protocolo de Transmisión de Control Simple.*
SGSN	Serving GPRS Support Node. *Nodo de Soporte de Servicios GPRS.*
SI	Stream Identifier. *Identificador de Flujo.*
SIM	Subscriber Identity Module. *Módulo de Identidad del Suscriptor.*
SM	Session Management. *Gestión de Sesión.*
SMS	Short Message Service. *Servicio de Mensajes Cortos.*
SSL	Secure Socket Layer. *Nivel de Socket Seguro.*
SN	Serving Network. *Red de servicios.*
SPI	Security Parameter Index. *Índice de Parámetros de Seguridad.*
SQN	Sequence number. *Número Secuencial.*
SRNC	Serving RNC. *RNC de servicios.*
SSSAR	Service Specific Segmentation And Reassembly. *Segmentación y Reensamblaje con Características de Servicios.*
SSCF	Service Specific Co-ordination Function. Función de Coordinación Específica de Servicio.
SSCOP	Service Specific Connection Oriented Protocol.

	Protocolo de Servicio Específico Orientado a la Conexión.
SS7	Signalling System Nº 7. *Sistema de Señalización nº 7.*
SVC	Switched Virtual Circuit. *Circuito Virtual Conmutado.*
TAK	Temporary Authentication Key. *Clave de Autenticación Temporal.*
TCP	Transmission Control Protocol. *Protocolo de Control de Transmisión.*
TE	Terminal Equipment. *Equipo de Terminal*.
TEMSI	Temporary Encrypted Mobile Subscriber Identity. *Identidad de Suscriptor Móvil Encriptada Temporal.*
TI	Transaction Identifier. *Identificador de Transacción*.
TLS	Transport Layer Security. *Seguridad de Nivel de Transporte*
TMSI	Temporary Mobile Subscriber Identity. *Identidad de Suscriptor Móvil Temporal.*
TMUI	Temporary Mobile User Identity. *Identidad de Usuario Móvil Temporal.*
TTP	Trusted Third Party. *Tercer Elemento Verificado.*
UDP	User Datagram Protocol. *Protocolo de Datagramas de Usuario.*
UE	User Equipment. *Equipamiento de Usuario.*
UEA	UMTS Encryption Algorithm. *Algoritmo de Encriptación de UMTS.*
UIA	UMTS Integrity Algorithm. *Algoritmo de Integridad de UMTS.*
UICC	UMTS Integrated Circuit Card. *Tarjeta de Circuito Integrado UMTS*.
UIDN	User Identity Decryption Node. *Nodo de Desencriptación de la Identidad de Usuario.*
UMSC	UMTS MSC. *MSC para UMTS.*
UL	Up-link. *Conexión Ascendente.*
UMTS	Universal Mobile Telecommunication System. *Sistema de Telecomunicación Móvil Universal.*
UP	User Plane. *Plano de Usuario.*
URAN	UMTS Radio Access Network. *Red UMTS de Acceso a Radio*
UTRA	UMTS Terrestrial Radio Access. *Acceso UMTS Terrestre de Radio.*
UTRAN	UMTS Terrestrial Radio Access Network. Red UMTS de *Acceso Terrestre de Radio.*
USIM	User Services Identity Module. *Módulo de Identidad de Servicios de Usuario.*
VASP	Value Added Service Provider. *Servicio de Valor Añadido del Proveedor.*
VHE	Virtual Home Environment. *Entorno Particular Virtua.l.*
VLR	Visitor Location Register. *Registro de Ubicación de Visitantes.*
WAP	Wireless Application Protocol. *Protocolo de Aplicación Sin Cable.*
WDP	Wireless Datagram Protocol. *Protocolo de Datagrama Sin Cable.*
WSP	Wireless Session Protocol. *Protocolo de Sesión Sin Cable.*
WTLS	Wireless Transport Layer Security. *Seguridad del Nivel de Transporte Sin Cable.*
WTP	Wireless Transaction Protocol. *Protocolo de Transacción Sin Cable.*
XEMSI	ExtendedEncrypted Mobile Subscriber Identity. *Identidad de Suscriptor Móvil Encriptada Extendida.*
XRES	Expected Response. *Respuesta Esperada.*

4 Símbolos

Cu	Punto de referencia entre el USIM y el ME
Iu	Punto de referencia entre los dominios de Acceso y Red Servidor
Uu	Punto de referencia entre los dominios de Equipo de Usuario e Infraestructura, Interfaz de radio UMTS
[Yu]	Punto de referencia entre los dominios de Red Servidor y de Tránsito
[Zu]	Punto de referencia entre los dominios de Red Servidor y la Red Propia
||	Concatenación
⊕	OR exclusiva
f1	Función de autenticación de mensaje utilizada para calcular MAC
f2	Función de autenticación de mensaje utilizada para calcular RES y XRES
f3	Función generadora de Claves utilizada para calcular CK
f4	Función generadora de Claves utilizada para calcular IK
f5	Función generadora de Claves utilizada para calcular AK
f6	Función de encriptación utilizada para encriptar IMUI
f7	Función de desencriptación utilizada para desencriptar IMUI (= $f6^{-1}$)
f8	Función de algoritmo de cifrado
f9	Función de algoritmo de integridad
Gb	Interfaz entre SGSN y BSS
Gc	Interfaz entre GGSN y HLR
Gd	Interfaz entre SMS-GMSC y SGSN y, entre SMS-IWMSC y SGSN
Gf	Interfaz entre SGSN y EIR
Gi	Punto de referencia entre GPRS y una red de paquetes de datos externa
Gn	Interfaz entre dos GSNs dentro de una misma PLMN
Gp	Interfaz entre dos GSNs de diferentes PLMNs
Gr	Interfaz entre SGSN y HLR
Gs	Interfaz entre SGSN y MSC/VLR
Iu	Interfaz entre RNS y CN
Um	Interfaz entre MS y la parte de la red fija GSM
Uu	Interfaz entre MS y la parte de la red fija UMTS
K	Clave secreta compartida entre USIM y AuC

5Introducción

5.1 Objeto del documento

El objeto de este documento es exponer la Tesis Doctoral “Modelos de seguridad para móviles”. El principal objetivo de esta tesis es plantear un modelo de arquitectura de seguridad que permita a sistemas de seguridad de segunda generación asumir los servicios de seguridad que ofrece la tecnología de móviles de tercera generación (UMTS).

5.2 Introducción

La evolución de la telefonía móvil ha dejado en un segundo plano el desarrollo de unos servicios y mecanismos de seguridad acordes con este proceso evolutivo. Esta tesis, es el resultado de la necesidad de encontrar una solución a los problemas de seguridad existentes en los sistemas de telefonía móvil actuales.

El primer paso ha sido hallar un modelo de seguridad (requerimientos, servicios, mecanismos, etc.) correcto, para ello se ha tomado como punto de partida la especificación de seguridad definida para UMTS, o tecnología móvil de tercera generación. La elección de UMTS como referencia se ha considerado obligada ya que representa el futuro de las comunicaciones sin cable según los organismos estándar existentes La tecnología UMTS se presenta como el sistema de telefonía móvil “seguro”, proporciona nuevos servicios y mecanismos de seguridad que amplían y refuerzan los existentes hasta el momento. Incorpora además mejoras como pueden ser incremento de la velocidad de transmisión de datos, optimización de la gestión de recursos y nuevos mecanismos transmisión por radio.

Una vez fijado el modelo de referencia, se ha realizado un análisis exhaustivo de las especificaciones de seguridad definidas para GSM y GPRS (denominados sistemas de segunda generación, 2G y 2’5G) y se han concretado los elementos de seguridad a revisar., entiéndase por elementos a revisar, aquellos componentes (servicios y / o mecanismos) a mejorar o a incorporar en la especificación de seguridad de GSM y GPRS.

El capítulo “Requerimientos” en las secciones “UMTS: Amenazas, objetivos y servicios de seguridad” y “UMTS: Mecanismos de seguridad ”describe la especificación de seguridad para UMTS. Mientras que en el capítulo “Estado del Arte” se detalla el estado del arte, con respecto a seguridad, de los sistemas actuales GSM (2G) y GPRS (2,5G), a la vez que se realiza una comparativa con la especificación de seguridad para UMTS.

A continuación, una vez realizado el análisis del estado del arte de los sistemas actuales y la comparativa con UMTS, se ha procedido a detallar los requerimientos de diseño deseados para el modelo de arquitectura a proponer. Las restricciones impuestas al modelo de seguridad marcan la pauta del diseño realizado y como resultado ofrecen una arquitectura de componentes estándar de amplia difusión y adaptabilidad a nuevas necesidades de seguridad.

Finalmente se ha creado el modelo de arquitectura de seguridad para móviles de segunda generación, este modelo ofrece todos los servicios de seguridad definidos hasta el momento y ha sido denominado “Modelo de arquitectura WTLS sobre IP”. Consecuencia de este modelo ha sido diseñado el “Modelo de arquitectura IP”, este segundo proyecto sería la consecución óptima del modelo de arquitectura de seguridad para telefonía móvil aunque su implantación requeriría grandes cambios en los sistemas actuales.

Dentro de esta tesis se han considerado también dos factores importes, el primero ha sido la especificación de un valor de MTU para movilidad IP, siendo ésta un elemento de primer orden en los modelos propuestos. El segundo ha sido la realización de una valoración comparativa de las implementaciones que ofrece movilidad IP.

El capítulo “Soluciones” en el apartado “Modelos de Arquitectura de Seguridad” explica los requerimientos aplicados a los modelos de arquitectura y describe los diseños creados en el marco de esta tesis. La sección “Movilidad IP aplicada a los Modelos de Arquitectura de Seguridad”, describe las razones para la selección de un valor de MTU específico y se analiza en profundidad el análisis comparativo entre las movilidad IPV4, movilidad IPv4 con optimización de direccionamiento, movilidad IPv6 y movilidad IPv6 con optimización de direccionamiento.

Las conclusiones se presentan en el capítulo “Conclusiones”.

5.3 Objetivos

El objetivo de este trabajo de tesis es la definición de una arquitectura de seguridad para los sistemas de telefonía móvil de segunda generación, que permita soslayar los problemas de seguridad que éstos plantean, y que permita la coexistencia de éstos con los de tercera generación, sin que ello signifique renunciar a los servicios de seguridad ofrecidos por ésta. En definitiva lo que se pretende es uniformizar los servicios de seguridad ofrecidos por los sistemas de telefonía móvil de las generaciones 2G y 3G en el límite superior, es decir el ofrecido por los sistemas de tercera generación.

Además de este requerimiento funcional, se impuso uno adicional de tipo pragmático, consistente en imponer la restricción de que fuese realizable empleando componentes existentes en el mercado, puesto que las redes IP ya ofrecen estos servicios de seguridad y debía ser posible definir una arquitectura que permitiese garantizar la seguridad de las comunicaciones extremo-a-extremo, sin perder aspectos tan importantes como la confidencialidad o la acreditación del origen en pasarelas intermedias entre las distintas redes de telecomunicaciones existentes actualmente (fija, móvil, IP).

Dado que una de las premisas de la arquitectura de comunicaciones seguras era su factibilidad, se ha buscado el refrendo de la propuesta realizada por parte de algún operador de telefonía móvil, y hasta el momento se ha conseguido con Airtel.

Dentro de esta tesis se han considerado también dos factores importantes, el primero ha sido la especificación de un valor de MTU para movilidad IP y el segundo ha sido la realización de una valoración comparativa de las implementaciones que ofrece movilidad IP. La evaluación de

estos factores permite seleccionar la mejor opción para la implementación de los modelos de arquitectura propuestos.

5.4 Estructura de la tesis

Los capítulos “Referencias” , “Definiciones”, “Abreviaturas” y “Símbolos” detallan los documentos de referencia considerados en esta tesis y la notación utilizada en la misma.

Los requerimientos de seguridad planteados se detallan en el capítulo “Requerimientos”. Este capítulo describe la especificación de seguridad existente para UMTS e incluye las secciones “UMTS: Amenazas, objetivos y servicios de seguridad”, “UMTS: Mecanismos de seguridad”.

El estado del arte de los sistemas de segunda generación (GSM, GPRS y UMTS) se define en el capítulo del mismo nombre, “Estado del Arte” donde se realiza una comparativa entre los sistemas de segunda generación y UMTS.

Las aportaciones principales de esta tesis se incluyen en el capítulo “Soluciones” en los apartados “Modelos de Arquitectura de Seguridad”, donde se detallan los dos diseños propuestos, con un análisis sobre las implicaciones que comportaría su implementación y las mejoras aportadas por cada modelo y en el apartado “Movilidad IP aplicada a los Modelos de Arquitectura de Seguridad” , donde se especifica el valor de la Unidad Máxima de Transmisión sugerido para el uso de IP y donde se realiza una comparativa sobre las diferentes implementaciones de movilidad IP.

El capítulo “Conclusiones” presenta un sumario de las aportaciones realizadas dentro de la tesis “Modelos de seguridad para móviles” y una propuesta de trabajos futuros.

Los anexos “Arquitectura UMTS”, “Arquitectura General de una PLMN”, “IPSec”, “Movilidad IP”, “Red de Acceso a Radio Terrestre de UMTS (UTRAN)”, “GPRS en UMTS” y “Tecnología WAP”, complementan el estudio realizado sobre las diferentes tecnologías existentes en el mercado. Algunos de estos anexos han sido fruto del análisis realizado en una primera fase de esta tesis, en la que se pretendía aprovechar las características de tecnología ATM, para intentar mejorar a nivel de transporte la seguridad para los sistemas de telefonía móvil de segunda generación. Esta opción se descartó basándose en los requerimientos evolutivos de GSM y GPRS que implican la compatibilidad entre todas sus versiones.

6 Requerimientos

Este capítulo realiza una descripción detallada de la especificación de seguridad de UMTS.

6.1 UMTS: Amenazas, objetivos y servicios de seguridad

En los siguientes apartados se describirán los objetivos de seguridad de UMTS y las posibles amenazas a los mismos. También se detallan los principales requerimientos y servicios de seguridad que ofrece UMTS.

6.1.1 Objetivos

Los objetivos principales de seguridad de UMTS son:

- *Asegurar el acceso y la integridad de la información de usuario*
- *Asegurar el correcto acceso y uso de los recursos y servicios de red*
- *Interoperabilidad*
  Garantizar que los mecanismos de seguridad de UMTS son compatibles con los mecanismos de seguridad disponibles.
- *Estandarización*
  Garantizar la estandarización de los mecanismos de seguridad de UMTS a fin de asegurar la interoperabilidad y la transmisión entre diferentes redes de servicios.
- *Alto nivel de protección*
  Asegurar un nivel de protección para usuarios y proveedores de servicios mejor que el existente, a día de hoy, en redes fijas y móviles
- *Implementación de mecanismos de seguridad flexible*
  Asegurar que la implementación de mecanismos de seguridad en UMTS puede adaptarse, si fuera necesario, a nuevas amenazas y servicios.

6.1.2 Amenazas

La clasificación de posibles amenazas puede ser múltiple, en este caso, se han clasificado según el punto de ataque. Así comentaremos amenazas asociadas con ataques a la interfaz de radio, amenazas asocias con ataques a otras partes del sistema y amenazas asociadas al terminal y al UICC / USIM.

Como amenazas a la interfaz de radio se consideran:

- Acceso no autorizado a datos
- Integridad
- Negación de servicio

Como amenazas a otras partes del sistema se consideran:

- Acceso no autorizado a datos

- Integridad
- Negación de servicio
- Repudio
- Acceso no autorizado a servicios

Como principales amenazas asociadas a UICC / USIM se determinan:

- Robos de terminal y UICC
- Integridad de datos de un terminal o USIM
- Uso de un terminal no estándar o barrado
- Escucha de la comunicación de la interfaz UICC - terminal
- Suplantación de la identidad del receptor de la interfaz UICC - terminal

6.1.3 Requerimientos de Seguridad

Los requerimientos de seguridad, en general, se definen a partir del estudio de las posibles amenazas, a continuación se presenta un lista de los requerimientos más importantes clasificados por roles.

- Usuarios de sistema UMTS

  Acceso seguro a servicios UMTS
  Protección de datos relativos al usuario transmitidos
  Protección de datos relativos al usuario almacenados
  Seguridad extremo a extremo

- Proveedor

  USIM seguro
  Terminal seguro
  Administración de servicios UMTS de forma segura

- Órganos reguladores[1]

  Interceptar por ley

6.1.3.1 Acceso seguro a servicios UMTS

UMTS debe garantizar el acceso a servicios de UMTS de forma fiable considerando,

- La obtención de servicios UMTS, por parte de usuarios no autorizados, por suplantación de la identidad de un usuario autorizado.
- La obtención, por parte de intrusos, de servicios ya asignados a un usuario.
- La imposibilidad de imponer tasas injustificadas a los usuarios

[1] Organismos autorizados a publicar leyes o guías de funcionamiento referentes a la oferta o uso de servicios UMTS, terminales UMTS o equipamiento de red.

- Verificar la posibilidad de la red de servicios, de ofrecer de forma autorizada, los servicios UMTS.
- En el caso de acceso simultáneo de múltiples usuarios desde un mismo terminal, la seguridad del acceso individual a los servicios UMTS debe mantenerse.
- Confidencialidad e integridad de datos de señalización y de control.

6.1.3.2 Protección de información de usuario transmitida

UMTS debe garantizar la transmisión de información de usuario de forma confidencial e íntegra considerando,

- Protección de la confidencialidad de tráfico de usuario.
- Protección de la confidencialidad de información relativa a la identidad de usuario.
- Protección de la confidencialidad de la ubicación de la información de usuarios.
- Protección de la confidencialidad, frente a usuarios no autorizados, de la ubicación de la información de usuarios participantes de un servicio UMTS específico, frente a las otras partes concurrentes en el mismo servicio.
- Integridad de datos.
- Verificar que el tráfico es seguro.

6.1.3.3 Protección de datos de usuarios almacenados

UMTS debe garantizar la confidencialidad y el acceso a los datos de usuario almacenados en el sistema considerando,

- Integridad de la información de usuario procesada o almacenada por un proveedor.
- Confidencialidad de la información de usuario almacenada o procesada por un proveedor.
- Integridad de la información de usuario almacenada en el terminal o USIM.
- Confidencialidad de la información de usuario almacenada en el terminal o USIM.

6.1.3.4 Seguridad extremo a extremo

Garantizar la seguridad de la comunicación (datos, servicios, conexión,…) extremo a extremo considerando,

- El usuario debe poder efectuar una llamada permaneciendo en el anonimato, excepto en llamadas de emergencia.
- UMTS no debe excluir la implementación de servicios de seguridad extremo a extremo sobre portadores de UMTS

6.1.3.5 Seguridad del USIM

UMTS debe garantizar el correcto acceso a USIM considerando,

- Para acceder a servicios de UMTS debe ser necesario un USIM válido, teniendo como posible excepción, las llamadas de emergencia.
- Excluir el uso de un USIM específico para acceder a servicios UMTS.

- Control de acceso a datos en el USIM.
- No disponibilidad de datos de uso interno del USIM (claves de autenticación, algoritmos,...)
- En el caso de un UICC con más de un USIM, diferentes entornos particulares sólo tendrán acceso al USIM correspondiente a sus usuarios
- En el caso de un UICC con más de un USIM, la seguridad de gestión de datos de cada USIM se controlará de forma independiente.
- Será posible el control de acceso a, y la selección de, USIMs o aplicaciones no UMTS grabadas en el mismo UICC.
- Posibilidad de verificar el origen y la integridad de las aplicaciones y datos del UICC.

6.1.3.6 Seguridad del terminal

UMTS debe garantizar la identidad del terminal y los accesos a los servicios a partir de un terminal específico considerando,

- Poder determinar el robo de terminales
- Impedir el acceso a servicios UMTS a terminales concretos.
- Dificultar el cambio de identificación de un terminal
- Posibilidad de verificar el origen y la integridad de las aplicaciones y datos del terminal.

6.1.3.7 Servicios de UMTS seguros

UMTS debe garantizar el correcto uso y acceso a los servicios considerando,

- Los proveedores podrán autentificar usuarios, tanto al inicio del proceso como durante el uso de un servicio.
- Detección y prevención de uso fraudulento de servicios (alarmas y registros de auditoría)
- Finalización súbita de todos los servicios ofrecidos a un entorno particular por cualquier usuario de dicho entorno.
- Las redes de servicios podrán autenticar el origen del tráfico de usuario, de los datos de señalización y de control de la interfaz de radio.
- Impedir el uso de servicios por parte de intrusos en el sistema.

6.1.3.8 Interceptar por ley

UMTS debe garantizar la posibilidad de visualizar y registrar cualquier intento, fallido o no, de atentar contra la ley nacional.

6.1.4 Servicios de seguridad de UMTS

Para cada servicio de seguridad se describen las diferentes posibilidades a contemplar.

6.1.4.1 Autenticación

6.1.4.1.1 Fijar mecanismo de autenticación

Este servicio permite a SN y a MS acordar el mecanismo de autenticación que utilizarán. Las entidades involucradas son:

- USIM
- MSC / VLR

6.1.4.1.2 Autenticación del usuario a la red

Este servicio permite a SN corroborar la Identidad Internacional del Usuario Móvil (IMUI) de MS. Las entidades involucradas son:

- USIM
- MSC / VLR
- HLR / AuC

6.1.4.1.3 Autenticación de la red al usuario

Este servicio permite a MS verificar, para el entorno particular del usuario, que SN está autorizada para ofrecer los servicios que demanda el usuario. Las entidades involucradas son

- USIM
- MSC / VLR
- HLR / AuC

6.1.4.1.4 Identificación del equipo de usuario a la red

Este servicio permite a SN corroborar la Identidad Internacional del Equipamiento Móvil (IMEI). Las entidades involucradas son:

- UE
- MSC / VLR

6.1.4.1.5 Autenticación del usuario a USIM

Este servicio permite restringir el uso de USIM a usuarios autorizados. Las entidades implicadas en esta prestación son:

- USIM
- UE
- usuario

6.1.4.1.6 Autenticación de USIM a UE

Este servicio permite restringir el uso de UE a USIMs autorizados. Involucradas en este servicio están:

- USIM
- UE

6.1.4.2 Confidencialidad

6.1.4.2.1 Fijar algoritmo de cifrado

Este servicio permite a SN y a MS acordar el mecanismo de cifrado a utilizar. Las entidades implicadas en esta prestación son:

- UE
- MSC / VLR
- USIM

6.1.4.2.2 Establecimiento de clave de cifrado derivada

Este servicio permite a MS y a SN garantizar la renovación de la DCK. Las entidades implicadas son:

- USIM
- UE
- RNC
- VLR
- HLR

6.1.4.2.3 Confidencialidad de datos de usuario

Este servicio permite preservar la información de usuario transmitida por radio. Involucradas en estas prestación están:

- UE
- RNC

6.1.4.2.4 Confidencialidad de información de señalización

Este servicio permite preservar la información de señalización transmitida por radio. Las entidades implicadas son:

- UE
- RNC

6.1.4.2.5 Confidencialidad de la identidad de usuario

Este servicio permite preservar en el anonimato la identidad del usuario al acceder a servicios. Involucradas en esta prestación están:

- USIM
- VLR

6.1.4.2.6 Indicador de Cifrado

Este servicio permite manifestar si la confidencialidad de los datos está asegurada. La entidad implicada es:

- UE

6.1.4.3 Integridad de datos y autenticación del origen de los datos transmitidos

6.1.4.3.1 Fijar algoritmo de integridad

Este servicio permite a SN y a MS acordar el algoritmo de integridad a utilizar. Las entidades implicadas son:

- MSC / VLR
- USIM

6.1.4.3.2 Establecimiento de clave de integridad derivada

Este servicio permite a MS y a SN garantizar la renovación de la DIK. Están involucradas en esta prestación:

- USIM
- VLR
- HLR

6.1.4.3.3 Integridad de datos y autenticación del origen de elementos de señalización

Este servicio permite a MS y a SN verificar la integridad y el origen de determinados elementos de señalización transmitidos por radio. Las entidades implicadas en este servicio son:

- USIM
- MS
- SN

6.2 UMTS: Mecanismos de seguridad

Esta sección presenta la arquitectura de seguridad de UMTS y los diferentes mecanismos utilizados para ofrecer los servicios de seguridad de tercera generación. La mayoría de estos dispositivos son una evolución de los mecanismos presentes en GSM / GPRS.

6.2.1 Arquitectura de seguridad en UMTS

Las figuras siguientes dan una visión, desde perspectivas diferentes, de la arquitectura de seguridad de UMTS.

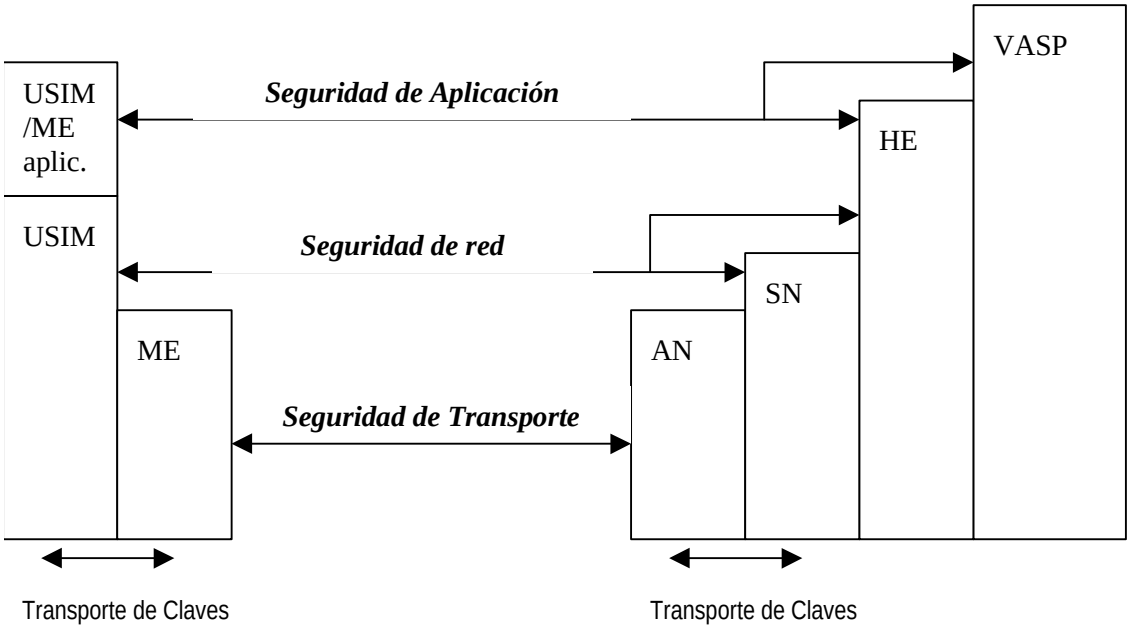


Figura 1. Arquitectura de seguridad de UMTS (dominios)

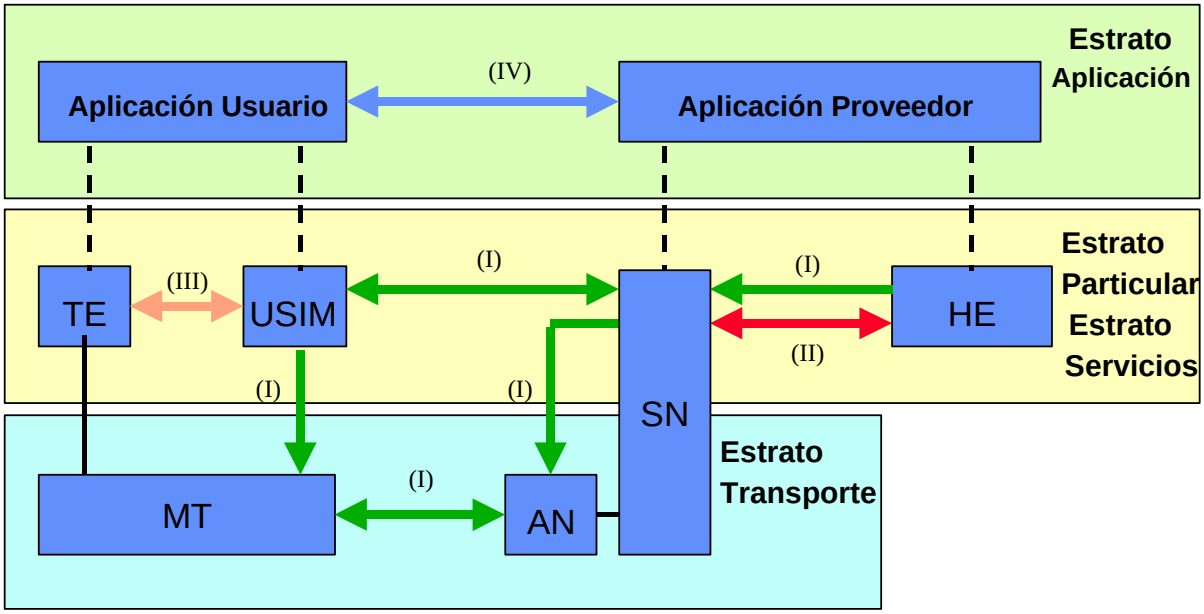


Figura 2. Arquitectura de Seguridad de UMTS (estratos)

Leyenda:

(I) Seguridad de acceso a Red: Conjunto de funcionalidades que ofrecen al usuario acceso seguro a los servicios 3G y en particular protección contra los ataques a la conexión de radio.

(II) Seguridad del dominio de Red: Conjunto de funcionalidades que permiten a los nodos del dominio del proveedor intercambiar información de señalización de forma segura y además ofrecen protección contra ataques a la red.

(III) Seguridad del dominio de Usuario: Conjunto de funcionalidades que ofrecen acceso seguro a los terminales móviles.

(IV) Seguridad del dominio de aplicación: Conjunto de funcionalidades que permiten el intercambio seguro de mensajes entre aplicaciones del dominio de usuario y del proveedor.

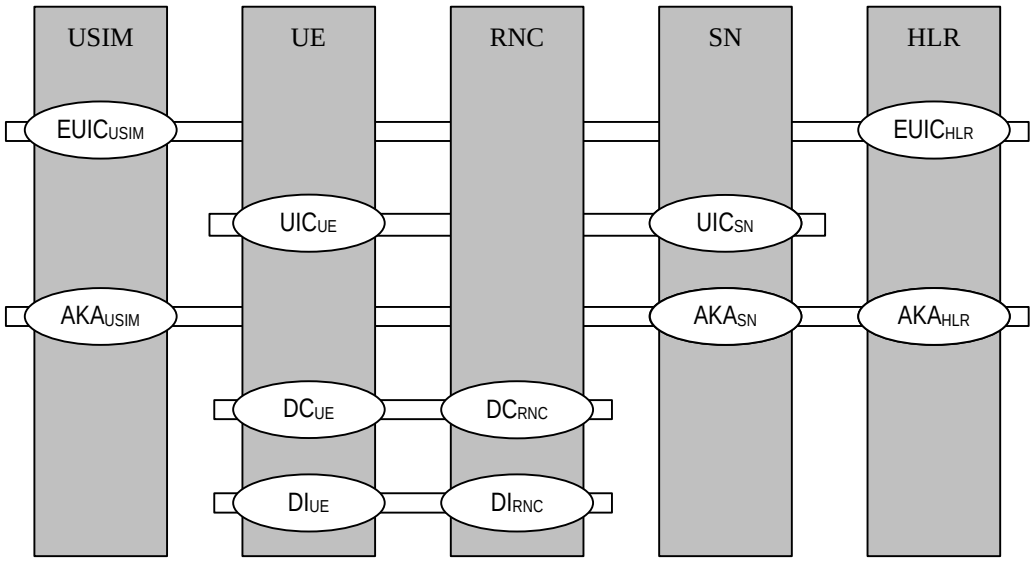


Figura 3. Arquitectura funcional de seguridad de UMTS

Las barras verticales representan los elementos de la red, en el dominio de usuario: USIM y UE, en el dominio de la red de servicios: RNC, VLR/SGSN y en el dominio de entorno particular: HLR/AuC y UIDN.

Las barras horizontales representan los mecanismos de seguridad:

EUIC: mecanismo de confidencialidad de identidad de usuario fuerte (opcional, entre usuario y HE).
UIC: mecanismo convencional de confidencialidad de identidad de usuario (entre usuario y SN).
AKA: mecanismos de autenticación y acuerdo de claves, incluyendo la funcionalidad de relanzar el mecanismo de autentificación por parte del usuario.
DC: mecanismo de confidencialidad de datos de usuario y de información de señalización.
DI: mecanismo de integridad de datos de señalización.

La figura presentada a continuación muestra los principios de conexión y de registro de UE en UMTS con dominio CS y PS.

La identificación de usuario (temporal), la autenticación y el acuerdo de claves tendrán lugar de forma independiente para cada dominio. El tráfico de usuario se encriptará utilizando la clave correspondiente al dominio de servicio mientras que, los datos del plano de control se cifrarán y se aplicará la protección de integridad de uno de los dominios.

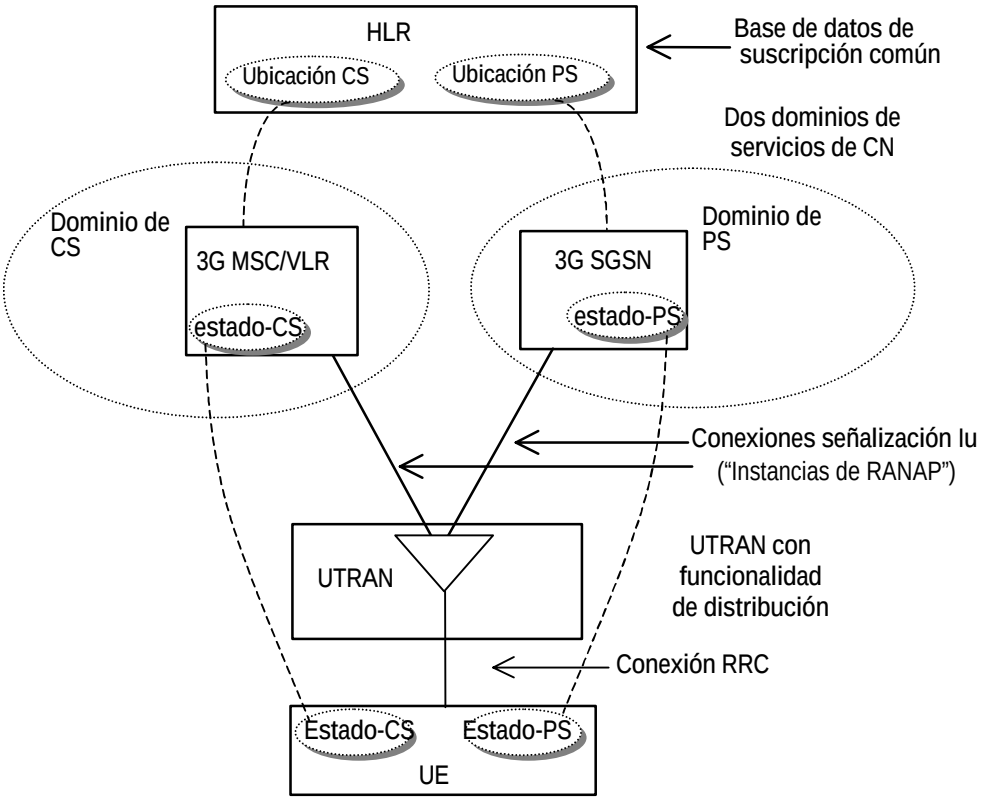


Figura 4. Vista de conexiones y Registro de UE para UMTS con arquitectura CN separada para los dominios CS y PS

6.2.2 Servicios de Seguridad

6.2.2.1 Seguridad de Acceso de Red

6.2.2.1.1 Confidencialidad de la Identidad de Usuario

Se ofrecen los siguientes servicios relacionados con la confidencialidad de la identidad de usuario:

- Confidencialidad de la identidad de usuario

  Para evitar que la identidad permanente de un usuario (IMUI), al que se le están ofreciendo determinados servicios, pueda obtenerse a partir de la conexión de radio.

- Confidencialidad de la ubicación de usuario

  Para evitar que la presencia o la llegada de un usuario a un área específica no pueda ser descubierta en la conexión de radio.

- Imposibilidad de seguimiento de usuario

  Para evitar que un intruso pueda averiguar los servicios ofrecidos a un usuario concreto a partir de la conexión de radio

Existen diversos mecanismos para conocer la identidad de usuario, el primero permite al usuario identificarse en el canal de radio por medio de una identidad temporal por la cual ya es conocido en SN., el segundo método permite al usuario identificarse por medio de una identidad permanente encriptada y el tercero le permite transmitir la identidad permanente sin encriptar. Tanto el segundo como tercer mecanismo se aplican en el caso de que la identidad temporal de usuario no se conozca en SN.

A fin de no permitir el seguimiento de los servicios ofrecidos a un usuario, se obliga a no utilizar por mucho tiempo la misma clave temporal o encriptada. Es necesario también, que cualquier dato de señalización o usuario que pueda revelar la identidad, se transmita en modo cifrado por la conexión de radio.

6.2.2.1.2 Autenticación de Entidad

Se ofrecen los siguientes servicios relacionados con la autenticación de entidades:

- Acuerdo de mecanismo de autenticación

  Funcionalidad que permite al usuario y a SN negociar de forma segura el mecanismo para autenticación y acuerdo de claves.

- Autenticación de usuario

  Propiedad por la cual la red corrobora la identidad de usuario.

- Autenticación de la red

  Mecanismo por el que un usuario puede verificar si la SN a la que está conectado tiene autorización para proporcionar los servicios que requiere y la garantía de que la autorización, en caso de disponer de ella, es reciente.

A fin de conseguir estos objetivos se asume que la autenticación de usuario sucede en cada establecimiento de conexión entre red y usuario. Para ello se ofrecen dos mecanismos, el primero utiliza un vector de autenticación entregado por el HE del usuario a SN y que además de los servicios citados anteriormente establece una CK e IK secretas entre el usuario y SN. Este mecanismo se invoca desde SN después del primer registro de un usuario y después de una petición de servicio, petición de actualización de ubicación, petición de adherencia, petición de abandono o de reestablecimiento de conexión, siempre que el número máximo de usos de la clave de integridad derivada haya sido alcanzado. El segundo método, denominado mecanismo de autenticación local, utiliza la clave de integridad establecida entre usuario y SN durante una ejecución previa del procedimiento de establecimiento de clave y autenticación y siempre que el

número máximo de uso de la clave no haya sido alcanzado. La autenticación local se aplica después de una petición de servicio, petición de actualización de ubicación, petición de adherencia, petición de abandono o de reestablecimiento de conexión.

6.2.2.1.3 Confidencialidad

Se ofrecen los siguientes servicios relacionados con la confidencialidad:

- Acuerdo de algoritmo de cifrado

  Propiedad por la cual MS y SN pueden negociar de forma segura el algoritmo a utilizar.

- Acuerdo de clave de cifrado

  Fijar entre MS y SN la clave a utilizar con el algoritmo de cifrado.

- Confidencialidad de datos de usuario

  Permitir la transmisión de los datos de usuario por la interfaz de radio sin peligro de escucha.

- Confidencialidad de datos de señalización

  Permitir la transmisión de los datos de señalización por la interfaz de radio sin peligro de escucha.

El establecimiento de la clave de cifrado se efectúa mediante el mecanismo de autenticación y establecimiento de clave. La selección del algoritmo de cifrado se hace mediante el mecanismo de negociación del modo de seguridad entre usuario y red; este servicio también permite la aplicación del algoritmo de cifrado y de la clave establecida.

6.2.2.1.4 Integridad de datos

Se ofrecen los siguientes servicios relacionados con la integridad de datos:

- Acuerdo de algoritmo de integridad

  Negociación segura del algoritmo de integridad a utilizar entre MS y SN.

- Acuerdo de clave de integridad

  Funcionalidad que permite fijar la clave de integridad a utilizar con el algoritmo de integridad.

- Integridad de datos y autenticación del origen de datos de señalización

Propiedad por la cual la entidad receptora (MS o SN) es capaz de verificar que los datos de señalización no han sido alterados y que provienen de la entidad que lo proclama.

El acuerdo de claves de integridad se realiza en el mecanismo de autenticación y de acuerdo de claves. La selección del algoritmo de integridad se hace en el mecanismo de negociación del modo de seguridad entre usuario y red. Este servicio también permite la aplicación del algoritmo de integridad y de la clave de integridad fijada.

6.2.2.1.5 Identificación de equipamiento móvil

En determinados caso SN puede realizar una petición a MS para recibir la identidad del equipamiento móvil del terminal (IMEI). Esta identidad sólo se enviará después de proceder a la autenticación de SN, con excepción de las llamadas de emergencia.

6.2.2.2 Seguridad del dominio de Red

6.2.2.2.1 Autenticación de Entidad

Se ofrecen los siguientes servicios relacionados con la autenticación de elementos de red:

- Acuerdo de mecanismo de autenticación

  Propiedad por la que dos entidades de la red negocian de forma segura el mecanismo para autenticación y acuerdo de claves.

- Autenticación de elemento de red

  Propiedad por la cual un elemento de la red corrobora la identidad de otro.

A fin de conseguir estos objetivos se utiliza el mecanismo de autenticación de entidades, implícito o explícito, cada vez que se intercambian datos entre dos entidades de red. La autenticación implícita se realiza mediante el intercambio de mensajes encriptados y el servicio de autenticación explícita puede conseguirse mediante el uso de protocolos simétricos o asimétricos, por ejemplo utilizando firma digital.

6.2.2.2.2 Confidencialidad de datos

Se ofrecen los siguientes servicios relacionados con la confidencialidad de datos intercambiados entre elementos de red:

- Acuerdo de algoritmo de cifrado

  Propiedad por la cual dos elementos de red pueden negociar de forma segura el algoritmo a utilizar.

- Acuerdo de clave de cifrado

Funcionalidad que permite a dos elementos de red, fijar la clave a utilizar con el algoritmo de cifrado.

- Confidencialidad de datos

  Propiedad por la cual los datos transmitidos entre dos elementos de red no pueden ser interpretados.

Los dos primeros servicios pueden conseguirse en el transcurso del proceso de autenticación de los elementos de red. La clave de cifrado fijada entre ambos, se utiliza posteriormente para proteger los datos de señalización y de usuario.

6.2.2.2.3 Integridad de datos

Se ofrecen los siguientes servicios relacionados con la integridad de datos intercambiados entre dos elementos de red:

- Acuerdo de algoritmo de integridad

  Negociación segura del algoritmo de integridad a utilizar entre los elementos de red.

- Acuerdo de clave de integridad

  Fijar la clave de integridad a utilizar con el algoritmo de integridad.

- Integridad de datos y autenticación del origen de datos de señalización

  Propiedad por la cual el elemento receptor es capaz de verificar que los datos de señalización no han sido alterados y que provienen del elemento que lo proclama.

Los dos primeros servicios pueden conseguirse en el transcurso del proceso de autenticación de los elementos de red; la clave de integridad se utiliza posteriormente para proteger los datos mediante el algoritmo de integridad fijado.

6.2.2.2.4 Información contra Fraude

Deben definirse servicios y mecanismos de protección contra el fraude.

6.2.2.3 Seguridad del dominio de usuario

6.2.2.3.1 Autenticación de Usuario - USIM

Este servicio ofrece un acceso restringido del uso de USIM hasta que éste haya identificado al usuario. Generalmente el USIM dispone de una clave secreta, por ejemplo un PIN, que el usuario debe conocer para poder acceder al USIM.

6.2.2.3.2 Conexión USIM -Terminal

El acceso a un terminal u otro equipamiento de usuario está restringido a USIMs autorizados. USIM y terminal deben compartir una clave secreta y el USIM necesita demostrar que la conoce para poder utilizar el terminal.

6.2.2.4 Seguridad de Aplicación

En este apartado se incluye :

- Mensajes seguros entre USIM y red

  Para permitir el desarrollo de aplicaciones residentes en USIM es necesario disponer de la certeza de la transmisión segura de mensajes entre la red y las aplicaciones, con el nivel de seguridad designado por el operador de red o el proveedor de la aplicación.

- Confidencialidad de tráfico de usuario en la red

  Confidencialidad de los datos de usuario en toda la red, no sólo en la conexión de radio y en la red de acceso.

6.2.2.5 Visibilidad de seguridad y Configurabilidad

Normalmente los mecanismos de seguridad deben de ser aplicados de forma transparente al usuario aunque, a petición del usuario, el sistema debe ser capaz de notificar el uso de confidencialidad en la red de acceso, confidencialidad en toda la red y el nivel de seguridad de la red visitada.

La configurabilidad se basa en la aplicación de ciertos servicios dependiendo de los servicios de seguridad en funcionamiento, por ejemplo aceptación / rechazo de llamadas recibidas no cifradas o permitir / prohibir la autenticación de usuario-USIM.

6.2.3 Mecanismos de seguridad

6.2.3.1 Identificación por identidad temporal

Este mecanismo permite la identificación de un usuario en la conexión de acceso de radio mediante la identidad de suscriptor móvil temporal (TMSI / PTMSI). Esta identidad sólo tiene sentido localmente, es decir, dentro de su área de ubicación o área de direccionamiento en la que el usuario está registrado; fuera de este área TMSI / PTMSI debe ir acompañado de LAI o de RAI, para evitar ambigüedades. La asociación entre la identidad temporal y la identidad permanente se guarda en el VLR / SGSN en el cual está registrado el usuario.

La finalidad de este mecanismo es asociar una nueva identidad TMUI / LAI (respectivamente RAI) a un usuario, momento a partir del cual, dicho usuario será conocido por esta nueva identidad. Este procedimiento debe realizarse después del inicio del proceso de cifrado.

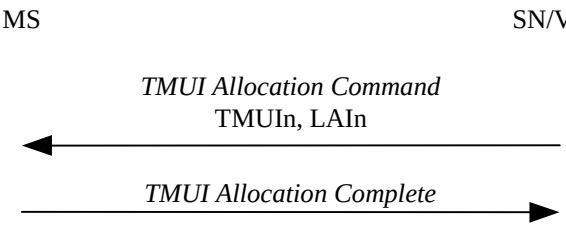


Figura 5. Asociación TMUI

El procedimiento es iniciado por VLR quien genera una nueva identidad temporal y guarda esta identidad y la identidad permanente (IMUI) en su base de datos. VLR envía TMUI y, si fuera necesario, LAI/RAI al usuario.

Al recibir la identidad temporal el usuario almacena esta información y elimina la asociación con la identidad TMUI previa. Posteriormente devuelve un ACK a VLR.

Si recibe el ACK, VLR elimina la asociación con la identidad vieja (TMUIo) y el IMUI, si existía, de su base de datos. Si VLR no recibe el ACK del usuario, la red mantendrá la asociación IMUI-TMUIo y IMUI-TMUIn. Después, en el caso de recibir un transacción originada por el usuario, la red permitirá al usuario identificarse bien por TMUIo o por TMUIn, lo que permitirá a la red determinar la identidad temporal almacenada en MS. La red mantendrá la asociación con la identidad de MS y eliminará la otra de su base de datos. Para transacciones originadas por la red, ésta identificará a MS por su identidad permanente (IMUI) y al establecer una conexión de radio forzará al usuario a eliminar cualquier identidad temporal almacenada. Cuando la red recibe la confirmación de que han sido eliminadas, borra cualquier asociación entre la identidad permanente y las posibles identidades temporales del usuario.

6.2.3.2 Actualización de ubicación

En el caso de que sea el usuario quien se identifique a si mismo utilizando TMUIo/LAIo (RAIo respectivamente), siendo el par asignado por el VLR visitado (VLRn), la identidad permanente, puede ser obtenida directamente de la base de datos. Si no fuera este el caso, el VLRn visitado pediría al usuario que se identificara por su IMUI.

Si el usuario se identifica a si mismo utilizando TMUIo/LAIo (RAIo respectivamente), no siendo el par asignado por el nuevo VLR (VLRn) y VLRn intercambia información con el anterior VLRo, VLRn pedirá a VLRo la identificación permanente de usuario. Este mecanismo está integrado dentro del mecanismo de distribución de datos de autenticación entre VLRs. Si VLRo no es accesible o no puede proporcionar IMUI, VLRn puede realizar la petición de identidad permanente directamente al usuario.

6.2.3.3 Identificación por identidad permanente

Este mecanismo permite la identificación del usuario en el canal de radio mediante la identidad permanente del usuario (IMUI).

La identificación por IMUI, es invocada por SN cuando el usuario no puede ser identificado por su identidad temporal y siempre que el usuario se registra por primera vez en una SN.

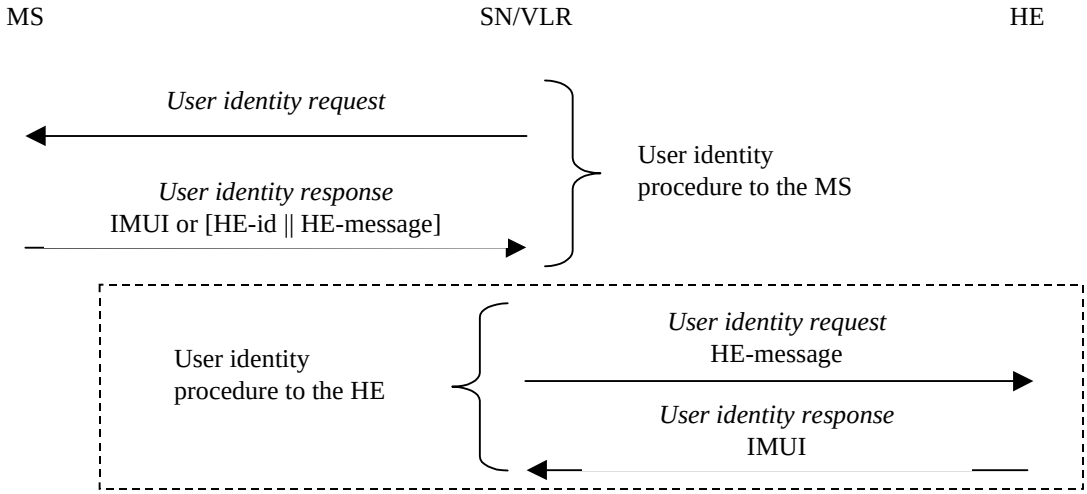


Figura 6. Identificación por identidad permanente

El mecanismo lo inicia SN/VLR quien realiza la petición al usuario de enviar su identidad permanente. De acuerdo con las preferencias del usuario contendrá bien IMSI sin cifrar o bien XEMSI. Un MS configurado para Confidencialidad de Identidad de Usuario Fuerte utilizará siempre XEMSI. La identidad de suscriptor móvil encriptada extendida consiste en una dirección de Nodo de Desencriptación de Identidad de Usuario (UIDN_ADR), y un contenedor con EMSI. UIDN_ADR es un nombre global de acuerdo con E164.

Si MS envía IMSI el proceso ya ha finalizado. Si no es así, SN/VLR/SGSN transmite EMSI al HE/UIDN con la petición de IMSI y TEMSI de usuario. El HE/UIDN del usuario deriva IMSI a partir de EMSI, calcula TEMSI y los devuelve a SN/VLR/SGSN. Para un usuario con confidencialidad de identidad de usuario fuerte, SN utilizará TEMSI en vez de IMSI.

Por parte de UE, el USIM calculará y almacenará TEMSI y lo transmitirá a UE. En ambos lados, UE y VLR/SGSN, TEMSI estará activa si el siguiente procedimiento de autenticación se ejecuta con éxito. Después de que la actual TEMSI haya sido utilizada con éxito una vez, SN debe lanzar una Petición de Identidad de Usuario para establecer una nueva TEMSI.

Para el servicio de Confidencialidad de Identidad de Usuario Fuerte se ha introducido un nuevo nodo lógico en la red. Este nodo se encarga de la desencriptación de IMSI a partir del EMSI de MS y del cálculo de TEMSI. Puede coexistir con HLR.

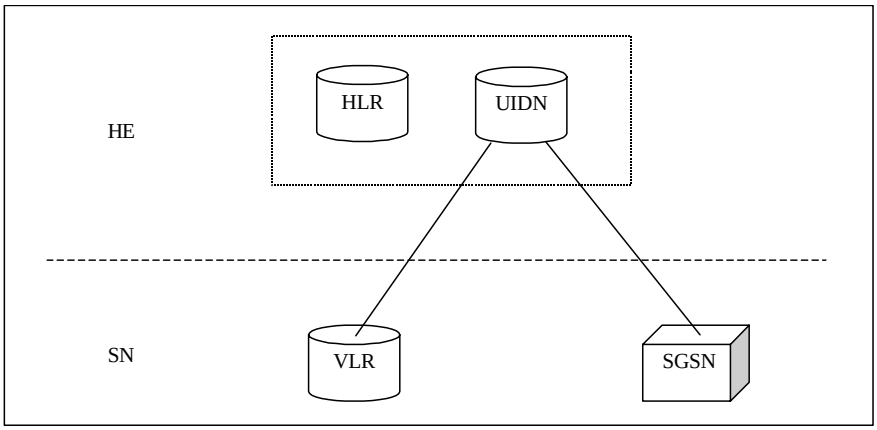


Figura 7. Arquitectura de Red Troncal para Confidencialidad de Identidad de Usuario Fuerte

6.2.3.4 Autenticación y acuerdo de claves

Este mecanismo tiene como objetivo conseguir la autenticación mutua del usuario y de la red mostrando conocimiento de una clave secreta K compartida y disponible sólo para USIM y AuC en el HE del usuario. Además permite a USIM y HE actualizar los contadores SEQ_{MS} y SEQ_{HE} respectivamente para soportar la autenticación de la red.

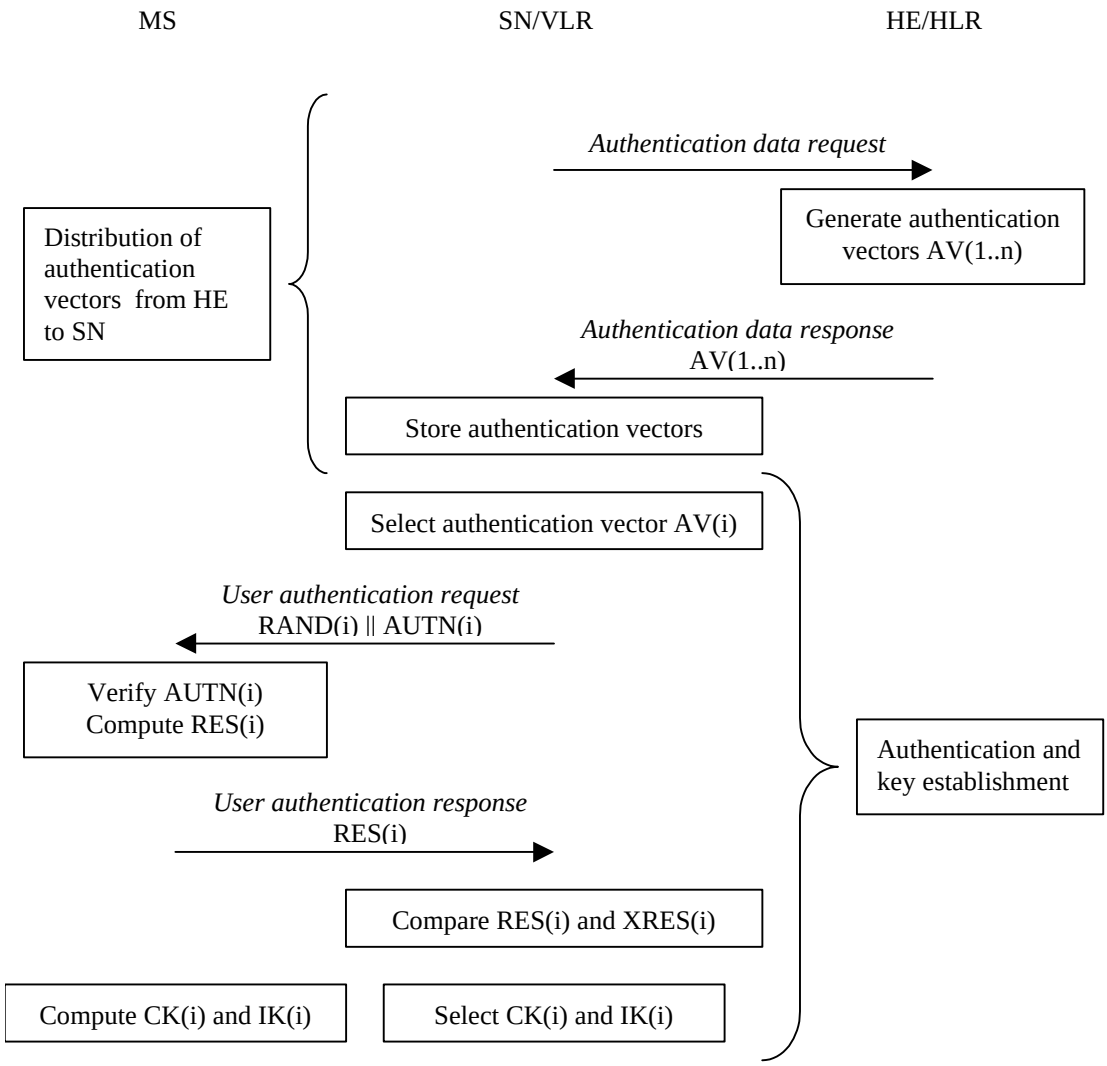


Figura 8. Autenticación y acuerdo de claves

Al recibir la petición del VLR/SGSN, el HE/AuC envía una cadena ordenada de n vectores a VLR/SGSN. Cada vector de autenticación consiste en: un número aleatorio RAND, una respuesta esperada XRES, una clave de cifrado CK, una clave de integridad IK y un vector de autenticación AUTN. Cada vector de autenticación sirve para una autenticación y acuerdo de claves entre VLR/SGSN y USIM.

Cuando VLR/SGSN inicia una autenticación y acuerdo de claves selecciona el siguiente vector de autenticación de la cadena y envía al usuario los parámetros RAND y AUTN. El USIM verifica si AUTN es aceptable y si es así, genera una respuesta RES en contestación a VLR/SGSN. El USIM a la vez calcula CK e IK. VLR/SGSN compara RES y XRES, si son iguales considera el proceso finalizado con éxito, e IK y CK se envían desde el USIM y desde VLR/SGSN a las entidades que ejecutan las funciones de integridad y cifrado.

En el caso de que las conexiones HE/AuC no estén disponibles, VLR/SGSN permite el uso de IK y CK previamente derivadas para ofrecer al usuario una conexión segura sin la necesidad de una autenticación y acuerdo de claves.

6.2.3.4.1 Distribución de datos de autenticación de HE a SN

El objeto de este procedimiento es enviar a VLR/SGSN una cadena de vectores de autenticación nuevos.

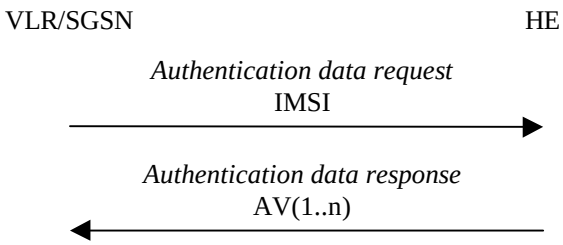


Figura 9. Distribución de información de autenticación de HE a SN

VLR/SGSN realiza la petición incluyendo IMSI. Al recibir la petición, HE/AuC envía la respuesta a VLR/SGSN conteniendo una cadena ordenada de vectores de autenticación AV(1..n).

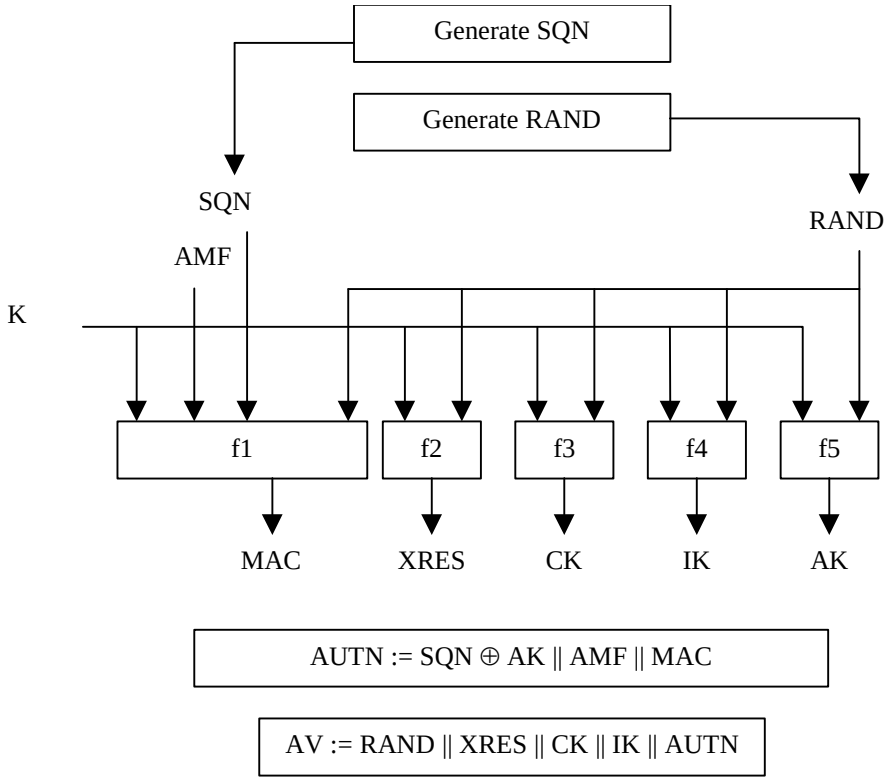


Figura 10. Generación de vectores de autenticación

HE / AuC inicia el proceso generando un número nuevo SQN y un valor aleatorio RAND.

Para cada usuario HE mantiene un contador SEQ_{HE}. El mecanismo asegura que un número secuencial es aceptado si pertenece a los anteriores 50 números secuenciales generados. El uso de SEQ_{HE} es específico de cada método de generación de números secuenciales.

En el valor de autenticación de cada vector de autenticación, se incluye un campo de autenticación y gestión de claves, AMF. Este campo puede tener diferentes usos, puede ser utilizado para indicar el algoritmo y la clave a utilizar para generar un vector de autenticación particular, puede usarse ,en otros casos, para indicar la diferencia máxima admisible entre SEQ_{MS} y SEQ_{HE}, finalmente, también puede servir al operador para limitar la cantidad de información protegida por una conjunto de claves determinado.

Se calculan los siguientes campos:

- $MAC = f1_K(SQN \,||\, RAND \,||\, AMF)$ donde f1 es la función de autenticación de mensaje.
- $XRES = f2_K(RAND)$ donde f2 es una función de autenticación de mensaje.
- $CK = f3_K(RAND)$ donde f3 es una función generadora de claves.
- $IK = f4_K(RAND)$ donde f4 es una función generadora de claves.
- $AK = f5_K(RAND)$ donde f5 es una función generadora de claves o $f5 \equiv 0$.

Finalmente se construye el valor de autenticación AUTN = SQN ⊕ AK || AMF || MAC.

6.2.3.4.2 Autenticación y acuerdo de claves

El propósito de este proceso es autenticar al usuario y establecer un nuevo par de claves de cifrado y de integridad entre VLR/SGSN y el USIM.

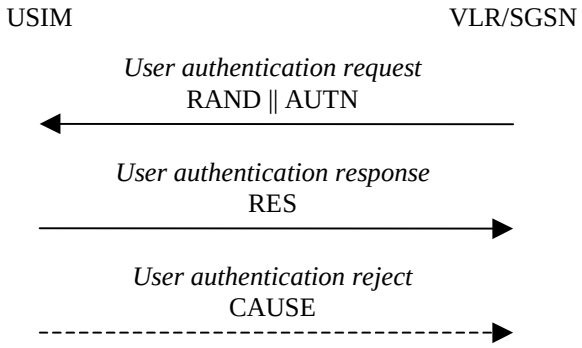


Figura 11. Autenticación y establecimiento de claves

VLR/SGSN inicia el procedimiento seleccionando el primer vector de autenticación no utilizado de la cadena ordenada de vectores de autenticación de la base de datos de VLR/SGSN. Después envía al USIM los parámetros RAND y AUTN para la autenticación de la red.

Al recibir el mensaje el usuario procede tal y como muestra la siguiente figura:

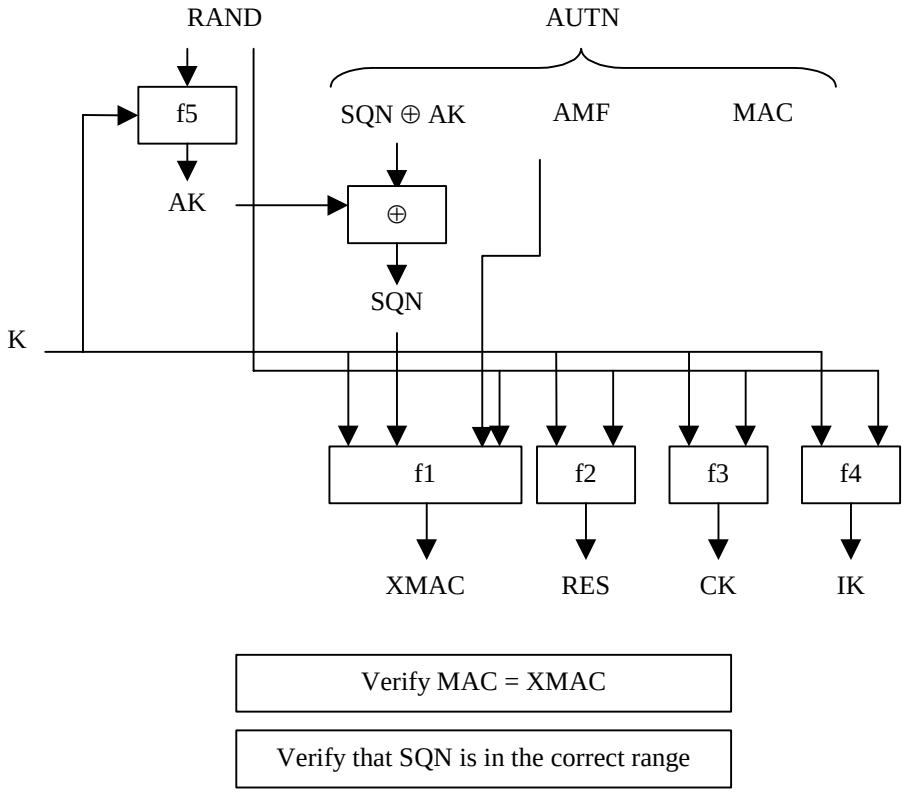


Figura 12. Función de autenticación de usuario en el USIM

Al recibir RAND y AUTN, el USIM calcula $f5_K$(RAND) y obtiene SQN = (SQN ⊕ AK) ⊕ AK. Posteriormente el USIM calcula XMAC = $f1_K$(SQN || RAND || AMF) y lo compara con el MAC incluido en AUTN, si son diferentes envía un mensaje "User Authentication Reject" indicando la causa y abandona el proceso, al recibir este mensaje VLR/SGSN inicia un proceso de "Authentication Failure Report" hacia HLR. VLR/SGSN puede decidir iniciar una nueva identificación y un nuevo proceso de autenticación con el usuario.

Si XMAC = MAC, el USIM verifica si el número de secuencia está en el rango correcto. Si no lo está envía un "Synchronisation Failure" y abandona el proceso. Si SEQ es correcto, calcula RES = $f2_K$(RAND) y lo incluye en el mensaje "User Authentication Response" que enviará a VLR/SGSN. Finalmente USIM calcula CK = $f3_K$(RAND) e IK = $f4_K$(RAND). El USIM guardará las claves CK e IK originales hasta la siguiente ejecución con éxito de AKA, así como también mantendrá el valor de RAND, hasta completar la actual AKA con fines de resincronización.

Al recibir el mensaje "User Authentication Response", VLR/SGSN compara RES con XRES si son iguales el proceso ha sido completado con éxito y VLR/SGSN selecciona las claves CK e IK del vector de autenticación. Si no ha sido así, inicia el proceso de "Authentication Failure Report" hacia HLR.

6.2.3.4.3 Distribución de IMSI y datos de autenticación temporal dentro de una red de servicios

El objetivo de este procedimiento es dar a un MSC/VLR o SGSN nuevo los datos de autenticación temporal de un MSC/VLR o SGSN previamente visitado dentro del mismo dominio de red de servicios.

La siguiente figura muestra el proceso a seguir.

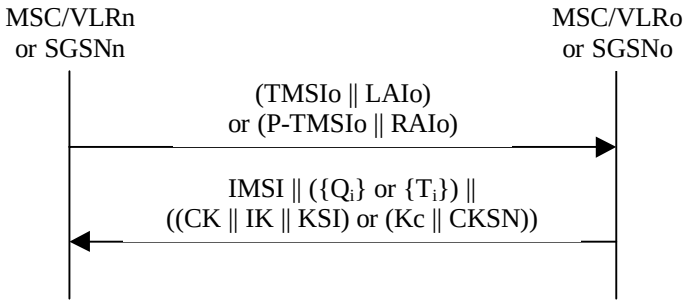


Figura 13. Distribución de IMSI y datos de autenticación temporal en un dominio de red de servicios

MSC/VLRn (SGSN respectivamente) inicia el proceso después de recibir una petición de actualización de ubicación (petición de actualización de área de direccionamiento respectivamente) del usuario, donde el usuario esta identificado por medio de una identidad temporal de usuario TMSIo (PTMSIo respectivamente) y la identidad de área de localización LAIo (identidad área de direccionamiento respectivamente). MSC/VLRo o SGSNo pertenece a la misma red de servicios que MSC/VLRn o SGSNn.

Los pasos seguidos en el proceso son:

1. MSC/VLRn (o SGSN) envía un mensaje “User Identity Request” al MSC/VLRo (o SGSNo) conteniendo TMSIo y LAIo (o PTMSI y RAIo)

2. MSC/VLRo (SGSNo) busca la información en la base de datos, si la encuentra envía un mensaje “User Identity Response” conteniendo IMSI, el número de vectores de autenticación no utilizados y puede incluir también el contexto de seguridad actual CK, IK y KSI. Después de la transmisión del mensaje elimina los vectores de autenticación enviados y los elementos del contexto de seguridad actual.

   Si no encuentra la información requerida envía un “User Identity Response” indicando que la identidad del usuario no es accesible.

3. Si MSC/VLRn o SGSNn reciben un mensaje conteniendo IMSI, crean una entrada y almacenan la información recibida. Si no ha sido posible identificar al usuario, se inicia un proceso normal de identificación.

6.2.3.4.4 Procedimiento de Resincronización

VLR/SGSN mantiene dos tipos de peticiones de datos de autenticación con HE/AuC, el primer tipo sirve para obtener los vectores de autenticación y el segundo se utiliza en caso de problemas de sincronización.

Al recibir un mensaje "Synchronisation failure" del usuario, VLR/SGSN envía un "Authentication data request" con un indicador de error de sincronización a HE/AuC junto con los parámetros, RAND enviado a MS en la petición de autenticación de usuario previa y $RAND_{MS}$ || AUTS recibido por VLR/SGSN en respuesta a la petición hecha al usuario.

VLR/SGSN no reacciona a indicaciones de problemas de sincronización enviados por MS si no responden a una petición, asimismo tampoco iniciará ninguna petición de autenticación de usuario hasta haber obtenido una respuesta de HE/AuC (o hasta que expire la petición realizada).

HE/AuC al recibir un mensaje de "Authentication data request" con indicador de error de sincronización realiza los siguientes pasos:

1. Obtiene SEQ_{MS} a partir de Conc(SEQ_{MS}) calculando $f5_K$(MAC).[2]
2. Verifica que SEQ_{MS} esté en el rango correcto
3. Si SEQ_{MS} es correcto continua con el paso 6 sino con el paso 4
4. Verifica AUTS
5. Si AUTS es correcto entonces reinicia el valor del contador SEQ_{HE} a SEQ_{MS}
6. Envía un mensaje "Authentication data response" con un nuevo conjunto de vectores de autenticación a VLR/SGSN.

VLR/SGSN al recibir los nuevos vectores de autenticación elimina los anteriores para ese usuario.

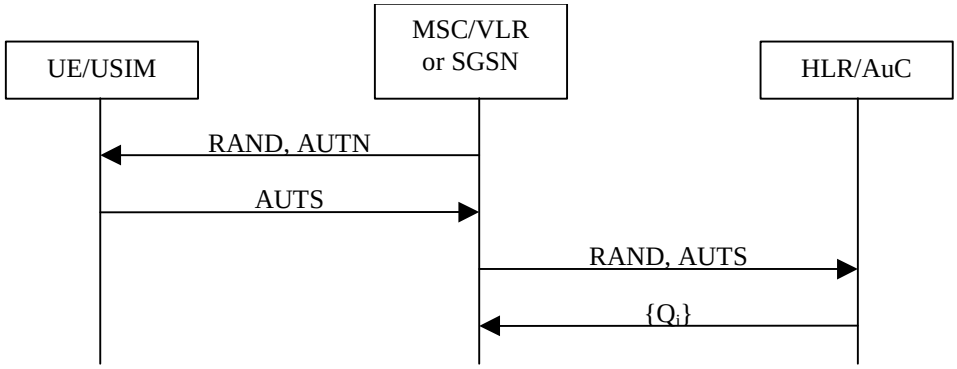


Figura 14. Mecanismo de resincronización

[2] Donde Conc(SEQ_{MS}) es $SEQ_{MS} \oplus f5_K$(MAC)

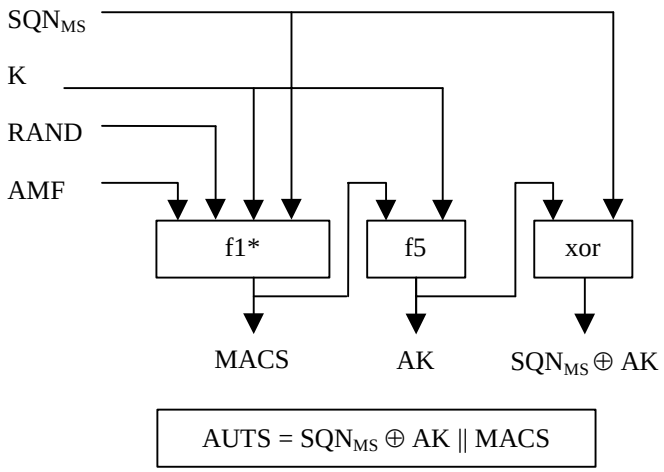


Figura 15. Construcción de AUTS

6.2.3.5 Notificación de errores de autenticación de SGSN / VLR a HLR

La finalidad de dicho mecanismo es notificar a HLR los errores producidos durante el proceso de autenticación.

La recepción de un mensaje de error puede inducir a HLR a cancelar la ubicación de un usuario.

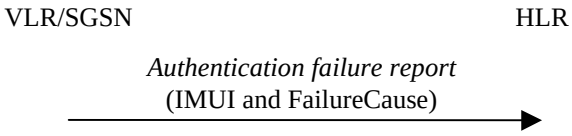


Figura 16. Notificación de error de autenticación

6.2.3.6 Autenticación Local y establecimiento de conexión

La autenticación local se obtiene a partir de la aplicación de la funcionalidad de integridad.

El proceso de autenticación y establecimiento de clave se lanzan en el proceso de autenticación descrito en el apartado anterior. Este proceso puede iniciarse una vez que VLR / SGSN conocen la identidad del usuario móvil. Las claves IK y CK se almacenan en VLR / SGSN y se transfieren a RNC cuando es necesario. Las claves del dominio CS se almacenan en el USIM y se actualizan en la siguiente autenticación para ese dominio. Las claves del dominio PS también se almacenan en el USIM y se actualizan para la siguiente autenticación del dominio PS.

Si u n proceso de autenticación tiene lugar durante una conexión (modo PS o CS), la nueva clave de cifrado y de integridad se usará en ambos, RNC y UE, como parte de la negociación del modo de seguridad que sigue al proceso de autenticación.

Cuando MS desea establecer una conexión con la red, debe indicar a la red en los datos sobre clase de MS / USIM y los algoritmos de cifrado e integridad que soporta. Esta información puede estar protegida por medio de la función de integridad.

La red comparará sus capacidades y preferencias de integridad así como los requerimientos de suscripción del MS, a partir de estos datos actuará según las siguientes reglas:

1. Si el MS y la red no tiene versiones de UIA comunes, la conexión finalizará
2. Si existe al menos una versión de UIA común, la red seleccionará una de ellas para aplicar a la conexión
3. Si el MS y la red no tiene versiones de UIA comunes y la red puede utilizar una conexión no protegida, se usará este modo.

La red comparará sus capacidades y preferencias de cifrado así como los requerimientos de suscripción del MS, a partir de estos datos actuará según las siguientes reglas:

1. Si el MS y la red no tiene versiones de UEA comunes ni está preparada para usar una conexión no cifrada, la conexión se finalizará
2. Si existe al menos una versión de UEA común, la red seleccionará una de ellas para aplicar a la conexión
3. Si el MS y la red no tiene versiones de UEA comunes y la red puede utilizar una conexión no protegida, se usará este modo.

Debido a la separación de gestión de movilidad para servicios PS y CS, un dominio de CN puede, independientemente del otro, establecer una conexión con un MS. El cambio de los algoritmos de cifrado y de integridad en el establecimiento de una segunda conexión MS-CN no está permitido. Las preferencias y requerimientos especiales para el modo de integridad y cifrado deben ser iguales para ambos dominios.

6.2.3.6.1 Tiempo de vida de clave de cifrado y clave de integridad

La proceso de autenticación y acuerdo de claves que genera claves de cifrado / integridad no es obligatorio en el establecimiento, por ello existe un mecanismo, basado en un contador, que delimita el número máximo de veces que puede ser utilizada una clave.

6.2.3.6.2 Identificación de clave de cifrado y clave de integridad

La identificación de las claves se realiza mediante el Identificador de Conjunto de Claves (KSI). KSI es un número asociado con las claves de integridad y cifrado derivadas en el proceso de autenticación y la red lo envía junto con el mensaje “Authentication request”. El USIM al recibirlo almacena un KSI / CK_{SN} para el dominio PS y un KSI / CK_{SN} para el dominio CS.

La finalidad de KSI es permitir a la red identificar las claves de integridad y cifrado sin necesidad de lanzar un proceso de autenticación. Esto permite la reutilización de las claves en los siguientes establecimientos de conexión.

6.2.3.6.3 Procedimiento de Inicio del Modo de seguridad

En este apartado se describe un procedimiento común para el inicio/establecimiento de la protección por cifrado e integridad. Es obligatorio comenzar la protección de integridad de mensajes de señalización utilizando este procedimiento para cada nuevo establecimiento de conexión entre MS y VLR/SGSN, con tres excepciones:

1. La finalidad del establecimiento de la conexión y el resultado de la misma es el registro periódico de la ubicación.
2. No existe señalización alguna entre MS-VLR (o MS-SGSN) después del mensaje de señalizaciónL3 inicial
3. Si el único mensaje de señalización después del mensaje de señalización L3 inicial, aparte de petición de identidad de usuario y autenticación, es un mensaje de señalización rechazada y la liberación de la conexión.

Los únicos procesos entre MS y VLR/SGSN permitidos entre la petición inicial de conexión y antes del establecimiento del modo de seguridad son:

1. Identificación por identidad permanente
2. Autenticación y acuerdo de claves

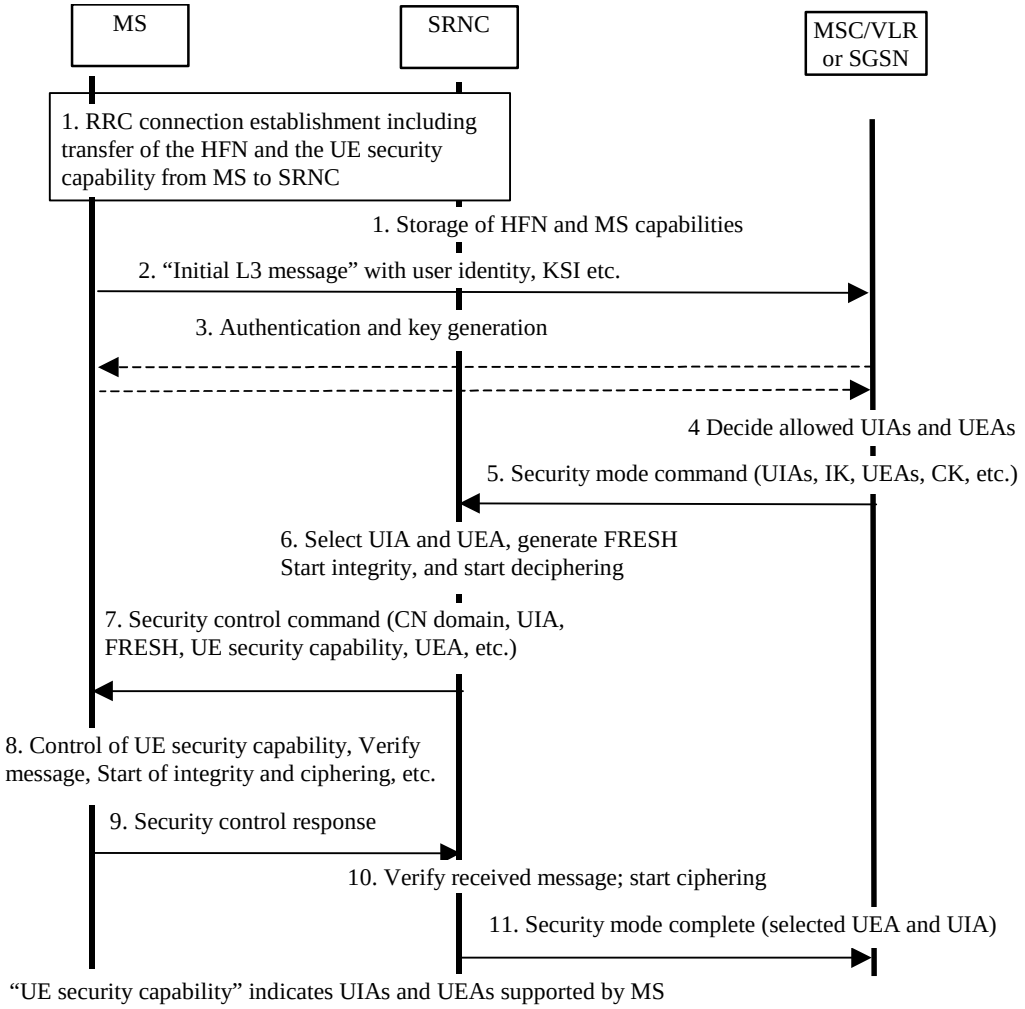


Figura 17. Autenticación local e inicio conexión

1. El establecimiento de la conexión RRC incluye la transferencia de características de seguridad de UE y el número de hipermarco, valor del parámetro COUNT, a utilizar como parte de uno de los parámetros para el algoritmo de integridad y de cifrado.

2. MS envía el mensaje inicial de L, por ejemplo una petición de actualización de ubicación, petición de servicio CM, petición de actualización de área de direccionamiento, etc., al dominio pertinente.

3. Puede lanzarse el proceso de autenticación y generación de nuevas claves de seguridad.

4. El nodo CN determina los UIAs y UEAs permitidos.

5. CN inicia la funcionalidad de integridad (y posiblemente confidencialidad) enviando el mensaje de RANAP "Security Mode Command" a SRNC.

6. SRNC decide los algoritmos a utilizar, seleccionándolos de la lista de algoritmos permitidos. SRNC genera un número aleatorio FRESH e inicia el proceso descendente de integridad. En el caso de no soportar ningún UIA de la lista envía un mensaje " Security Mode Reject" a CN.

7. SRNC genera el mensaje "Security control command" de RRC indicando el dominio de la IK a usar. Antes de enviar el mensaje calcula MAC-I, MAC para integridad, y lo añade al mensaje.

8. MS verifica las capacidades de UE recibidas, comparándolas con las enviadas al inicio del proceso. Calcula XMAC-I utilizando el UIA indicado y lo compara con el valor de MAC-I recibido. También almacena COUNT-I y FRESH.

9. Si todos los controles son correctos, MS interpreta el mensaje recibido y genera un MAC-I para el mensaje. Si algún control no ha sido correcto se envía "Security Control Reject".

10. Al recibir la respuesta de MS, el SRNC calcula XMAC-I del mensaje y lo compara con el MAC-I recibido.

11. Para finalizar el proceso SRNC envía a CN el mensaje de RANAP "Security Mode Complete".

6.2.3.6.4 Procedimiento de Señalización para autenticación local periódica

RNC utiliza este proceso para ejecutar de forma periódica el procedimiento de autenticación local. También lo usan RNC y UE para la comprobación periódica del volumen de información enviado por la conexión RRC.

Todos los mensajes incluidos en este mecanismo están protegidos por integridad.

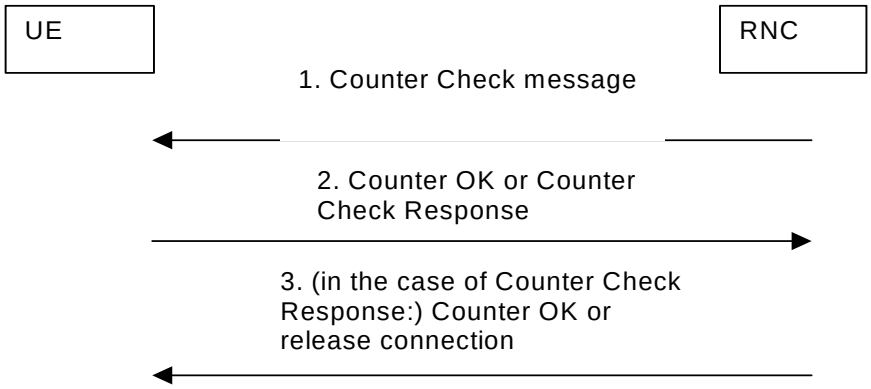


Figura 18. Procedimiento de autenticación local periódica de RNC

1. RNC envía un mensaje conteniendo las partes más significativas de los valores de los contadores para cada identificador de canal lógico de radio activo.

2. Los valores de los contadores son verificados por UE y si se consideran correctos, envía el mensaje “Counter OK”, si no es así envía un “Counter Check Response”.

3. Si el SRNC recibe un “Counter OK”, el proceso acaba. Si recibe un “Counter Check Response” compara los valores de MS y los suyos, si son iguales o la diferencia es aceptable, se finaliza el proceso enviando a MS un “Counter OK”. Si las diferencias no están dentro del margen permitido, se elimina la conexión.

6.2.3.7 Integridad de conexión de acceso

Después del establecimiento de una conexión RRC y de la ejecución del proceso de inicialización del modo de seguridad, todos los mensajes de señalización de control, por ejemplo RRC, MM, CM, GMM , a enviar entre MS y la red deben ser protegidos por integridad.

La integridad se aplicará a nivel RRC y consistirá en la generación de un MAC por mensaje.

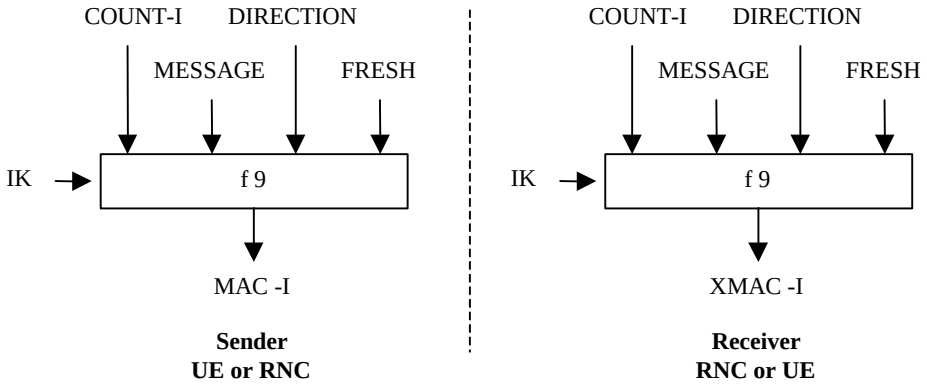


Figura 19. Generación de MAC-I (XMAC-I) de un mensaje de señalización

Los parámetros de entrada para el algoritmo son IK, el número de secuencia de integridad (COUNT-I), un número aleatorio generado por la red (FRESH), el bit de dirección (DIRECTION) y el mensaje de señalización (MESSAGE). A partir de esta información el usuario calcula el MAC asociado al mensaje con la función f9. Una vez calculado el MAC se añade al mensaje y se envía por la conexión de acceso a radio.

El receptor calcula XMAC-I sobre el mensaje recibido y verifica el resultado comparándolo con el MAC-I del mensaje.

Existe un valor COUNT-I por canal de señalización lógico. El parámetro FRESH tiene un valor por usuario y el identificador de dirección, DIRECTION, se utiliza para evitar que el algoritmo

de cálculo de MAC pueda utilizar los mismos parámetros para los mensajes descendentes y ascendentes.

Un detalle a tener en cuenta, es que los servicios de datos de señalización ofrecidos para ambos dominios se envían sobre canales de señalización lógicos comunes y éstos están protegidos por integridad con la clave IK del dominio de servicio para el cual ha tenido lugar la negociación de modo de seguridad más reciente.

Los valores definidos para UIA son:

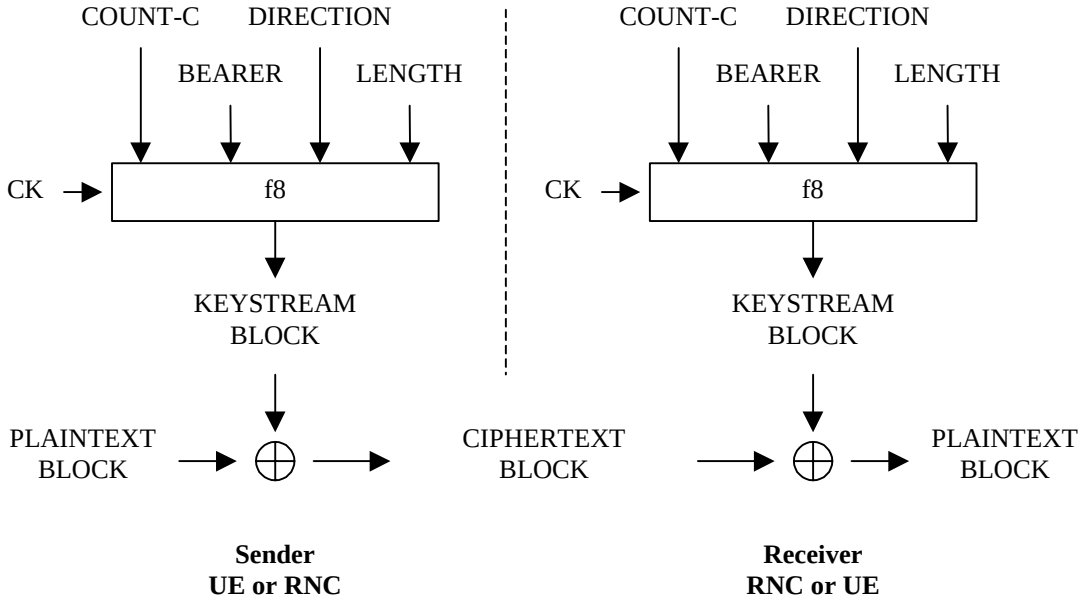
0 0 0 1	UIA1, Kasumi
x x x x	No definido, donde x x x x es cualquier codificación no utilizada con anterioridad

6.2.3.8 Confidencialidad de conexión de acceso

Los datos de usuario y alguna información de señalización necesitan protección de confidencialidad. La función de confidencialidad se aplica sobre canales dedicados entre UE y RNC y se hace utilizando la identidad temporal de usuario.

La función de cifrado se aplica en el subnivel de RLC o en el de MAC.

En la siguiente figura se observa el uso del algoritmo de cifrado f8.



Los parámetros de entrada al algoritmo son la clave de cifrado CK, un contador (COUNT-C) variable en el tiempo, el identificador de canal lógico (BEARER), la dirección de transmisión (DIRECTION) y la longitud del flujo requerida (LENGTH).

Los servicios de datos de señalización ofrecidos para ambos dominios se envían sobre canales de señalización lógicos comunes y éstos están protegidos por integridad con la clave CK del dominio de servicio para el cual ha tenido lugar la negociación de modo de seguridad más reciente.

Los valores definidos para UEA son:

0 0 0 0	No se utiliza encriptación
0 0 0 1	UEA1, Kasumi
x x x x	No definido, donde x x x x es cualquier codificación no utilizada con anterioridad

6.2.3.9 Encriptación Total de Red

Este mecanismo es una extensión del mecanismo de encriptación que ofrece un modo de transmisión protegido para canales de tráfico de usuario a través de toda la red. Este mecanismo se realiza utilizando cifrado de flujo sincronizado.

Para satisfacer los requerimientos de intercepción por ley es necesario poder desencriptar mensaje de tráfico encriptado extremo a extremo en CN para ofrecer acceso a datos de usuario no cifrados.

Un posible esquema de gestión de claves se muestra en la siguiente figura.

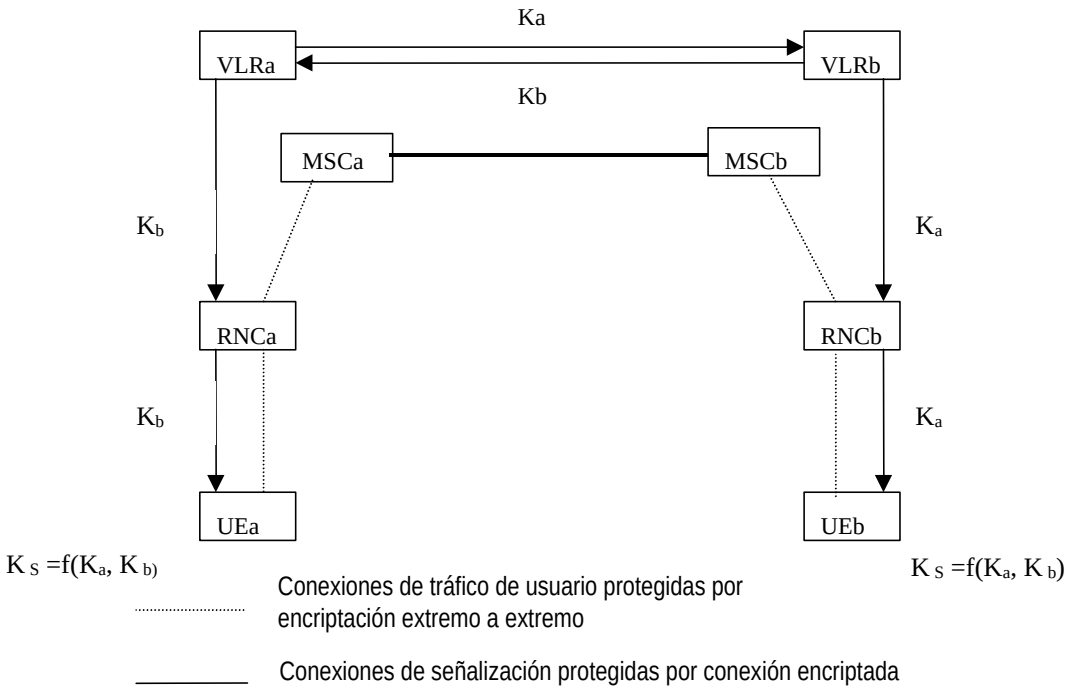


Figura 20. Gestión de claves para encriptación total de red

7Estado del Arte

7.1 Introducción

En esta sección se describe el estado del arte de los sistemas de telefonía móvil con respecto al tema de seguridad. El apartado “Evolución de GSM,GPRS hacia UMTS”, realiza un estudio de la seguridad en los sistemas actuales, GSM (2G) y GPRS (2’5G), y analiza la especificación planteada para UMTS con respecto a la de los sistemas de segunda generación.

7.2 Evolución de GSM / GPRS hacia UMTS

En este apartado se describen los puntos que marcarán el desarrollo de los nuevos sistemas de tercera generación (3G), haciendo hincapié en los aspectos relacionados con la seguridad.

7.2.1 GSM

Las funciones / servicios de seguridad básicos de GSM son:

- Confidencialidad de la identidad del suscriptor
- Autenticación de la identidad del suscriptor
- Confidencialidad de datos, incluyendo elementos de información de señalización, datos de usuario y datos de conexiones físicas

7.2.1.1 Confidencialidad de la identidad del suscriptor

El objetivo de esta función es evitar la posibilidad de que un intruso pueda averiguar que suscriptor está utilizando un servicio de radio y pueda localizar al usuario GSM.

Para conseguir estos objetivos la Identidad del Suscriptor Móvil Internacional (IMSI) se transmitirá sólo en caso de necesidad, utilizándose, si es posible, una identidad temporal (TMSI). Esta identidad temporal es un número local, que sólo tiene sentido dentro del área de localización y debe ir acompañado del Identificador del Área de Localización (LAI). Asimismo, siempre que se pueda se transmitirán los elementos de información de señalización cifrados.

La red, por ejemplo VLR, gestiona las bases de datos necesarias para mantener la relación entre TMSI e IMSI. Cuando se recibe un TMSI en una LAI que no se corresponde con el VLR actual, VLR requiere la transmisión de IMSI al VLR al que corresponde el identificador del área de localización o sino a MS. Cada vez que se ejecuta un procedimiento de actualización de localización, es necesario establecer un nuevo TMSI que implicará la eliminación del anterior.

7.2.1.2 Autenticación de la identidad del Suscriptor

El proceso de autenticación de la identidad del suscriptor, se realiza después de que la identidad del usuario GSM (TMSI / IMSI) sea conocida por la red y antes de la encriptación del canal. Este procedimiento se utiliza también para fijar la clave de cifrado.

La autenticación se compone de dos procesos diferenciados, el procedimiento de autenticación y la gestión de claves dentro del subsistema fijo.

7.2.1.2.1 Procedimiento de autenticación

El procedimiento de autenticación sigue los pasos descritos a continuación:

- El subsistema fijo transmite un número aleatorio RAND hacia MS
- MS calcula la firma de RAND, SRES, utilizando el algoritmo A3 y Ki (o clave de Autenticación de Suscriptor Individual)
- MS transmite SRES a la parte fija del subsistema
- La parte fija de GSM verifica SRES

Ki junto con IMSI, se graban en MS en el momento de la suscripción. Por parte de la red, Ki se almacena en el Centro de Autenticación (AuC). Esta entidad, puede estar físicamente integrada en otra entidad como, por ejemplo, el Registro de Ubicación Particular (HLR).

7.2.1.2.1.1 Procedimiento General

Para cada MS y, en el momento en que son necesarias, BSS / MSC / VLR realizan peticiones de información de seguridad a HLR / AuC. Estas peticiones tienen como resultado la generación de cadenas de parejas de valores correspondientes a RAND y SRES. Esta información se almacena en VLR y en el momento de realizarse el proceso de autenticación VLR selecciona un valor de RAND y compara la respuesta de la estación móvil con el valor asociado al número aleatorio enviado SRES. Si ambos valores coinciden se acepta la autenticación, si no es así, el proceso se descarta.

7.2.1.3 Confidencialidad

La confidencialidad de la identidad de usuario implica la transmisión de TMSI en modo protegido, siempre que sea posible. La confidencialidad de los datos de usuario no orientados a la conexión, implica la protección de aquellas partes del mensaje perteneciente al nivel 4 de la torre OSI o superiores. Finalmente, la confidencialidad de información de usuario de conexiones físicas concierne a los datos transmitidos por la interfaz MS-BSS, siendo éste último un servicio no extremo a extremo. Estos requerimientos de confidencialidad se obtienen a través del cifrado.

Los puntos principales de este mecanismo son el método de cifrado, el establecimiento de claves, el inicio del proceso de cifrado / descifrado y la sincronización entre las entidades involucradas.

7.2.1.3.1 Método de cifrado

El mensaje transmitido a nivel 1 se cifra bit a bit o por cadenas de cifrado. Por ejemplo, el flujo de datos en la comunicación de radio se obtiene por la OR binaria bit a bit de la información de usuario y de una cadena de cifrado. Esta cadena de cifrado esta generada por un algoritmo A5 utilizando una clave de cifrado denominada Kc.

El mecanismo de descifrado es el mismo que el utilizado para el cifrado de la información.

7.2.1.3.2 Establecimiento de claves

El establecimiento de claves es el procedimiento que permite que la estación móvil y la red fijen una clave de cifrado, Kc, para utilizar con el algoritmo A5. El proceso se activa con el mecanismo de autenticación y puede ser ejecutado por la red tantas veces como desee el operador, siempre que se conozca la identidad del suscriptor.

La transmisión de Kc se realiza de forma indirecta, derivándose Kc a partir del valor RAND utilizando el algoritmo A8 y la clave de autenticación del suscriptor Ki. El valor de Kc se calcula junto con los valores de SRES, consistiendo la información relativa a seguridad en tres valores: RAND, SRES y Kc.

Kc es válida hasta el siguiente proceso válido de autenticación.

7.2.1.3.2.1 Número de secuencia de clave de cifrado

Cada clave de cifrado tiene un número de secuencia asociado que se almacena tanto en MS como en la red.

7.2.1.3.3 Inicio de los procesos de cifrado / descifrado

MS y BSS coordinan el momento de cifrado / descifrado de forma que BSS envía un mensaje “Start cipher” a MS, éste al recibirlo contesta con un mensaje cifrado dirigido a BSS El proceso de descifrado se inicia en MS según el mismo método.

El inicio de cifrado empieza en BSS cuando éste es capaz de descifrar correctamente un mensaje de MS

7.2.2 GPRS

GPRS utiliza una técnica de modo paquete para transmitir datos de alta y baja velocidad así como, información de señalización de forma eficiente, optimizando el uso de la red y los recursos de radio. Mantiene una estricta separación entre el subsistema de radio y el subsistema de red, lo que permite que el subsistema de red pueda utilizar diferentes tecnologías de acceso a radio sin implicar ningún cambio en la base instalada de MSC. En GPRS se han definido canales de radio de asociación flexible y los recursos de la interfaz de radio se distribuyen de forma dinámica entre servicios de voz y datos, llegando a tasas de hasta 150Kbits por usuario. Soporta aplicaciones basadas en protocolos estándar y se ha definido la interrelación con redes IP y X.25.

GPRS introduce dos nuevos nodos de red respecto al diseño de PLMN de GSM, el Nodo de Soporte GPRS de Servicios (SGSN) al mismo nivel que MSC, gestiona los servicios de localización y ejecuta funciones de seguridad y control de acceso. El segundo nodo incorporado es la Pasarela de GSN (GGSN) que ofrece interrelación con redes de paquetes conmutados externas y está conectada con SGSN a través de una red GPRS-IP. HLR contiene información de suscripción de usuarios GPRS. SMS-GMSC y SMS-IWMSC se actualizan para soportar la transmisión de SMS vía SGSN. Opcionalmente, MSC / VLR puede unirse para proporcionar una

mayor coordinación de servicios y funcionalidades GPRS, no-GPRS y para actualizaciones de localización combinadas GPRS y no-GPRS.

Los datos de usuario se trasmiten de forma transparente entre MS y las redes de datos externas mediante encapsulación y túnel.

La funcionalidad de seguridad en GPRS es idéntica a la funcionalidad de seguridad en GSM. Si bien es SGSN quien ejecuta los procedimientos de autenticación y cifrado, éstos se basan en los mismos algoritmos, claves y criterios que los existentes en GSM: El algoritmo de cifrado está optimizado para la transmisión de paquetes de datos.

Como en GSM, las funciones de seguridad ofrecidas son autenticación, confidencialidad de la identidad de usuario (identificación temporal y cifrado) y confidencialidad de datos de usuario (cifrado).

7.2.2.1 Confidencialidad de la Identidad de Usuario

Al igual que en GSM, se utiliza una identidad temporal que para SGSN se denomina Identidad de Suscriptor Móvil Temporal de Paquetes (P-TMSI). Este valor se almacena en SGSN y MS.

En el caso de que SGSN incluya la firma digital de P-TMSI en algún mensaje enviado a MS, este debe hacer lo propio en los siguientes mensajes de actualización de área de direccionamiento o de establecimiento de conexión a fin de que SGSN pueda comprobar ambos valores.

7.2.2.2 Autenticación del Suscriptor

El procedimiento de autenticación es el mismo que el definido para GSM con la diferencia que los procesos se ejecutan desde SGSN. El mecanismo de autenticación de GPRS ofrece autenticación del suscriptor, selección del algoritmo de cifrado y sincronización de cifrado. La información relativa a la seguridad por parte del subsistema de red se almacena en SGSN.

MSC / VLR autentica a MS durante el establecimiento de la conexión CS.

7.2.2.3 Confidencialidad de datos de usuario y de datos de señalización GMM / SM

A diferencia del ámbito de cifrado existente en GSM (un único canal entre BTS y MS), en GPRS el ámbito de cifrado abarca desde SGSN hasta MS. El cifrado se realiza en el nivel de LLC y para las conexiones de radio establecidas MS-BTS de GSM, las PDUs de LLC se transmiten sin cifrar.

Debe realizarse un proceso de selección del algoritmo de cifrado a utilizar con GPRS y para la gestión de claves, se utiliza el procedimiento establecido para Kc en GSM.

7.2.3 UMTS

Los principios de seguridad de UMTS se basan en un desarrollo de los elementos definidos para sistemas de segunda generación (2G), tales como GSM y GPRS.

Los fundamentos de seguridad que se mantienen, con o sin modificaciones, de los sistemas de 2G son:

- Autenticación de los suscriptores para acceder a los servicios,
- Encriptación de la interfaz de radio, de forma que el mecanismo de encriptación sea más "fuerte" que el existente en 2G, (se considera el término fuerte como una combinación entre el diseño del algoritmo de encriptación y la longitud de la clave),
- Confidencialidad de la identidad del usuario en la interfaz de radio, mejorando el nivel de seguridad,
- SIM, como concepto de elemento de hardware y módulo de seguridad independiente del terminal,
- Las características de seguridad del conjunto de aplicaciones del SIM que ofrecen un canal seguro a nivel de aplicación entre el SIM y el servidor de HN. Incremento del número de aplicaciones,
- Elementos de seguridad independientes del usuario. Mejora de la visibilidad de seguridad de forma que el usuario pueda, por ejemplo, saber si está accediendo a redes de menor nivel de seguridad que la red actual,
- Reducción de la dependencia de funcionalidad de seguridad entre HE y SN.

UMTS además, pretende corregir aquellos aspectos de seguridad de los sistemas 2G que han sido reconocidos como débiles o como mejorables. Los elementos más destacados son:

- Posibilidad de atacar al sistema con "un falso BTS",
- Las claves de autenticación y cifrado se transmiten en modo texto entre / dentro de redes,
- El mecanismo de encriptación no cubre completamente el sistema, de forma que los datos de usuario y de señalización se transmiten en modo texto entre las conexiones de microondas. Por ejemplo, en GSM entre BTS y BSC,
- La autenticación de usuario utilizando una clave previamente establecida / generada y la protección contra "robo" del canal, radica en el uso de la encriptación que ofrece autenticación de usuario implícita. No todas las redes utilizan encriptación, lo que ofrece posibilidades de fraude,
- No ofrecen integridad de datos,
- Uso de IMEI, considerado como un tipo de identificación insegura,
- Los sistemas de 2G no ofrecen flexibilidad de actualización o mejora de las funcionalidades de seguridad

Finalmente UMTS ofrecerá nuevas características de seguridad y nuevos servicios de 3G seguros.

7.2.3.1 Seguridad en aplicaciones

Uno de los aspectos de seguridad que UMTS intenta mejorar, es la seguridad en aplicaciones. Ofrecer a los operadores o proveedores, la posibilidad de crear aplicaciones residentes en el USIM, para ello es necesario que el sistema sea capaz de ofrecer el nivel de seguridad seleccionado, por el operador o el proveedor de la aplicación, en la transmisión de mensajes entre la red 3G y la aplicación del USIM.

Las puntos más destacados de la oferta propuesta son:

- ***Autenticación de la entidad de la aplicación***, propiedad que permite que dos aplicaciones sean capaces de corroborar su identidad,
- ***Autenticación del origen de los datos de aplicación***, propiedad que permite a la aplicación receptora verificar el origen de los datos recibidos,
- ***Integridad de los datos de aplicación***, propiedad que permite a la aplicación receptora comprobar que los datos enviados por la aplicación par no han sido modificados,
- ***Detección de reenvío de datos de aplicación***, propiedad por la que una aplicación es capaz de detectar que los datos recibidos no han sido reenviados,
- ***Integridad de la secuencia de datos de aplicación***, propiedad que permite que una aplicación verifique los datos recibidos están en la secuencia correcta,
- ***Comprobante de recepción***, propiedad que permite a la aplicación origen demostrar que la aplicación receptora ha recibido los datos enviados,
- ***Confidencialidad de los datos de aplicación***, propiedad que permite que los datos de la aplicación no sean conocidos por elementos no autorizados.

Todos estos aspectos de seguridad se basan en el conjunto de Herramientas de Aplicación de SIM que ofrece actualmente GSM.

7.2.3.2 Visibilidad

En UMTS se pretende que el usuario disponga de mayor visibilidad de las operaciones de seguridad disponibles. Para ello se ofrecerá:

- ***Indicación de encriptación en la red de acceso***, propiedad que permite al usuario conocer si los datos de usuario están protegidos por confidencialidad en la conexión de red de radio, en concreto cuando se establecen llamadas no cifradas,
- ***Indicación de encriptación completa***, propiedad que permite al usuario conocer si los datos de usuario están protegidos por confidencialidad en todo el camino de comunicación,
- ***Indicación del nivel de seguridad***, propiedad que permite al usuario conocer el nivel de seguridad que ofrece la red visitada, en particular cuando el usuario se mueve a una red con inferior nivel de seguridad (3G $\rightarrow$2G).

7.2.3.3 Otros aspectos de UMTS

Un hecho importante que marca la evolución de UMTS, es la necesidad de garantizar temporalmente la compatibilidad con los sistemas de segunda generación existentes. Esto provoca que en el diseño y desarrollo de UMTS, sobretodo en la primera fase, deban tenerse en cuenta los siguientes puntos:

- UMTS debe soportar una CN basada en una evolución de MSC y de SGSN de 2G,
- Opcionalmente debe disponer de una interfaz Gs evolución de la interfaz Gs de 2G,
- UMTS debe ofrecer compatibilidad con móviles GSM, al menos con los de clase A,
- Debe permitir al operador elegir, para transmitir, entre una CN integrada o con dominios separados para CS y PS,
- Debe permitir configurar MSC/VLR y SGSN separadamente o de forma combinada,
- Debe permitir el uso de varios planos de usuario para nodos CN,
- Con respecto a la movilidad, UMTS debe considerar:
  - La posibilidad de conectar UTRAN a ambos dominios de CN o sólo a uno,
  - Una única conexión RRC debe transportar todos los flujos de usuario/señalización de/hasta UE,
  - Debe ofrecer compatibilidad con las redes GSM desde el punto de vista de navegación y sincronización, para ello:
    1. La identidad común utilizada entre ambos dominios será IMSI,
    2. Se aplicará señalización común de MAP a GSM y a UMTS. Se utilizará, tanto como sea posible, los servicios de MAP definidos para GSM,
    3. Los parámetros y recursos de radio se limitarán a UTRAN.
  - A fin de facilitar la flexibilidad en la gestión de movilidad de UMTS, debería ser posible el uso de mecanismos combinados de actualización para fines de gestión de ubicación y adherencia/abandono de LA y RA, de forma similar a los procesos combinados de GSM y GPRS.
  - Las técnicas de LM/MM utilizadas en UMTS deben minimizar el uso de recursos de radio en UTRA.
  - GPRS permite diferentes redes de acceso a radio, se desea que UMTS (durante su evolución), también lo permita.
  - El soporte de aplicaciones multimedia añade diferentes requerimientos, los más importantes son el ancho de banda relacionado con la tecnología de transporte, en particular la conmutación y transporte de capacidades deben soportar hasta 2Mbits/s, la gestión eficiente de los recursos de red, negociación de todos los atributos para el servicio de canales lógico en el establecimiento de la llamada y renegociación de los mismos durante la llamada, independientemente de si ha sido iniciada por el terminal o por la red, soportar diferentes tipos de tráfico (tasa de bit constante, tasa variable, tasa no definida, tasa disponible).

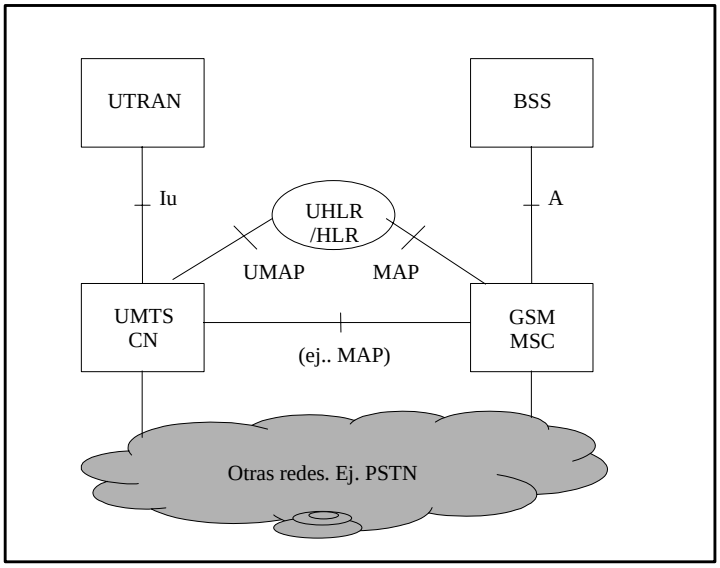


Figura 21. GSM y UMTS

7.2.3.3.1 Movilidad

- El concepto de movilidad definido para UMTS respecto al dominio PSTN/ISDN es idéntico al concepto de movilidad definido para GSM. El dominio de IP presenta algunas diferencias respecto al modelo de GSM, los principales cambios son:

  - El proceso de "Actualización de celda" se mueve del nivel de GMM en GSM al nivel de RRC en UMTS,
  - El proceso de "Actualización de área de direccionamiento" ejecutada en standby en GMM de GSM, se ejecuta a nivel de RRC en UMTS y se corresponde con el procedimiento de "Actualización de URA",
  - En UMTS, en estado PS-IDLE, se introduce un nuevo caso de "Actualización de área de direccionamiento" hacia SGSN,
  - En UMTS, se introduce un nuevo estado PS-CONNECTED y en este estado la movilidad de UE hacia CN se gestiona a través de procedimientos UTRAN-CN no a nivel de MM.
  - Posibilidad de combinar diferentes sistemas de gestión de movilidad. Por ejemplo, el uso de MIP para gestionar la movilidad entre redes de acceso mientras que el nodo SGSN de GSM/GPRS se encarga de la gestión de los datos de autorización del suscriptor, mecanismos de cobro y gestión de claves de encriptación. El proceso de introducción de MIP en CN tiene tres variantes:
    - Variante 1: Representa una configuración mínima para el operador. Se mantiene la estructura GPRS actual con la que se gestiona la movilidad dentro de la PLMN. MIP sólo se utiliza para la movilidad con otros sistemas.

- Variante 2: SGSN y GGSN se pueden ubicar conjuntamente, sin ninguna alteración de las interfaces. Permitiendo, para obtener un direccionamiento más eficiente, la posibilidad de que MS modifique GGSN/FA una vez finalizada la transferencia de datos.
- Variante 3: En esta fase, MIP gestiona la movilidad del sistema, incluyendo la sincronización entre GGSNs o IGSNs. Opcionalmente, pueden mantenerse las interfaces de Gn y Gp para aquellos clientes que no soporten MIP.

7.2.3.3.2 Punto de referencia Iu

Inicialmente UMTS se basará en las redes GSM/GPRS. Debido a las diferencias entre los dominios, el punto de referencia Iu se ejecutará mediante dos instancias Iu, una para cada dominio. Este hecho permitirá que cada uno de los dominios evolucione independientemente del otro.

El protocolo de RANAP, protocolo de señalización que controlará la interfaz de Iu, tendrá como base el uso de BSSMAP y BSSGP/GTP.

8Soluciones

8.1 Modelos de Arquitectura de Seguridad

8.1.1 Introducción

UMTS aporta servicios de seguridad que cubren y amplían los servicios ofrecidos por GSM/GPRS. Las aportaciones principales de UMTS en temas de seguridad son:

- Seguridad extremo a extremo
- Integridad de datos
- Flexibilidad y Adaptabilidad

Tomando como base la arquitectura definida para GSM/GPRS se han creado dos modelos de arquitectura de seguridad que ofrecen todos los servicios de seguridad de UMTS a partir de los estándares actuales. El primero de los modelos (denominado “Modelo de arquitectura WTLS sobre IP”), permite la aplicación todos los servicios de seguridad (encriptación, integridad, intercambio de claves, etc.) que ofrece UMTS con la tecnología actual, incorporando los mínimos cambios. Este modelo se basa en la aplicación de tecnología WAP sobre IP y requiere la implantación de tecnología WAP en el terminal. El segundo de los modelos(recibe el nombre de “Modelo de arquitectura IP”), se presenta como arquitectura óptima no aplicable a corto plazo. Al igual que el primer modelo, posibilita la aplicación de todos los servicios de seguridad de UMTS con la tecnología actual pero que además ofrece una arquitectura mínima, entendiendo por arquitectura mínima aquella que dispone de menos niveles de protocolos. El Modelo de Arquitectura IP requiere cambios en el módulo de SGSN y GGSN de forma que pasen a formar un único módulo de gestión de conexiones IP, esta arquitectura optimiza la transmisión de datos ya que incorpora una mínima sobrecarga en los mensajes y se basa en la utilización de IPSec y movilidad IP.

8.1.1.1 Origen de los modelos de arquitectura propuestos

En las figuras presentadas a continuación podemos observar la arquitectura de los planos de usuario y de control para GPRS. Los modelos “WTLS sobre IP” e “IP” han sido desarrollados a partir de esta arquitectura estándar.

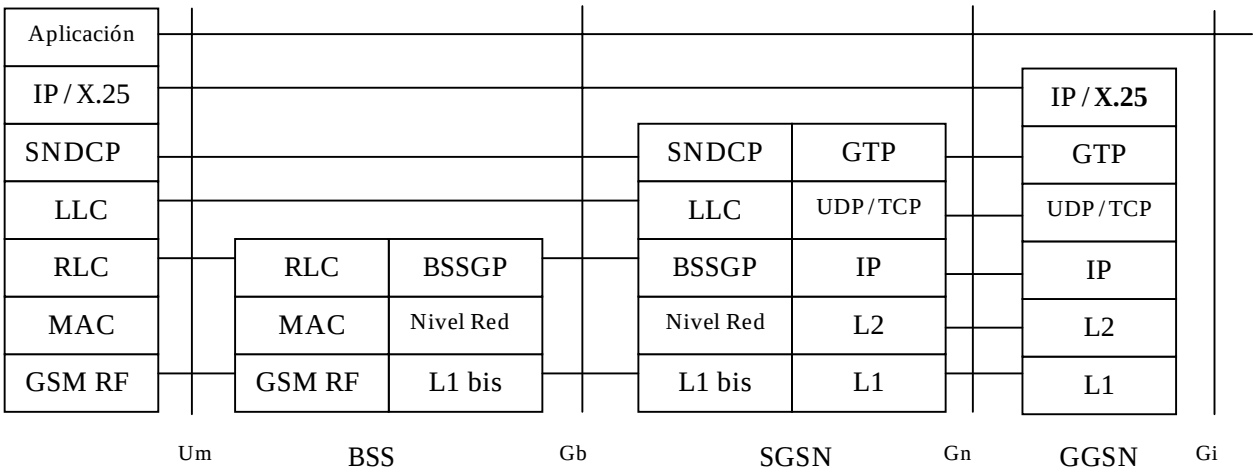


Figura 22. GPRS. Plano de Usuario

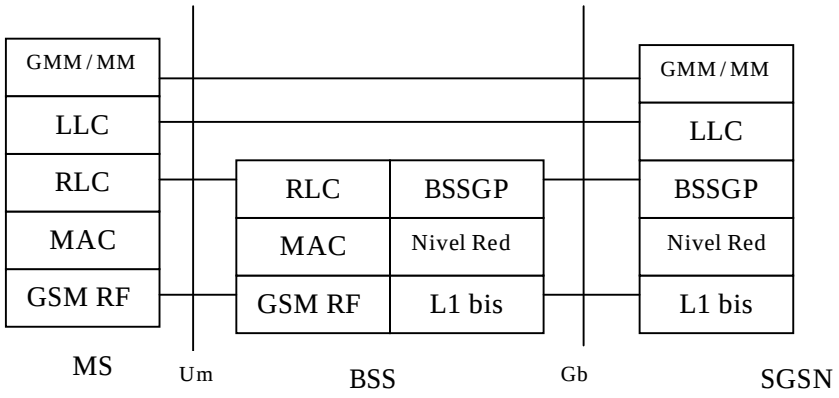


Figura 23. GPRS. Plano de Control

Los estándares de segunda generación no consideran el uso de Movilidad IP para gestionar la movilidad, esta idea aparece en los documentos de referencia de UMTS. El anexo “Movilidad IP” (5) ofrece una descripción general del mecanismo de MIP.

8.1.1.2 Requerimientos de los modelos de arquitectura propuestos

En el diseño de los modelos de arquitectura se ha exigido una serie de requerimientos, estos se basan en la utilización de los sistemas estándares presentes en el mercado y en la independencia de dispositivos de forma que los diferentes componentes puedan evolucionar por separado. Los requerimientos considerados son:

Uso de los elementos actuales
Es indispensable partir de la base del mercado actual, de forma que el modelo implique los mínimos cambios en los elementos de tecnología móvil existentes hoy en día.

Aplicación de tecnología disponible en el mercado
Se considerarán protocolos existentes en el mercado o protocolos disponibles en breve.

Mínimos cambios
La incorporación de los modelos de arquitectura propuestos, debe implicar modificaciones reducidas en tiempo y complejidad.

Seguridad de tercera generación
La arquitectura considerada debe ofrecer todos los servicios de seguridad que ofrece UMTS y además debe proporcionar el mismo nivel de seguridad o superior.

Fácil incorporación
La "migración" entre sistemas actuales GSM/GPRS a los sistemas propuestos debe poder ser sencilla y rápida.

Tecnología estándar
Sólo se considerarán protocolos/tecnologías estándar.

Tecnología de amplia difusión
Los protocolos a tener en cuenta deben estar aceptados por el mercado.

Independencia de elementos
Los elementos considerados como parte de la arquitectura, entendiendo por elementos tanto los protocolos como los módulos del sistema, deben ser independientes. Así cada uno de los elementos puede evolucionar a ritmo diferente sin que por ello se vea comprometida la funcionalidad ofrecida al sistema.

Interoperabilidad
El modelo propuesto debe permitir diferentes tecnologías de acceso a red, independencia de dispositivos, conexión con cualquier tipo de red, como mínimo, en el mismo grado que lo permite GSM/GPRS.

8.1.2 Modelo de Arquitectura: WTLS sobre IP

En este modelo se propone el uso de tecnología WAP y en concreto el uso del nivel de seguridad WTLS sobre IP, para alcanzar los objetivos de seguridad citados con anterioridad.

La tecnología WAP, a nivel de seguridad, proporciona autenticación, integridad, confidencialidad, protección contra negación de servicio y además seguridad extremo a extremo entre dos elementos con tecnología WAP, es decir, entre el terminal móvil y el servidor WAP. El problema radica en el momento en que se desea acceder a objetos ubicados en un servidor de Internet. En este caso sólo podemos confirmar el nivel de seguridad extremo a extremo si:

- El servidor de Internet dispone de tecnología WAP
- El servidor WAP está ubicado físicamente en el mismo lugar seguro que el servidor de Internet

dado que nunca se puede certificar esta situación para todos los posibles servidores de Internet, no es posible garantizar la seguridad extremo a extremo aplicando únicamente los mecanismos de seguridad que ofrece WAP, por ello es necesario además, un mecanismo diferente que nos proporcione el nivel de seguridad requerido, este mecanismo es Movilidad IP. La utilización de MIP nos permite el acceso a cualquier servidor de Internet de manera segura, confirmándose así la seguridad extremo a extremo en todo nuestro sistema.

Evidentemente este modelo plantea el inconveniente de sobrecarga del mensaje al incluir, cuando es necesario, información relativa a los protocolos de WAP y movilidad IP. Considerando que WTLS es un protocolo modular que permite la selección de los mecanismos a aplicar dependiendo de los requerimientos de la aplicación en curso y de las características de la red utilizada, puede limitarse el uso de aquellos servicios que se consideren prescindibles.

La Movilidad IP (MIP) es independiente del sistema de acceso y permite al usuario navegar de un entorno a otro, entre sistemas fijos y móviles tanto de redes públicas como privadas, es decir, admite movilidad entre sistemas heterogéneos. En este primer modelo, se mantendrá la estructura de GPRS utilizando la gestión de movilidad “clásica” para el direccionamiento dentro de la PLMN, mientras que MIP permitirá al usuario acceder a otros sistemas sin perder la sesión.

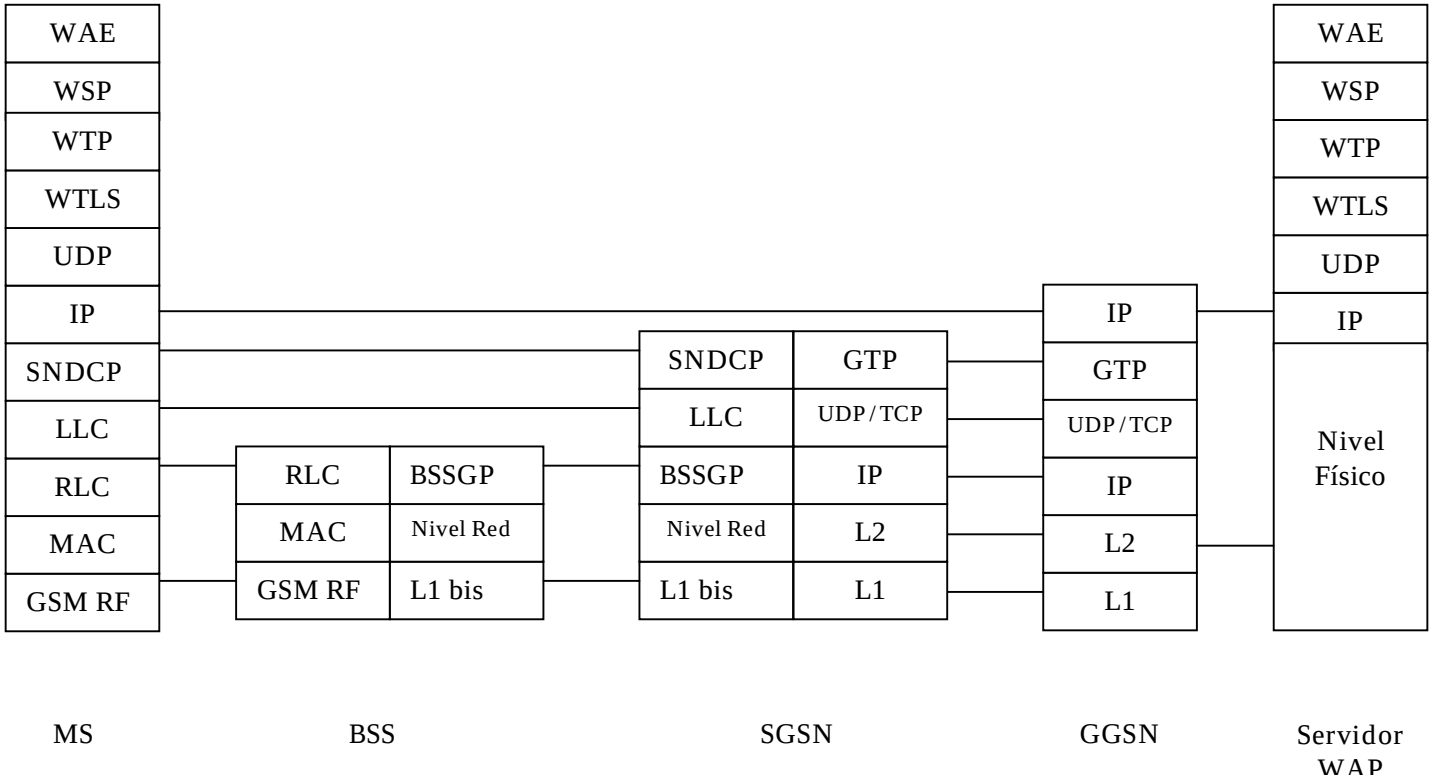


Figura 24. Modelo de Arquitectura de Seguridad WTLS sobre IP.Plano de Usuario

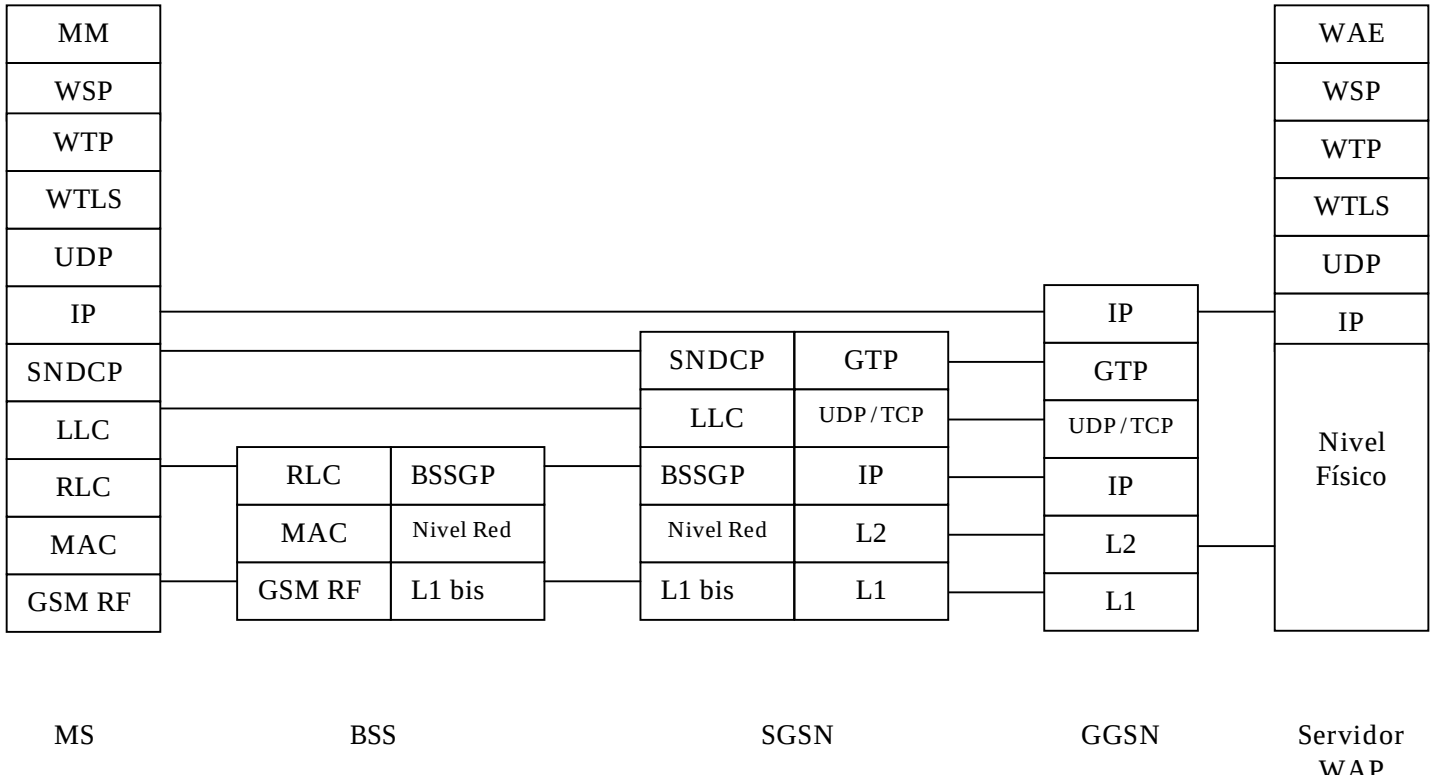


Figura 25. Modelo de Arquitectura de Seguridad WTLS sobre IP.Plano de Control

Los requisitos de esta propuesta son:

- ME debe ser capaz de encontrar un FA. Se asume que FA está ubicado en GGSN y que no todos los nodos GGSN tienen que disponer de un FA, de hecho dentro de una PLMN un único FA daría servicio para MIP aunque es recomendable por capacidad y eficiencia tener más de un FA implementado. El terminal debe establecer un contexto PDP con el GGSN que tenga funcionalidad FA, para ello existen dos posibles implementaciones, la primera consistiría en definir un nuevo tipo de PDP y la segunda definir un Nombre de Punto de Acceso (APN) que permita la conexión con el GGSN-FA.
- Durante el establecimiento del contexto PDP, ME debe ser informado de los parámetros de red del FA, por ejemplo care-of-address.

Dependiendo de las características de la red visitada, se identifican dos esquemas de navegación, movilidad GPRS y movilidad MIP. La movilidad GPRS implica la navegación a través de la interfaz Gp y el uso de GGSN en la red particular, esto es necesario en aquellas redes que no ofrecen la funcionalidad FA. Si la red visitada dispone de GGSN/FA y en la red particular también existe esta funcionalidad, es independiente el FA a utilizar. En la siguiente figura puede observarse una red con la propuesta de movilidad comentada.

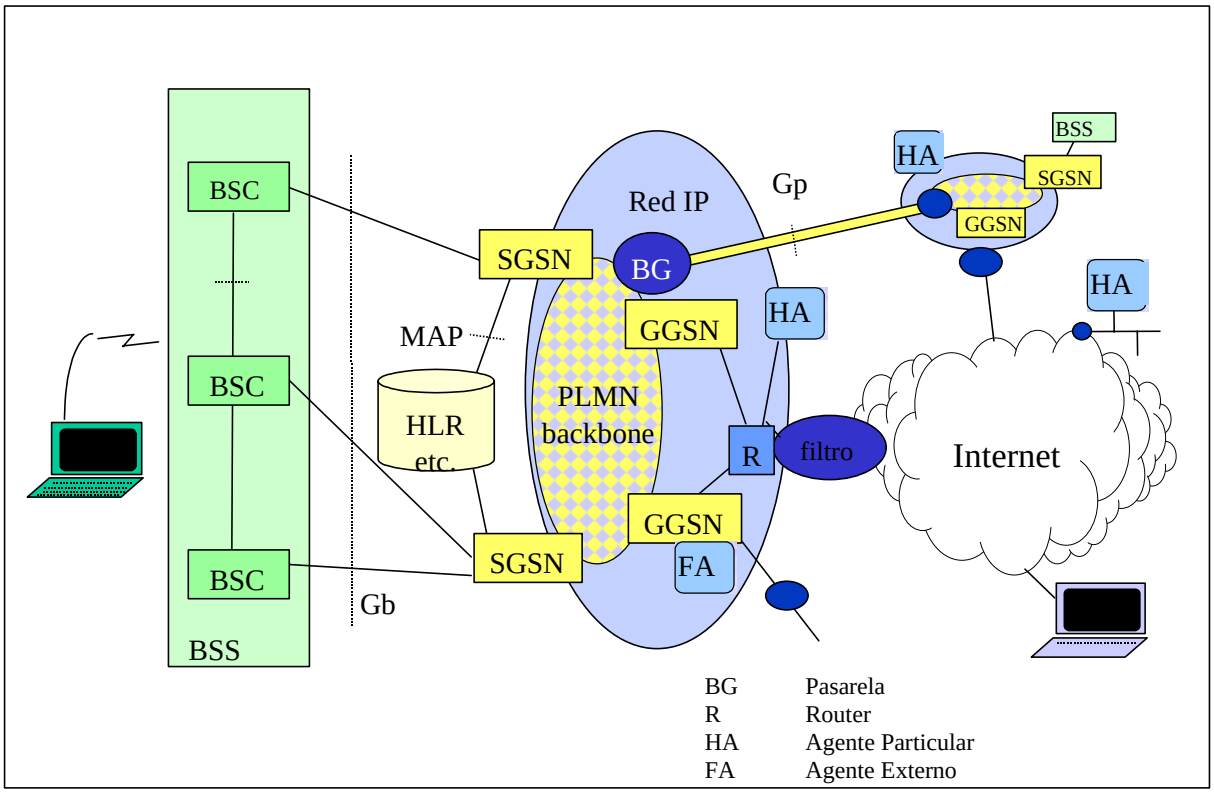


Figura 26. MM de GPRS en y entre PLMNs y MIP entre diferentes tipos de sistemas y opcionalmente entre PLMNs de GPRS.

8.1.3 Modelo de Arquitectura IP

Este modelo de arquitectura de seguridad toma como referencia IPSec y Movilidad IP, así el modelo propuesto sería:

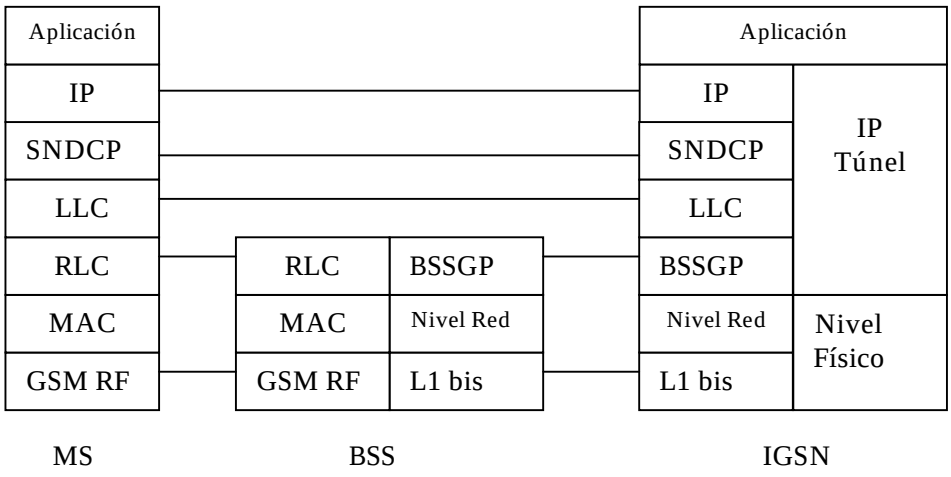


Figura 27. Modelo de Arquitectura de Seguridad IP. Plano de Usuario

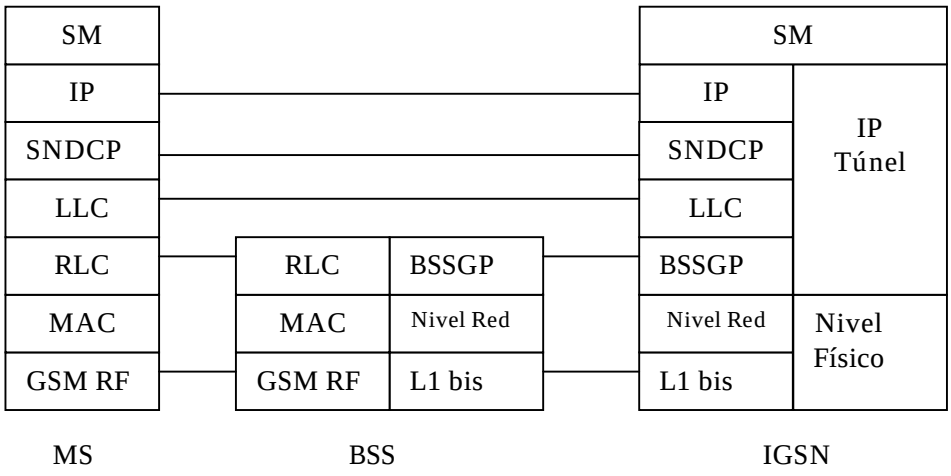


Figura 28. Modelo de Arquitectura de Seguridad IP. Plano de Control

Este modelo utiliza MIP para la gestión de movilidad entre PLMNs y también para la gestión de movilidad entre sistemas. La funcionalidad de SGSN y GGSN se combina en un único nodo, Nodo de Soporte GPRS de Internet (IGSN), añadiendo la funcionalidad necesaria para la gestión de Movilidad IP entre IGSNs. Para permitir la compatibilidad con redes GPRS que no disponen de esta funcionalidad se debe permitir el uso de IGSN como SGSN durante un cierto período de transición. La funcionalidad básica de IGSN sería:

- Gestión de movilidad GPRS entre BSSs, es decir, la funcionalidad que ofrece SGSN actualmente.
- Soportar el protocolo de Parte de Aplicación Móvil (MAP) para comunicarse con los nodos específicos de GPRS como HLR, EIR, SMS y la funcionalidad de gestión de información de/para estos nodos como puede ser autenticación y gestión de claves para la encriptación de la interfaz de radio.
- Interacción con HLR y AAA para la gestión de información de suscripción.
- Recolección de información de tasas.
- Soportar Movilidad IP.

Debe considerarse que la Movilidad IP sólo gestiona aquellos eventos que tienen como resultado que el terminal entre en el dominio de un agente de movilidad diferente del actual.

8.1.3.1 Movilidad IP con IPv4/IPv6

Las diferencias principales en el uso de MIP con IPv4 o con IPv6 son :

- El uso de MIPv4 permite el uso de un FA para direccionar el tráfico necesitando una care-of-address para múltiples MS, o el uso de COAs. De todas maneras debido a los problemas de direcciones en IPv4 se recomienda siempre el uso de un agente externo. Movilidad IP con IPv6 sólo permite COAs.
- La optimización del mecanismo de direccionamiento MIPv6 es parte integral de su especificación, no así en MIPv4 donde esta optimización es un addendum.
- En MIPv4 la optimización de direccionamiento requiere que el tráfico sea enviado por túnel entre el servidor y MS, mientras que en MIPv6 se produce mediante el anexamiento de una cabecera de direccionamiento al mensaje IP.
- En MIPv4 en el caso de optimización de direccionamiento HA se ve involucrado. En MIPv6, MS puede iniciar el proceso de optimización al servidor correspondiente sin necesidad de incluir a HA en el proceso, lo que provoca un procedimiento más rápido y eficiente.
- La comunicación de mensajes específicos de MIP hacia FA, HA y el host correspondiente (en el caso de optimización de direccionamiento) es obligatoria en MIPv4. En MIPv6 los mensajes de MIP pueden transmitirse conjuntamente con mensajes de datos.
- MIPv4 requiere el uso de túneles de inversión para evitar problemas de filtro de mensajes entrantes debido a que los paquetes se envían con la dirección particular como origen. En MIPv6 no se producen problemas de filtro de paquetes entrantes porque puede utilizarse como dirección origen la COA asignada.
- MIPv6 utiliza como protocolo de seguridad IPSec mientras que MIPv4 utiliza sus propios mecanismos de seguridad.

8.1.3.2 Seguridad en Movilidad IP

En el caso de MIPv4 se requiere una clave compartida entre MS y HA que se utilizará al cambiar de HA. También es requisito una clave compartida entre agentes de movilidad, por ejemplo HA y FA, para asegurar el intercambio de mensajes de control de MIP dado que HA y FA pueden pertenecer a dominios de seguridad diferentes. En conclusión, un operador GPRS que desee ofrecer navegación en su red de acceso hacia su red particular o en su intranet corporativa, necesita dos claves compartidas.

Cuando se trata de MIPv6 la diferencia principal es la ausencia de FA, de forma que MIPv6 sólo requiere asociaciones de seguridad de ME a HAs y sus nodos correspondientes.

Al ofrecer un servicio de acceso a una red de datos, existen dos formas de autenticar, autorizar y gravar. Una de las maneras es utilizando la información residente en HLR y modificando la información de los registros de tasas, como normalmente se hace en GSM, y la segunda es reutilizando los protocolos de AAA utilizados en las redes de datos, por ejemplo RADIUS.

MIPv4 utiliza los protocolos AAA de redes de datos y usa los procedimientos de navegación vía las extensiones del Identificador de Acceso de Redes, NAI. Los mecanismos para IPv6 todavía no se han presentado pero puede esperar que sean similares a los ofrecidos por MIPv4.

8.1.3.2.1 IPSec en MIP

El uso de asociaciones de IPSec permanentes , establecidas y mantenidas por IGSN, a través del backbone, permitiría la transmisión de mensajes de señalización de forma segura. Así, IGSN podría disponer de una dirección IP específica sólo utilizada con fines de transmisión de mensajes de señalización. Las conexiones de IPSec aunque permanentes deberían modificar sus claves cada cierto intervalo de tiempo a fin de dificultar la obtención de las mismas.

Los riesgos de seguridad detectados en IP, saber quién ha realizado una conexión y los ataques de reenvío, se solucionan en Movilidad IP de forma nativa. En MIPv4 el mecanismo utilizado es la autenticación mediante clave compartida entre ME y HA de 128 bits, esto no excluye otros posibles mecanismos. Esta clave es independiente de la clave Ki y por ello deben disponer de otra clave para el intercambio de mensajes MIP. Otras formas de autenticación sería mediante el uso de Autoridades de Certificación (CA) o mediante el uso de claves públicas. MIPv6 soporta de forma nativa la autenticación y la encriptación mediante IPSec. Así para cada mensaje MIP que genera el ME, es necesario establecer una nueva conexión IPSec hacia el HA o utilizar una conexión preexistente no expirada. Es posible, también el uso de certificados.

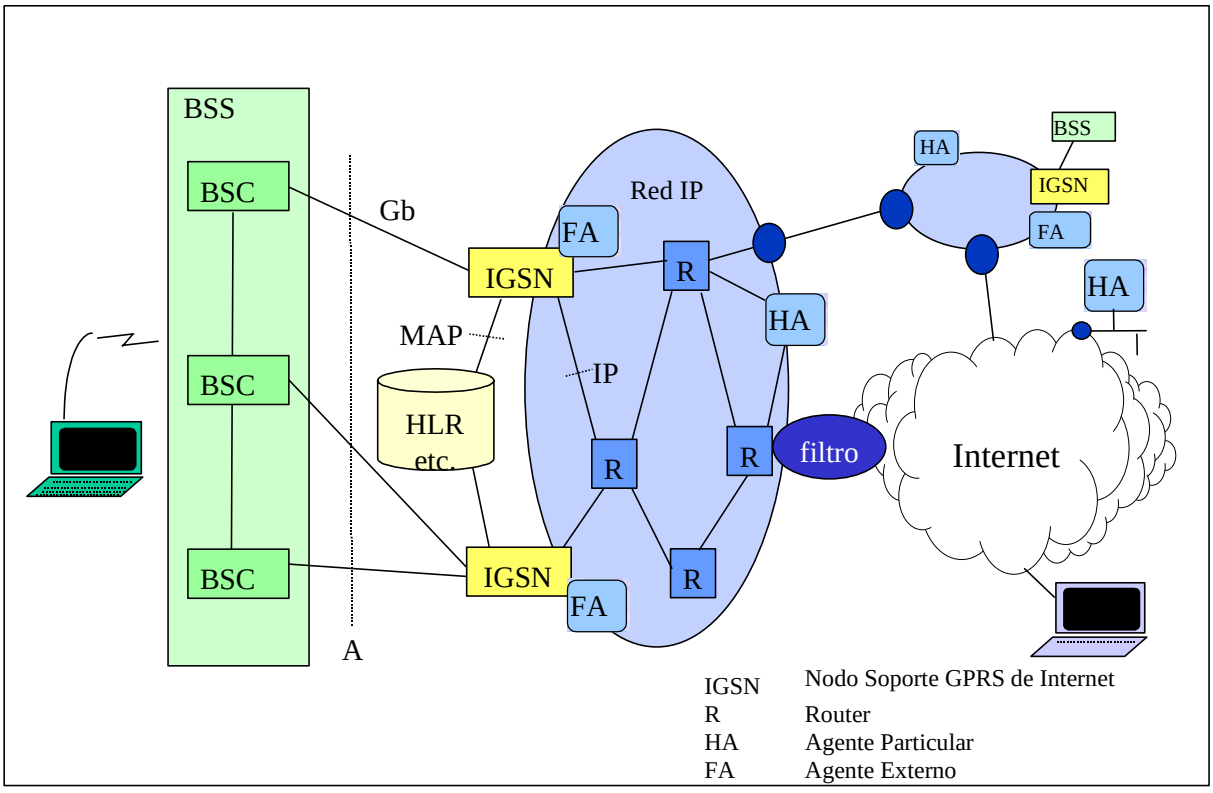


Figura 29. Movilidad IP entre PLMs y entre sistemas

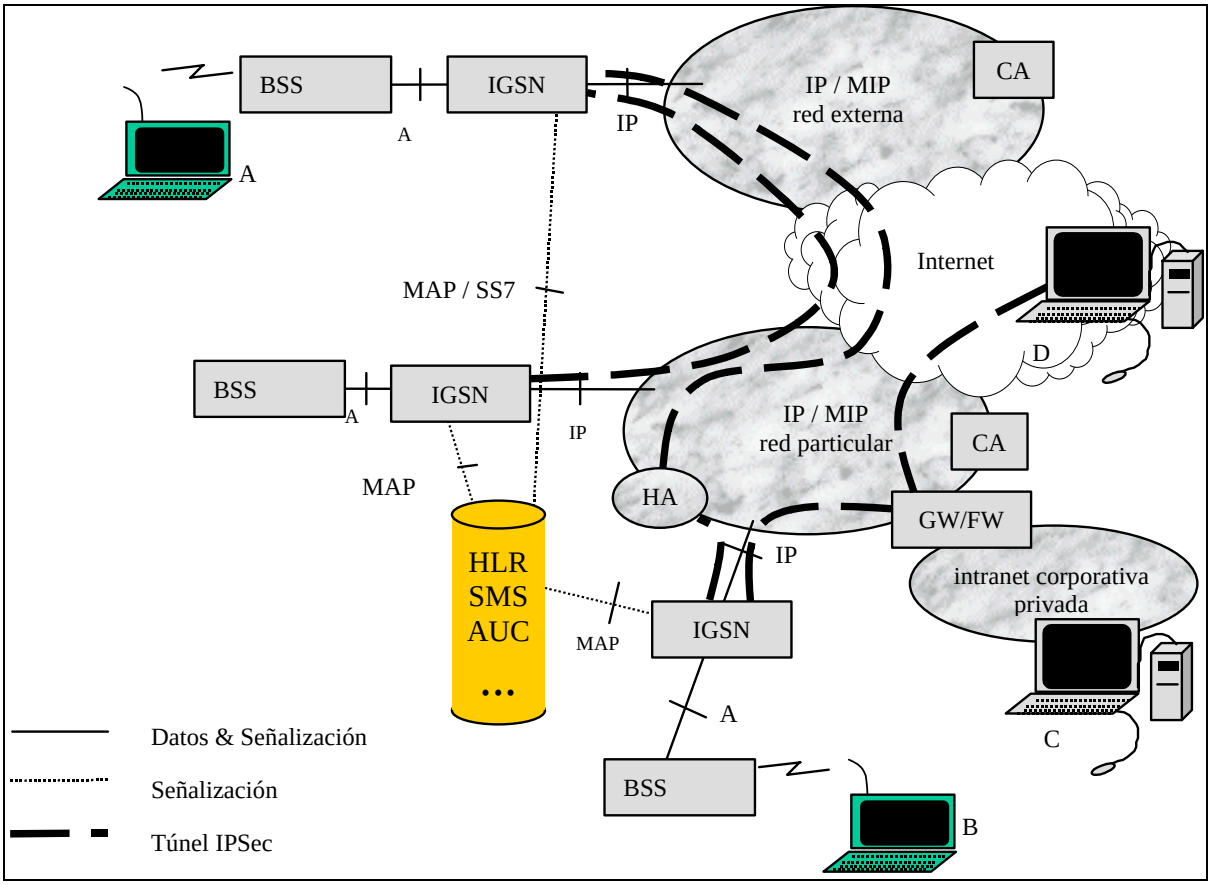


Figura 30. Uso de Túnel IPSEc

8.1.4 Consideraciones sobre MIP

Independientemente del modelo de MIP aplicado, deben considerarse los siguientes puntos:

- En el terminal se implementa IP con Movilidad IP y será ME el nodo con dirección IP.
- Se asume que el nodo GGSN incluye la funcionalidad de Agente Externo.
- La red particular es la red donde el terminal tiene su suscripción de MIP. El agente particular utilizado por MS, está ubicado en la red particular.
- El uso de AAA no implica ningún cambio en los estándares existentes ya que es una entidad externa a la red GPRS.
- Para notificar la presencia del FA, éste puede difundir mensajes de "Notificación de Agente" regularmente. Para evitar la transmisión de tráfico innecesario sobre la interfaz de radio, el terminal puede realizar una petición de "Solicitud de Agente" cuando lo necesite o bien GGSN / FA al detectar un nuevo ME en la red, puede enviar un mensaje de "Notificación de Agente" a ese terminal concreto. El mensaje de "Notificación de Agente" se envía en el plano de usuario en una dirección de difusión limitada (255.255.255.255) ya que ME no dispone todavía de dirección IP.
- Los mensajes de señalización de MIP se envían en el plano de usuario.

8.1.5 Mejoras de seguridad incorporadas por los Modelos de Arquitectura propuestos

Los modelos de arquitectura presentados, representan una innovación tecnológica al incluir servicios de seguridad no ofrecidos hasta el momento en los móviles de segunda generación[3], servicios por otra parte, muy relevantes como pueden ser la integridad de la información, la seguridad extremo a extremo y un abanico más amplio de algoritmos de confidencialidad e integridad[4]. Otro de los puntos a tener en cuenta es la escalabilidad de los modelos, todos los modelos permiten el desarrollo de los protocolos de forma independiente.

La aplicación del modelo de arquitectura de seguridad de WTLS sobre IP, concede al mismo tiempo, la posibilidad de aplicar seguridad a nivel WTLS sin necesidad de aplicar Movilidad IP, lo que otorgaría seguridad entre el terminal y el servidor WAP, mejorándose el ámbito de seguridad actual (GPRS abarca desde el terminal hasta SGSN)[5]. La aplicación conjunta de seguridad a nivel WTLS más Movilidad IP ofrece el servicio de seguridad extremo a extremo.

Finalmente es importante destacar que plantear la seguridad extremo a extremo implica que la seguridad pasa a depender del usuario, mejor dicho, de la funcionalidad ofrecida por el terminal y deja de ser voluntad del operador de red, como era hasta el momento.

[3] Capítulo "Evolución de GSM / GPRS hacia UMTS" (8)
[4] Anexo "IPSec" (3)
[5] Capítulo "Evolución de GSM / GPRS hacia UMTS" (8), anexo "Tecnología WAP" (8) y anexo "GPRS en UMTS" (18)

La aplicación de Movilidad IP con IPv4 o con IPv6, o la selección del uso de Movilidad IP con optimización de direccionamiento puede valorase en el capítulo siguiente donde se expone una comparativa de las diferentes implementaciones que ofrece Movilidad IP.

En la figura presentada a continuación puede verse el área de cobertura de seguridad en las diferentes arquitecturas presentadas.

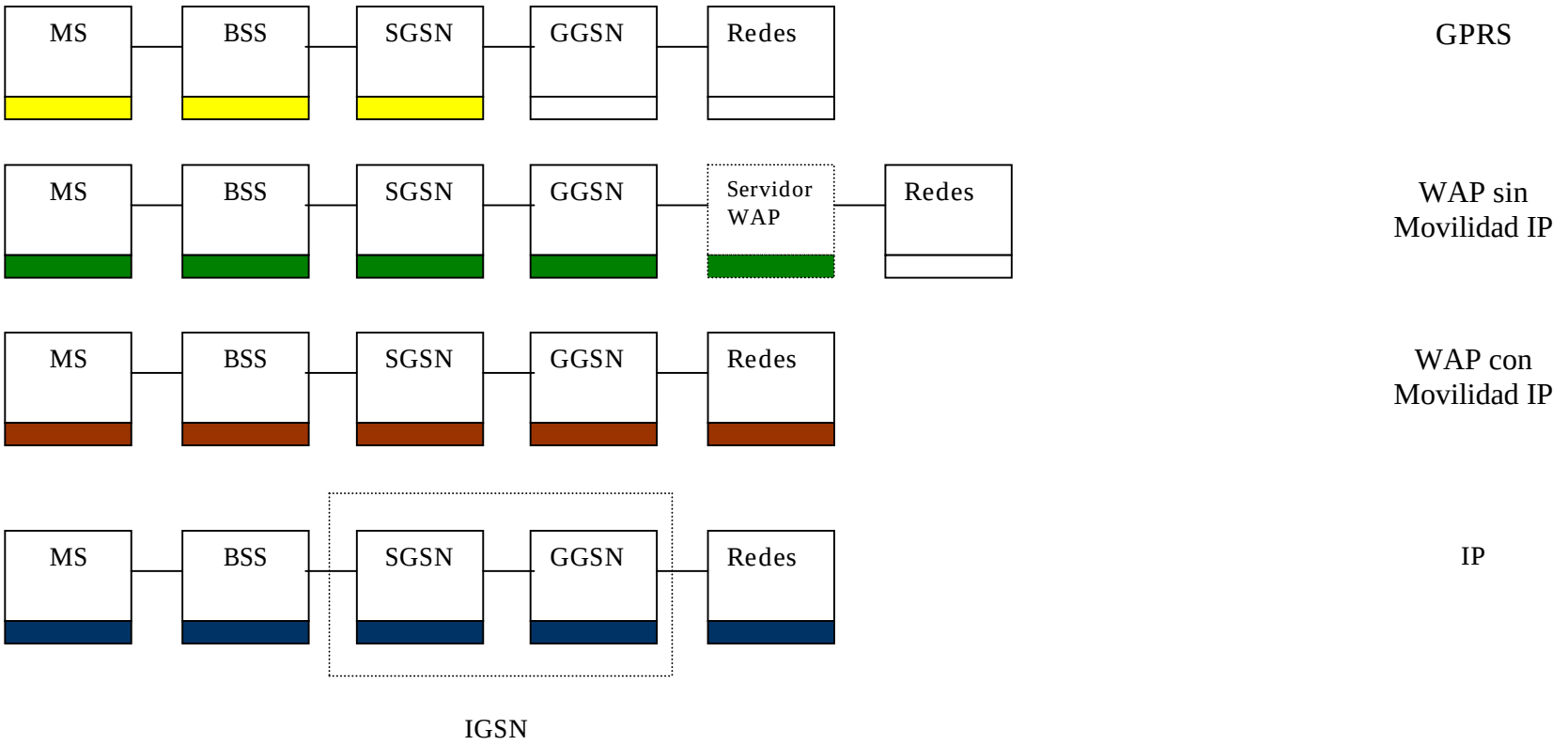


Figura 31. Área de seguridad

8.2 Movilidad IP aplicada a los Modelos de Arquitectura de Seguridad

En el primer apartado de este capítulo se especifica el valor óptimo de MTU en la aplicación de Movilidad IP con los diseños de arquitectura propuestos y en la segunda sección se crean modelos matemáticos para la evaluación comparativa de Movilidad IPv4, Movilidad IPv4 con optimización de direccionamiento, Movilidad IPv6 y Movilidad IPv6 con optimización de direccionamiento.

El anexo “Movilidad IP” (5) ofrece una descripción general del mecanismo de MIP.

8.2.1 Movilidad IP y MTU

Los mecanismos de movilidad IP llevan asociados una serie de requerimientos que determinan el rango de selección de MTU. Uno de los principales requerimientos es el uso de mecanismos de túnel, lo que implica restricciones en el tamaño del paquete si se intenta evitar la fragmentación del mensaje, debiendo para ello limitar la MTU del paquete a la MTU del túnel menos la longitud de las cabeceras añadidas por el proceso de tunelización. La siguiente imposición que determina el valor de MTU, es la necesidad de limitar el tiempo de respuesta del circuito de movilidad IP, es decir, acotar al mínimo el tiempo transcurrido desde el envío de un mensaje desde la estación A al terminal B, hasta la recepción de una posible respuesta de dicho terminal a A.

Teniendo en cuenta todos estos puntos se recomienda para IPv6 una MTU de 1280 octetos y para IPv4 una MTU de 1300 octetos. Estos valores se corresponden con el valor mínimo de MTU para IPv6 y con el valor de encapsulamiento de un paquete IPv6 sobre un dominio de IPv4, situación muy probable en el estado actual de predominio de dominios IPv4 sobre dominios IPv6.

8.2.2 Evaluación del rendimiento de IPv4 vs IPv6

En este apartado se realiza un análisis en profundidad de los mecanismos de Movilidad IP definidos para IPv4 y para IPv6 a fin de cuantificar el porcentaje de mejora de rendimiento de MIPv6 respecto a MIPv4. Para ello se crean modelos matemáticos para la evaluación de las diferentes implementaciones que ofrece Movilidad IP.

La terminología a aplicar en este apartado es:

p Tiempo de procesamiento

MTU’ Unidad de transmisión máxima (incluyendo las cabeceras IP del mensaje inicial), la suma de MTU’ y los octetos añadidos en los procesos de encapsulamiento y en el caso de IPv6 de transmisión de la extensión “Binding Update”, no pueden superar MTU.

mtu Unidad de transmisión mínima (cabeceras IP del mensaje inicial más opciones mínimas). El valor de mtu y los octetos añadidos en los procesos de encapsulamiento y en el caso de IPv6 de transmisión de la extensión “Binding Update”, no pueden superar MTU

l Longitud del mensaje, l es una variable aleatoria comprendida entre MTU’ y mtu

l’ Longitud del mensaje, l es una variable aleatoria comprendida entre MTU’ y mtu

bps Velocidad de transmisión (bits / segundo)

En el momento de realizar la petición de registro con el agente externo o con el agente propio, se indica el tipo de encapsulación a utilizar, siendo posible seleccionar Ensapsulación Mínima o Encapsulación GRE. La opción Encapsulación Mínima, representa un incremento de 8 a 12 octetos, dependiendo de la presencia o no del campo "Dirección de Fuente Origen Presente". La opción de Encapsulación GRE, propone un incremento de 4 a 8 octetos, dependiendo de la presencia del campo "Checksum" y "Reservado". Finalmente podemos optar también por la encapsulación de paquetes sobre

IPv4, proceso que incluye en el mensaje una cabecera de entre 20 y 32 octetos dependiendo de la presencia de la opción de seguridad en el mensaje original.

Resumiendo, el proceso de encapsulación de los mensajes añade entre 4 y 32 octetos a la longitud inicial del mismo, este incremento se desestima dado que la relevancia de este valor (tiempo de transmisión de estos octetos adicionales) es del orden de 0,09 segundos[6] en el peor de los casos. Por lo tanto en todos los modelos se considerará un incremento mínimo de 4 octetos, sin tener en cuenta el tipo de encapsulación seleccionado.

También es posible utilizar el mecanismo de compresión de cabecera Van Jacobson, esta opción, en el caso de no poder comprimir la cabecera envía el mensaje tal y como lo recibe y en la mayoría de los casos se estima una mejora de 10 octetos, se desestima este parámetro porque su incidencia en el proceso de transmisión es del orden de 0,03[7] segundos. Para más detalles sobre el mecanismo de comprensión de cabecera de Van Jacobson ver [64].

Otro de los puntos considerados en los apartados posteriores es que no se produce fragmentación, este hecho sólo provocaría un incremento del tiempo de procesamiento del mensaje que resaltaría todavía más las diferencias entre MIPv4 y MIPv6. De esta forma los valores obtenidos serán aquellos que definan el mínimo porcentaje de rendimiento comparativo entre ambas tecnologías.

Los procesos utilizados para la definición de los modelos son idénticos para los diferentes tipos de movilidad, MIPv4, MIPV4 con optimización de direccionamiento, MIPv6 y MIPv6 con optimización de direccionamiento. En el primer modelo consideraremos que todos los mensajes implican una respuesta del terminal a la estación emisora, mientras que en el segundo modelo, se tomará en cuenta la posición contraria, ningún mensaje necesita respuesta. Así el resultado final será un porcentaje mínimo con la variabilidad máxima aplicable.

[6] Este valor representa el tiempo de transmisión de 28 octetos a una velocidad de 2400 bps, definida en [72] como la velocidad para GSM.
[7] Este valor representa el tiempo de transmisión de 10 octetos a una velocidad de 2400 bps, definida en [72] como la velocidad para GSM.

8.2.2.1 Modelo 1

En este modelo se tomará como hipótesis que todos los mensajes generan respuesta del terminal a la estación origen de la emisión.

8.2.2.1.1 Modelo de Movilidad IP con IPv4

En la siguiente figura podemos observar el proceso de movilidad IP con IPv4.

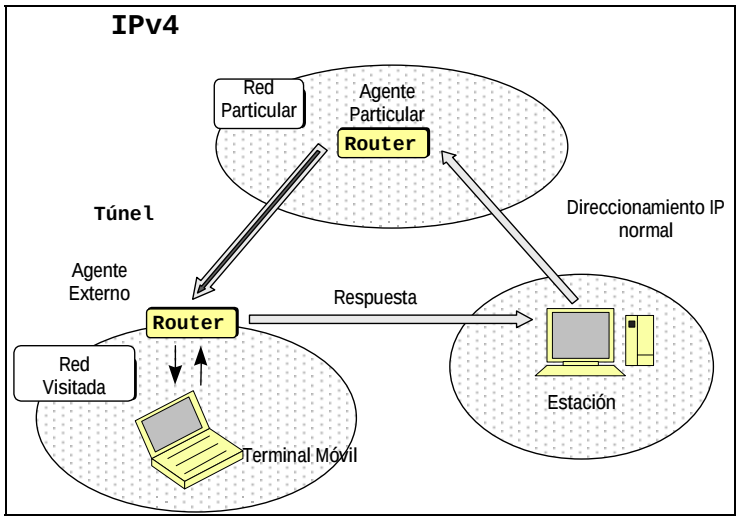


Figura 32. Movilidad IP en IPv4

Los pasos son:

1Transmisión del mensaje desde la estación a HA

Tiempo = l / bps

2Procesamiento y encapsulación del mensaje desde HA a FA

Tiempo = p + (l+4) / bps

3Procesamiento y transmisión del mensaje desde el FA al terminal correspondiente

Tiempo = p + l / bps

4Procesamiento y transmisión de la respuesta desde el terminal al FA

Tiempo = p + l / bps

5Procesamiento y transmisión del mensaje desde el FA a la estación

Tiempo = p + l / bps

Resultando un tiempo total de :

$$\textbf{Tiempo}_{\text{MIPv4}} = 4*p + (5*l + 4) / bps$$

8.2.2.1.2 Modelo de Movilidad IPv4 con Optimización de Direccionamiento

En la siguiente figura se detalla el proceso de MIPv4 con optimización de direccionamiento.

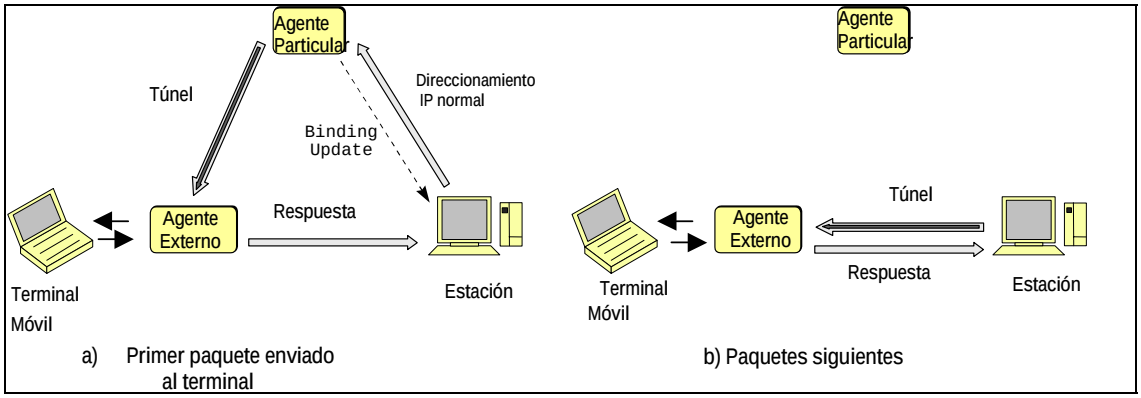


Figura 33. Movilidad IPv4 con optimización de direccionamiento

Los pasos son:

1Transmisión del mensaje desde la estación a HA

Tiempo = l'/bps

2Procesamiento y encapsulación del mensaje desde el HA a FA

Tiempo = p + (l'+4)/bps

3Transmisión de un mensaje "Binding Update" desde HA a la estación.

Este mensaje no se tendrá en cuenta en el cálculo ya que no determina ninguna implicación en el terminal ni en el computo del tiempo total de transmisión de un mensaje desde la estación origen hasta su recepción por el terminal.

4Procesamiento y transmisión del mensaje desde el FA al terminal correspondiente

Tiempo = p + l'/bps

5Procesamiento y transmisión de la respuesta desde el terminal al FA

Tiempo = p + l'/bps

6Procesamiento y transmisión del mensaje desde el FA a la estación

Tiempo = p + l'/bps

7Transmisión de un mensaje desde la estación al FA

Tiempo = l/bps

8Procesamiento y transmisión del mensaje desde el FA al terminal correspondiente

Tiempo = p + l/bps

9 Procesamiento y transmisión de la respuesta desde el terminal al FA

Tiempo = p + l/bps

10 Procesamiento y transmisión del mensaje desde el FA a la estación

Tiempo = p + l/bps

Así el total del proceso realizado para el primer paquete (pasos 1-6) es:

$$\textbf{Tiempo}_{MIPv4\_OD1} = 4*p + (5*l' + 4) / bps$$

El tiempo de gestión del resto de paquetes será:

$$\textbf{Tiempo}_{MIPv4\_OD} = 3*p + 4*l / bps$$

8.2.2.1.3 Modelo de Movilidad IPv6

En la siguiente figura se detalla el proceso de MIPv6

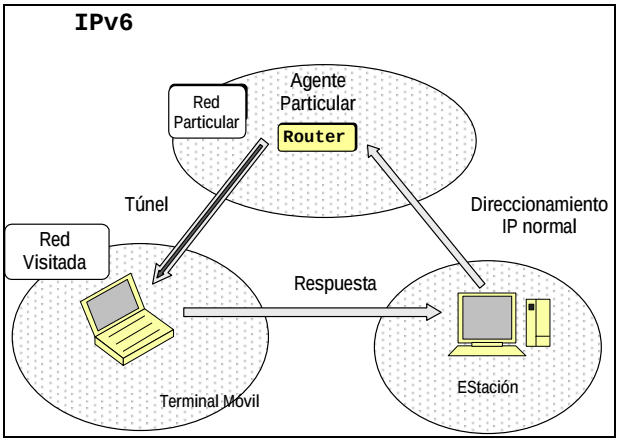


Figura 34. Movilidad IP en IPv6

Los pasos son:

1Transmisión del mensaje desde la estación a HA

Tiempo = l / bps

2Procesamiento y encapsulación del mensaje desde el HA al terminal correspondiente[8]

Tiempo = p + (l+4) / bps

3Procesamiento y transmisión de la respuesta desde el terminal a la estación

Tiempo = p + l / bps

Resultando un tiempo total de :

$$\textbf{Tiempo}_{\textbf{MIPv6}} = 2*p + (3*l + 4) / bps$$

[8] Si se requiere el direccionamiento forzoso de un paquete en IPv6 se utiliza la extensión de "Direccionamiento", siempre que el paquete no se haya originado en otro nodo, en cuyo caso se utiliza el proceso normal de tunelización

8.2.2.1.4 Modelo de Movilidad IPv6 con Optimización de Direccionamiento

En la siguiente figura podemos observar el proceso de MIPv6 con optimización de direccionamiento.

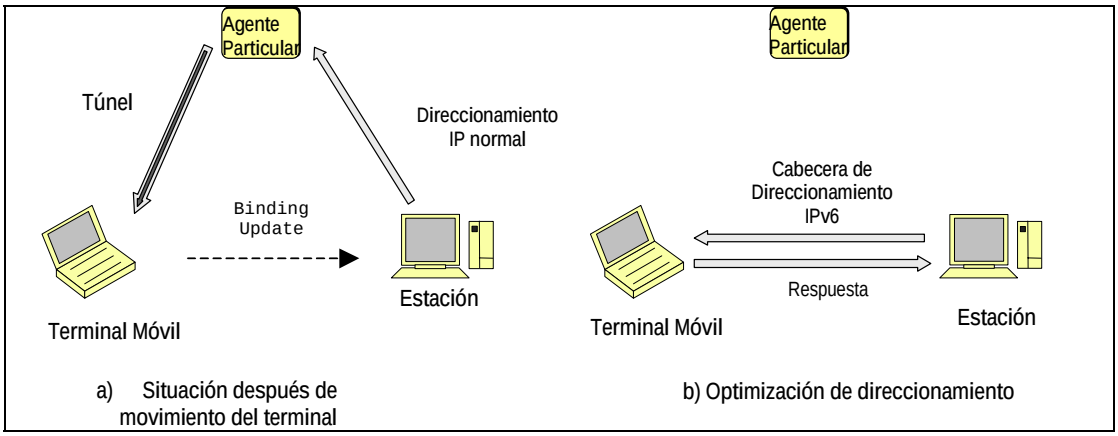


Figura 35. Movilidad IPv6 con optimización de direccionamiento

Los pasos son:

1Transmisión del mensaje desde la estación al HA

Tiempo = l'/bps

2Procesamiento y encapsulación del mensaje desde el HA al terminal correspondiente[9]

Tiempo = p + (l'+4)/bps

3Procesamiento y transmisión de la respuesta desde el terminal a la estación (incluyendo la opción "Binding Update")

Tiempo_min = p + (l'+10)/bps
Tiempo_max = p + (l'+82)/bps

La opción "Binding Update" tiene una longitud fija de 10 octetos, más una longitud opcional de 22 octetos correspondiente a las subopciones "Subopción de Identificador Único" (4 octetos) y "Subopción de Dirección Alternativa de Care-of-Address" (18 octetos). Los posibles problemas de posicionamiento en el datagrama pueden forzar el uso de 6 octetos de relleno, lo que hace una longitud máxima de 38 octetos. La opción de "Binding Update" debe ir siempre acompañada de la opción "Dirección Particular" lo que implica que si no estaba incluida en el mensaje debe ser añadida, esta opción tiene una longitud de 18 octetos y un posible campo de relleno de 6 octetos por problemas de posicionamiento en el datagrama. Además es obligatorio añadir la opción de autenticación, protección de integridad y protección contra reenvío mediante una opción AH, lo que implica información adicional de mínimo 20 octetos. Así finalmente, podemos deducir que la longitud de "Binding Update" puede representar entre 10 y 82 octetos.

[9] Si se requiere el direccionamiento forzoso de un paquete en IPv6 se utiliza la extensión de "Direccionamiento", siempre que el paquete no se haya originado en otro nodo, en cuyo caso se utiliza el proceso normal de tunelización.

4Transmisión del mensaje desde la estación al terminal

Tiempo = l / bps

5Procesamiento y transmisión de la respuesta desde el terminal a la estación

Tiempo = p + l / bps

Así el total del proceso realizado para el primer paquete (pasos 1-3) es:

$$\textbf{Tiempo\_min}_{\textbf{MIPv6\_OD1}} = \textbf{2*p + (2*l' + 10) / bps}$$

$$\textbf{Tiempo\_max}_{\textbf{MIPv6\_OD1}} = \textbf{2*p + (2*l' + 82) / bps}$$

En los siguientes cálculos se considerará el caso peor, es decir, $\text{Tiempo\_max}_{\textbf{MIPv6\_OD1}}$, como el tiempo de procesamiento general para el primer paquete de movilidad IPv6 con optimización de direccionamiento, ya que lo que se desea es encontrar el mínimo porcentaje de mejora de rendimiento al utilizar MIPv6 en vez de MIPv4. Se hará referencia a $\text{Tiempo\_max}_{\textbf{MIPv6\_OD1}}$, como $\text{Tiempo}_{\textbf{MIPv6\_OD1}}$.

El tiempo de gestión del resto de paquetes será:

$$\textbf{Tiempo}_{\textbf{MIPv6\_OD}} = \textbf{3*p + 2*l / bps}$$

8.2.2.2 Modelo 2

En este modelo se tomará como hipótesis que ningún mensaje genera respuesta del terminal a la estación origen de la emisión.

8.2.2.2.1 Modelo de Movilidad IP con IPv4

En la siguiente figura podemos observar el proceso de movilidad IP con IPv4.

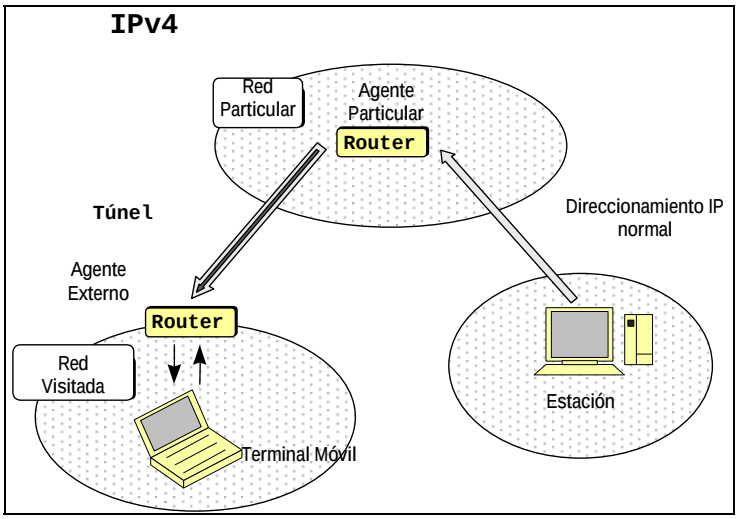


Figura 36. Movilidad IP en IPv4

Los pasos son:

1Transmisión del mensaje desde la estación a HA

Tiempo = l / bps

2Procesamiento y encapsulación del mensaje desde el HA al FA

Tiempo = p + (l+4) / bps

3Procesamiento y transmisión del mensaje desde el FA al terminal correspondiente

Tiempo = p + l / bps

Resultando un tiempo total de :

$$\textbf{Tiempo}_{\text{MIPv4}} = 2*p + (3*l + 4) / bps$$

8.2.2.2.2 Modelo de Movilidad IPv4 con Optimización de Direccionamiento

En la siguiente figura se detalla el proceso de MIPv4 con optimización de direccionamiento.

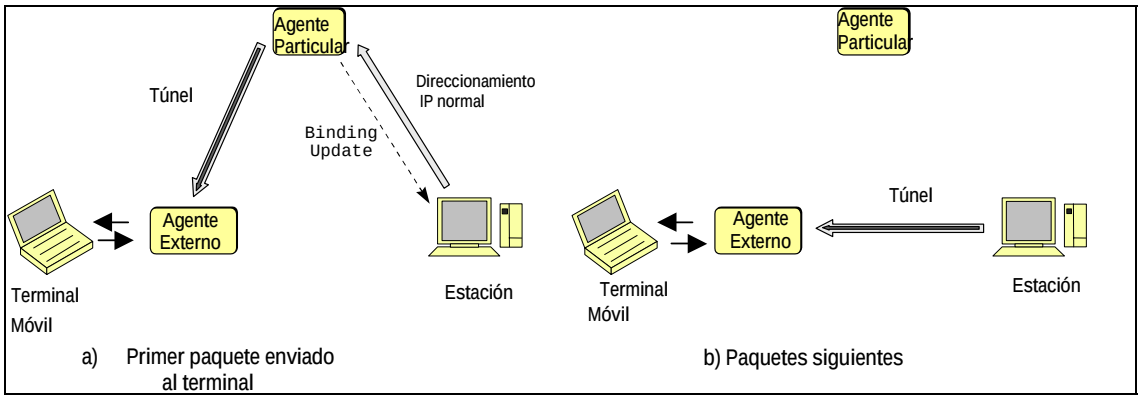


Figura 37. Movilidad IPv4 con optimización de direccionamiento

Los pasos son:

1Transmisión del mensaje desde la estación a HA

Tiempo = l'/bps

2Procesamiento y encapsulación del mensaje desde el HA al FA

Tiempo = p + (l'+4)/bps

3Transmisión de un mensaje "Binding Update" desde HA a la estación.

Este mensaje no se tendrá en cuenta en el cálculo ya que no determina ninguna implicación en el terminal ni en el cómputo del tiempo total de transmisión de un mensaje desde la estación origen hasta su recepción por el terminal.

4Procesamiento y transmisión del mensaje desde el FA al terminal correspondiente

Tiempo = p + l'/bps

5Transmisión de un mensaje desde la estación al FA

Tiempo = l/bps

6Procesamiento y transmisión del mensaje desde el FA al terminal correspondiente

Tiempo = p + l/bps

Así el total del proceso realizado para el primer paquete (pasos 1-4) es:

Tiempo $_{MIPv4\_OD1}$ = 2*p + (3*l' + 4) / bps

El tiempo de gestión del resto de paquetes será:

Tiempo $_{MIPv4\_OD}$ = p + 2*l / bps

8.2.2.2.3 Modelo de Movilidad IPv6

En la siguiente figura se detalla el proceso de MIPv6

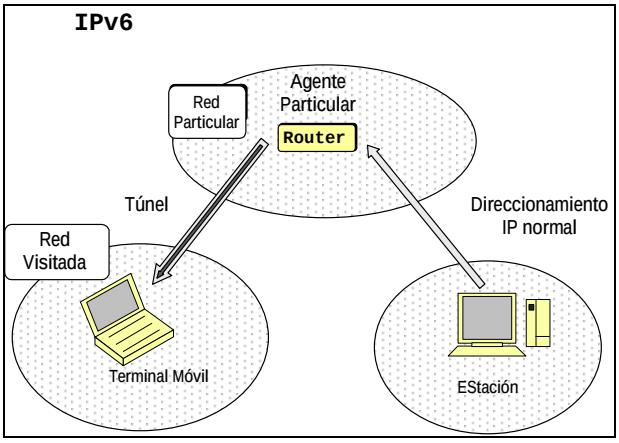


Figura 38. Movilidad IP en IPv6

Los pasos son:

1Transmisión del mensaje desde la estación a HA

Tiempo = l / bps

2Procesamiento y encapsulación del mensaje desde el HA al terminal correspondiente[10]

Tiempo = p + (l+4) / bps

Resultando un tiempo total de :

Tiempo $_{MIPv6}$ = p + (2*l + 4) / bps

[10] Si se requiere el direccionamiento forzoso de un paquete en IPv6 se utiliza la extensión de "Direccionamiento", siempre que el paquete no se haya originado en otro nodo, en cuyo caso se utiliza el proceso normal de tunelización.

8.2.2.2.4 Modelo de Movilidad IPv6 con Optimización de Direccionamiento

En la siguiente figura podemos observar el proceso de MIPv6 con optimización de direccionamiento.

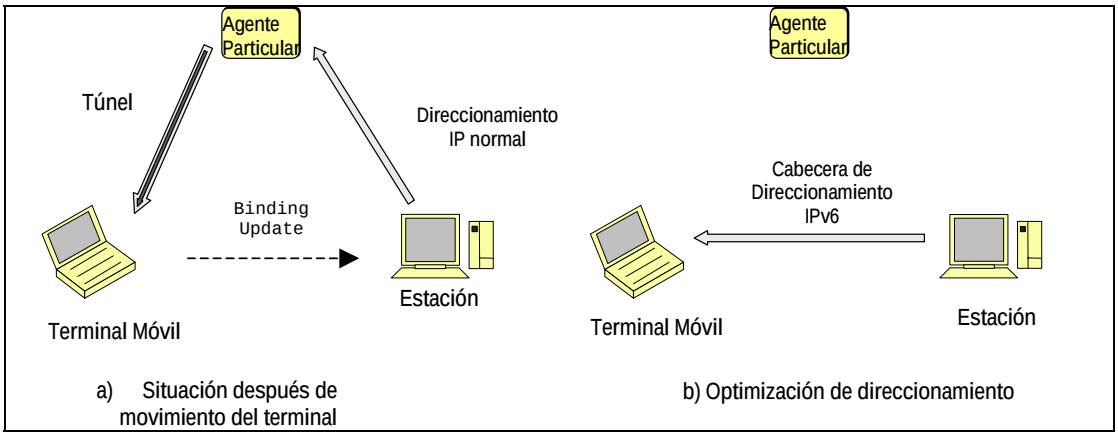


Figura 39. Movilidad IPv6 con optimización de direccionamiento

Los pasos son:

1Transmisión del mensaje desde la estación a HA

Tiempo = l' / bps

2Procesamiento y encapsulación del mensaje desde el HA al terminal correspondiente[11]

Tiempo = p + (l'+4) / bps

3Transmisión del mensaje "Binding Update"

Tiempo = 116 / bps

El mensaje de "Binding Update" debe contener la cabecera de IPv6 (40 octetos), opciones de destino (2 octetos), la subopción "Binding Update" (32 octetos), la opción de AH (mínimo 20 octetos), la opción "Dirección Particular" (18 octetos) y un posible campo de relleno de 4 octetos para incluir la opción de "Dirección Particular".

4Transmisión del mensaje desde la estación al terminal

Tiempo = l / bps

Así el total del proceso realizado para el primer paquete (pasos 1-3) es:

$$\textbf{Tiempo}_{MIPv6\_OD1} = 2*p + (2*l' + 116) / bps$$

El tiempo de gestión del resto de paquetes será:

$$\textbf{Tiempo}_{MIPv6\_OD} = l / bps$$

[11] Si se requiere el direccionamiento forzoso de un paquete en IPv6 se utiliza la extensión de "Direccionamiento", siempre que el paquete no se haya originado en otro nodo, en cuyo caso se utiliza el proceso normal de tunelización.

8.2.2.3 Procedimiento de Cálculo

La base para el estudio comparativo presentado a continuación son:

- Se considerará un tiempo de vida de registro (TTL) idéntico para MIPv4 y MIPv6.
- Se supone que durante todo el TTL se están transmitiendo mensajes secuenciales desde la estación emisora al terminal.

El valor obtenido de la ecuación de igualar el tiempo total del proceso de MIP con el TTL, nos da como resultado un valor equivalente a la suma las longitudes de los mensajes transmitidos, lo que nos permite obtener un dato cuantitativo representativo del "rendimiento" del procedimiento.

Así las ecuaciones planteadas para el modelo 1 serían:

Opción	Ecuación
IPv4	**4*p + (5*l + 4) / bps = TTL**
IPv4 con Optimización de Direccionamiento	**(4*p + (5*l' + 4) / bps) + (3*p + 4*l / bps) = TTL**
IPv6	**2*p + (3*l + 4) / bps = TTL**
IPv6 con Optimización de Direccionamiento	**(2*p + (2*l' + 82) / bps) + (3*p + 2*l / bps) = TTL**

de lo que se deduce que el valor de l, la suma de las longitudes de los datagramas enviados, será igual a :

Opción	Ecuación
IPv4	**l = ((bps*(TTL-4*p)) - 4) / 5**
IPv4 con Optimización de Direccionamiento	**l = ((bps*(TTL-7*p)) – 5*l' – 4) / 4**
IPv6	**l = ((bps*(TTL-2*p)) – 4) / 3**
IPv6 con Optimización de Direccionamiento	**l = ((bps*(TTL-5*p)) – 2*l' – 82) /2**

A partir de los modelos establecidos podemos comprobar que para valores idénticos de bps, p y TTL, el rendimiento obtenido con el algoritmo de MIPv4 con respecto a MIPv4 con optimización de direccionamiento supondrá alrededor de un 80%, con respecto a MIPv6 cerca de un 60% y comparándolo con MIPv6 con optimización de direccionamiento alcanzará un porcentaje cercano al 40%.

Para el modelo 2 las ecuaciones son:

Opción	Ecuación
IPv4	**2*p + (3*l + 4) / bps = TTL**
IPv4 con Optimización de Direccionamiento	**(2*p + (3*l' + 4) / bps)+ (p + 2*l / bps)= TTL**
IPv6	**p + (2*l + 4) / bps = TTL**
IPv6 con Optimización de Direccionamiento	**(p + ((2*l' + 4) + 116) / bps)+ l / bps)= TTL**

de lo que se deduce que el valor de l, la suma de las longitudes de los datagramas enviados, será igual a :

Opción	Ecuación
IPv4	**l = ((bps*(TTL-2*p)) - 4) / 3**
IPv4 con Optimización de Direccionamiento	**l = ((bps*(TTL-3*p)) – 3*l' – 4) / 2**
IPv6	**l = ((bps*(TTL-p)) - 4) / 2**
IPv6 con Optimización de Direccionamiento	**l = (((bps*(TTL-p)) - 2*l' – 4 - 116)**

A partir de los modelos establecidos podemos comprobar que para valores idénticos de bps, p y TTL, el rendimiento obtenido con el algoritmo de MIPv4 con respecto a MIPv4 con optimización de direccionamiento supondrá alrededor de un 66%, con respecto a MIPv6 cerca de un 66% y comparándolo con MIPv6 con optimización de direccionamiento alcanzará un porcentaje cercano al 33%.

Las tablas presentadas a continuación contrastan a partir de valores numéricos las estimaciones obtenidas de forma analítica. En el caso de algoritmos con optimización de direccionamiento consideraremos siempre el peor de los casos, es decir, aquel cuyo primer mensaje tiene una longitud l' igual a MTU'.

En el caso de bps, la selección de valores viene determinada por la velocidad de transmisión definida para GSM en [72], la velocidad máxima de CDMA definida en [72] y la velocidad para GPRS de [23] (2400, 14400 y 150000). En el caso de p, se ha considerado el valor definido en [62] de 100 milisegundos y el valor de 1 milisegundo como representación de tiempo mínimo de procesamiento. Para TTL se ha tomado en cuenta el valor por defecto del campo tiempo de vida de registro, para un terminal móvil y su agente de movilidad, definido en [62] que corresponde a 1800 segundos, el otro TTL considerado corresponde a la mitad de dicho valor para casos de tiempos de vida limitados. Finalmente, los valores de MTU' se han seleccionado considerando en primer lugar la estimación definida en [63] para un paquete de tamaño medio, 452 octetos, en segundo lugar el valor de rango similar al propuesto como MTU para IPv6 que correspondería a 1280 octetos, y en tercer lugar se ha considerado el valor definido en [64] para los paquetes de IPv6 transmitidos sobre dominios de IPv4, 1480 octetos.

bps	TTL	p	MTU'	IPv4	IPv4_OD	IPv6	IPv6_OD	%v4-v4_OD	%v4-v6	%v4-v6_OD	%v4	OD-v6	OI	%v6-v6_OD
2400	**1800**	**0,1**	**452**	863807,2	1079014,0	1439838,7	2158907,0	80,055	59,993	40,011		49,980		66,693
2400	**1800**	**0,1**	**1280**	863807,2	1077979,0	1439838,7	2158079,0	80,132	59,993	40,027		49,951		66,719
2400	**1800**	**0,1**	**1480**	863807,2	1077729,0	1439838,7	2157879,0	80,151	59,993	40,030		49,944		66,725
2400	**1800**	**0,001**	**452**	863997,3	1079429,8	1439997,1	2159501,0	80,042	60,000	40,009		49,985		66,682
2400	**1800**	**0,001**	**1280**	863997,3	1078394,8	1439997,1	2158673,0	80,119	60,000	40,024		49,956		66,708
2400	**1800**	**0,001**	**1480**	863997,3	1078144,8	1439997,1	2158473,0	80,137	60,000	40,028		49,949		66,714
2400	**900**	**0,1**	**452**	431807,2	539014,0	719838,7	1078907,0	80,111	59,987	40,023		49,959		66,719
2400	**900**	**0,1**	**1280**	431807,2	537979,0	719838,7	1078079,0	80,265	59,987	40,053		49,902		66,770
2400	**900**	**0,1**	**1480**	431807,2	537729,0	719838,7	1077879,0	80,302	59,987	40,061		49,888		66,783
2400	**900**	**0,001**	**452**	431997,3	539429,8	719997,1	1079501,0	80,084	60,000	40,018		49,970		66,697
2400	**900**	**0,001**	**1280**	431997,3	538394,8	719997,1	1078673,0	80,238	60,000	40,049		49,913		66,748
2400	**900**	**0,001**	**1480**	431997,3	538144,8	719997,1	1078473,0	80,275	60,000	40,056		49,899		66,761
14400	**1800**	**0,1**	**452**	5182847,2	6476914,0	8639038,7	12955907,0	80,020	59,993	40,004		49,992		66,680
14400	**1800**	**0,1**	**1280**	5182847,2	6475879,0	8639038,7	12955079,0	80,033	59,993	40,006		49,987		66,685
14400	**1800**	**0,1**	**1480**	5182847,2	6475629,0	8639038,7	12954879,0	80,036	59,993	40,007		49,986		66,686
14400	**1800**	**0,001**	**452**	5183987,7	6479408,8	8639989,1	12959471,0	80,007	60,000	40,002		49,997		66,669
14400	**1800**	**0,001**	**1280**	5183987,7	6478373,8	8639989,1	12958643,0	80,020	60,000	40,004		49,993		66,674
14400	**1800**	**0,001**	**1480**	5183987,7	6478123,8	8639989,1	12958443,0	80,023	60,000	40,005		49,992		66,675
14400	**900**	**0,1**	**452**	2590847,2	3236914,0	4319038,7	6475907,0	80,041	59,987	40,007		49,984		66,694
14400	**900**	**0,1**	**1280**	2590847,2	3235879,0	4319038,7	6475079,0	80,066	59,987	40,013		49,974		66,702
14400	**900**	**0,1**	**1480**	2590847,2	3235629,0	4319038,7	6474879,0	80,072	59,987	40,014		49,972		66,705
14400	**900**	**0,001**	**452**	2591987,7	3239408,8	4319989,1	6479471,0	80,014	60,000	40,003		49,995		66,672
14400	**900**	**0,001**	**1280**	2591987,7	3238373,8	4319989,1	6478643,0	80,040	60,000	40,008		49,985		66,680
14400	**900**	**0,001**	**1480**	2591987,7	3238123,8	4319989,1	6478443,0	80,046	60,000	40,009		49,983		66,683
150000	**1800**	**0,1**	**452**	53987999,2	67473184,0	89989998,7	134962007,0	80,014	59,993	40,002		49,994		66,678
150000	**1800**	**0,1**	**1280**	53987999,2	67472149,0	89989998,7	134961179,0	80,015	59,993	40,003		49,994		66,678
150000	**1800**	**0,1**	**1480**	53987999,2	67471899,0	89989998,7	134960979,0	80,016	59,993	40,003		49,994		66,679
150000	**1800**	**0,001**	**452**	53999879,2	67499171,5	89999898,7	134999132,0	80,001	60,000	40,000		50,000		66,667
150000	**1800**	**0,001**	**1280**	53999879,2	67498136,5	89999898,7	134998304,0	80,002	60,000	40,000		49,999		66,667
150000	**1800**	**0,001**	**1480**	53999879,2	67497886,5	89999898,7	134998104,0	80,002	60,000	40,000		49,999		66,668
150000	**900**	**0,1**	**452**	26987999,2	33723184,0	44989998,7	67462007,0	80,028	59,987	40,005		49,988		66,689
150000	**900**	**0,1**	**1280**	26987999,2	33722149,0	44989998,7	67461179,0	80,030	59,987	40,005		49,987		66,690
150000	**900**	**0,1**	**1480**	26987999,2	33721899,0	44989998,7	67460979,0	80,031	59,987	40,005		49,987		66,690
150000	**900**	**0,001**	**452**	26999879,2	33749171,5	44999898,7	67499132,0	80,002	60,000	40,000		49,999		66,667
150000	**900**	**0,001**	**1280**	26999879,2	33748136,5	44999898,7	67498304,0	80,004	60,000	40,001		49,998		66,668
150000	**900**	**0,001**	**1480**	26999879,2	33747886,5	44999898,7	67498104,0	80,005	60,000	40,001		49,998		66,668

Tabla 1. Evaluación de Movilidad IP según modelo 1

bps	TTL	p	MTU'	IPv4	IPv4_OD	IPv6	IPv6_OD	%v4-v4_OD	%v4-v6	%v4-v6_OD	%v4	OD-v6	OI	%v6-v6_OD
2400	**1800**	**0,1**	**452**	1439838,7	2158960,0	2159878,0	4318736,0	66,691	66,663	33,339		49,991		50,012
2400	**1800**	**0,1**	**1280**	1439838,7	2157718,0	2159878,0	4317080,0	66,730	66,663	33,352		49,981		50,031
2400	**1800**	**0,1**	**1480**	1439838,7	2157418,0	2159878,0	4316680,0	66,739	66,663	33,355		49,979		50,036
2400	**1800**	**0,001**	**452**	1439997,1	2159316,4	2159996,8	4318973,6	66,688	66,667	33,341		49,996		50,012
2400	**1800**	**0,001**	**1280**	1439997,1	2158074,4	2159996,8	4317317,6	66,726	66,667	33,354		49,986		50,031
2400	**1800**	**0,001**	**1480**	1439997,1	2157774,4	2159996,8	4316917,6	66,735	66,667	33,357		49,984		50,036
2400	**900**	**0,1**	**452**	719838,7	1078960,0	1079878,0	2158736,0	66,716	66,659	33,345		49,981		50,024
2400	**900**	**0,1**	**1280**	719838,7	1077718,0	1079878,0	2157080,0	66,793	66,659	33,371		49,962		50,062
2400	**900**	**0,1**	**1480**	719838,7	1077418,0	1079878,0	2156680,0	66,811	66,659	33,377		49,957		50,071
2400	**900**	**0,001**	**452**	719997,1	1079316,4	1079996,8	2158973,6	66,709	66,667	33,349		49,992		50,024
2400	**900**	**0,001**	**1280**	719997,1	1078074,4	1079996,8	2157317,6	66,785	66,667	33,375		49,973		50,062
2400	**900**	**0,001**	**1480**	719997,1	1077774,4	1079996,8	2156917,6	66,804	66,667	33,381		49,968		50,071
14400	**1800**	**0,1**	**452**	8639038,7	12957160,0	12959278,0	25917536,0	66,674	66,663	33,333		49,994		50,002
14400	**1800**	**0,1**	**1280**	8639038,7	12955918,0	12959278,0	25915880,0	66,680	66,663	33,335		49,992		50,005
14400	**1800**	**0,1**	**1480**	8639038,7	12955618,0	12959278,0	25915480,0	66,682	66,663	33,335		49,992		50,006
14400	**1800**	**0,001**	**452**	8639989,1	12959298,4	12959990,8	25918961,6	66,670	66,667	33,335		49,999		50,002
14400	**1800**	**0,001**	**1280**	8639989,1	12958056,4	12959990,8	25917305,6	66,677	66,667	33,337		49,998		50,005
14400	**1800**	**0,001**	**1480**	8639989,1	12957756,4	12959990,8	25916905,6	66,678	66,667	33,337		49,997		50,006
14400	**900**	**0,1**	**452**	4319038,7	6477160,0	6479278,0	12957536,0	66,681	66,659	33,332		49,988		50,004
14400	**900**	**0,1**	**1280**	4319038,7	6475918,0	6479278,0	12955880,0	66,694	66,659	33,337		49,984		50,010
14400	**900**	**0,1**	**1480**	4319038,7	6475618,0	6479278,0	12955480,0	66,697	66,659	33,338		49,984		50,012
14400	**900**	**0,001**	**452**	4319989,1	6479298,4	6479990,8	12958961,6	66,674	66,667	33,336		49,999		50,004
14400	**900**	**0,001**	**1280**	4319989,1	6478056,4	6479990,8	12957305,6	66,686	66,667	33,340		49,995		50,010
14400	**900**	**0,001**	**1480**	4319989,1	6477756,4	6479990,8	12956905,6	66,690	66,667	33,341		49,995		50,012
150000	**1800**	**0,1**	**452**	89989998,7	134976820,0	134992498,0	269983976,0	66,671	66,663	33,332		49,994		50,000
150000	**1800**	**0,1**	**1280**	89989998,7	134975578,0	134992498,0	269982320,0	66,671	66,663	33,332		49,994		50,000
150000	**1800**	**0,1**	**1480**	89989998,7	134975278,0	134992498,0	269981920,0	66,671	66,663	33,332		49,994		50,001
150000	**1800**	**0,001**	**452**	89999898,7	134999095,0	134999923,0	269998826,0	66,667	66,667	33,333		50,000		50,000
150000	**1800**	**0,001**	**1280**	89999898,7	134997853,0	134999923,0	269997170,0	66,668	66,667	33,334		50,000		50,000
150000	**1800**	**0,001**	**1480**	89999898,7	134997553,0	134999923,0	269996770,0	66,668	66,667	33,334		50,000		50,001
150000	**900**	**0,1**	**452**	44989998,7	67476820,0	67492498,0	134983976,0	66,675	66,659	33,330		49,989		50,000
150000	**900**	**0,1**	**1280**	44989998,7	67475578,0	67492498,0	134982320,0	66,676	66,659	33,330		49,988		50,001
150000	**900**	**0,1**	**1480**	44989998,7	67475278,0	67492498,0	134981920,0	66,676	66,659	33,330		49,988		50,001
150000	**900**	**0,001**	**452**	44999898,7	67499095,0	67499923,0	134998826,0	66,667	66,667	33,334		50,000		50,000
150000	**900**	**0,001**	**1280**	44999898,7	67497853,0	67499923,0	134997170,0	66,669	66,667	33,334		49,999		50,001
150000	**900**	**0,001**	**1480**	44999898,7	67497553,0	67499923,0	134996770,0	66,669	66,667	33,334		49,999		50,001

Tabla 2. Evaluación de Movilidad IP según modelo 2

La tabla siguiente presenta la media de los resultados obtenidos en las tablas correspondientes al modelo 1 y al modelo 2, se obtiene así un porcentaje medio de rendimiento de los diferentes mecanismos de movilidad IP con respecto al procedimiento de movilidad IP definido para IPv4.

bps	TTL	p	%v4-v4_OD	%v4-v6	%v4-v6_OD	%v4 OD-v6 OD	%v6-v6_OD
2400	**1800**	**0,1**	73,416	63,328	36,686	49,971	58,369
2400	**1800**	**0,001**	73,408	63,333	36,686	49,976	58,364
2400	**900**	**0,1**	73,500	63,323	36,705	49,941	58,405
2400	**900**	**0,001**	73,483	63,333	36,705	49,953	58,394
14400	**1800**	**0,1**	73,354	63,328	36,670	49,990	58,344
14400	**1800**	**0,001**	73,346	63,333	36,670	49,996	58,338
14400	**900**	**0,1**	73,375	63,323	36,673	49,981	58,355
14400	**900**	**0,001**	73,358	63,333	36,673	49,992	58,344
150000	**1800**	**0,1**	73,343	63,328	36,667	49,994	58,339
150000	**1800**	**0,001**	73,335	63,333	36,667	50,000	58,334
150000	**900**	**0,1**	73,353	63,323	36,668	49,988	58,345
150000	**900**	**0,001**	73,336	63,333	36,667	49,999	58,334
MEDIA			73,384	63,329	36,678	49,982	58,355

Tabla 3. Valores medios de evaluación de Movilidad IP según los modelos 1 y 2

8.2.2.4 Sumario

En este apartado se ha realizado una comparativa entre las opciones que presenta Movilidad IP, de forma clara el rendimiento óptimo se corresponde con la aplicación de Movilidad IPv6 con optimización de direccionamiento. No se pretende descartar ninguna implementación dado que no sólo es relevante el rendimiento sino la aplicabilidad de la misma y a día de hoy existen muchos sistemas con IPv4 que por razones obvias, no pueden disponer de la opción con mejor rendimiento.

La ventaja que ofrece el estudio realizado es que la presentación de los modelos matemáticos permite evaluar el rendimiento aportado por las diferentes opciones de MIP para cualquier sistema, independientemente de las características del mismo.

9Conclusiones

En esta tesis se ha planteado un modelo de arquitectura de seguridad, “WTLS sobre IP”, que permite a sistemas de telefonía móvil de segunda generación la mejora de su oferta de servicios de seguridad, incorporando características tan importantes como pueden ser la aplicación de seguridad extremo a extremo, disponibilidad del servicio de integridad y la capacidad de adaptación a nuevos mecanismos y servicios. Es destacable la relevancia de la seguridad extremo a extremo que facilita la posibilidad de que el usuario gestione el nivel de seguridad deseado sin estar a disposición del operador de telefonía móvil.

En el desarrollo de la tesis y resultado de los estudios realizados se gestó el modelo de seguridad “IP”, este modelo es un modelo “teórico”, es decir, no siendo un modelo aplicable en el mercado en poco tiempo (uno de los requisitos fundamentales en el planteamiento del modelo de arquitectura de seguridad) se ha considerado como el modelo óptimo de seguridad que ofrece las mismas características que el modelo de seguridad de “WTLS sobre IP” y tiene una arquitectura mínima.

Se ha realizado también un seguimiento de las posibles decisiones a tomar en el proceso de implementación, por ello se ha planteado el tema de MTU(tanto para IPv4 como para IPv6) y el modelo matemático de MIP, que permite la comparación entre las posibles metodologías a utilizar en el uso de Movilidad IP. Tal y como ya se comentó en el capítulo correspondiente, “Movilidad IP aplicada a los Modelos de Arquitectura de Seguridad”, el resultado de la comparación entre las diferentes implementaciones de MIP es que a nivel de rendimiento la metodología mejor es MIPv6 con optimización de direccionamiento.

Otro hecho a considerar es que los estándares de telefonía móvil de EEUU y de Japón, difieren bastante de los estándares europeos. Este punto ha hecho aparecer las primeras voces que proclaman que el sistema estándar mundial no será UMTS sino un sistema de cuarta generación. Esto hace que sea más importante, si cabe, la creación del modelo de arquitectura de seguridad que permite mejorar la seguridad en los sistemas de segunda generación.

9.1 Aportaciones

La realización de esta tesis me ha permitido obtener conocimientos más extensos de tecnologías como UMTS, movilidad IP, WAP a la vez que me ha ofrecido la posibilidad de introducirme en el mundo de la telefonía móvil, aportándome una visión completa de la evolución de la misma, sobretodo a nivel de seguridad.

9.2 Trabajos futuros

Considero que la tesis “Modelos de Seguridad para móviles” podría tener una continuidad en el estudio de los estándares de EEUU y Japón y en la creación de una especificación de seguridad

para móviles que permita aunar los estándares de Europa, EEUU y Japón en una especificación única.

10 Anexo 1: Arquitectura UMTS

En esta sección se ofrece una visión general de UMTS, tanto desde el punto de vista de su arquitectura como de la funcionalidad asociada a cada nivel de su estructura.

10.1 Introducción

Al referirnos a la arquitectura de UMTS empleamos el término dominio para definir las diferentes partes físicas que la componen. Entre dos dominios relacionados se definen puntos de referencia.

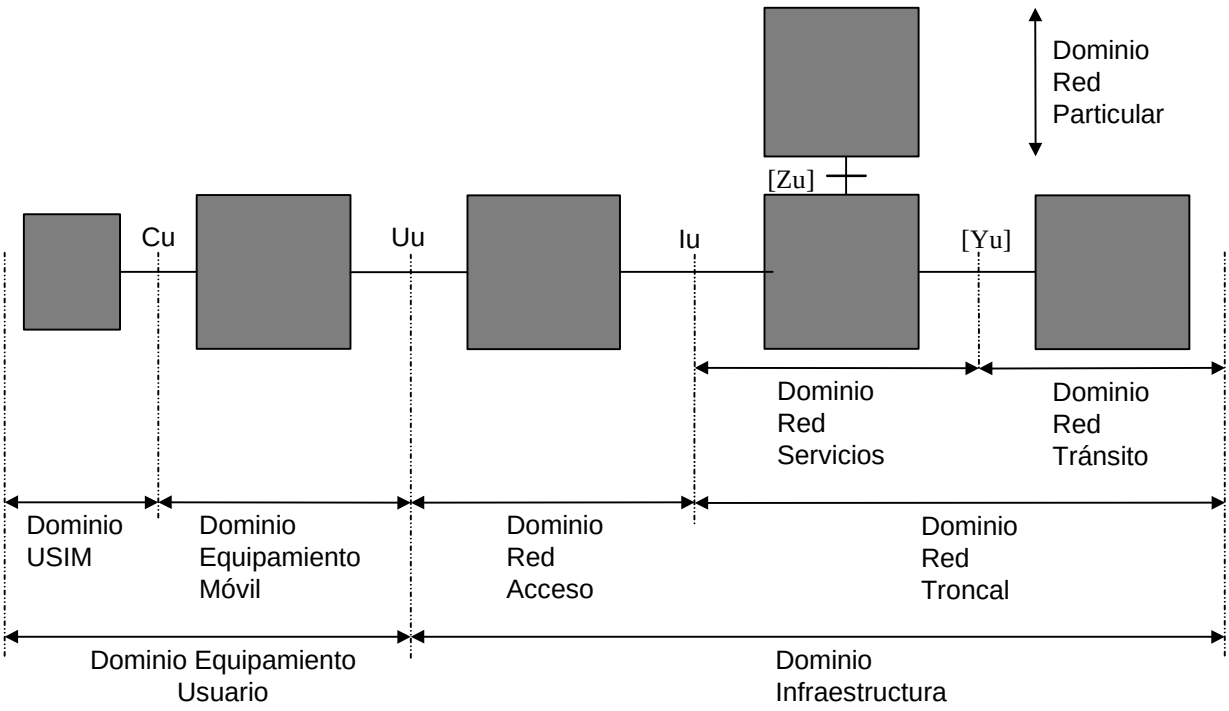


Figura 40. Dominios de UMTS y puntos de referencia

Tal y como se observa en la figura anterior la arquitectura se divide en dos dominios básicos, **Dominio de Equipamiento de Usuario**, es decir, el equipamiento utilizado por el usuario para acceder a los servicios UMTS, terminales y **Dominio de Infraestructura**, que consiste en dos nodos físicos que ofrecen aquellas funciones requeridas para incluir la interfaz de radio y soportar los requerimientos de los servicios de telecomunicación de los usuarios. Este dominio es un recurso compartido que provee servicios a todos aquellos usuarios autorizados dentro de su área de cobertura.

El punto de referencia entre ambos dominios es "Uu", interfaz de radio UMTS.

10.2 Dominio de Equipamiento de Usuario

Este dominio incluye una variedad de equipamientos con diferentes niveles de funcionalidad, estos equipos se denominan equipamientos de usuarios (terminales) y pueden asimismo ser compatibles con uno o más tipos de interfaces de acceso existentes (fijas o por radio). El dominio de equipamiento de usuario se subdivide en **Dominio de Equipamiento Móvil (ME)** y **Dominio del Módulo de Identificación de Servicios de Usuario (USIM).**

El punto de referencia entre estos dominios se denomina "Cu".

10.2.1 Dominio de Equipamiento Móvil

Este dominio ejecuta la transmisión por radio y contiene aplicaciones. El equipamiento móvil puede ser subdividido en diferentes entidades, por ejemplo. **Terminación Móvil (MT)** que ejecuta la transmisión por radio y las funciones relacionadas y **Equipamiento de Terminal (TE)** que contiene las aplicaciones extremo a extremo. Estos niveles se utilizan en la descripción funcional de las comunicaciones pero no se definen puntos de referencia entre ambos.

10.2.2 Dominio USIM

Este dominio contiene datos y funciones, en general registradas en una tarjeta específica, que de manera inequívoca y de forma segura le identifican. Este dispositivo se asocia a un usuario determinado y permiten su identificación independientemente del ME que utilice.

10.3 Dominio de Infraestructura

Este domino se divide en **Dominio de Red de Acceso**, en contacto con el Equipamiento de Usuario, y en **Dominio de Red Troncal**.

El dominio de Red de Acceso comprende principalmente las funciones específicas a las técnicas de acceso mientras que dominio de la red Troncal puede ser utilizado con flujos de información independientemente del modo de acceso.

El punto de referencia entre ambos dominios se denomina "Iu".

10.3.1 Dominio de Red de Acceso

Este dominio lo forman aquellas entidades físicas que gestionan los recursos de la red de acceso y que ofrecen al usuario mecanismos de ingreso al dominio de red troncal.

10.3.2 Dominio de Red Troncal

Este dominio está compuesto por aquellas entidades físicas que ofrecen soporte a las especificaciones de red y servicios de telecomunicaciones, incluyendo funcionalidades como la gestión de información de localización del usuario, control de las características de red y

servicios, mecanismos de transferencia (conmutación y transmisión) de señalización y de información generada por el usuario.

El dominio de red troncal se subdivide en Dominio de Red de Servicios, Dominio de Red Particular y Dominio de Red de Tránsito.

El punto de referencia entre el dominio de red de servicios y el dominio de red particular se denomina [Zu] y el punto de referencia entre el dominio de red de servicios y el dominio de red de tránsito [Yu].

10.3.2.1 Dominio de Red de Servicios

Es el dominio incluido dentro del dominio de Red Troncal al cual está conectado el Dominio de Red de Acceso. Contiene aquellas funciones que son locales al punto de acceso de usuario y aquellas cuya ubicación varía cuando el usuario se mueve. Es responsable de marcar la ruta de las llamadas y transportar la información / datos del usuario del origen al destino y de interactuar con el dominio particular para consultar datos / servicios específicos de usuario y con el dominio de tránsito para datos / servicios no específicos.

Las responsabilidades de este dominio incluyen las siguientes áreas:
- Ofrecer y gestionar recursos de radio asegurando la confidencialidad del tráfico de usuario.
- Ofrecer y gestionar recursos fijos, características portadoras, conexiones y rutas.
- Recuperar toda la información sobre el coste de los servicios ofrecidos y transmisión de dicha información al entorno particular y a otros operadores de red.
- Interacción con el dominio de entorno particular para identificar, autentificar, autorizar y ubicar a usuarios.

10.3.2.2 Dominio de Red Particular

Este dominio contiene aquellas funciones de la red troncal de ubicación permanente sin importar la localización del punto de acceso de usuario. El USIM se relaciona por suscripción con el dominio de red particular, que contiene la información específica del usuario y gestiona la información de suscripción. Asimismo puede ofrecer servicios específicos, potencialmente no pertenecientes al dominio de red de servicios.

Las responsabilidades de este dominio incluyen las siguientes áreas:
- Ofrecer, distribuir y gestionar las cuentas de suscripción.
- Ofrecer y mantener el servicio de perfiles de usuarios, incluyendo el control de acceso a dichos perfiles.
- Negociación con los operadores de red de las características necesarias para ofrecer servicios UMTS a usuarios.

10.3.2.3 Dominio de Red de Tránsito

Este dominio está localizado entre el dominio de red de servicios y la parte remota. Si para una llamada determinada la parte remota está localizada en la misma red que el UE origen entonces no se activa ninguna instancia del dominio de tránsito.

10.4 Funcionalidad de UMTS

En el aspecto funcional UMTS se divide en estratos cada uno de ellos comprendiendo uno o más dominios.

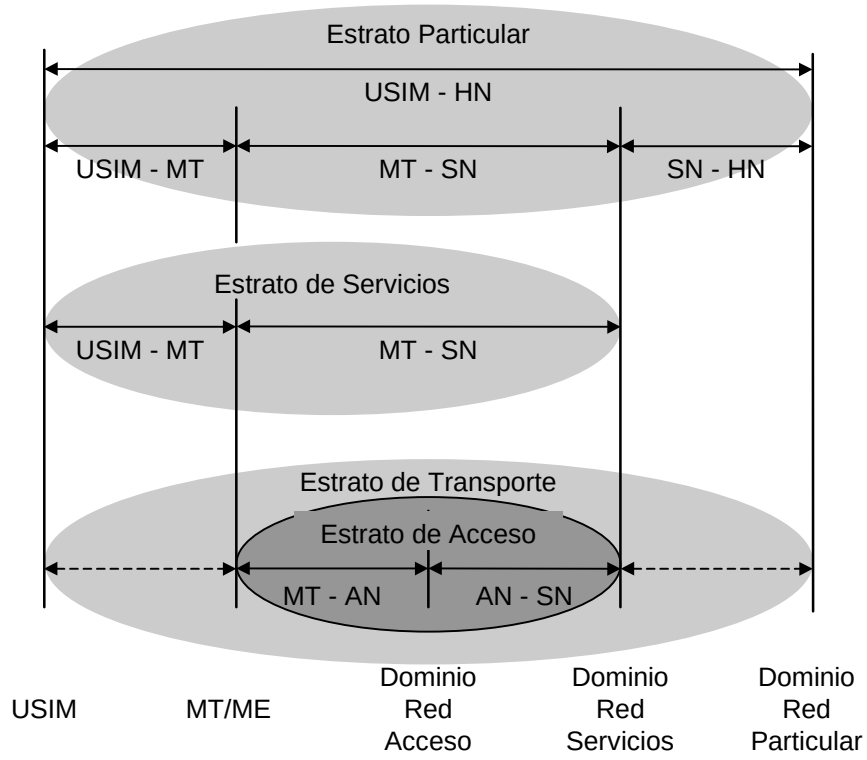


Figura 41. Flujos funcionales entre los dominios de USIM, MT/ME, Red de Acceso, Red de Servicios y Red Particular

Los estratos definidos, como puede observarse en la figura 2 y 3, son:

Estrato de Transporte,
Estrato de Servicios,
Estrato Particular y
Estrato de Aplicación

El estrato de Transporte incluye todos los dominios, el estrato de Servicio todos excepto el dominio particular, el Estrato Particular incluye los dominios de USIM, ME, Red de Acceso, Red de Servicios, Red Particular y el Estrato de Aplicación incluye los dominios de TE, MT, Red de Acceso, Red de Servicios, Red de Tránsito y la parte remota.

Los flujos directos entre dominios no contiguos, no conectados directamente, se transportan de forma transparente entre todos los dominios e interfaces situados entre el dominio origen y el de destino.

Las líneas punteadas indican que el protocolo utilizado no es específico de UMTS.

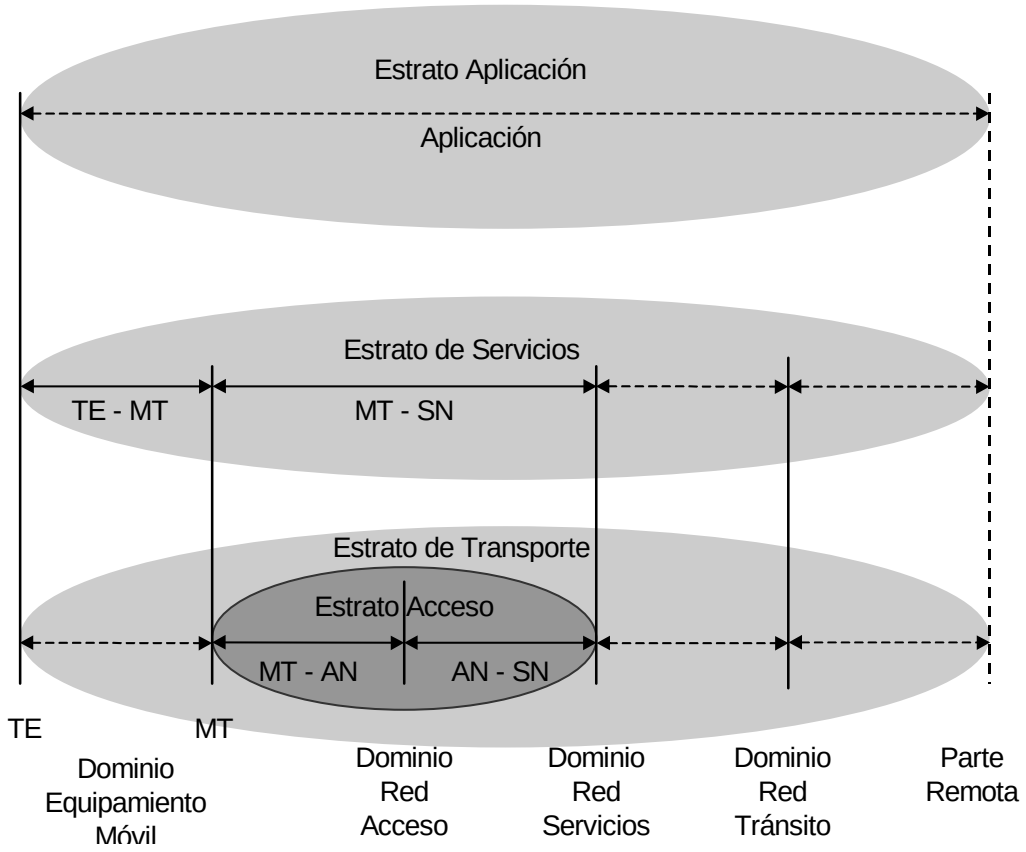


Figura 42. Flujos funcionales entre los dominios de TE, MT, Red de Acceso, Red de Servicios, Red de Tránsito y Parte Remota

La "Parte Remota" indica el usuario final o máquina destino de la transmisión.

10.4.1 Estrato de Transporte

Este estrato soporta el transporte de datos de usuario y la señalización de control de red de otros estratos hacia UMTS, incluyendo:

Formato de transmisión física utilizado,
Mecanismos de corrección de error y recuperación,
Mecanismos de adaptación de los datos al formato físico ofrecido (si es necesario) y,
Mecanismos de transformación de datos para un uso eficiente, por ejemplo,. interfaz de radio (si es necesario)

Puede incluir distribución de recursos y de rutas locales entre las diferentes interfaces.

Dentro del Estrato de Transporte se define el Estrato de Acceso, específico de UMTS, y que se ubica entre el nodo final del dominio de Red de Servicios y MT.

10.4.1.1 Estrato de Acceso

Es la agrupación funcional de las partes de la infraestructura y del equipamiento de usuario así como de los protocolos entre estas partes específicas de la técnica de acceso. Ofrece servicios relacionados con la transmisión de datos en la interfaz de radio y la gestión de ésta con otras partes de UMTS. Los protocolos considerados dentro del estrato de acceso son:

Terminación Móvil - Red de Acceso
Este protocolo permite la transmisión de información detallada relacionada con el acceso por radio para coordinar los recursos de radio entre MT y Red de Acceso

Red de Acceso - Red de Servicios
Este protocolo gestiona el acceso de la red de servicios a los recursos ofrecidos por la red de acceso, independientemente de la estructura de radio específica de la red de acceso.

10.4.1.1.1 SAPs del Estrato de Acceso

Los Puntos de Acceso a Servicio (SAPs) del estrato de acceso son:

GC (Control General)
Se utilizan para permitir a Red Troncal dar información y disponer de comandos no relativos a un usuario concreto o a funcionalidades (por ejemplo grupo de llamadas, conferencia) específicas. En general existe un SAP de Control General por punto de conexión AN/CN.

NT (Notificación)
Se utilizan para distribuir datos a determinados usuarios (diseminación).En general existe un SAP de Notificación por cada punto de conexión AN/CN.

DC (Control Dedicado)
Se utilizan para establecer conexiones con Equipamiento de Usuario específico y para intercambiar información relativa a estas conexiones. Se entiende por conexión una relación entre contextos temporales de AN y de CN, iniciada en el momento del establecimiento de la conexión y finalizada al acabar la conexión, independientemente del tipo de conexión (por ejemplo conexión por punto, grupo de conexiones,...)

En general existen un gran número de SAPs de Control General por punto de conexión AN/CN, identificados unívocamente por el SAPI, el cual se utiliza como identificador de la conexión.

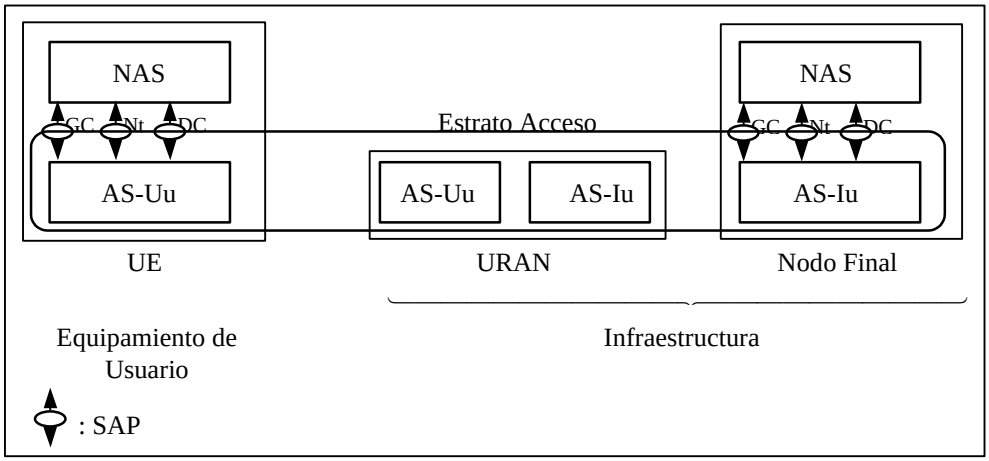


Figura 43. Puntos de Acceso a Servicios del Estrato de Acceso

10.4.2 Estrato de Servicios

Este estrato incluye los protocolos y funciones para definir la ruta y transmitir la información de usuario o de red, desde el origen hasta el destino, independientemente de que el origen y el destino estén el la misma o en diferentes redes. Las funciones relacionadas con servicios de telecomunicaciones están ubicadas en este estrato.

Los protocolos pertenecientes al estrato de servicio son:

USIM - Terminación Móvil
Este protocolo ofrece acceso a la información concreta de un suscriptor para funciones pertenecientes al dominio de equipamiento de usuario.

Terminación Móvil - Red de Servicios
Este protocolo ofrece acceso desde MT a los servicios del dominio de red de servicios.

Equipamiento de Terminal - Terminación Móvil
Este protocolo gestiona el intercambio de información de control entre el dominio TE y el dominio de MT.

10.4.3 Estrato Particular

Este estrato contiene los protocolos y funciones relacionados con la gestión y almacenamiento de la información de suscripción y opcionalmente de servicios específicos de la red particular. También incluye las funciones que permiten a otros dominios actuar sobre la red particular. Las funciones relacionadas con la gestión de los datos de suscripción, control de usuario (incluyendo facturación y cobro), gestión de movilidad y autenticación se ubican en este estrato.

El estrato particular incluye los siguientes protocolos:

USIM - Red Particular
Este protocolo gestiona la coordinación entre la información específica del suscriptor entre el USIM y la red particular.

USIM-MT
Este protocolo permite al dominio MT el acceso a información específica de usuario y a los recursos necesarios para actuar sobre la red particular.

MT - Red de Servicios
Este protocolo permite el intercambio de información específica de usuario entre el MT y la red de servicios.

Red de Servicios - Red Particular
Este protocolos permite a la red de servicios acceder a los datos y recursos de la red particular necesarios para actuar sobre HN, por ejemplo, comunicaciones de usuarios, servicios y características (incluyendo VHE[12]).

10.4.4 Estrato de Aplicación

Este estrato incluye los protocolos extremo a extremo y las funciones que utilizan los servicios ofrecidos por los estratos particular, de servicios y de transporte así como la infraestructura para soportar los servicios y / o servicios de valor añadido.

Las funciones extremo a extremo son aplicaciones utilizadas por los usuarios al final de / fuera de la red. Los usuarios, autorizados para estas aplicaciones, pueden acceder a ellas utilizando cualquier variedad disponible de equipamiento de usuario.

[12] El Entorno Particular Virtual (VHE) es un concepto para permitir la portabilidad de servicios personalizados independientemente de la red, del terminal (dentro de las capacidades del terminal) y de la ubicación del usuario.

11 Anexo2: Arquitectura General de una PLMN

En este apartado se presenta la estructura básica de una Red Móvil Terrestre Pública (PLMN). Ver figura.

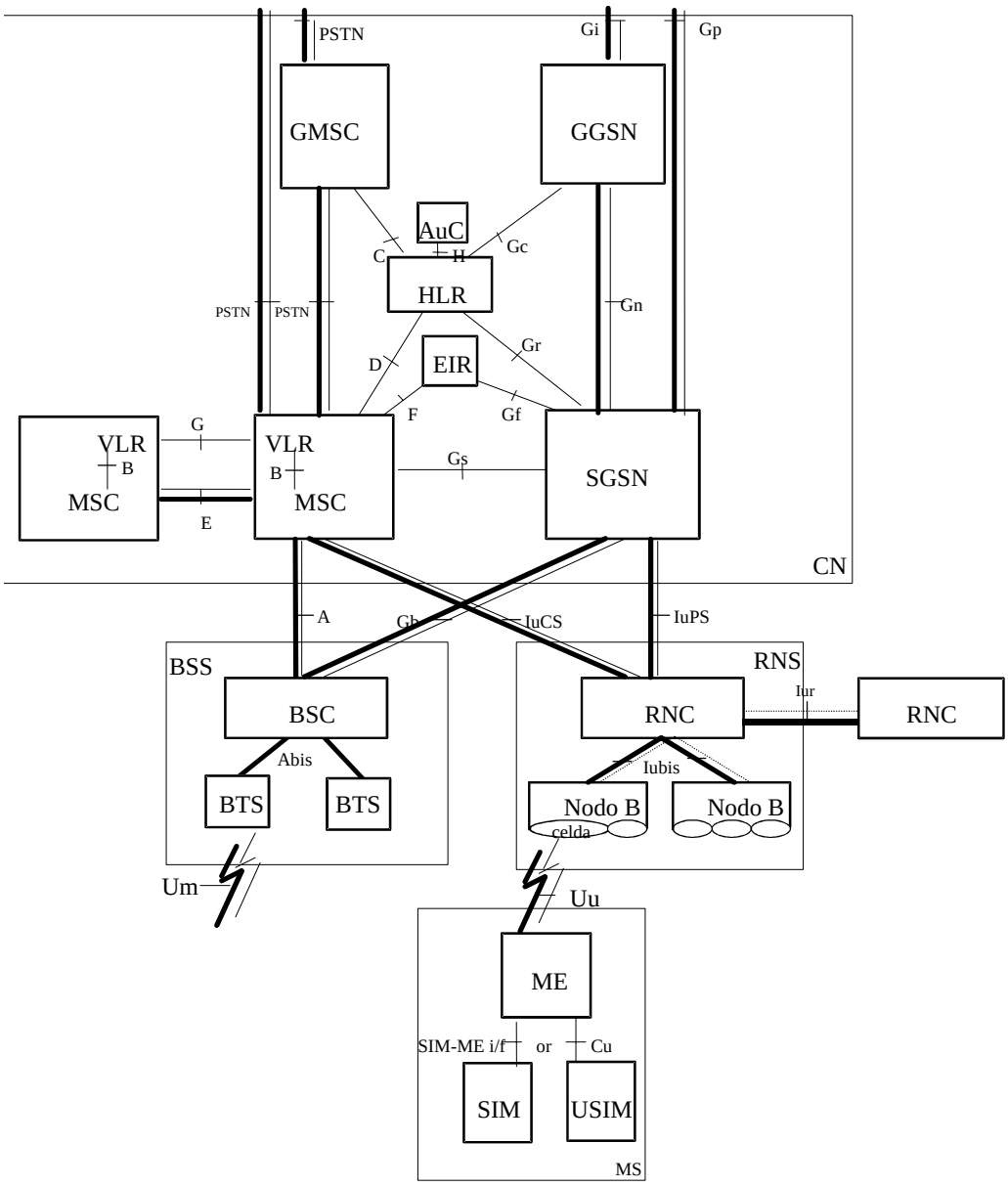


Figura 44. Configuración básica de una PLMN con servicios e interfaces CS y PS

Leyenda:

--- interfaces de señalización.

– interfaces de tráfico de usuario.

La configuración aquí diseñada muestra todas las interfaces de señalización posibles en una PLMN asociando cada funcionalidad a un equipo diferente. La implementación de la PLMN, puede hacer que un mismo equipo realice diversas funciones por lo que las interfaces serían internas.

11.1 Interfaces definidas

La implementación de los servicios móviles con distribución internacional obliga al intercambio de información entre los equipamientos implicados en el servicio.

11.1.1 Interfaces entre MS e Infraestructura fija

En este apartado se incluyen:

1. Interfaz entre MS y Sistema de Estación Base (BSS): **Um**

2. Interfaz entre MS y Sistema de Red de Radio (RNS): **Uu**

11.1.2 Interfaz entre CN y Red de Acceso

Se presentan cuatro interfaces básicas:

1. Interfaces entre el dominio CS y Red de Acceso

   1.1. Interfaz entre MSC y Sistema de Estación Base: ***A***

   Esta interfaz transporta información sobre el control de BSS, la gestión de llamadas y datos relativos a movilidad.

   1.2. Interfaz entre MSC y RNS: ***Iu_Cs***

   Esta interfaz transporta información sobre el control de RNS, la gestión de llamadas y datos relativos a movilidad

2. Interfaces entre el dominio PS y la Red de Acceso

   2.1. Interfaz entre SGSN y BSS: ***Gb***

   Esta interfaz tramita información relativa a gestión de movilidad y transmisión de paquetes de datos.

   2.2. Interfaz entre SGSN y RNS: ***Iu_PS***

11.1.3 Interfaces internas de Red de Acceso

En este apartado se incluyen tres tipos de interfaces.

1. Interfaz entre BSC y BTS. **Abis**

   Cuando BSS consiste en un Controlador de Estación Base (BSC) y una o más Estaciones Transmisoras Base (BTS), esta interfaz se utiliza para gestionar los servicios ofrecidos a los usuarios GSM y suscriptores

   También permite el control de equipamiento de radio y de la frecuencia de radio en BTS.

2. Interfaz entre RNC y Nodo B. **Iubis**

3. Interfaz entre dos RNCs: **Iur**

11.1.4 Interfaces internas de Red Troncal

Las interfaces definidas en esta sección son:

1. Interfaces internas del dominio CS

   1.1. Interfaz entre MSC y su VLR asociado: ***B***

   VLR es la base de datos para la gestión y ubicación de los suscriptores móviles en el área controlada por el MSC asociado. Cuando MSC necesita datos relativos a una estación móvil actualmente localizada en su área, obtiene la información necesaria de VLR. Si una estación móvil inicia la actualización de su localización es MSC quien informa a su VLR, el cual dispondrá de datos actuales. Asimismo cuando el suscriptor activa un servicio suplementario o modifica datos referentes a un servicio, MSC informa (a través de VLR) a HLR quien guarda dicha información y si es necesario, actualiza VLR.

   1.2. Interfaz entre HLR y MSC: ***C***

   La pasarela de MSC accede al HLR del suscriptor requerido para obtener información de ruta para una llamada o mensaje corto dirigido a este suscriptor.

   1.3. Interfaz entre HLR y VLR: D

   Esta interfaz se utiliza para intercambiar información relativa a la ubicación de la estación móvil y a la gestión del suscriptor. Para poder ofrecer el servicio de recepción de llamadas en todo el área, VLR y HLR intercambian datos cuando el suscriptor móvil requiere un servicio concreto, cuando quiere modificar datos de su suscripción o cuando algunos parámetros de la suscripción se modifican por medios administrativos.

1.4. Interfaz entre MSCs: ***E***

Cuando una estación móvil de un área MSC se mueve a otra durante una llamada, se debe ejecutar un procedimiento para poder continuar con la comunicación, es por ello que los MSCs involucrados en el proceso, deben intercambiar información y después realizar la operación de actualización de área.

1.5. *Interfaz entre MSC y EIR:* ***F***

La finalidad de esta interfaz es permitir que EIR obtenga el estado del IMEI de MS.

1.6. Interfaz entre VLRs: ***G***

Cuando un suscriptor móvil se cambia de área VLR, tiene lugar un Registro de Ubicación que puede incluir la obtención del IMSI y de los parámetros de autenticación del antiguo VLR. Estas operaciones están a cargo de la interfaz G.

2. Interfaces internas al dominio PS

2.1. Interfaz entre SGSN y HLR: ***Gr***

Esta interfaz se utiliza para intercambiar información relativa a la ubicación de la estación móvil y a la gestión del suscriptor. Para poder ofrecer el servicio de recepción de llamadas en toda el área, HLR y SGSN intercambian datos cuando el suscriptor móvil requiere un servicio concreto, cuando quiere modificar datos de su suscripción o cuando algunos parámetros de la suscripción se modifican por medios administrativos.

2.2. Interfaz entre SGSN y GGSN: ***Gn y Gp***

Su uso es ofrecer el servicio de movilidad entre SGSN y GGSN. La interfaz Gn se utiliza cuando GGSN y SGSN están en la misma PLMN y la interfaz Gp cuando están en diferentes PLMN. Gn / Gp también incluyen procesos para permitir a SGSN comunicar datos de usuario y de suscriptor cuando se cambia de SGSN.

La señalización de esta interfaz utiliza UDP / IP.

2.3. Camino de señalización entre GGSN y HLR: ***Gc***

Es opcional y es utilizado por GGSN para obtener información sobre ubicación y servicios a ofrecer al suscriptor móvil, a fin de ser capaz de activar una dirección de red para paquetes de datos.

2.4. Interfaz entre SGSN y EIR : ***Gf***

Esta interfaz se utiliza entre SGGN y EIR para el intercambio de datos y su finalidad es permitir a EIR verificar el estado del IMEI de MS.

3. Interfaces utilizadas por los dominios CS y PS

3.1. Interfaz entre MSC/VLR y SGSN : ***Gs***

Es una interfaz opcional que permite a SGSN enviar información de ubicación a MSC / VLR, y a éste enviar a SGSN peticiones de páginas o comunicarle que está ocupado en un servicio gestionado por MSC.

3.2. Interfaz entre HLR y AuC: ***H***

Esta interfaz es utilizada por HLR si al recibir una petición de autenticación y cifrado de datos de un suscriptor móvil no es capaz de encontrar una respuesta, entonces se realiza la petición a AuC.

El protocolo utilizado por esta interfaz no es estándar.

12Anexo 3: IPSec

En esta sección se reflejarán los fundamentos de la seguridad en redes IP, en particular se describirán los protocolos de seguridad, Cabecera de Autenticación (AH) y Seguridad de Encapsulamiento de Carga Útil (ESP), las Asociaciones de Seguridad, la Gestión de Claves (Protocolo de Intercambio de Claves de Internet, IKE) y los algoritmos definidos para los procesos de autenticación y encriptación.

IPSec, Especificación de Seguridad para IP, está diseñada para ofrecer interoperabilidad y seguridad basada en la criptografía para IPv4 y IPv6. Los servicios de seguridad ofrecen control de acceso, integridad no orientada a la conexión, autenticación del origen de los datos, protección contra reenvío y confidencialidad. Asimismo IPSec permite al usuario controlar el nivel de seguridad que ofrece un servicio, para ello incorpora formas de seleccionar que servicios de seguridad utilizar y con qué parámetros, los algoritmos criptográficos a usar y el grado de seguridad a aplicar.

Estos mecanismos de seguridad sólo se aplican a nivel de IP y ofrecen protección a nivel de IP y niveles superiores como pueden ser TCP o UDP. No interfieren con el uso de host, o elementos de red que no soporten IPSec y además están diseñados para ser independientes del algoritmo utilizado.

La implementación de IPSec se ubica en un host o en un entorno de pasarela seguro. La protección que ofrece se basa en unos requerimientos definidos por una Base de Datos Policía de Seguridad (SPD) o una aplicación y se clasifican los paquetes, dependiendo de la información de la cabecera de nivel de transporte y de IP, en paquetes descartados, paquetes con IPSec o paquetes sin IPSec.

12.1 Protocolos de Seguridad

IPSec dispone de dos protocolos para asegurar el tráfico:

- Cabecera de Autenticación (AH)

  Ofrece integridad no orientada a la conexión, autenticación del origen de los datos y un servicio opcional de protección contra reenvío.

- Seguridad de Encapsulamiento de Carga Útil (ESP)

  Ofrece confidencialidad por encriptación y confidencialidad de flujo de tráfico limitada, también al igual que AH dispone de servicios de integridad no orientada a la conexión, autenticación del origen de los datos y protección contra reenvío.

Ambos protocolos proporcionan control de acceso basado en la distribución de claves criptográficas y en la gestión de flujos de tráfico relativos a los protocolos de seguridad. Los dos pueden aplicarse solos o en combinación con otros protocolos.

Existen dos formas de uso para AH y ESP:

Modo transporte

En este caso el protocolo ofrece protección sobretodo a protocolos de niveles superiores.

Modo túnel

En este caso los protocolos se aplican a paquetes IP por túnel.

12.2 Asociaciones de Seguridad

Se entiende por Asociación de Seguridad (SA), en el contexto de IPSec, una conexión simple que ofrece servicios de seguridad para los datos transmitidos. Dichos servicios se ofrecen mediante los protocolos descritos anteriormente, AH y ESP, pero en el caso de desear aplicar ambos protocolos deben generarse dos, o más, SAs.

Una Asociación de Seguridad se identifica por un tripleto compuesto de:

1. Índice de Parámetros de Seguridad (SPI),
2. Dirección IP de destino[13]
3. Identificador de Protocolo de seguridad (AH, ESP)

Al igual que los protocolos, las Asociaciones de Seguridad disponen de dos tipos, modo transporte y modo túnel. En el modo transporte las SA son asociaciones de seguridad entre dos hosts, en este caso el protocolo ESP proporciona servicios a protocolos superiores y no para la cabecera de IP o extensiones de la cabecera previas a la cabecera ESP, AH sin embargo, proporciona protección a partes seleccionadas de la cabecera IP. En el modo túnel, la SA se aplica a un túnel IP.

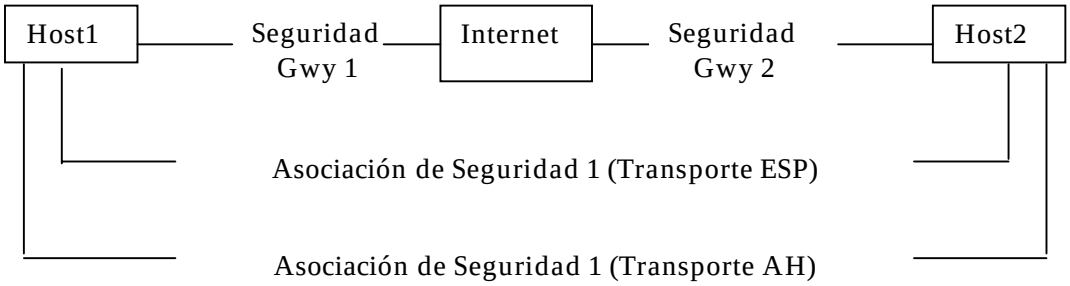
El conjunto de servicios de seguridad ofrecido por una SA depende del protocolo de seguridad seleccionado, del modo de la SA, de los extremos de la SA y de las preferencias de servicios opcionales del protocolo elegido. El protocolo de AH es adecuado si no se requiere confidencialidad, en el caso de necesitar confidencialidad debe escogerse el ESP recordando siempre que, el servicio de autenticación ESP no permite proteger todas las cabeceras IP.

12.2.1 Múltiples Asociaciones de Seguridad

Dependiendo de los servicios de seguridad a aplicar, a veces, es necesario utilizar más de una SA, por ejemplo si se desea aplicar AH y ESP. El conjunto de SA aplicadas a un flujo de datos se denomina Grupo de Asociaciones.

[13] Normalmente los mecanismos de IPSec de gestión de Asociaciones de Seguridad sólo están definidos para SAs sin diseminación.

Las Asociaciones pueden combinarse por transporte adyacente o por túnel iterado. El transporte adyacente se refiere a la aplicación de uno o más protocolos de seguridad al mismo datagrama IP sin utilizar túnel.



El túnel iterado se refiere a la aplicación de múltiples niveles de protocolos de seguridad sobre túnel IP. Permite diferentes niveles de anidamiento ya que cada túnel puede empezar o terminar en diferentes elementos de IPSec. Existen tres posibles configuraciones, aunque sólo la segunda y tercera opción son obligatorias en una implementación de IPSec:

1. Los extremos de las SAs son idénticos
2. Uno de los extremos de la SA es idéntico
3. Ninguno de los extremos es igual

12.2.2 Bases de Datos de IPSec

En la implementación de IPSec se requieren dos bases de datos diferentes, Base de Datos de Policía de Seguridad (SPD) y Base de Datos de Asociación de Seguridad (SAD), la primera especifica las políticas que determinan, por ejemplo, la disposición de todos los tráficos IP de entrada y salida de un host y la segunda contiene parámetros de las asociaciones de seguridad activas. Generalmente se requieren bases de datos de entrada y de salida separadas de SAD y SPD.

12.2.3 Gestión de Claves y Asociaciones de Seguridad

IPSec permite la gestión de claves y SAs de forma tanto automática como manual, la elección de una u otra opción puede influenciar en los servicios proporcionados por los protocolos de seguridad, por ejemplo, el servicio de protección de reenvío exige gestión automática de SAs.

Técnicas Manuales

Una persona de forma manual configura cada sistema con las claves y los datos de gestión de la asociación de seguridad

Técnicas Automáticas

El sistema automáticamente gestiona las claves de seguridad. El protocolo, por defecto, para la gestión de claves de forma automática es IKE, aunque pueden utilizarse otros protocolos.

12.3 Cabecera de Autenticación (AH)

Tal y como ya se ha comentado con anterioridad, el protocolo AH se utiliza para ofrecer integridad no orientada a la conexión, autenticación del origen de los datos para datagramas IP y protección contra reenvío[14]. Este último servicio puede ser seleccionado por el receptor al establecer una asociación de seguridad. Aquellos campos de la cabecera de IP que pueden ser modificados en el trayecto hasta el destino no se protegen con AH.

12.3.1 Ubicación de AH

AH puede utilizarse tanto en modo transporte como en modo túnel. En modo transporte se inserta después de la cabecera IP y antes del protocolo de nivel superior, por ejemplo TCP, o antes de cualquier otra cabecera de IPSec que ya este insertada en el mensaje. En el contexto de IPv4 esto se traduce por la ubicación de AH después de la cabecera de IP pero antes del protocolo de nivel superior.

Antes de aplicar AH			
Cabecera IP origen		TCP	Datos
Después de aplicar AH			
Cabecera IP origen	AH	TCP	Datos

Tabla 4. Ejemplo de AH en IPv4

En IPv6, AH se ve como un datagrama extremo a extremo y por lo tanto aparece después de las cabeceras de extensiones de salto-a-salto, direccionamiento y fragmentación. La cabecera de extensiones de opciones del destino puede ir tanto antes como después de AH.

Antes de aplicar AH					
Cabecera IP	Cabeceras de extensiones (si existen)	TCP	Datos		
Después de aplicar AH					
Cabecera IP	salto-a-salto,dest. (nota), direccionamiento, fragmentación	AH	Opciones dest. (nota)	TCP	Datos

Tabla 5. Ejemplo de AH en IPv6

nota: Si existen puede ser, antes de AH, después o ambos.

En modo túnel, la posición de AH, relativa a la cabecera de IP de salida, es la misma que la de AH en el modo de transporte.

[14] A partir de este punto el conjunto de servicios se denomina autenticación.

Después de aplicar AH				
Nueva cabecera IP	AH	Cabecera de IP origen	TCP	Datos

Tabla 6. Ejemplo de AH en IPv4 modo túnel

Después de aplicar AH						
Nueva cabecera IP	Cabeceras de extensiones (si existen)	AH	Cabecera de IP origen	Cabeceras de extensiones (si existen)	TCP	Datos

Tabla 7. Ejemplo de AH en IPv6 modo túnel

12.3.2 Algoritmos de Autenticación

Los algoritmos de autenticación empleados para el cálculo de ICV son específicos de la SA. Para conexiones punto-a-punto se incluyen algoritmos de MAC basados en la encriptación simétrica (por ejemplo DES) o en funciones de hash (por ejemplo MD5 o SHA-1) y en el caso de conexiones diseminadas, algoritmos de hash combinados con algoritmos de firma asimétricos.

12.3.3 Procesamiento de Paquetes "Salientes"

Para el procesamiento de paquetes “salientes” se efectúa el cálculo del Valor de Comprobación de Integridad.

12.3.3.1 Fragmentación

En el caso de requerirse fragmentación IP, ésta tiene lugar después del procesamiento de AH. En el caso de AH en modo transporte se aplica sólo a datagramas IP enteros (no a fragmentos), si un paquete IP al que se le ha aplicado AH se fragmenta durante la transmisión debe reensamblarse antes de procesar AH en el receptor. En modo túnel, el mecanismo de AH se aplica a un paquete IP que puede estar fragmentado.

12.3.4 Procesamiento de paquetes "Entrantes"

Si existe más de una cabecera / extensión de IPSec, el procesamiento de cada una de ellas ignora cualquier cabecera IPSec aplicada con posterioridad a la que se está procesando.

El reensamblaje se aplica con anterioridad al procesamiento de AH.

12.3.4.1 Asociaciones de Seguridad y procesamiento

Al recibir un paquete que contiene una Cabecera de Autenticación IP, el receptor determina la correspondiente SA, basándose en la dirección IP de destino, el protocolo de seguridad (AH) y el

SPI. La Asociación de Seguridad indica si el campo Número Secuencial debe considerarse, los algoritmos utilizados para calcular ICV y la clave para validar ICV.

Si no existe una SA válida para esta sesión, se descarta el paquete

Si el número secuencial es correcto, es decir, si es mayor que el último número secuencial válido recibido o es nuevo, se verifica ICV. El valor de este campo, se calcula sobre determinados campos del paquete, aplicando los algoritmos de autenticación especificados y comprobando que sea igual al codificado en el campo ICV de Datos de Autenticación, si esto es cierto el datagrama es válido sino se descarta.

12.3.5 Requerimientos de conformidad

Una implementación conforme con AH debe ofrecer, como mínimo, los siguientes algoritmos:

- HMAC con MD5
- HMAC con SHA-1

12.4 Seguridad por Encapsulamiento de Carga Útil(ESP

El protocolo ESP ofrece confidencialidad, integridad no orientada a la conexión, autenticación del origen de los datos para datagramas IP, protección contra reenvío y confidencialidad de flujo de tráfico limitado. El conjunto de servicios depende de las opciones seleccionadas al establecer la asociación de seguridad.

El servicio de confidencialidad puede seleccionarse independientemente del resto de servicios, de todas formas el uso de la confidencialidad sin integridad/autenticación permite ciertos ataques contra el tráfico. La autenticación del origen de los datos y la integridad no orientada a la conexión son servicios conjuntos[15] y se ofrecen como una opción a utilizar con/sin confidencialidad. El servicio contra reenvío puede seleccionarse sólo con autenticación. La confidencialidad de flujo de tráfico requiere la selección del modo túnel. Aunque la confidencialidad y la autenticación son servicios opcionales, al menos debe seleccionarse uno de ellos.

12.4.1 Ubicación de ESP

ESP puede utilizarse tanto en modo transporte como en modo túnel. En modo transporte se inserta después de la cabecera IP y antes del protocolo de nivel superior, por ejemplo TCP, o antes de cualquier otra cabecera de IPSec que ya este insertada en el mensaje. En el contexto de IPv4, esto se traduce por la ubicación de ESP después de la cabecera de IP pero antes del protocolo de nivel superior.

[15] A partir de este punto el conjunto de servicios se denomina autenticación.

Antes de aplicar ESP					
Cabecera IP			TCP	Datos	
Después de aplicar ESP					
Cabecera IP	Cabecera ESP	TCP	Datos	Cola ESP	ESP Auten.

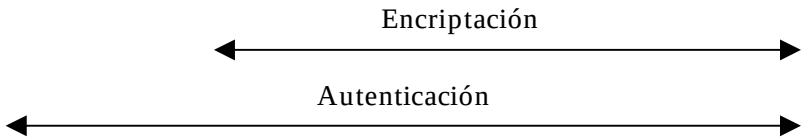


Tabla 8. Ejemplo de ESP en IPv4

En IPv6, ESP se ve como un datagrama extremo a extremo y por lo tanto aparece después de la cabeceras de extensiones de salto-a-salto, direccionamiento y fragmentación. La cabecera de extensiones de opciones para el destino puede ir tanto antes como después de ESP.

Antes de aplicar ESP							
Cabecera IP	Cabeceras de extensiones (si existen)		TCP		Datos		
Después de aplicar ESP							
Cabecera IP	salto-a-salto, dest (nota), direccionamiento, fragmentación	ESP	Opciones dest. (nota)	TCP	Datos	Cola ESP	ESP Auten.

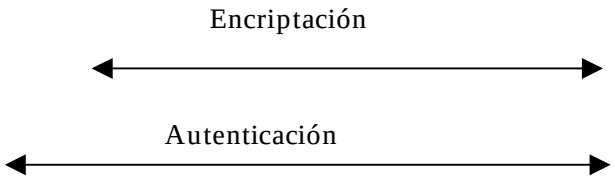


Tabla 9. Ejemplo de ESP en IPv6

nota: Si existen puede ser, antes de ESP, después o ambos.

En modo túnel, la posición de ESP, relativa a la cabecera de IP de salida, es la misma que la de ESP en el modo de transporte.

Después de aplicar ESP						
Nueva cabecera IP	ESP	Cabecera de IP origen	TCP	Datos	Cola ESP	ESP Auten.

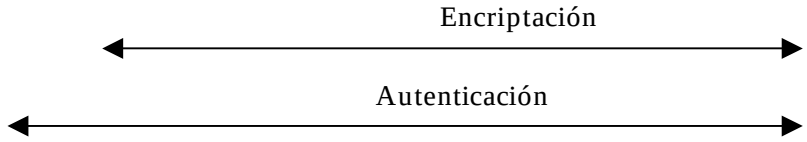


Tabla 10. Ejemplo de ESP en IPv4 modo túnel

Después de aplicar ESP								
Nueva cabecera IP	Cabeceras de extensiones (si existen)	ESP	Cabecera de IP origen	Cabeceras de extensiones (si existen)	TCP	Datos	Cola ESP	ESP Aut.

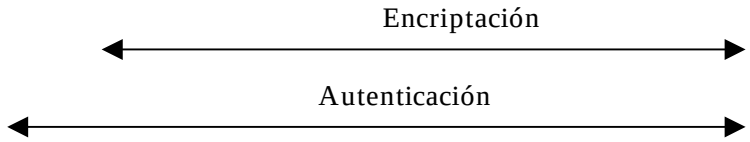


Tabla 11. Ejemplo de ESP en IPv6 modo túnel

12.4.2 Algoritmos de Autenticación

Los algoritmos de autenticación empleados para el cálculo de ICV son específicos de la SA. Para conexiones punto-a-punto se incluyen algoritmos de MAC basados en la encriptación simétrica (por ejemplo DES) o en funciones de hash (por ejemplo MD5 o SHA-1), en el caso de conexiones diseminadas, algoritmos de hash combinados con algoritmos de firma asimétricos.

12.4.3 Algoritmos de Encriptación

Los algoritmos de encriptación, que deben ser simétricos para ESP, son específicos de la SA. Debido a que los paquetes IP pueden llegar desordenados, cada paquete debe transportar la información necesaria para permitir al receptor establecer la sincronización criptográfica para la desencriptación. Estos datos pueden definirse en la parte del mensaje de carga útil, por ejemplo como un vector de inicialización, o pueden derivarse de la cabecera del paquete.

Los algoritmos de encriptación de ESP deben disponer de características para su aplicación en modo bloque o flujo.

12.4.4 Procesamiento de Paquetes "Salientes"

El protocolo ESP se aplica a un paquete saliente, sólo después de que IPSec determine que el paquete esta asociado a una SA que requiere ESP.

12.4.4.1 Encriptación de Paquetes

Se entiende que el servicio de "No confidencialidad" se ofrece utilizando el algoritmo de encriptación NULO.

Los pasos a seguir por el emisor en el proceso de encriptación son:

1. Encapsular (en el mensaje ESP):
   1.1. Para modo transporte: Información del protocolo de nivel superior
   1.2. Para modo túnel: todo el datagrama IP original
2. Añadir el relleno necesario
3. Encriptar el resultado (Datos de ESP, Relleno, Longitud de relleno y Siguiente Cabecera) utilizando la clave, el algoritmo de encriptación y el modo de algoritmo indicado por la SA y los datos de sincronización criptográfica si existen.

Si también se desea el servicio de autenticación, primero se ejecuta la encriptación y ésta no tiene en cuenta el campo de Datos de Autenticación. Este orden facilita la rápida detección y rechazo de paquetes no válidos antes de desencriptarlos.

12.4.4.2 Cálculo de Valor de Comprobación de Integridad

El ICV se calcula sobre el campo ESP excepto la información de Datos de Autenticación. En el caso de que la cadena sobre la que debe calcularse el ICV no sea un múltiplo del tamaño de bloque del algoritmo especificado, debe añadirse un relleno implícito al final del paquete ESP antes de efectuar el cálculo del ICV. Los octetos de relleno deben tener por valor cero y no se transmiten con el paquete.

12.4.4.3 Fragmentación

En el caso de requerirse fragmentación IP, ésta tiene lugar después del procesamiento de ESP. En el caso de ESP en modo transporte se aplica sólo a datagramas IP enteros (no a fragmentos), si un paquete IP al que se le ha aplicado ESP se fragmenta durante la transmisión debe reensamblarse antes de procesar ESP en el receptor. En modo túnel, ESP se aplica a un paquete IP que puede estar fragmentado.

12.4.5 Procesamiento de paquetes "Entrantes"

El reensamblaje se aplica con anterioridad al procesamiento de ESP.

12.4.5.1 Asociaciones de Seguridad y procesamiento

Al recibir un paquete que contiene una Cabecera de Autenticación IP, el receptor determina la correspondiente SA, basándose en la dirección IP de destino, el protocolo de seguridad (ESP) y el SPI. La Asociación de Seguridad indica si el campo Número Secuencial debe considerarse, si el campo Datos de Autenticación debe estar presente y cuales serán los algoritmos y las claves utilizados para desencriptar y calcular ICV, si fuera necesario.

Si no existe una SA válida para esta sesión, se descarta el paquete

En el caso de aplicar el servicio de autenticación y el de protección contra reenvío, si el número secuencial es correcto, es decir es mayor que el último válido recibido o es nuevo, se verifica ICV. El valor de este campo se calcula sobre los campos de ESP excepto el campo Datos de Autenticación aplicando el algoritmo de autenticación especificado y comprobando que sea igual al codificado en el campo ICV de Datos de Autenticación, si esto es cierto el datagrama es válido sino se descarta.

12.4.5.2 Desencriptación de Paquetes

Se entiende que el servicio de "No confidencialidad" se ofrece utilizando el algoritmo de encriptación NULO.

Los pasos a seguir por el emisor en el proceso de encriptación son:

1. Desencriptar los campos: Datos de ESP, Relleno, Longitud de relleno y Siguiente Cabecera, utilizando la clave, el algoritmo de encriptación y el modo de algoritmo indicado por la SA y los datos de sincronización criptográfica si existen.
2. Procesar cualquier información de relleno tal y como define la especificación del algoritmo de encriptación
3. Reconstruir el datagrama IP original:
   3.1. Para el modo transporte: la cabecera IP original más la información del protocolo de nivel superior en el mensaje de ESP
   3.2. Para el modo túnel: la cabecera IP y el datagrama IP entero en el mensaje de ESP

12.4.6 Requerimientos de conformidad

Una implementación conforme con ESP debe ofrecer los siguientes algoritmos:

- DES en modo CBC
- HMAC con MD5
- HMAC con SHA-1
- Algoritmo de Autenticación NULO
- Algoritmo de Encriptación NULO

12.5 ISAKMP

Los protocolos descritos con anterioridad (ESP, AH) se engloban dentro del Protocolo de Gestión de Claves y Asociaciones de Seguridad de Internet (ISAKMP), este protocolo define los procedimientos para autenticar entidades en comunicación, creación y gestión de asociaciones de seguridad y técnicas de generación de claves. Es decir, todos los procesos necesarios para establecer y mantener comunicaciones seguras, con servicios de seguridad IP u otros, en Internet.

Las asociaciones de seguridad ofrecen / soportan diferentes algoritmos de encriptación, de autenticación y de establecimiento de claves así como certificados de host para protocolos de nivel inferior y certificados de usuarios para protocolos de niveles superiores.

En el paso inicial se fijan una serie de atributos / parámetros de seguridad, tales como método de autenticación o método de intercambio de claves. Una vez se han establecido estos parámetros se procede a la autenticación y a la generación de las claves requeridas.

ISAKMP puede implementarse sobre cualquier protocolo de transporte o sobre IP.

12.5.1 Autenticación

Los mecanismos de autenticación se clasifican en: *débiles*, mecanismos fácilmente eliminados (incluyendo la posibilidad de no encriptar la información) o *fuertes*, mecanismos difíciles de evitar, por ejemplo RSA, DSS.

Los requerimientos de autenticación de ISAKMP son el uso de mecanismos fuertes y la utilización de firma digital.

12.5.2 Intercambio de Claves

En el tema del Establecimiento de claves existen dos métodos: Transporte y Generación. En el método de transporte se genera una clave de forma aleatoria, se encripta utilizando mecanismos de clave pública y se envía al receptor, así emisor y receptor comparten la misma clave. El método de generación involucra ambas entidades, cada una de ellas combina la información pública de la entidad contraria con su clave secreta de forma que comparten un valor secreto sólo conocido por las entidades en comunicación.

La autenticación del Intercambio de claves puede hacerse durante el protocolo o al finalizar el mismo. La autenticación durante el protocolo se realiza cuando ambas partes ofrecen pruebas de que conocen la clave secreta durante el intercambio de datos del protocolo. Si la autenticación tiene lugar después de la finalización del protocolo, ésta se realiza en comunicaciones posteriores.

El requerimiento de este servicio para ISAKMP es ofrecer un intercambio de claves autentificado.

12.5.3 Otros servicios

ISAKMP además ofrece protección contra diferentes ataques como pueden ser:

Denegación de servicio

Utilizando un valor (ACT).

Secuestro de la Conexión

Este ataque se repele mediante la asociación de los intercambios de autenticación, intercambio de claves y asociaciones de seguridad.

Interceptación o Modificación de mensajes

12.5.4 Negociación de ISAKMP

Inicialmente se establece una asociación de seguridad ISAKMP entre dos entidades y fijan las características de los servicios de seguridad a aplicar, es lo que se denomina "primera fase" de la negociación. El siguiente paso, "segunda fase" es el establecimiento de las asociaciones de seguridad para los protocolos acordados en la primera fase.

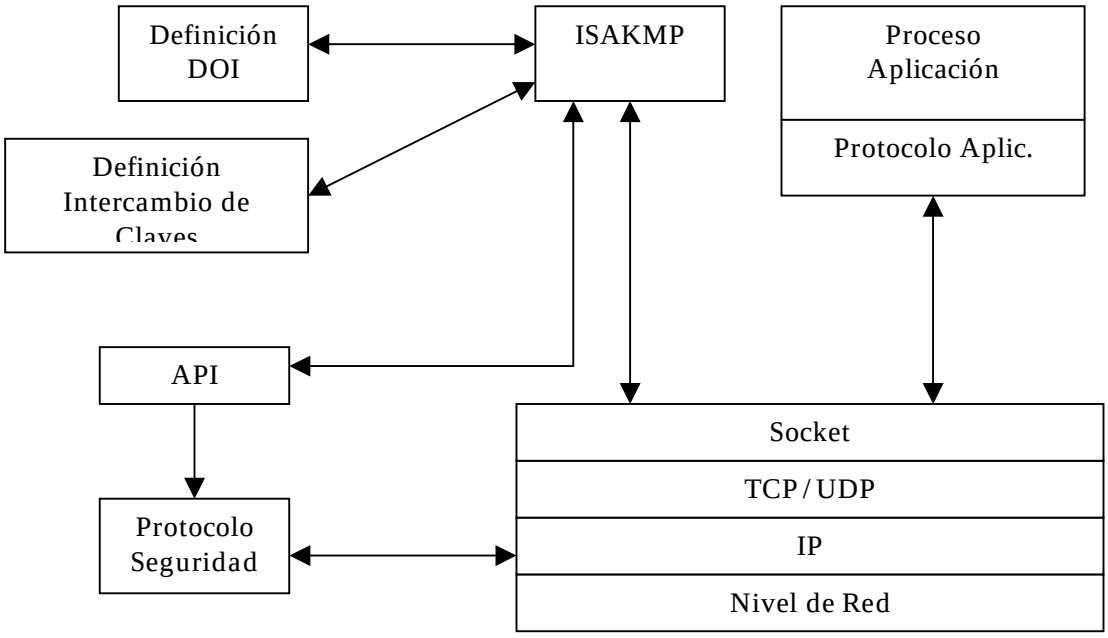


Figura 45. ISAKMP

En la primera fase una entidad asume el rol de iniciador / emisor y la otra el de respondedor / receptor, pero una vez establecida la SA, ambas entidades pueden iniciar la negociación de la segunda fase.

El iniciador emite un mensaje con todas las propuestas, que considera adecuadas según su política de seguridad, en orden de preferencia decreciente. Una vez el emisor recibe la información, éste elige aquella propuesta que mejor se adapta a su política de seguridad y notifica al emisor su selección.

12.5.5 Mensajes de ISAKMP

La cabecera contiene una estructura fija seguida de un número variable de campos. La parte fija contiene la información necesaria para mantener el estado, procesar el datagrama y prevenir, generalmente, la negación de servicio o el reenvío de datos. En los apartados posteriores puede consultarse el formato de los mensajes.

Los campos más destacados son:

- Campo de Asociación de Seguridad : Permite negociar los atributos de seguridad y el DOI asociado a la SA.
- Campo de Propuesta: Como su nombre indica, contiene los mecanismos de seguridad a negociar.
- Campo de Transformación: Información sobre un mecanismo de seguridad concreto.
- Campo de Intercambio de Claves: Define los mecanismos o técnicas utilizados para el Intercambio de claves.
- Campo de Identificación: Contiene información identificativa del DOI.
- Campo de Certificación: De acuerdo con su nombre, se usa para la transmisión de certificados.
- Campo de Petición de Certificado: Mecanismo de petición de certificados.
- Campo de Hash: Datos generados a partir de la aplicación de la función de hash sobre un mensaje.
- Campo de Firma: Firma digital de un mensaje.
- Campo de Número: Genera números aleatorios.
- Campo de Notificación: Transmisión de información entre entidades.
- Campo de Eliminación: Se utiliza para eliminar una SA.
- Campo de Identificador de vendedor: Fija el vendedor.

12.5.6 Intercambios de ISAKMP

En esta sección se describen los procedimientos para el establecimiento de SA y la modificación de las SAs.

El protocolo de Gestión de Claves y Asociaciones de Seguridad de Internet permite el intercambio de mensajes para el establecimiento de una SA y las claves de seguridad asociadas. Existen cinco Tipos de Intercambio definidos en ISAKMP, estos definen el contenido y el orden de los mensajes durante la comunicación.

Los tipos de intercambio definidos son:

- Intercambio Básico
- Intercambio de Protección de Identidad
- Intercambio sólo de Autenticación
- Intercambio Agresivo
- Intercambio Informativo

Para la especificación de los Tipos de Intercambio se aplica la siguiente notación:

HDR Cabecera de ISAKMP cuyo tipo de intercambio define el orden de los campos

SA	Campo de negociación de SA con uno o más campos de Propuesta o Transformación
KE	Campo de Intercambio de Claves
IDx	Campo de identificación para "x". Los posibles valores de x son:

Tipo	**Valor**
Iniciador	ii
Respondedor	ir
Usuario Iniciador (proxy)	ui
Usuario Respondedor (proxy)	ur

HASH	Campo de Hash
SIG	Campo de Firma
AUTH	Mecanismo de autenticación genérico
NONCE	Campo de Número
'*'	Encriptación del campo después de la cabecera ISAKMP
→	Comunicación iniciador - respondedor
←	Comunicación respondedor - iniciador

Establecimiento de Asociaciones de Seguridad

Las Asociaciones de Seguridad de Propuesta y Transformación se utilizan para construir mensajes ISAKMP para la negociación y establecimiento de SAs. El mensaje de establecimiento de una asociación de seguridad consiste en un campo de asociación, uno o más campos de Propuesta y uno o más campos de Transformación ligados a cada campo del tipo Propuesta.

Una Propuesta ofrece a la entidad iniciadora la capacidad de presentar a la entidad receptora los protocolos de seguridad y los mecanismos de seguridad a negociar.

La Transformación ofrece múltiples mecanismos o transformaciones para un protocolo determinado. La Propuesta identifica el protocolo y la Transformación los mecanismos aceptables para dicho protocolo.

La entidad receptora del mensaje de Asociación de Seguridad debe enviar un mensaje de Asociación de Seguridad con la Propuesta seleccionada, que pueden ser uno o más mensajes de Propuesta con un único campo de Transformación asociado. La entidad iniciadora debe verificar que los mensajes enviados se corresponden con alguno de los enviados inicialmente.

Modificación de Asociación de Seguridad

La modificación de una Asociación de Seguridad dentro del protocolo ISAKMP se reduce a la creación de una nueva SA y a iniciar las comunicaciones con esa nueva Asociación de Seguridad. La eliminación de la SA vieja se realiza una vez se ha establecido la nueva SA.

12.5.6.1 Intercambio Básico

Este tipo de Intercambio permite la transmisión conjunta de información relativa al Intercambio de Claves y de Autenticación. No ofrece protección de la identidad de las entidades involucradas en la comunicación.

En el primer mensaje el iniciador genera una propuesta adecuada a su política de seguridad. El campo de Asociación de Seguridad está compuesto por los mensajes de Asociación de Seguridad, Propuesta y Transformación.

En el segundo mensaje el receptor indica la selección realizada con la Asociación de Seguridad, la Propuesta y la Transformación.

El tercer y cuarto mensaje se utilizan para transmitir información sobre el intercambio de claves a fin de llegar a compartir un secreto común. Esta información se transmite con autenticación.

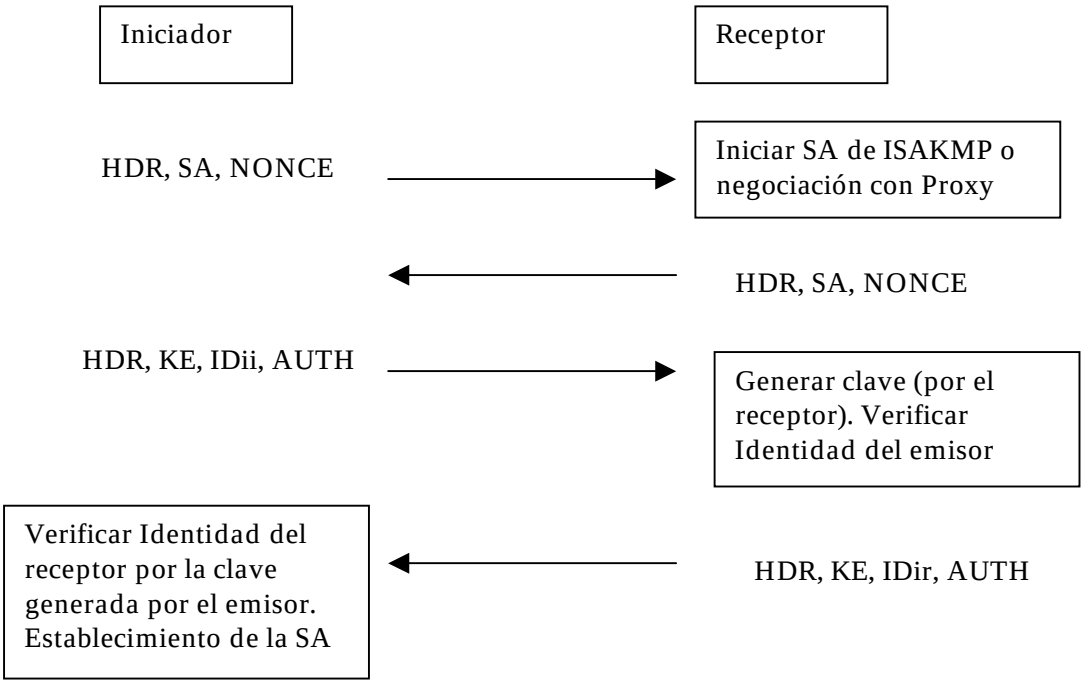


Figura 46. Diagrama de Intercambio Básico

12.5.6.2 Intercambio de Protección de Identidad

Este Intercambio ofrece la protección de la identidad de las entidades en comunicación separando la información sobre Intercambio de Claves, de la información relativa a Identidad y Autenticación.

En el primer mensaje el emisor genera una Propuesta adecuada a su política de seguridad. El mensaje de la Asociación de Seguridad está compuesto por los campos de Asociación de Seguridad, Propuesta y Transformación.

En el segundo, el receptor indica la selección realizada con la Asociación de Seguridad, la Propuesta y la Transformación.

El tercer y cuarto mensaje se utilizan para el transmitir información sobre el intercambio de claves a fin de llegar a compartir un secreto común.

En el quinto y sexto mensaje, emisor y receptor transmiten información de identificación y los resultados de la función de autenticación acordada.

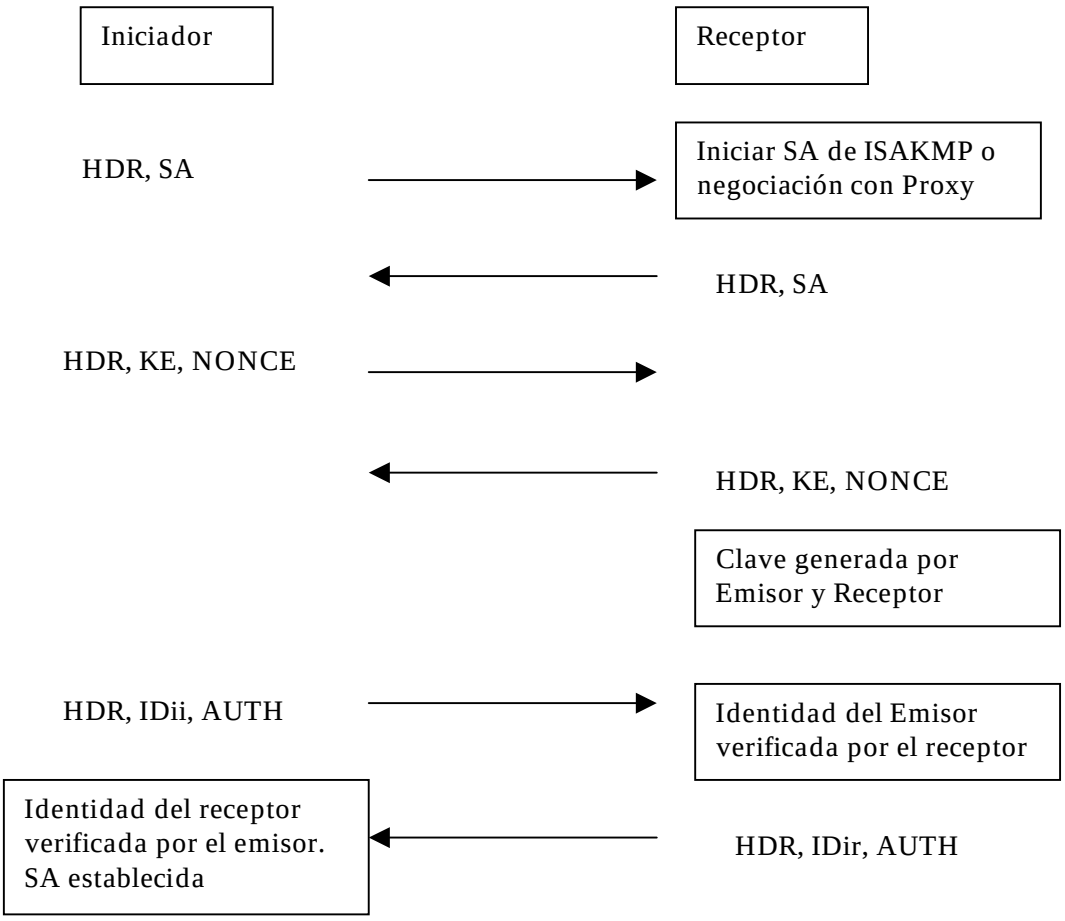


Figura 47.Intercambio de Protección de Identidad

12.5.6.3 Intercambio sólo de Autenticación

El Intercambio sólo de Autenticación como su nombre indica, solamente permite la transmisión de información de autenticación. Los datos transmitidos durante este proceso no están encriptados.

En el primer mensaje el emisor genera una Propuesta adecuada a su política de seguridad.

En el segundo el receptor indica la selección efectuada con los campos de Asociación de Seguridad, Propuesta y Transformación.

En el tercer mensaje el emisor transmite la información de la identidad, protegida con la función de autenticación acordada.

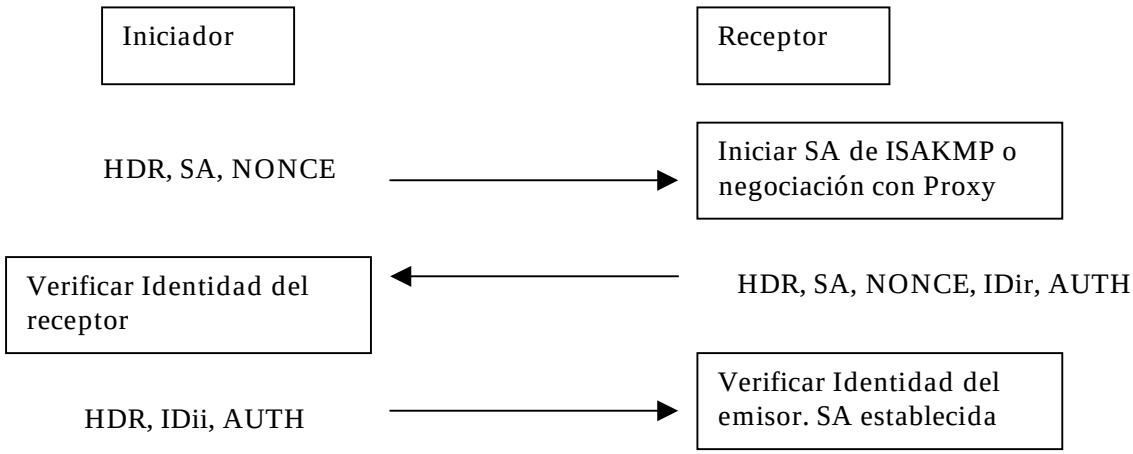


Figura 48. Intercambio sólo de Autenticación

12.5.6.4 Intercambio Agresivo

Este tipo de intercambio permite la transmisión conjunta de mensajes de Asociación de Seguridad, Intercambio de Claves y Autenticación.

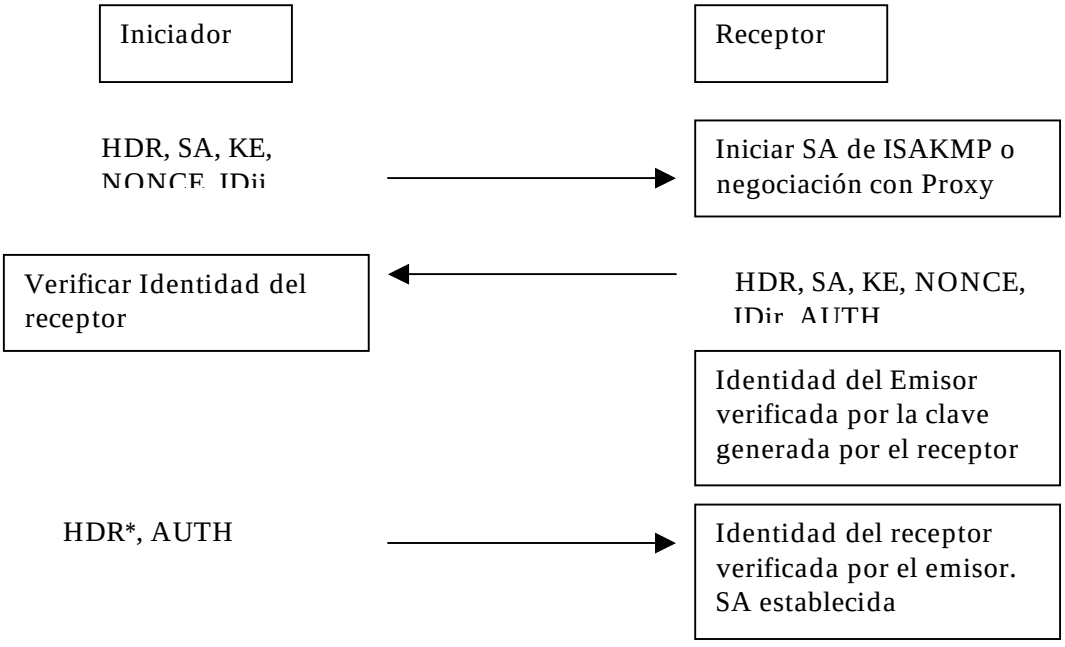


Figura 49. Intercambio Agresivo

En el primer mensaje el emisor genera una Propuesta adecuada a su política de seguridad. El mensaje de la Asociación de Seguridad está compuesto por los campos de Asociación de Seguridad, Propuesta y Transformación.

En el segundo mensaje el receptor indica la selección realizada con los campos de Asociación de Seguridad, Propuesta y Transformación.

En el tercer mensaje el emisor transmite los resultados de la función de autenticación acordada.

12.5.6.5 Intercambio Informativo

Consiste en la transmisión de datos utilizados para la gestión de la asociación de seguridad.

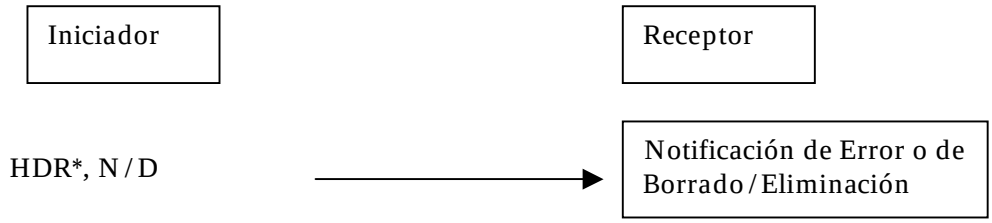


Figura 50. Intercambio Informativo

En el mensaje, el emisor o el receptor transmiten un mensaje de Notificación ISAKMP o de Eliminación.

12.6 IKE

ISAKMP describe un entorno para la autenticación e intercambio de claves pero no define estos procesos. El Protocolo de Gestión de Claves y Asociaciones de Seguridad de Internet está diseñado para ser independiente del intercambio de claves utilizado.

El protocolo de Intercambio de Claves de Internet (IKE), define un mecanismo para obtener claves autenticadas para utilizar con ISAKMP y otras asociaciones de seguridad como AH y ESP.

IKE soporta el modo cliente, es decir, permite que las entidades negociadoras no sean las entidades finales para las cuales está teniendo lugar la negociación de la asociación de seguridad. De esta forma, la identidad de los entidades finales no es conocida.

Los diferentes tipos de intercambios se definen como modos y operan en una de las dos fases de ISAKMP. La primera fase, llamada Asociación de Seguridad de ISAKMP, se produce cuando dos entidades desean establecer un canal autenticado seguro por el cual comunicarse. En esta fase se utiliza el “Modo Principal” y el “Modo Agresivo”. La segunda fase permite la negociación de la SA sobre servicios como IPSec u otros servicios que necesiten del intercambio de claves y / o de negociación de parámetros. En esta fase se utiliza el “Modo Rápido”. Existe otra forma

denominada “Modo de Grupo Nuevo” que no es realmente de fase 1 o de fase 2 pero obligatoriamente debe ejecutarse después de la fase 1 y permite establecer un nuevo grupo que puede ser utilizado en negociaciones futuras.

La SA de ISAKMP es bidireccional, es decir, una vez establecida cualquier parte puede iniciar los intercambios de “Modo Rápido”, Informativo o “Nuevo Grupo”. Una única fase 1 puede servir para varias fases 2, además una negociación de fase 2 puede requerir de múltiples SAs.

En la fase 1 el “Modo Principal”, ofrece protección de identidad, en el caso de no ser necesaria, puede utilizarse el “Modo Agresivo”. En el caso de utilizar encriptación por clave pública para autenticación en “Modo Agresivo”, éste también proporciona protección de identidad.

IKE utiliza los siguientes atributos y todos ellos se negocian como parte de la SA de ISAKMP:

- algoritmo de encriptación
- algoritmo de hash
- método de autenticación
- información sobre uso del grupo Diffie-Hellman

opcionalmente también puede negociarse una función pseudoaleatoria (PRF), en caso de no negociarla, se utiliza la versión de HMAC del algoritmo de hash como función pseudoaleatoria. Todas las implementaciones de IKE deben aceptar los siguientes valores de atributos:

- DES en modo CBC
- MD5 y SHA
- Autenticación a partir de claves precompartidas
- MODP sobre grupo por defecto número 1

y deberían aceptar también:

- 3DES para encriptación
- Tiger para hash
- Firma Digital Estándar
- Firmas RSA y autenticación con encriptación con clave pública RSA
- MODP número 2

12.6.1 Intercambios

12.6.1.1 Notación

En este apartado se utilizará la siguiente notación:

HDR	Cabecera de ISAKMP
HDR*	Encriptación de información de la cabecera de ISAKMP
<P>_b	Cuerpo del mensaje
SAi_b	Cuerpo de todo el mensaje de la SA (menos la cabecera genérica de ISAKMP)
CKY-I, CKY-R	Cookie Iniciador, Cookie Respondedor respectivamente

g^xi, g^xr	Valores públicos de Diffie-Hellman para iniciador, respondedor respectivamente
g^xy	Clave secreta compartida de Diffie-Hellman
KE	Mensaje de intercambio de clave que contiene la información pública transmitida en un intercambio Diffie-Hellman
Ni,Nr	Mensaje de número de iniciador, respondedor respectivamente
IDii, IDir, IDui, IDur	Mensaje de identificación durante la fase 1 de negociación para el iniciador y el respondedor (ii, ir) respectivamente; o mensaje de identificación durante la fase 2 para el usuario iniciador y el respondedor (ui,ur) respectivamente
SIG	Mensaje de firma
CERT	Mensaje de certificado
HASH, HASHx	Mensaje de hash. x es cualquier carácter adicional ej HASH_I
prf(key,msg)	Función pseudoaleatoria para generación de claves y autenticación
SKEYID	Cadena derivada a partir de la información del material de claves secreto, conocido sólo por los interlocutores
SKEYID_e	Material de clave utilizado por la SA de ISAKMP para proteger la confidencialidad de sus mensajes
SKEYID_a	Material de clave utilizado por ISAKMP para autenticar mensajes
SKEYID_d	Material de clave utilizado para derivar claves de SA no ISKAMP
<x>y	Notificación de elemento x encriptado con clave y
-->	Comunicación iniciador – respondedor
<--	Comunicación respondedor – iniciador
x | y	Concatenación de información x con información y
[x]	Notificación de que x es opcional

12.6.1.2 Intercambios de IKE

Tal y como se ha comentado anteriormente, existen dos métodos básicos utilizados para establecer un intercambio de clave autenticada: el “Modo Principal” y el “Modo Agresivo”. Cada uno de ellos genera material de claves autenticado de un intercambio Diffie-Hellman.

Todas las implementaciones de IKE deben implementar el Modo Principal y se recomienda la implementación del Modo Agresivo. Asimismo el Modo Rápido debe estar implementado como mecanismo para generar refresco de clave y para negociar servicios de seguridad no ISAKMP. El Modo Nuevo Grupo debería estar incluido en la implementación a fin de permitir definir grupos privados para intercambio Diffie-Hellman.

El intercambio de información se realiza de acuerdo con la sintaxis y los parámetros definidos para ISAKMP. El Modo Principal es una instancia del Intercambio de Protección de Identidad de ISAKMP. Los primeros dos mensajes negocian la política de seguridad, los dos mensajes siguientes transmiten los valores públicos de Diffie-Hellman y los datos necesarios para el intercambio y, finalmente los dos últimos mensajes autentican el intercambio Diffie-Hellman.

De forma similar, el Modo Agresivo es una instancia del Intercambio Agresivo de ISAKMP. Los dos primeros mensajes negocian la política de seguridad, intercambian los valores públicos de Diffie-Hellman, la información necesaria para el intercambio y las identidades. Además el

segundo mensaje autentica al contestador. El tercer mensaje autentica al iniciador del intercambio y ofrece una prueba de su participación en el proceso.

Los intercambios de mensajes en IKE tienen un número definido de mensajes, así la petición de un certificado nunca debe sobrepasar el número fijado de mensajes.

El Modo Rápido y el Modo Nuevo Grupo, no tienen análogo en ISAKMP.

Con los Modos Principal y Agresivo puede optarse entre cuatro métodos de autenticación diferentes:

- firma digital,
- autenticación con encriptación con clave pública (2 formas),
- clave precompartida

El valor de SKEID se calcula de forma diferente dependiendo del método de autenticación:

- Firma digital: SKEYID = prf (Ni_b | Nr_b, g^xy)
- Encriptación con clave pública: SKEYID = prf(hash(Ni_b | Nr_b), CKY-I | CKY-R)
- Claves precompartidas: SKEYID = prf(clave precompartida, Ni_b | Nr_b)

El resultado de los Modos Principal y Agresivo es un conjunto de tres grupos de material de claves de autenticación:

- SKEYID_d = prf(SKEYID, g^xy | CKY-I | CKY-R | 0)
- SKEYID_a = prf(SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
- SKEYID_e = prf(SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)

y un acuerdo sobre la política a aplicar para proteger las comunicaciones.

Los valores 0, 1 y 2 se representan en un octeto. La clave utilizada para encriptación se deriva a partir de SKEYID_e dependiendo del algoritmo a utilizar.

Para autentificar cada intercambio el iniciador del protocolo genera HASH_I y la entidad paralela genera HASH_R:

- HASH_I = prf(SKEYID, g^xi | g^xr | CKY-I | CKY-r | SAi_b | IDii_b)
- HASH_R = prf(SKEYID, g^xr | g^xi | CKI-R | CKY-I | SAi_b | IDir_b)

En el caso de autenticación con firmas digitales, HASH_I y HASH_R se firman y se verifican. Para la autenticación con clave pública o clave precompartida, HASH_I, HASH_R directamente autentifican el intercambio. Se ejecuta la función de hash para el campo de ID (excluyendo la cabecera genérica) tanto para HASH_I como para HASH_R.

12.6.1.3 Fase 1 de IKE con autenticación con firma

El intercambio se autentica firmando un hash que puede ser obtenido por las dos entidades involucradas en el intercambio.

Modo Principal

Iniciador		***Respondedor***
HDR, SA	-->	
	<--	HDR, SA
HDR, KE, Ni	-->	
	<--	HDR, KE, Nr
HDR*, IDii, [CERT], SIG_I	-->	
	<--	HDR*, IDir, [CERT], SIG_R

Modo Agresivo

Iniciador		***Respondedor***
HDR, SA, KE, Ni, IDii	-->	
	<--	HDR, SA, KE, Nr, IDir, [CERT], SIG_R
HDR, [CERT], SIG_I	-->	

En ambos modos el valor de SIG_I, SIG_R es el resultado de aplicar el algoritmo de firma digital a HASH_I / HASH_R respectivamente.

Opcionalmente pueden enviarse uno o más campos de certificación.

12.6.1.4 Fase 1 de IKE con autenticación con encriptación con clave pública

El intercambio se autentica a partir de la habilidad de cada una de las partes de reconstruir un hash, probando con ello que la otra entidad ha desencriptado un número (previamente transmitido de forma encriptada). El iniciador debe disponer de la clave pública del respondedor. En el caso de que éste disponga de varias claves públicas, un hash del certificado que el iniciador esta utilizando para encriptar la información se transmite como parte del tercer mensaje, de forma que el respondedor sepa que clave privada debe utilizar para desencriptar la información.

En este intercambio el contenido de los mensajes de número y de identidad se encriptan con la clave pública de la entidad par.

Modo Principal

Iniciador		***Respondedor***
HDR, SA	-->	
	<--	HDR, SA
HDR, KE, [HASH(1)], <IDii_b>PubKey_r, <Ni_b>PubKey_r	-->	
	<--	HDR, KE, <IDir_b>PubKey_i, <Nr_b>PubKey_i
HDR*, HASH_I	-->	
	<--	HDR*, HASH_R

Modo Agresivo

Iniciador		***Respondedor***
HDR, SA, [HASH(1)], KE, <IDii_b>PubKey_r, <Ni_b>PubKey_r	-->	
	<--	HDR, SA, Ke, <IDir_b>PubKey_i, <Nr_b>PubKey_i, HASH_R
HDR, HASH_I	-->	

Donde HASH(1) es el hash del certificado que esta utilizando el iniciador para encriptar el número y la identidad.

El uso de encriptación como forma de autenticación ofrece un intercambio que puede negarse, no existe prueba alguna de que la comunicación haya tenido lugar puesto que cada una de las entidades puede reconstruir ambas partes del intercambio

12.6.1.5 Fase 1 de IKE con autenticación con modo revisado de encriptación con clave pública

En este modo, el número se encripta utilizando la clave pública de la entidad, pero la identidad se encripta utilizando el algoritmo de encriptación simétrica negociado (en la información de SA) con una clave derivada del número.

Al igual que en el método con clave pública, en el caso de que el respondedor tenga más de un certificado que contenga claves públicas, es necesario enviar un mensaje de hash indicando el certificado seleccionado.

Modo Principal

Iniciador		***Respondedor***
HDR, SA	-->	
	<--	HDR, SA
HDR, [HASH(1)], <Ni_b>PubKey_r, <KE_b>Ke_i, <IDii>Ke_i, [<Cert-I>Ke_i]	-->	
	<--	HDR, <Nr_b>PubKey_i, <Ke_b>Ke_r, <IDir_b>Ke_r
HDR*, HASH_I	-->	
	<--	HDR*, HASH_R

Modo Agresivo

Iniciador		***Respondedor***
HDR, SA, [HASH(1)], <Ni_b>PubKey_r, <KE_b>Ke_i, <IDii_b>Ke_i, [<Cert-I_b>Ke_i]	-->	
	<--	HDR, SA, <Nr_b>PubKey_i, <KE_b>Ke_r, <IDir_b>Ke_r, HASH_R
HDR, HASH_I	-->	

Donde HASH(1) es el hash del certificado que esta utilizando el iniciador para encriptar el número y la identidad.

Ke_i y Ke_r son las claves de encriptación simétricas negociadas en el mensaje de SA. Las claves de encriptación simétricas se calculan como:

Ne_i = prf(Ni_b, CKY-I)
Ne_r = prf(NR_b, CKY-R)

12.6.1.6 Fase 1 de IKE con autenticación con clave precompartida

El proceso a seguir es:

Modo Principal

Iniciador		***Respondedor***
HDR, SA	-->	
	<--	HDR, SA
HDR, KE, Ni	-->	
	<--	HDR, KE, Nr
HDR*, IDii, HASH_I	-->	
	<--	HDR*, IDir, HASH_R

Modo Agresivo

Iniciador		***Respondedor***
HDR, SA, KE, Ni, IDii	-->	
	<--	HDR, SA, KE, Nr, IDir, HASH_R
HDR, HASH_I	-->	

12.6.1.7 Fase 2 de IKE Modo Rápido

El Modo Rápido no es, en sí, un intercambio completo, pero se utiliza como parte del proceso de negociación de SA (fase2), para derivar material de clave y negociar la política compartida para SAs no ISAKMP. La información intercambiada durante el proceso debe ser protegida por la SA de ISAKMP, tal y como se verá en el gráfico posterior, un campo de hash acompaña a la cabecera de ISAKMP autenticando el mensaje y el resto de mensaje de SA le sigue.

Este proceso de la fase 2 es básicamente una negociación de SAs y un intercambio de números que ofrece protección de reenvío. El Modo Rápido ofrece refresco del material de clave derivado de la exponenciación de la fase 1 (sin PFS), pero utilizando el mensaje de KE opcional, además de la exponenciación se ofrece PFS para el material de clave.

Se asume implícitamente que las identidades de las SAs negociadas en el proceso son las direcciones IP de las entidades ISAKMP. Si ISAKMP está actuando como negociador para un cliente, las identidades de las partes deben transmitirse como IDci, IDcr. Estas identidades se usan para identificar y direccionar el tráfico hacia el túnel apropiado si existen diversos túneles entre las dos entidades implicadas en el intercambio.

Modo Rápido

Iniciador		***Respondedor***
HDR*, HASH(1), SA,Ni, [KE], [IDci, IDcr]	-->	
	<--	HDR*, HASH(2), SA, Nr, [Ke], [IDci, IDcr]
HDR*, HASH (3)	-->	

Donde:

HASH(1) es el prf sobre el identificador del mensaje (M-ID), de la cabecera de ISAKMP concatenado con el mensaje que sigue incluyendo el hash y todas las cabeceras de campos pero, excluyendo el relleno añadido para la encriptación.

HASH(1) = prf(SKEYID_a, M-ID |SA | Ni | [KE] | [IDci | IDcr])

HASH(2) es idéntico al HASH(1) pero teniendo en cuenta el número del iniciador (Ni) menos la cabecera de la información. HASH(2) se añade después del M-ID pero antes del resto del mensaje.

HASH(2) = prf(SKEYID_a, M-ID | Ni_b |SA | Nr | [KE] | [IDci | IDcr])

HASH(3) es el prf sobre el valor cero representado en un octeto seguido de la concatenación del identificador del mensaje y de los dos números (iniciador|respondedor) menos la cabecera del mensaje.

HASH(3) = prf(SKEYID_a, 0 | M-ID | Ni_b | Nr_b)

Si no se utilizan campos de KE, el material de clave es:

KEYMAT = prf(SKEYID_d, protocolo | SPI | Ni_b | Nr_b)

Si se desea pfs y se intercambian campos de KE, el material de clave se define como:

KEYMAT = prf(SKEYID_d, g(qm)^xy | protocolo |SPI | Ni_b | Nr_b)

donde g(qm)^xy es el secreto compartido por el intercambio de Diffie-Hellman del Modo Rápido.

El protocolo y SPI, en ambos casos, se obtienen del campo de Propuesta de ISAKMP que contiene la Transformada negociada.

Una única negociación de SA da como resultado dos asociaciones de seguridad, una para cada sentido de la transmisión. Los SPI seleccionados por el iniciador y el receptor (diferentes SPI), garantizan claves diferentes para cada sentido. El SPI elegido por el destino de la SA se utiliza para la derivación de KEYMAT para esa SA.

En el caso de desear material de clave de longitud mayor que el obtenido de la función prf, se realimenta la función prf concatenando los resultados hasta conseguir la longitud deseada.

Utilizando el Método Rápido pueden negociarse múltiple claves y SAs dentro de un mismo intercambio.

12.6.1.8 Modo Nuevo Grupo

Este proceso, aún no siendo una fase 2, no puede ejecutarse nunca antes de haber establecido la SA de ISAKMP.

Modo Nuevo Grupo

Iniciador		***Respondedor***
HDR*, HASH(1), SA	-->	
	<--	HDR*, HASH(2), SA

donde:

HASH(1) es el resultado de prf utilizando SKEYID_a como clave y el identificador del mensaje de la cabecera de ISAKMP concatenado con la propuesta de SA (cuerpo y cabecera), como datos.

HASH(1) = prf(SKEYID_a, M-ID | SA)

HASH(2) es el resultado de la ejecución de prf con SKEYID_a como clave y el identificador de la cabecera de ISAKMP concatenado con la contestación, como datos.

HASH(2) = prf(SKEYID_a, M-ID |SA)

La propuesta de ISAKMP debe especificar todas las características del grupo.

12.6.1.9 Intercambios de Información en ISAKMP

Una vez establecida la asociación de seguridad de ISAKMP, pueden realizarse los Intercambios de Información de ISAKMP con protección.

Iniciador		***Respondedor***
HDR*, HASH(1), N / D	-->	

donde:
N / D es un mensaje de notificación ISAKMP o un mensaje de Eliminación.

HASH(1) es el resultado de ejecutar prf, teniendo como clave SKEYID_a y el identificador de mensaje de la cabecera de ISAKMP concatenado con el mensaje de información como datos.

HASH(1) = prf(SKEYID_a, M-ID | N / D)

Si la asociación de seguridad no ha sido establecida en el momento de intercambio de información, este proceso se realiza sin protección alguna.

12.6.2 Consideraciones de seguridad

El uso de los algoritmos de encriptación ofrece confidencialidad. La autenticación esta asegurada por el uso de un método negociado, bien un algoritmo de firma digital, un algoritmo de clave pública o una clave precompartida.

12.7 Formato de AH

La cabecera del protocolo, IPv4, IPv6 o Extensiones, precedente a la cabecera de AH, contendrá el valor de 51 en el campo protocolo (para IPv4) o el campo Siguiente Cabecera para IPv6 o Extensiones.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente Cabecera							
x.2	Longitud mensaje							
x.3	Reservado							
x.4	Reservado (continuación)							
x.5–x.8	Índice de Parámetros de Seguridad (SPI)							
x.9- x.12	Número Secuencial							
x.13(etc)	Datos de Autenticación							

Octeto x.1. Siguiente Cabecera

Identifica el tipo del siguiente mensaje después del mensaje de AH. Este valor se elige a partir del conjunto de Números de Protocolo IP definidos en el RFC de "Números Asignados".

Octeto x.2. Longitud mensaje

Longitud de AH menos "2".

Octeto x.3 - x.4. Reservado

Campo reservado para su uso futuro. Se codifica con valor cero.

Octeto x.5 - x.8. Índice de Parámetros de Seguridad (SPI)

Valor arbitrario que en combinación con la dirección IP del destinatario y el protocolo de seguridad (AH) identifican de forma única la asociación de seguridad para el datagrama. Los valores comprendidos entre 1 y 255 están reservados para uso futuro y el valor cero se reserva para uso específico de la implementación.

Octeto x.9 - x.12. Número Secuencial

Es un campo obligatorio que consiste en un contador que se incrementa de forma secuencial. Su presencia es independiente de si se requiere o no el servicio de protección contra reenvío para una Asociación de Seguridad concreta.

El contador se inicia a cero cuando se establece una SA. En el caso de utilizar el servicio contra reenvío, no se permite el uso cíclico del contador y al llegar al valor máximo, el contador del emisor y del receptor se reinicializan estableciendo una nueva SA y una nueva clave.

Octeto x.13 - .... Datos de Autenticación

Contiene el Valor de Comprobación de Integridad (ICV) para el paquete. En el caso de IPv4 debe ser un valor de longitud múltiple de 32 bits y en el caso de IPv6 múltiple de 64 bits.

12.8 Formato de ESP

La cabecera del protocolo IPv4, IPv6 o Extensiones precedente a la cabecera de ESP, contendrá el valor de 50 para el campo protocolo en IPv4 o el campo Siguiente Cabecera para IPv6 o Extensiones.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1-x.4	Índice de Parámetros de Seguridad (SPI)							
x.5-x.8	Número Secuencial							
x.9 (etc)	Datos Mensaje							
x.10-x.13	Relleno							
x.14	Longitud Relleno							
x.15	Siguiente Cabecera							
x.16(etc)	Datos de Autenticación							

Octeto x.1 - x.4. Índice de Parámetros de Seguridad (SPI)

Valor arbitrario que en combinación con la dirección IP del destinatario y el protocolo de seguridad (AH) identifican de forma única la asociación de seguridad para el mensaje. Los valores comprendidos entre 1 y 255 están reservados para uso futuro y el valor cero se reserva para uso específico de la implementación.

Octeto x.5 - x.8. Número Secuencial

Es un campo obligatorio que consiste en un contador que se incrementa de forma secuencial. Su presencia es independiente de si se requiere o no el servicio de protección contra reenvío para una Asociación de Seguridad concreta.

El contador se inicia a cero cuando se establece una SA. En el caso de utilizar el servicio contra reenvío, no se permite el uso cíclico del contador y al llegar al valor máximo, el contador del emisor y del receptor se reinicializan estableciendo una nueva SA y una nueva clave.

Octeto x.9 -... Datos de Mensaje

Campo de longitud variable que contiene la información descrita por el campo "Siguiente Cabecera"

Octeto x.10 - 13. Relleno

El emisor puede añadir de 0 a 255 bytes de relleno, bien sea para asegurar que los bits a encriptar sean un múltiplo del tamaño de bloque del algoritmo, en este caso el cálculo de relleno se aplica a los datos del mensaje excluyendo los campos IV, Longitud de relleno y Siguiente Cabecera, bien sea para asegurar que los Datos de autenticación son múltiplos de 4 bytes, en este caso el cálculo de relleno se aplica a los datos del mensaje incluyendo los campos IV, Longitud de relleno y Siguiente Cabecera.

Octeto x.14. Longitud de relleno

Longitud del campo de Relleno. Valor comprendido entre 0 y 255.

Octeto x.15. Siguiente Cabecera

Identifica el tipo del siguiente mensaje.

Octeto x.16 - .... Datos de Autenticación

Contiene el Valor de Comprobación de Integridad (ICV) calculado para el paquete ESP menos los Datos de Autenticación. La longitud del campo la determina la función de autenticación seleccionada.

Este campo es opcional y sólo se incluye si se ha seleccionado el servicio de autenticación.

12.9 Cálculo de Valor de Comprobación de Integridad para AH

El ICV se calcula sobre:

- Los campos de la cabecera IP que no han sido modificados en la transmisión o que tienen un valor predecible a su llegada al destino para la SA de AH
- La cabecera del AH y los octetos de relleno explícitos (si existen).
- Los datos de protocolos de nivel superior.

Los campos modificables, se toman con valor cero para obtener el ICV, si el campo es modificable pero predecible se inserta el valor supuesto en el campo para calcular ICV. El campo de Datos de Autenticación se inicializa a cero para los cálculos.

12.9.1.1.1 Cálculo de ICV para IPv4

En la siguiente tabla se define el tratamiento que reciben los campos de IPv4 con referencia al ICV.

Tipo	Observaciones
No modificables	
Versión	

Longitud Cabecera Internet	
Longitud Total	
Identificación	
Protocolo	Valor de AH
Dirección Fuente	
Dirección Destino	sin direccionamiento de fuente
Modificables y predecibles	
Dirección Destino	con direccionamiento de fuente
Modificables	Convertidos a cero antes de calcular ICV
Tipo de servicio (TOS)	
Flags	
Offset de Fragmento	
Tiempo de Vida (TTL)	
Checksum de cabecera	

Las opciones se consideran de forma unitaria, así si una única opción es modificable todas las especificadas se tratan como modificables.

12.9.1.1.2 Cálculo de ICV para IPv6

En la siguiente tabla se define el tratamiento que reciben los campos de IPv6 con referencia al ICV.

Tipo	**Observaciones**
No modificables	
Versión	
Longitud Mensaje	
Siguiente Cabecera	Valor de AH
Dirección Fuente	
Dirección Destino	sin cabecera de extensión de direccionamiento
Modificables y predecibles	
Dirección Destino	con cabecera de extensión de direccionamiento
Modificables	Convertidos a cero antes de calcular ICV
Clase	
Etiqueta de Flujo	
Límite de Salto	

Las cabeceras de extensión que contienen opciones éstas se consideran de forma unitaria, así si una única opción es modificable todas las especificadas se tratan como modificables. En el caso de cabeceras de extensión sin opciones, consultar [14] para obtener más detalles sobre su clasificación.

12.10 Formato de ISAKMP

Este protocolo ofrece mensajes construidos de forma modular, la presencia de campos en ISAKMP depende del Tipo de Intercambio definido en la cabecera de ISAKMP.

12.10.1 Formato de Cabecera de ISAKMP

La cabecera contiene una estructura fija seguida de un número variable de campos. La parte fija contiene la información necesaria para mantener el estado, procesar el mensaje y en la medida de lo posible, prevenir la negación de servicio o el reenvío de datos.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1-x.8	Cookie Iniciador							
x.9-x.15	Cookie Respondedor							
x.16	Siguiente mensaje							
x.17	Versión Mayor				Versión Menor			
x.18	Tipo de Intercambio							
x.19	Flags							
x.20-x.23	Identificador de Mensaje							
x.24-x.27	Longitud							

Octeto x.1 - x.8. Cookie Iniciador

Cookie de la entidad que inicia el establecimiento de la SA, la notificación o eliminación de la SA.

Octeto x.9 - x.15. Cookie Respondedor

Cookie de la entidad que responde al establecimiento de la SA, la notificación o eliminación de la SA.

Octeto x.16. Siguiente mensaje

Indica el tipo del primer campo del mensaje. Los posibles valores de este campo son:

Tipo	**Valor**
Ninguno	0
Asociación de Seguridad (SA)	1
Propuesta (P)	2
Transformación (T)	3
Intercambio de Clave (KE)	4
Identificación (ID)	5
Certificado (CERT)	6
Petición de Certificado (CR)	7

Hash (HASH)	8
Firma (SIG)	9
Número (NONCE)	10
Notificación (N)	11
Eliminar (D)	12
Identificador de Vendedor (VID)	13
Reservado	14 - 127
Uso Privado	128 - 255

Octeto x.17 bits 8-5. Versión Mayor

Versión del protocolo ISAKMP utilizado. Este campo toma por valor 1 si se utiliza la versión definida en [17] y 0 si se utilizan versiones anteriores.

Octeto x.17 bits 4-1. Versión Menor

Versión del protocolo ISAKMP utilizado. Este campo toma por valor 0 si se utiliza la versión definida en [17] y 1 si se utilizan versiones anteriores.

Octeto x.18. Tipo de Intercambio

Indica el tipo de intercambio a utilizar, determina el mensaje y la ordenación de los campos en el intercambio de mensajes de ISAKMP. Los posibles valores de este campo son:

Tipo	**Valor**
Ninguno	0
Base	1
Protección de Identidad	2
Sólo Autenticación	3
Agresivo	4
Informativo	5
Uso futuro	6 - 31
Uso específico DOI	32 - 239
Uso Privado	240 - 255

Octeto x.19 Flags

Este campo determina opciones específicas para el intercambio de mensajes de ISAKMP. Los bits definidos a continuación se ubican ordenados del bit menos importante al bit más importante, el resto de bits deben codificarse a cero.

E (bit de encriptación), si toma por valor 1 todos los campos después de la cabecera se encriptan según el algoritmo de encriptación definido en la SA de ISAKMP.

C (bit de transacción), se utiliza para la sincronización de intercambio de claves. Asegura que no se reciben datos encriptados antes de completar el establecimiento de la SA.

Ambas entidades pueden activar este bit, una vez activo la entidad par debe esperar un Intercambio Informativo con mensaje de Notificación de la entidad que ha puesto a 1 el bit de transacción.

A (bit de Autenticación), su uso se restringe al Intercambio Informativo con mensaje de Notificación y permite la transmisión de información con verificación de integridad pero sin encriptación.

Octeto x.20 - x.23 Identificador de Mensaje

Identificador de mensaje único, utilizado para identificar el estado del protocolo durante la fase 2 de las negociaciones. En la fase 1 este campo debe codificarse con valor cero y en la fase 2 el iniciador generará el identificador de forma aleatoria.

Octeto x.24 - x.27 Longitud

Longitud en octetos del mensaje, cabecera y campos.

12.10.2 Formato Genérico de Cabecera de Mensaje

Los mensajes definidos en el campo Siguiente Cabecera del ISAKMP, comparten un formato de cabecera común.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

12.10.3 Atributos de Datos

Algunos tipos de mensaje necesitan de atributos de datos que contienen información necesaria para ese mensaje, la longitud de los atributos puede ser 2 octetos o estar definida por el campo de Longitud del Atributo. El formato de los atributos es:

Bits								
octetos	8	7f	6	5	4	3	2	1
x.1	AF	Tipo de Atributo						
x.2	Tipo de Atributo (Continuación)							
x.3 (etc)	AF=0 Longitud del Atributo AF=1 Valor del Atributo							
x.4(etc)	AF=0 Valor del Atributo AF=1 No se transmite							

Octeto x.1 bit 8. Formato del Atributo (AF)

Si el valor de este campo es 0 entonces el formato del atributo es Tipo / Longitud / Valor (TLV), si el valor es 1 sigue el formato Tipo / Valor (T / V)

Octeto x.1 bits 7-0 -x.2. Tipo de Atributo

Identificador unívoco del tipo de atributo.

Octeto x.3 - ... Longitud del Atributo

Longitud en octetos del Valor del Atributo.

Octeto x.4 - ... Valor del Atributo

Valor del atributo, si el formato del atributo es TLV, la longitud del campo es variable, si es TV la longitud del campo es de 2 octetos.

12.10.4 Asociación de Seguridad

Se utiliza para negociar atributos de seguridad y para indicar el Dominio de Interpretación y Situación bajo el cual la negociación está teniendo lugar.

Bits								
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5-x.8	DOI							
x.9 (etc)	Situación							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 - x.8. Dominio de Interpretación (DOI)

Entero positivo de 32 bits, identificador del DOI. Los posibles valores de este campo son:

Tipo	**Valor**
SA de ISAKMP Genérica[16]	0
DOI de IPSec	1
Reservados para uso futuro	> 1

Octeto x.9 - .... Situación

Campo específico del DOI.

12.10.5 Propuesta

La propuesta contiene los mecanismos de seguridad, o transformaciones, a utilizar para asegurar las comunicaciones en el canal.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5	Número de Propuesta							
x.6	Identificador del Protocolo							
x.7	Longitud del SPI							
x.8	Número de Transformaciones							
x.9 (etc)	SPI							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0. Este campo sólo puede tomar como valores 2 ó 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

[16] Puede ser utilizada por cualquier protocolo durante la segunda fase de la negociación

Octeto x.5. Número de Propuesta

Número de propuesta dentro del mensaje actual.

Octeto x.6. Identificador de Protocolo

Identificador del protocolo, por ejemplo IPSec ESP, IPSec AH, TLS o OSPF.

Octeto x.7. Longitud del SPI

Longitud en octetos del SPI, valor dependiente del protocolo utilizado. En el caso ISAKMP el valor está comprendido entre 0 y 16.

Octeto x.8. Número de Transformaciones

Número de transformaciones para la propuesta. Cada una de las transformaciones esta detallada en un mensaje de transformaciones.

Octeto x.9 - ... SPI

SPI de la entidad emisora.

12.10.6 Transformación

Consiste en un mecanismo de seguridad específico a utilizar para asegurar el canal de comunicación. El mensaje de transformación contiene también los atributos de la asociación de seguridad.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5	Número de Transformación							
x.6	Identificador de la Transformación							
x.7-x.8	Reservado							
x.9 (etc)	Atributos de SA							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5. Número de Transformación

Número de transformación dentro del mensaje actual.

Octeto x.6. Identificador de Transformación

Identificador de la transformación.

Octeto x.7 - x.8. Reservado

Reservado para uso futuro, codificado con valor 0.

Octeto x.9 - ... Atributos de la Asociación de Seguridad

Atributos de SA asociados al Identificador de Transformación y codificados según el formato definido anteriormente para los atributos. Longitud variable.

12.10.7 Intercambio de Claves

Define las técnicas utilizadas para el Intercambio de Claves.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5 (etc)	Datos de Intercambio de Clave							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 - ... Datos de Intercambio de Clave

Campo de longitud variable que contiene la información necesaria para generar una clave de sesión. También puede contener indicadores de clave ya ubicados.

12.10.8 Identificación

Contiene datos específicos del DOI, se utiliza para intercambiar información de identificación.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5	Tipo de Identificación							
x.6-x.8	Datos de Identificación Específicos del DOI							
x.9 (etc)	Datos de Identificación							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 Tipo de Identificación

Tipo de identificación a utilizar

Octeto x.6 - x.8. Datos de Identificación específicos del DOI

Datos de Identificación específicos del DOI. Si no se utiliza este campo se codifica con valor 0.

Octeto x.9 - ... Información de Identificación

Campo de longitud variable con información de identificación.

12.10.9 Certificación

Es el método de transmitir certificados o información relativa a certificación.

Bits								
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5	Codificación de Certificado							
x.6 (etc)	Datos de Certificación							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 Codificación de Certificado

Indica el tipo de certificado o de información relativa a la certificación a transmitir. Los posibles valores son:

Tipo	**Valor**
Ninguno	0
PKCS #7 con Certificado X.509	1
Certificado PGP	2
Clave con firma DNS	3
Certificado X.509 - Firma	4
Certificado X.509 - Intercambio de Clave	5
Kerberos	6
Lista de Revocación de Certificado (CRL)	7
Lista de Revocación de Autoridades (ARL)	8
Certificado SPKI	9
Certificado X.509 - Atributo	10
Reservado	11 - 255

Octeto x.6 - ... Datos de Certificado

Campo de longitud variable con los datos del certificado.

12.10.10 Petición de Certificado

Mecanismo de petición de certificados vía ISAKMP. Si se requiere más de un certificado deben transmitirse más de un mensaje de petición de certificado.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5	Codificación de Certificado							
x.6 (etc)	Autoridad de Certificación							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 Codificación de Certificado

Indica el tipo de certificado o de información relativa a la certificación a transmitir.

Tipo	**Valor**
Ninguno	0
PKCS #7 con Certificado X.509	1
Certificado PGP	2
Clave con firma DNS	3
Certificado X.509 - Firma	4
Certificado X.509 - Intercambio de Clave	5
Kerberos	6
Lista de Revocación de Certificado (CRL)	7
Lista de Revocación de Autoridades (ARL)	8
Certificado SPKI	9
Certificado X.509 - Atributo	10
Reservado	11 - 255

Octeto x.6 - ... Autoridad de Certificación

Campo de longitud variable que contiene la codificación de una autoridad de certificación aceptada para el tipo de certificado requerido.

12.10.11 Hash

Contiene datos generados por la función de hash sobre parte del mensaje y/o estado de ISAKMP. Se utiliza para verificar la integridad de los datos del mensaje ISAKMP o para autenticar las entidades de la negociación.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5 (etc)	Datos de Hash							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 - ... Datos de Hash

Campo de longitud variable que contiene el resultado de aplicar la función de hash al mensaje ISAKMP y/o al estado.

12.10.11.1 Firma

Contiene datos generados por la función de firma digital sobre parte del mensaje y/o estado de ISAKMP. Se utiliza para verificar la integridad de los datos del mensaje ISAKMP y también puede hacerse servir para el servicio de no-repudio.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
	Datos de Firma							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 - ... Datos de Firma Digital

Campo de longitud variable que contiene el resultado de aplicar la firma digital al mensaje ISAKMP y/o al estado.

12.10.12 Número

Contiene datos generados aleatoriamente que garantizan el servicio de no-reenvío.

	Bits							
octetos	8		6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
	Longitud mensaje							
x.5 (etc)	Datos de Número							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 - ... Datos de Número

Campo de longitud variable que contiene los datos generados de manera aleatoria por la entidad emisora.

12.10.13 Notificación

Permite la transmisión de datos informativos, tales como condiciones de error, a una entidad ISAKMP par.

	Bits							
octetos	8	7	6		4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5-x.8	DOI							
x.9	Identificador de Protocolo							
x.10	Longitud del SPI							
x.11-x.12	Tipo de Mensaje de Notificación							
x.13(etc)	SPI							
x.14(etc)	Datos de Notificación							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 - x.8. Dominio de Interpretación (DOI)

Entero positivo de 32 bits, identificador del DOI. Los posibles valores de este campo son:

Tipo	**Valor**
SA de ISAKMP Genérica[17]	0
DOI de IPSec	1
Reservados para uso futuro	> 1

Octeto x.9. Identificador de Protocolo

Este campo identifica el protocolo a utilizar, por ejemplo IPSec ESP.

Octeto x.10. Longitud del SPI

[17] Puede ser utilizada por cualquier protocolo durante la segunda fase de la negociación

Longitud del SPI, valor dependiente del protocolo utilizado.

Octeto x.11-x.12. Tipo de Mensaje de Notificación

Tipo de Mensaje de Notificación. Los valores que puede tomar este campo son:

Errores	**Valor**
Tipo de Mensaje Incorrecto	1
DOI no soportado	2
Situación no soportada	3
Cookie Incorrecto	4
Versión Mayor Incorrecta	5
Versión Menor Incorrecta	6
Tipo de Intercambio Incorrecto	7
Flags Incorrectos	8
Identificador de Mensaje Incorrecto	9
Identificador de Protocolo Incorrecto	10
SPI Incorrecto	11
Identificador de Transformación Incorrecto	12
Atributos no soportados	13
No se ha seleccionado Propuesta	14
Sintaxis de Propuesta Incorrecta	15
Formato de Mensaje Incorrecto	16
Información de Clave Incorrecta	17
Información de Identificador Incorrecto	18
Codificación de Certificado Incorrecto	19
Certificado Incorrecto	20
Tipo de Certificado no soportado	21
Autoridad de Certificación Incorrecta	22
Información de Hash Incorrecta	23
Fallo de Autenticación	24
Firma Incorrecta	25
Notificación de Dirección	26
Notificación de tiempo de vida de SA	27
Certificado no disponible	28
Tipo de Intercambio no soportado	29
Longitud de Mensajes diferentes	30
Reservado para uso futuro	31 - 8191
Reservado para uso privado	16383

Tipos de Estados	**Valor**
Conectado	16384
Reservado para uso futuro	16385 - 24575
Códigos específicos de DOI	24576 - 32767
Uso Privado	32768 - 40959

Reservado para uso futuro	40960 - 65535

Octeto x.13-.... SPI

Campo de longitud variable que contiene el Indice de Parámetros de Seguridad, SPI.

Octeto x.14-.... Datos de Notificación

Campo de longitud variable que contiene datos informativos o de error transmitidos .

12.10.14 Eliminación

Contiene un identificador de asociación de seguridad específico del protocolo indicando que el emisor ha dejado la base de datos de la asociación de seguridad y por lo tanto ya no es válida.

	Bits							
octetos		7	6	5	4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5-x.8	DOI							
x.9	Identificador de Protocolo							
x.10	Longitud del SPI							
x.11-x.12	Número de SPIs							
x.13(etc)	SPIs							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 - x.8. Dominio de Interpretación (DOI)

Entero positivo de 32 bits, identificador del DOI. Los posibles valores de este campo son:

Tipo	**Valor**
SA de ISAKMP Genérica[18]	0
DOI de IPSec	1
Reservados para uso futuro	> 1

[18] Puede ser utilizada por cualquier protocolo durante la segunda fase de la negociación

Octeto x.9. Identificador de Protocolo

Este campo identifica la base de datos sobre la que se debe aplicar la petición de eliminación.

Octeto x.10. Longitud del SPI

Longitud del SPI, valor dependiente del protocolo utilizado.

Octeto x.11-x.12. Número de SPIs

Número de SPIs contenido en la petición, la longitud de cada SPI se indica en el campo anterior.

Octeto x.13-.... Indentificador(es) de Parámetros de Seguridad (SPIs)

Identificador(es) de la(s) asociación(es) de seguridad a eliminar.

12.10.15 Identificador de Vendedor

Contiene la constante identificadora de un vendedor/proveedor. Se utiliza para identificar y reconocer instancias remotas de implementaciones de un proveedor.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Siguiente mensaje							
	Reservado							
x.3-x.4	Longitud mensaje							
x.5 (etc)	Identificador del vendedor							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Campo no utilizado y codificado con valor 0.

Octeto x.3 - x.4. Longitud mensaje

Longitud del mensaje actual incluyendo la cabecera genérica.

Octeto x.5 - ... Identificador de Vendedor

Campo de longitud variable que contiene el hash del identificador del vendedor y la versión de la implementación.

12.11 Intercambio Completo de IKE

En este apartado se muestra un ejemplo del uso del protocolo de IKE para establecer un canal de comunicación seguro y autenticado entre procesos de ISAKMP (fase 1) y la generación de material de clave para una SA con IPSec (fase 2).

Fase 1 utilizando Modo Principal

El iniciador puede generar diversas propuestas, el respondedor sólo puede seleccionar una.

Bits								
octetos	8	7	6	5	4	3	2	1
x.1-x.3	Cabecera de ISAKMP con Intercambio de Modo Principal y Siguiente Mensaje de SA de ISAKMP							
x.4	0							
x.5	Reservado							
x.6-x.7	Longitud Mensaje							
x.8-x.11	DOI							
x.12-x.15	Situación							
x.16	0							
x.17	Reservado							
x.18-x.19	Longitud de Mensaje							
x.20	Propuesta # 1							
x.21	PROTO_ISAKMP							
x.22	Tamaño SPI = 0							
x.23	# Transformadas							
x.24	ISA_TRANS							
x.25	Reservado							
x.26-x.27	Longitud de Mensaje							
x.28	Transformada # 1							
x.29	KEY_OAKLEY							
x.30-x.31	Reservado2							
x.32-x.35	Atributos de SA preferidos							
x.36	0							
x.37	Reservado							
x.38-x.39	Longitud de Mensaje							
x.40	Transformada # 2							
x.41	KEY_OAKLEY							
x.42-x.43	Reservado2							
x.44-x.47	Atributos de SA alternativos							

El respondedor selecciona una respuesta y contesta con una transformada que contiene los atributos de la SA de ISAKMP.

Bits								
octetos	8	7	6	5	4	3	2	1
x.1-x.3	Cabecera de ISAKMP con Intercambio de Modo Principal y Siguiente Mensaje de ISA_KE							
x.4	ISA_NONCE							
x.5	Reservado							
x.6-x.7	Longitud Mensaje							
x.8-x.11	Valor Público de Diffie_Hellman							
x.12	0							
x.13	Reservado							
x.14-x.15	Longitud de Mensaje							
x.16	Ni o Nr (dependiendo de si es el iniciador o el respondedor)							

Las claves compartidas se utilizan para proteger y autenticar cualquier comunicación posterior.

Bits								
octetos	8	7	6	5	4	3	2	1
x.1-x.3	Cabecera de ISAKMP con Intercambio de Modo Principal y Siguiente Mensaje de ISA_ID y el conjunto de bit de encriptación							
x.4	ISA_SIG							
x.5	Reservado							
x.6-x.7	Longitud Mensaje							
x.8-x.11	Identificación del negociador de ISAKMP							
x.12	0							
x.13	Reservado							
x.14-x.15	Longitud de Mensaje							
x.16	Firma verificada por la clave pública del ID anterior							

Fase 2 con Modo Rápido

En el ejemplo se considera que los negociadores de ISAKMP son proxies que requieren autenticación para otras entidades.

Bits								
octetos	8	7	6	5	4	3	2	
x.1-x.3	Cabecera de ISAKMP con Intercambio de Modo rápido y Siguiente Mensaje de ISA_HASH y el conjunto de bits de encriptación							
x.4	ISA_SA							
x.5	Reservado							
x.6-x.7	Longitud Mensaje							
x.8-x.11	Hash del mensaje							
x.12	ISA_NONCE							

x.13	Reservado
x.14-x.15	Longitud de Mensaje
x.16-x.19	Dominio de Interpretación
x.20	Situación
x.21	0
	Reservado
x.23-x.24	Longitud de Mensaje
x.25	Propuesta # 1
x.26	PROTO_IPSEC_AH
x.27	Tamaño SPI = 4
x.28	# Transformadas
x.29-x.32	SPI
x.33	ISA_TRANS
x.34	Reservado
x.35-x.36	Longitud de Mensaje
x.37	Transformada # 1
x.38	AH_SHA
x.39-x.40	Reservado2
x.41-x.44	Otros Atributos de SA
x.45	0
x.46	Reservado
x.47-x.48	Longitud de Mensaje
x.49	Transformada # 2
x.50	AH_MD5
x.51-x.52	Reservado2
x.53-x.56	Otros Atributos de SA
x.57	ISA_ID
x.58	Reservado
x.59-x.60	Longitud de Mensaje
x.61-x.64	Número
x.65	ISA_ID
x.66	Reservado
x.67x.68	Longitud de Mensaje
x.69-x.72	ID de la fuente cliente de ISAKMP
x.73	0
x.74	Reservado
x.75-x.76	Longitud de Mensaje
x.77-x.80	ID del destino cliente de ISAKMP

El respondedor contesta seleccionando una transformada de AH

Bits								
octetos	8	7	6	5		3		1
	Cabecera de ISAKMP con Intercambio de Modo Rápido y Siguiente Mensaje de ISA_HASH y el conjunto de bit de encriptación							
x.4	0							
x.5	Reservado							
	Longitud Mensaje							
x.8-x.11	Datos de hash							

12.12 Dominio de Interpretación de ISAKMP

El protocolo de Gestión de Claves y Asociaciones de Seguridad de Internet (ISAKMP), define un entorno de gestión de asociaciones de seguridad y establecimiento de claves de encriptación para Internet. Este entorno consiste en intercambios definidos, mensajes y formas de procesamiento definidas dentro de un entorno de Interpretación (DOI).

En este apartado se describe el DOI definido para Seguridad IP de Internet (DOI de IPSec) utilizado en ISAKMP para negociar asociaciones de seguridad.

12.12.1 Requerimientos

El definición de DOI para ISAKMP conlleva los siguientes requerimientos:

- Define el esquema de nombres para los identificadores de protocolos específicos del DOI
- Define la interpretación del campo Situación
- Define el conjunto de políticas de seguridad aplicables
- Define la sintaxis de los atributos de SA específicos del DOI
- Define la sintaxis del contenido de los mensajes específicos del DOI
- Define tipos de Intercambio de Claves adicionales, si fuera necesario
- Define tipos de Mensajes de Notificación adicionales, si fuera necesario

12.12.2 Esquema de Nombre IPSec

Dentro de ISAKMP, todos los dominios de interpretación deben estar registrados en IANA. El número asignado en IANA al dominio de interpretación de IPSec es 1.

12.12.3 Definición de Situación en IPSec

El campo Situación ofrece información que puede ser utilizada por el receptor para tomar una decisión sobre como procesar la petición de Asociación de Seguridad. Para el DOI de IPSec, el campo Situación es un campo de 4 octetos con los siguientes valores:

0x01	SIT_IDENTITY_ONLY
0x02	SIT_SECRECY
0x04	SIT_INTEGRITY

SIT_IDENTITY_ONLY, especifica que la asociación de seguridad será identificada por la información de la identidad del origen presente en un Mensaje de Identificación y debe abortarse cualquier establecimiento de SA que no incluya el mensaje de Identificación. Este valor debe ser soportado por todas las implementaciones de IPSec.

Si el origen de los datos no soporta ni SIT_SECRECY ni SIT_INTEGRITY, la situación consiste sólo en los 4 octetos del campo situación y no tiene porque incluir el campo Identificador del Dominio Etiquetado.

SIT_SECRECY, especifica que la negociación de la SA se está haciendo en un entorno que necesita etiquetas de confidencialidad. Si el campo Situación tiene este valor, entonces irá seguido de información de longitud variable conteniendo un máscara de nivel y de compartición de datos.

Si el receptor no soporta este valor, enviará una Notificación de “Situation_not_supported” y la SA se eliminará.

SIT_INTEGRITY, especifica que la SA se está creando en un entorno que necesita etiquetas de integridad. Si el campo Situación tiene este valor, entonces irá seguido de información de longitud variable conteniendo un máscara de nivel y de integridad.

Si el receptor no soporta este valor, enviará una Notificación de “Situation_not_supported” y SA se eliminará.

12.12.4 Números Asignados a IPSec

12.12.4.1 Identificador de Protocolos de Seguridad IPSec

La sintaxis de esta propuesta permite la negociación de múltiples protocolos de seguridad en la fase 2 dentro de una misma negociación. Los posibles valores de Identificadores de Protocolos de Seguridad son:

0	Reservado
1	PROTO_ISAKMP
2	PROTO_IPSEC_AH
3	PROTO_IPSEC_ESP
4	PROTO_IPCOMP

PROTO_ISAKMP, especifica protección de mensaje requerida en la fase 1 del protocolo de ISAKMP. Este valor debe ser soportado por todas las implementaciones de IPSec.

PROTO_IPSEC_AH, especifica autenticación de paquete IP. La transformación de AH por defecto incluye origen de datos para autenticación, integridad y protección contra reenvío.

PROTO_IPSEC_ESP, especifica confidencialidad del paquete IP. Si fuera necesario autenticación, debería incluirse como parte del mensaje de Transformación de ESP. Por defecto, la

transformación de ESP incluye autenticación del origen de los datos, integridad, protección contra reenvío y confidencialidad.

PROTO_IPCOMP, especifica compresión del mensaje IP.

12.12.4.2 Identificadores de Transformaciones ISAKMP

La selección del mecanismo de Intercambio de Claves se hace a través del mensaje de Propuesta estándar de ISAKMP. Los identificadores de Transformación para el mensaje de Propuesta son:

0 Reservado
1 KEY_IKE

Dentro del entorno del DOI de IPSec es posible definir otros mecanismos de intercambio de claves.

KEY_IKE, especifica el tipo de intercambio definido en el Protocolo de Intercambio de Claves de Internet.

12.12.4.3 Identificadores de Transformaciones AH

El protocolo de Autenticación de Cabecera, define transformaciones para la autenticación, integridad y detección de reenvío. Los posibles valores son:

0 Reservado
1 Reservado
2 AH_MD5
3 AH_SHA
4 AH_DES

AH_MD5, especifica una transformación genérica de AH utilizando MD5. Este valor debe ser considerado en todas las implementaciones de IPSec. Se utiliza conjuntamente con el atributo Auth (KPDK[19]) para definir la transformación de AH.

AH_SHA, especifica una transformación genérica AH utilizando SHA-1. Todas las implementaciones de IPSec ofrecerán este valor con el atributo Auth(HMAC-SHA).

AH_DES, especifica una transformación genérica AH utilizando DES. Se define su uso con el atributo Auth(DES-MAC).

12.12.4.4 Identificadores de Transformaciones ESP

El protocolo de ESP, define transformaciones para la confidencialidad de datos. En el caso de requerir autenticación, protección de integridad y detección de reenvío, es necesario identificar el atributo del algoritmo de autenticación para el correcto uso de ESP con la política de seguridad a aplicar, por ejemplo para una petición de autenticación con HMAC-MD5 con 3DES,

[19] KPDK significa clave / relleno / datos / clave, traducido del inglés key / pad / data / key.

debe especificarse la transformación de ESP-3DES con el atributo de algoritmo de autenticación a HMAC-MD5.

Los posibles valores de transformaciones ESP son:

0	Reservado
1	ESP_DES_IV64
2	ESP_DES
3	ESP_3DES
4	ESP_RC5
5	ESP_IDEA
6	ESP_CAST
7	ESP_BLOWFISH
8	ESP_3IDEA
9	ESP_DES_IV32
10	ESP_RC4
11	ESP_NULL

ESP_DES_IV64, identifica la transformación para DES-CBC.

ESP_DES, especifica una transformación genérica DES utilizando DES-CBC. Se ofrece este servicio en todas las implementaciones de IPSec en conjunto con el atributo de algoritmo de autenticación Auth(HMAC-MD5).

ESP_3DES, especifica una transformación triple-DES, se utiliza con el algoritmo de autenticación HMAC-MD5.

ESP_RC5, especifica la transformación RC5.

ESP_IDEA, especifica la transformación IDEA.

ESP_CAST, especifica la transformación CAST.

ESP_BLOWFISH, especifica la transformación BLOWFISH.

ESP_3IDEA, especifica la transformación triple IDEA.

ESP_DES_IV32, especifica la transformación DES-CBC utilizando un vector de inicialización de 32 bits.

ESP_RC4, especifica la transformación RC4.

ESP_NULL, define la no confidencialidad ofrecida con ESP. Se utiliza al transmitir paquetes por túnel que sólo requieren autenticación, protección de integridad y detección de reenvío. Este valor debe estar soportado por todas las implementaciones de IPSec.

12.12.4.5 Identificadores de Transformaciones IPCOMP

Las transformaciones de Compresión IP, definen algoritmos opcionales de compresión. Los posibles valores son:

0	Reservado
1	IPCOMP_OUI
2	IPCOMP_DEFLATE
3	IPCOMP_LZS

IPCOMP_OUI, especifica una transformación de compresión propietaria. Debe ir acompañada del atributo que identifica al vendedor.

IPCOMP_DEFLATE, indica el uso del algoritmo deflate.

IPCOMP_LZS, especifica el uso del algoritmo LZS.

12.12.4.6 Atributos de SA

Las definiciones de los atributos de SA presentadas a continuación, se utilizan en la fase dos de la negociación de IKE. El tipo de atributos puede ser básico o de longitud variable, éstos últimos pueden codificarse como básicos si son de tamaño menor a dos octetos.

En el caso de recibir un atributo no conocido o no implementado se envía como respuesta un mensaje “Atributtes_not_support”.

Los posibles atributos son:

1	Tipo de vida de SA(básico)
2	Duración vida de SA (variable)
3	Descripción de grupo (básico)
4	Modo Encapsulación (básico)
5	Algoritmo de Autenticación (básico)
6	Longitud de clave (básico)
7	Redondeo clave (básico)
8	Tamaño Diccionario de Compresión (básico)
9	Algoritmo de Compresión Privado (variable)

Tipo de vida de SA, indica el tiempo de vida de la SA. Cuando expira, todas las claves negociadas bajo la asociación (AH o ESP) deben renegociarse. Los posibles valores son:

0	Reservado
1	Segundos
2	Kilobytes
3-61439	Reservados a IANA
61440-65535	Reservado para uso privado

Duración vida de SA, para un tipo de vida de SA, define el valor de tiempo de vida asociado a la SA, bien en segundos bien en Kb. Si no se define, el valor por defecto es 28800.

Un atributo de duración siempre debe ir seguido de un atributo de tipo de vida que indique las unidades. En el caso de que el tiempo de vida pedido exceda el considerado adecuado por la política de seguridad se envía una notificación al emisor.

Descripción de Grupo, especifica el grupo de Oakley a utilizar en una negociación.

Modo de Encapsulación, los posibles valores son:

0	Reservado
1	Túnel
2	Transporte
3-61439	Reservado a IANA
61440-65635	Reservado uso privado

Algoritmo de Autenticación, valores posibles:

0	Reservado
1	HMAC-MD5
2	HMAC-SHA
3	DES-MAC
4	KPDK
5-61439	Reservado a IANA
61440-65535	Reservado para uso privado

Es obligatorio especificar el valor de este atributo excepto en el caso de negociar ESP sin autenticación.

Longitud de Clave, el único valor asignado es 0 que está reservado. Para atributos de cifrado con longitud fija no debe incluirse este atributo.

Redondeo de Clave, el único valor asignado es 0 que está reservado.

Tamaño de Diccionario de Compresión, el único valor asignado es 0 que está reservado. Indica el log2 de la longitud máxima del diccionario.

Algoritmo de Compresión Privado, indica un algoritmo privado. Los tres primeros octetos identifican una compañía (OUI) y el siguiente octeto un subtipo de compresión específico del vendedor seguido de cero o más octetos de información del vendedor.

Es obligatorio que todas las implementaciones puedan negociar los atributos de Tipo de vida de SA, Duración de SA y Algoritmo de Autenticación.

12.12.5 Contenido de Mensaje de IPSec

En este apartado se definen los mensajes cuya representación es dependiente del DOI.

12.12.5.1 Asociación de Seguridad

En la figura presentada a continuación puede observarse el mensaje de Asociación de Seguridad correspondiente al DOI de IPSec

	Bits							
octetos	8	7	6		4	3	2	1
x.1	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5-x.8	Dominio de Interpretación							
x.9-x.12	Situación							
x.13-x.16	Identificador Dominio Etiquetado							
x.17-18	Longitud Encriptación							
	Reservado							
x.21-x.24	Nivel de Encriptación							
	Longitud de Cat. Encriptación							
x.27-x.28	Reservado							
	Categoría de Encriptación							
x.33-x.34	Longitud de Integridad							
x.35-x.36	Reservado							
x.37-x.40	Nivel de Integridad							
x.41-x.42	Longitud Cat. Integridad							
x.43-x.44	Reservado							
x.45-x.48	Categoría de Integridad							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Toma por valor 0.

Octeto x.3-x.4. Longitud mensaje

Longitud en octetos del mensaje actual, incluyendo la cabecera genérica.

Octeto x.5-x.8. Dominio de Interpretación

Especifica el Dominio de Interpretación de IPSec, se codifica con valor 1.

Octeto x.9-x.12. Situación

Codificación del parámetro de Situación. Los posibles valores son:

0x01	SIT_IDENTITY_ONLY
0x02	SIT_SECRECY
0x04	SIT_INTEGRITY

Octeto x.13-x.16 Identificador de Dominio Etiquetado

Número asignado por IANA para la interpretación de la información de Integridad y Confidencialidad. El único valor definido es 0.

Octeto x.17-x.18. Longitud de Encriptación

Longitud en octetos del identificador de nivel de encriptación, excluyendo los bits de relleno.

Octeto x.19-x.20. Reservado

Toma por valor 0.

Octeto x.21-x.24. Nivel de Encriptación

Nivel de Encriptación requerido. Si la codificación del nivel es inferior a 32 bits, debe completarse con bits de relleno (codificados con 0) hasta alcanzar los 32 bits.

Octeto x.25-x.26. Longitud de Categoría de Encriptación

Longitud en bits de la categoría de encriptación, excluyendo los bits de relleno.

Octeto x.27-x.28. Reservado

Toma por valor 0.

Octeto x.29-x.32. Categoría de Encriptación

Categoría de Encriptación requerida. Si la codificación de la categoría es inferior a 32 bits, debe completarse con bits de relleno (codificados con 0) hasta alcanzar los 32 bits.

Octeto x.33-x.34. Longitud de Integridad

Longitud en octetos del identificador de nivel de integridad, excluyendo los bits de relleno.

Octeto x.35-x.36. Reservado

Toma por valor 0.

Octeto x.37-x.40. Nivel de Integridad

Nivel de Integridad requerido. Si la codificación del nivel es inferior a 32 bits, debe completarse con bits de relleno (codificados con 0) hasta alcanzar los 32 bits.

Octeto x.41-x.42. Longitud de Categoría de Integridad

Longitud en bits de la categoría de integridad, excluyendo los bits de relleno.

Octeto x.43-x.44. Reservado

Toma por valor 0.

Octeto x.45-x.48. Categoría de Integridad

Categoría de Integridad requerida. Si la codificación de la categoría es inferior a 32 bits, debe completarse con bits de relleno (codificados con 0) hasta alcanzar los 32 bits.

12.12.5.2 Contenido del mensaje de Identificación

El mensaje de identificación se utiliza para identificar al origen de la asociación de seguridad. Esta información debe ser utilizada por el respondedor para determinar los requerimientos de la política de seguridad del host.

Durante la fase 1 de la negociación el ID del puerto y los campos del protocolo debe tener por valor 0 ó puerto 500 de UDP. Cualquier otro valor será tratado como un error.

Bits								
octetos	8	7		5		3	2	1
	Siguiente mensaje							
x.2	Reservado							
x.3-x.4	Longitud mensaje							
x.5	Tipo ID							
	ID Protocolo							
x.7-x.8	Puerto							
x.9-x.12	Información de Identificación							

Octeto x.1. Siguiente mensaje

Identificador del siguiente mensaje. Si el actual es el último, el campo se codifica con valor 0.

Octeto x.2. Reservado

Toma por valor 0.

Octeto x.3-x.4. Longitud mensaje

Longitud en octetos del mensaje actual, incluyendo la cabecera genérica.

Octeto x.5. Tipo de Identificación

Descripción de los datos de identificación contenidos en el campo "Información de Identificación". Los posibles valores de este campo son:

0	Reservado	Descripción
1	ID_IPV4_ADDR	Dirección de 4 octetos de IPv4
2	ID_FQDN	Nombre de dominio completamente calificado
3	ID_USER_FQDN	Nombre de usuario completamente calificado
4	ID_IPV4_ADDR_SUBNET	Rango de direcciones IPv4
5	ID_IPV6_ADDR	Dirección de 16 octetos de IPv6
6	ID_IPV6_ADDR_SUBNET	Rango de direcciones IPv6
7	ID_IPV4_ADDR_RANGE	Rango de direcciones IPv4
8	ID_IPV6_ADDR_RANGE	Rango de direcciones IPv6
9	ID_DER_ASN1_DN	Codificación DER de Nombre Diferenciado ASN.1
10	ID_DER_ASN1_GN	Codificación DER de Nombre General ASN.1
11	ID_KEY_ID	Datos específicos del vendedor

Octeto x.6. ID de Protocolo

Valor que especifica un identificador de protocolo asociado a IP , por ejemplo UDP/TCP. Si el campo toma por valor 0, no se tiene en cuenta.

Octeto x.7-x.8. Puerto

Puerto asociado. Si toma por valor 0, no se tiene en cuenta.

Octeto x.9-x.12. Información de Identificación

Identificación.

12.12.5.3 Tipos de Mensajes de Notificación

Existen dos tipos de mensajes de Notificación. Mensajes de notificación de errores, con código 8192 y los mensajes de tipos de estados. En esta segunda clase se encuentran los mensajes:

RESPONDER-LIFETIME	código 24576
REPLAY-STATUS	código 24577
INITIAL-CONTACT	código 24578

El mensaje de "Responder-lifetime" se utiliza para comunicar el tiempo de vida seleccionado por la entidad receptora para la SA de IPSEC. El mensaje "Replay-Status" se usa para la confirmación de la selección de protección de reenvío y finalmente el mensaje "Initial-Contact" permite a una entidad comunicar que es la primera SA establecida con el sistema remoto.

13Anexo 4: IPv6 versus IPv4

El incremento del uso de Internet junto con el aumento de la población, el hecho de que las personas dispongan de más de un ordenador, la necesidad de más de una dirección por interfaz, etc., ha provocado el crecimiento indiscriminado de demandas de direcciones e implicará en pocos años el agotamiento de direcciones posibles según el formato de IPv4. La limitación de direcciones de IPv4, generó en su día la necesidad de crear un nuevo protocolo de Internet y el resultado de esta necesidad es IPv6.

Las diferencias principales entre IPv6 e IPv4 radican en el formato de direccionamiento y en el formato de la cabecera de IPv6.

13.1 Formato de direccionamiento de IPv6

Las características básicas del formato de direccionamiento de IPv6 son:

- Longitud de 128 bits. Direcciones de longitud fija
- Permite múltiples interfaces por host
- Permite múltiples direcciones por interfaz
- Permite unicast, multicast
- Permite direcciones basadas en proveedor, locales a la conexión y/o locales a la ubicación
- Arquitectura de Direcciones Jerárquica

13.2 Cabecera

En las siguientes figuras pueden observarse las diferencias básicas entre las cabeceras de IPv6 e IPv4.

Versión	Prioridad	Etiqueta de Flujo	
Longitud Carga		Siguiente Cabecera	Límite de Salto
Dirección Origen			
Dirección Destino			

Figura 51. Cabecera de IPv6

Versión	IHL	Tipo de Servicio	Longitud Total
Identificación		Flags	Offset de Fragmento
Tiempo de Vida	Protocolo	Checksum Cabecera	
Dirección Origen			
Dirección Destino			
Opciones			Relleno

Figura 52. Cabecera de IPv4

Decimal	Clave	Tipo de Cabecera
	HBH	Salto-a-Salto (IPv6)
1	ICMP	Mensaje de Control de Internet (IPv4)
2	IGMP	Gestión de Grupo de Internet (IPv4)
2	ICMP	Mensaje de Control de Internet (IPv6)
3	GGP	Pasarela-to-Pasarela
4	IP	IP in IP (IPv4 encapsulamiento)
5	ST	Flujos
6	TCP	TCP
17	UDP	UDP
29	ISO-TP4	ISO-TP4
43	RH	Cabecera de Direccionamiento (IPv6)
44	FS	Cabecera de Fragmentación (IPv6)
45	IDRP	Direccionamiento interdominios
51	AH	Cabecera de Autenticación
52	ESP	Mensaje de Seguridad Encriptado
59	Null	No Siguiente Cabecera
60	ISO-IP	CLNP
88	IGRP	IGRP
89	OSPF	Primer Camino Corto Abierto

Figura 53 Tipos de Protocolos y Cabecera

Las cabeceras de IPv6 sólo duplican en longitud las cabeceras de IPv4 y únicamente mantiene su posición el campo número de versión. Otras características importantes son:

- Los campos longitud de cabecera, tipo de servicio, identificación, flags, offset de fragmento y checksum de cabecera desaparecen en la cabecera de IPv6.
- Se sustituyen los campos Longitud de Datagrama por Longitud Total, Tipo de Protocolo por Siguiente Cabecera y Tiempo de Vida por Límite de Salto.
- Se añaden los campos Etiqueta de Flujo y Prioridad.
- Los campos son de longitud fija.
- No existen campos opcionales, se reemplazan por extensiones de cabecera.
- El tamaño del campo “Límite de Salto” es de 8 bits, por lo que el número máximo de saltos es de 255.
- El valor del campo “Siguiente Cabecera” es de 6 para TCP y 17 para UDP

13.2.1 Extensiones de Cabecera

Cabecera base	Extensión 1		Extensión n	Datos

Los datos más representativos de las extensiones son:

- La mayoría de extensiones se examinan sólo en el destino
- Los routers de IPv6 transportan como mínimo 536 octetos de carga
- Autenticación
- Encapsulación de Seguridad: Confidencialidad
- Opción de Salto a Salto
- Opciones de Destino:
  - Sólo basado en la cabecera

Siguiente Cabecera Base =TCP	Segmento TCP

  - Basado en cabecera y una extensión de cabecera

Siguiente Cabecera Base=TCP	Siguiente Cabecera de Direccionamiento=TCP	Segmento TCP

  - Basado en cabecera y dos extensiones de cabecera

Siguiente Cabecera Base=TCP	Siguiente Cabecera de Direccionamiento=Auth	Siguiente Cabecera de Direccionamiento=TCP	Segmento TCP

14Anexo 5: Movilidad IP

El objetivo básico de MIP es conseguir que el terminal móvil sea capaz de comunicarse utilizando la misma dirección IP en todo momento, independientemente del punto de acceso a Internet, esto permite asegurar la continuidad de servicio de una sesión activa y que el movimiento es completamente transparente a las aplicaciones.

A cada terminal móvil se le asigna una dirección IP perteneciente a su red particular, esta dirección permanece inalterada aunque la ubicación del terminal varíe y cada paquete dirigido a él se envía a la dirección IP de la red particular.

Si la estación móvil se conecta a la subred particular, se comporta como cualquier terminal fijo, dado que posee una interfaz lógica configurada con su dirección particular y accesible a través del direccionamiento normal de IP. En el momento que la estación móvil abandona la subred particular el terminal no es accesible, disponiendo sólo de la información de su dirección particular, es necesario lo que se ha denominado care-of-address (COA), es decir, una dirección de la subred IP visitada. La COA identifica la ubicación instantánea del terminal y puede ser:

- La dirección de un router (agente extranjero (FA)) de la subred visitada, que gestione el tráfico hacia el terminal móvil.
- Una dirección conseguida por el terminal móvil a partir de un mecanismo de autoconfiguración, en este caso se denomina care-of-address ubicada.

El protocolo de gestión de movilidad se encarga de permitir que el terminal móvil pueda continuar comunicándose utilizando su dirección particular aunque esté fuera de su red. Para ello, uno de los routers conectados a la subred particular debe estar configurado como agente particular (HA).

En el momento en que el terminal móvil se mueve de una subred a otra, debe registrar su COA en el HA. El resto de estaciones desconocen la ubicación del terminal móvil y sólo pueden enviar paquetes a su dirección particular. A través del mecanismo de direccionamiento IP normal, el paquete llega a la red particular donde es interceptado por el HA quien lo redirecciona al terminal móvil mediante un mecanismo de túnel. El nodo móvil, por otra parte puede contestar a la estación emisora directamente, utilizando su dirección particular como la dirección origen.

La única diferencia entre el mecanismo de IPv4 y IPv6 consiste en que con IPv4 las direcciones se consiguen a partir del FA y en IPv6, deja de existir la imagen de FA, y todas las direcciones son de tipo care-of-address ubicada.

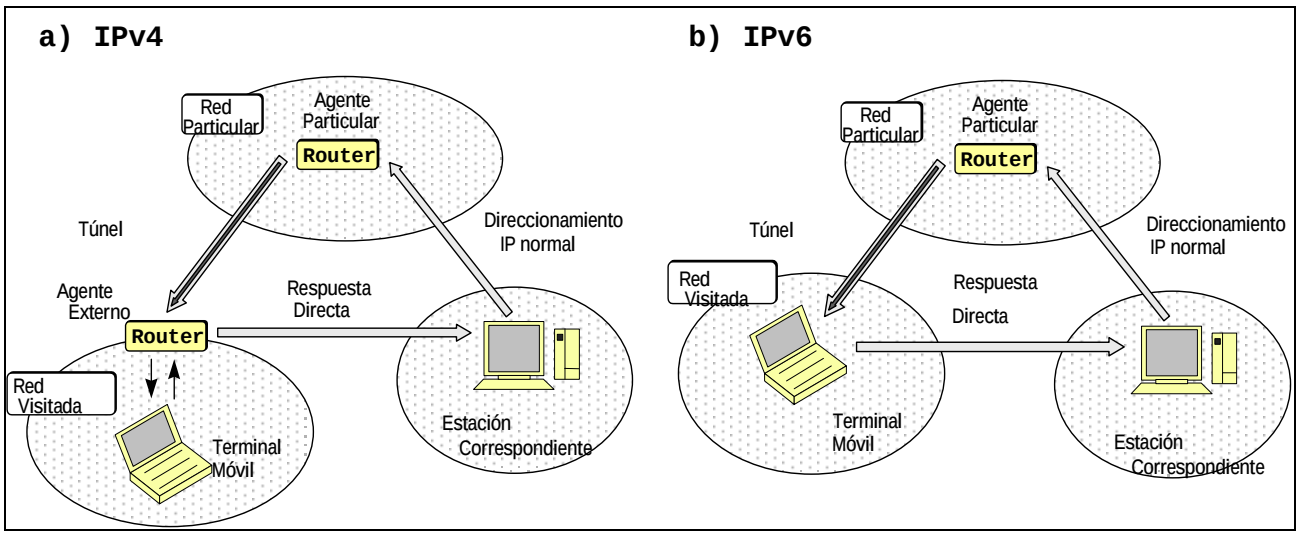


Figura 54. Arquitectura básica de Movilidad IP

14.1 Optimización de direccionamiento

El modo de operación descrito en el apartado anterior es muy simple y ocasiona una serie de inconvenientes a la hora de direccionar el tráfico desde la red particular a la red visitada:

- Se genera un tráfico adicional en la subred particular
- El tiempo de latencia al transferir el tráfico hasta el destino es largo

Estos aspectos han hecho que se considere la posibilidad de mejorar este protocolo con la introducción de un mecanismo que permite a cualquier estación, que tenga datos transferidos en curso (no sólo a HA), conocer la COA asociada al terminal de forma, que a partir del momento en que la dirección asociada al terminal es revelada a la estación, ésta puede direccionar el mensaje al terminal sin pasar por la red particular.

14.1.1 Optimización direccionamiento para IPv4

El protocolo especificado para IPv4 implica que HA indica la COA del terminal móvil al nodo correspondiente, cuando el terminal móvil esta fuera de su red particular. Después de recibir un mensaje para el terminal móvil, HA ejecuta el túnel hacia la adecuada COA y a la vez envía un mensaje “Binding Update” al nodo emisor. A partir de la recepción del mensaje, el nodo puede enviar el tráfico con destino al terminal móvil directamente a su dirección mediante el mecanismo de túnel.

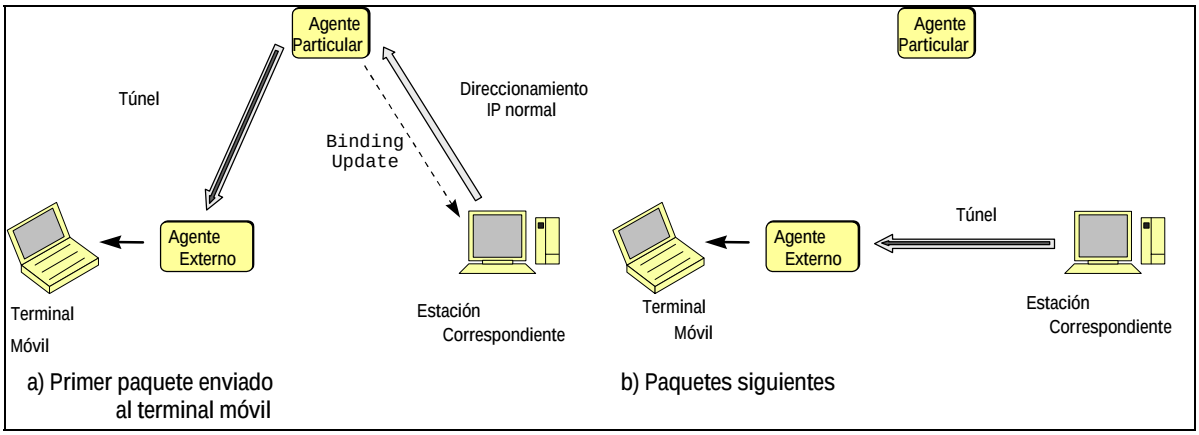


Figura 55. Optimización de direccionamiento en IPv4

El proceso definido hasta el momento no garantiza la optimización de direccionamiento permanente, es necesario un mecanismo a partir del cual la estación pueda conocer la nueva ubicación del terminal móvil cada vez que este se mueva. Para ello, el terminal móvil cada vez que se desplace a una nueva subred, debe comunicar su nueva dirección a su anterior FA. De esta manera, cuando un nodo intente alcanzar el terminal móvil con la care-of-address obsoleta, el FA recibirá el tráfico y mediante túnel lo reenviará a la nueva dirección, a la vez que comunicará al nodo emisor la COA actual del terminal.

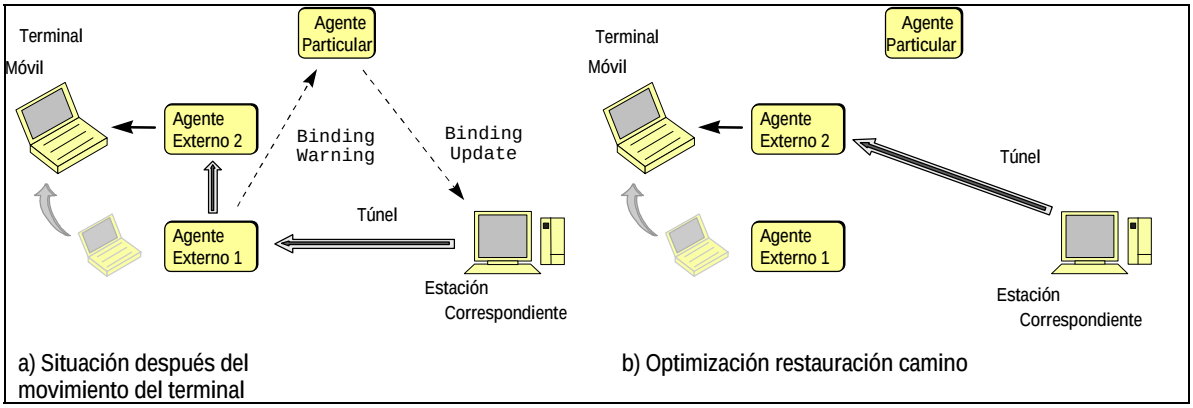


Figura 56. Movimiento del terminal móvil con notificación del FA anterior

En el caso de que el FA no conociera la nueva dirección del terminal, enviaría el tráfico al HA mediante túnel y éste a su vez, con el mismo mecanismo, lo redireccionaría al terminal. Al mismo tiempo notificaría al nodo emisor con un mensaje de “Binding Update” la nueva COA.

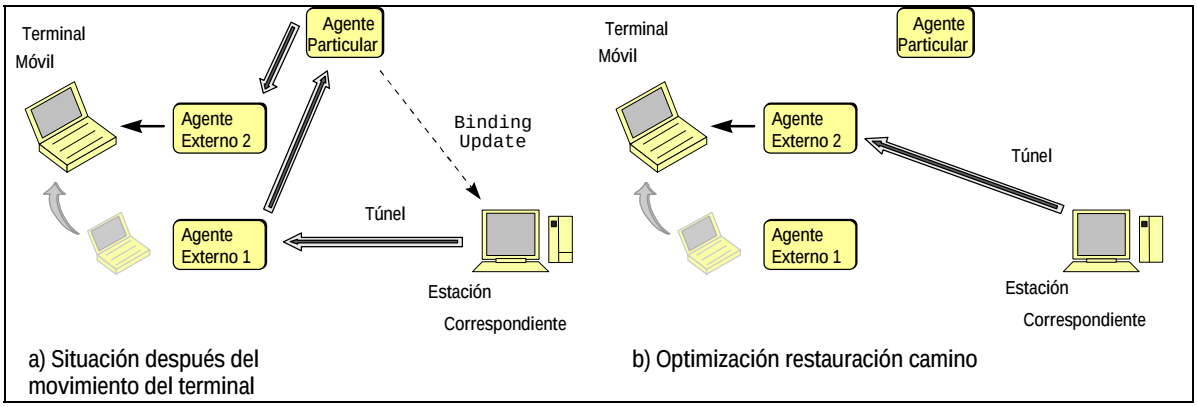


Figura 57. Movimiento del terminal móvil sin notificación al FA anterior

La optimización del direccionamiento tiene la ventaja de minimizar el tráfico de señalización entre el terminal móvil y el FA, dado que los mensajes "Binding Update" dirigidos al nodo se transmiten desde el agente particular. Este hecho es importante ya que este tipo de mensajes se codifican en paquetes UDP separados del tráfico de datos, lo que implica una sobrecarga de flujo importante para una conexión sin cables como es la del móvil y el FA.

14.1.2 Optimización del Direccionamiento para IPv6

A diferencia del protocolo definido para IPv4, el protocolo de Optimización del Direccionamiento para IPv6 requiere que sea el terminal móvil quien transmita directamente el mensaje "Binding Update" al nodo correspondiente. Esto reduce el tiempo de latencia de adquisición de la nueva care-of-address por parte del nodo.

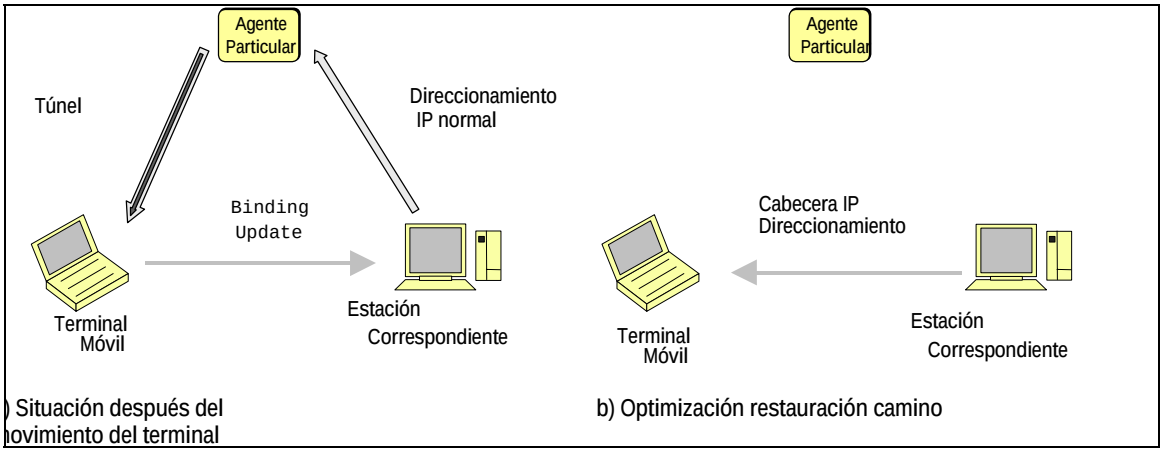


Figura 58. Optimización del Direccionamiento en IPv6

Esta solución es posible porque en la nueva versión del protocolo IP se codifica el mensaje de "Binding Update" como una extensión de cabecera IPv6.

14.2 Seguridad

Los aspectos de seguridad más relevantes al aplicar movilidad IP son:

- El HA debe ser capaz de autentificar los mensajes que recibe del terminal móvil para impedir que un registro falso pueda derivar en el direccionamiento del tráfico a una red IP diferente de la visitada
- Si se utiliza el protocolo de Optimización del Direccionamiento, cada nodo debe poder autentificar los mensajes “Binding Update” recibidos del terminal móvil o del HA. Esta capacidad implica desarrollar un mecanismo de acuerdo de claves de forma dinámica entre dos estaciones.

14.2.1 AAA (Autenticación, Autorización y Cuentas)

Cuando se ofrece un servicio de acceso a una red de datos, existen requerimientos de autenticación, autorización y de contabilidad. Uno de los requerimientos es la actualización de los registros de la base de datos de HLR con información de coste y otro es el uso de mecanismos de autenticación AAA. Este mecanismo está siendo definido por el IETF.

El objetivo de IETF es crear un servidor genérico AAA que soporte las necesidades de diferentes aplicaciones que requieren autenticación de usuarios, gestión de peticiones de autorización y información de cuentas. Esto podría realizarse a partir de una red de servidores AAA conectados. En la siguiente figura se observa un modelo de esta propuesta.

Leyenda:

1. Usuario que quiere acceder a un servicio o recurso.
2. Dominio de Usuario particular o, Autoridad Particular (AAAH). Dispone de un acuerdo con el usuario.
3. Servidor AAA proveedor del servicio o, Autoridad Local (AAAL), que autoriza el servicio.
4. Equipamiento de servicio del proveedor que ofrece el servicio en sí.

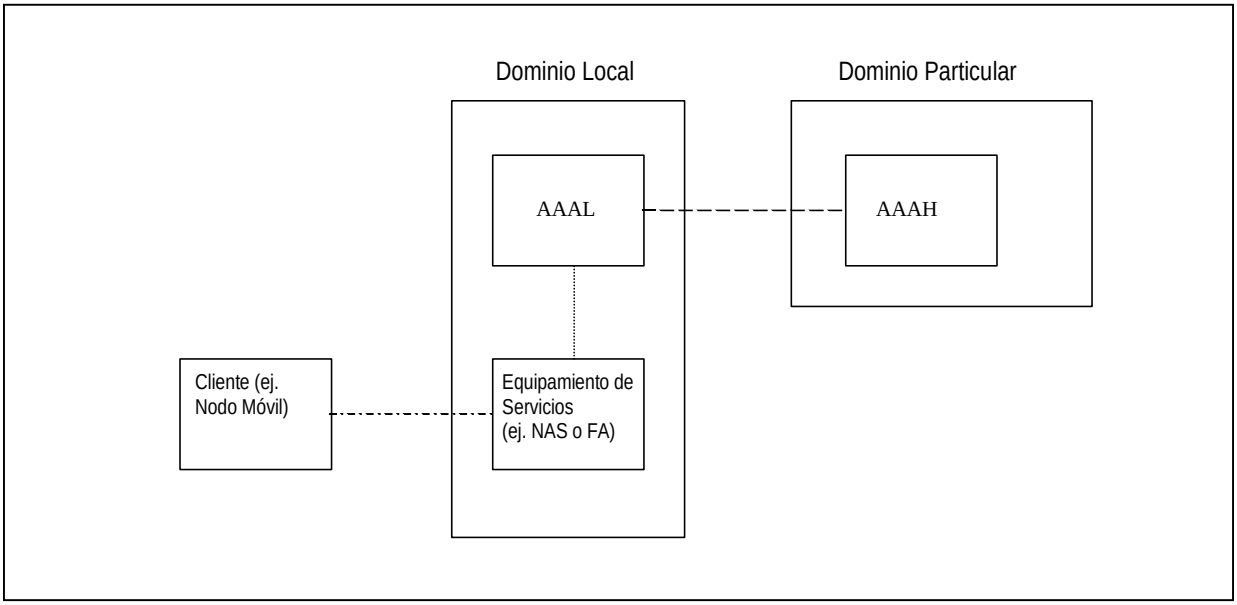


Figura 59. Modelo básico de AAA

14.2.2 MIP para UMTS

En este apartado se describe las propuestas de uso de MIP en UMTS. En [21], [5] pueden encontrarse más detalles.

Existen tres propuestas para la incorporación de MIP como sistema de movilidad de UMTS:

La primera consiste en utilizar la estructura GPRS actual para gestionar la movilidad en la PLMN, mientras se utiliza MIP para comunicación entre otros sistemas, por ejemplo LANs.

La segunda consiste en unir SGSN y GGSN sin alterar las interfaces, aunque para optimizar el direccionamiento se modifica el GGSN/FA después de que MS transfiera los datos.

La tercera, implica la utilización de MIP tanto para la movilidad interna de PLMN como para la relación con otros sistemas.

14.2.2.1 Propuesta 1

MIP ofrece la ventaja de ser independiente del sistema de acceso, lo que permite al usuario moverse de un sistema a otro. Asumiendo un impacto mínimo en GPRS, implica los siguientes requerimientos:

- MS debe ser capaz de encontrar un FA.
- Al establecer un contexto PDP, MS debe ser informado de los parámetros de red del FA.
- Se asume que MS mantendrá la misma COA mientras el contexto PDP esté activado.

En la siguiente figura se muestra un ejemplo de red con propuesta 1 aplicada.

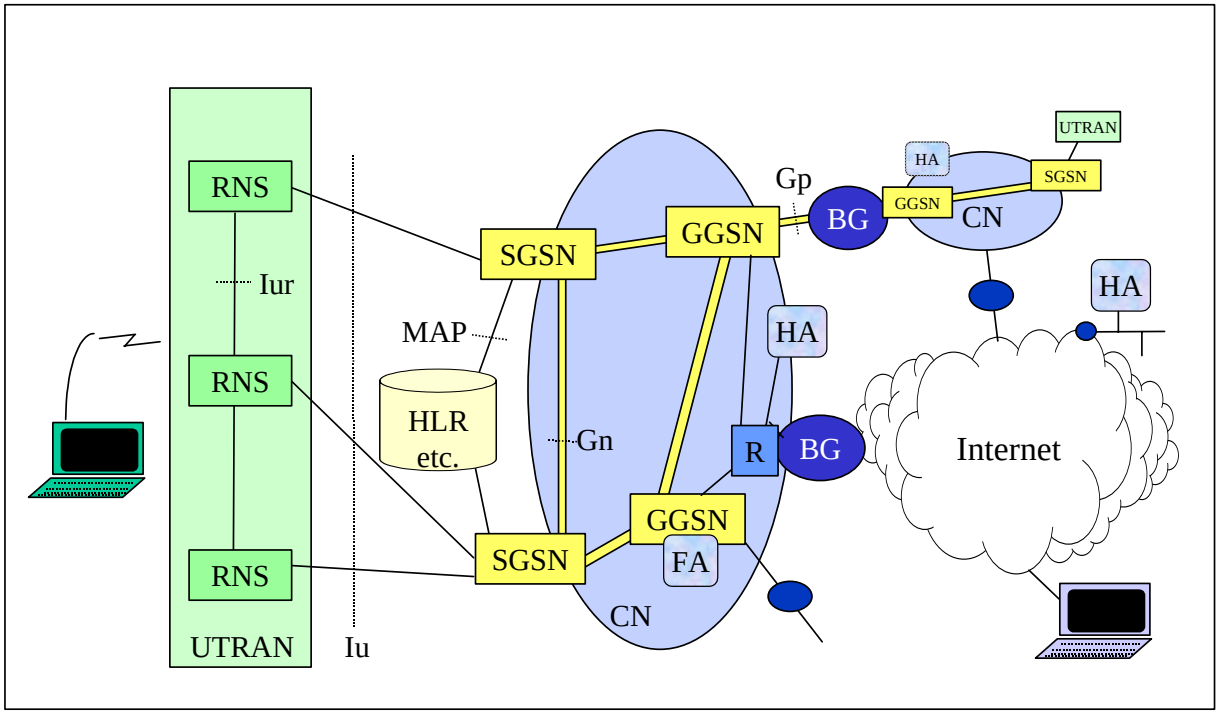


Figura 60. Arquitectura de Red con Movilidad de tipo propuesta 1

14.2.2.2 Propuesta 2

Esta propuesta se basa en un sistema GPRS - IP móvil intermedio. Una forma de implementarlo es juntar SGSN y GGSN, como puede verse en la siguiente figura.

En esta implementación MS no tiene porque mantener la misma COA durante una sesión. Si MS no está transmitiendo datos mientras se mueve de un SGSN a otro, puede establecerse un nuevo contexto PDP entre el nuevo SGSN y su GGSN asociado proporcionando a MS una nueva dirección. Si MS transmite datos entonces se mantiene el contexto PDP en el GGSN antiguo, mientras no finalice la transmisión. Al acabar ésta, el contexto PDP puede moverse al nuevo SGSN obteniendo la nueva COA.

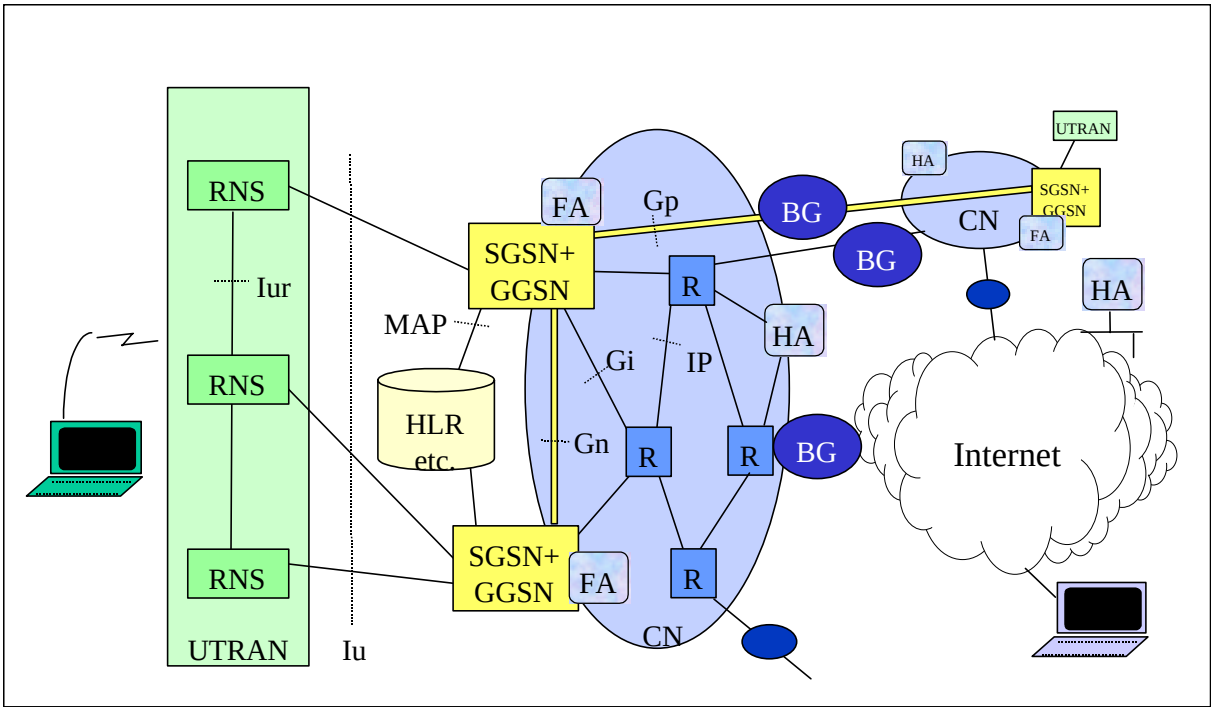


Figura 61. Arquitectura de Red con Movilidad de tipo propuesta 2

14.2.2.3 Propuesta 3

Esta propuesta se basa en dejar que MIP gestione toda la movilidad del sistema incluida la movilidad entre GGSNs. Para ello se combinan SGSN y GPRS en un único nodo llamado Nodo de soporte GPRS para Internet (IGSN). En el siguiente ejemplo puede observarse el proceso de cooperación entre GPRS y MIP cuando el terminal permanece en su red IP particular.

El proceso consta de los siguientes pasos:

1. El terminal llega a una nueva UTRAN y escucha los mensajes de radio que contienen información sobre los parámetros de radio, red, etc.
2. El terminal envía una petición de registro incluyendo parámetros como identidad, proveedor de servicio,...
3. UTRAN gestiona la petición de registro con IGSN quien:
   3.1. Contacta con el HLR del terminal móvil para obtener los datos necesarios para la autenticación
   3.2. Una vez comprobada la identidad del terminal con éxito y reconocer que se encuentra en la UTRAN actual, se encripta toda la información relativa a la interfaz de radio. La clave de encriptación se obtiene de HLR.
4. En este momento el terminal ya se puede comunicar a nivel IP. El terminal atiende a los mensajes del router y solicita al servidor de DHCP, Protocolo de Configuración de Host Dinámico, parámetros de configuración y una COA de MIP.

5. El terminal contacta entonces con su agente particular (HA) para registrar su nueva dirección COA de acuerdo con el estándar de MIP.
6. El HA debe decidir si aceptar o rechazar la COA. Antes de la decisión, HA puede contactar con HLR a través de una nueva interfaz, Gh, a fin de obtener información del terminal. Además las claves a utilizar para IPsec AH o ESP entre el terminal y el HA pueden obtenerse de HLR. El terminal móvil puede derivar sus claves a partir de la información de su USIM.
7. Mientras el terminal está conectado y transmite datos, IGSN gestiona los detalles de pagos y clientes, esta información también puede ser utilizada por UMTS.

El caso de que el terminal móvil esté en una red externa es similar, la única diferencia es que el nodo IGSN de la red visitada contacta con el HLR de la red particular del terminal, bien a través de SS7 o por mensajes de protocolo de MAP mediante un mecanismo de túnel por Internet o por una red PLMN IP.

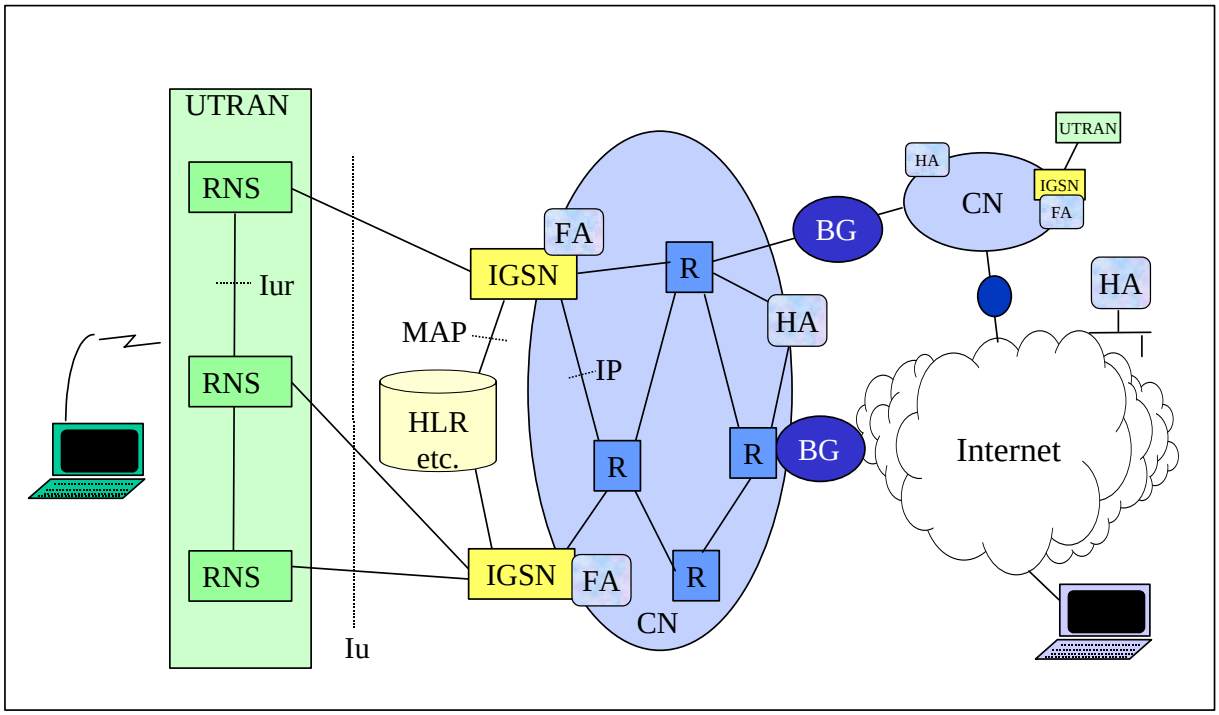


Figura 62. Arquitectura de Red con Movilidad de tipo propuesta 3

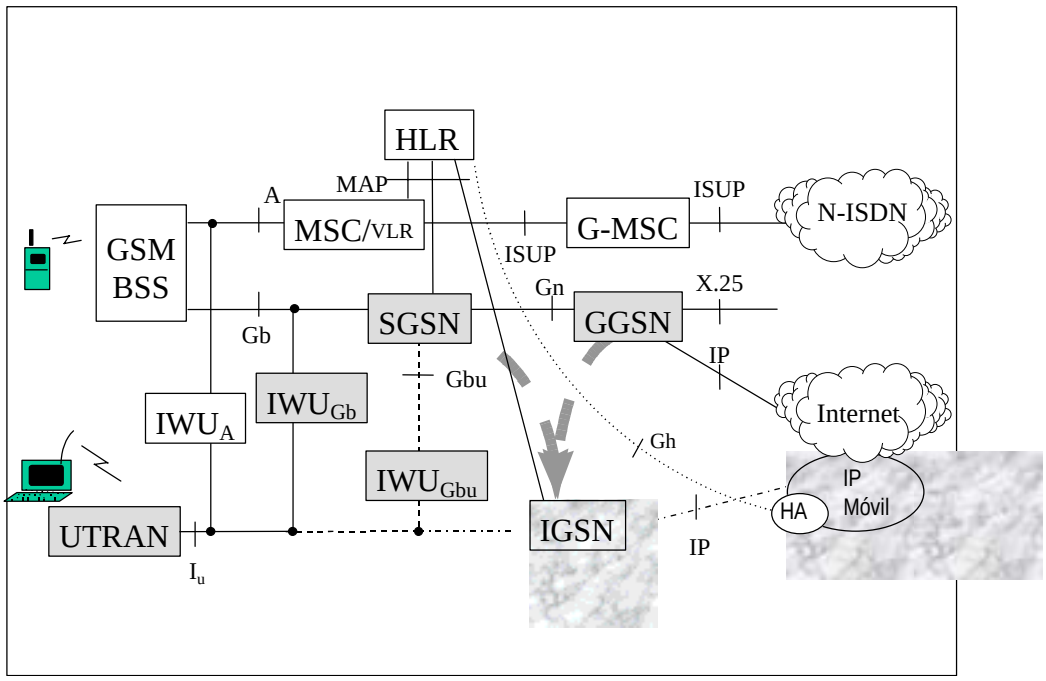
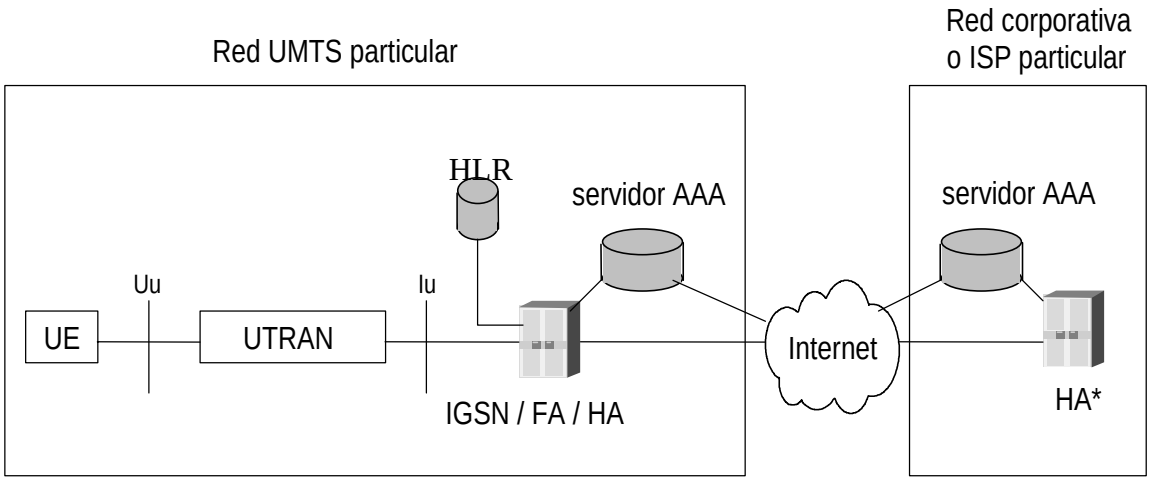


Figura 63. Interfaces de UMTS considerando IGSN

14.2.2.4 AAA de MIP para UMTS

El procedimiento de seguridad de MIP es independiente de los mecanismos establecidos en UMTS, la autorización basada en la autenticación de identidad de UMTS no es suficiente ya que la identidad de red de datos y la identidad de UMTS no tienen porque estar relacionadas. La seguridad a nivel de MIP se basa en la interacción de servidores AAA.

La movilidad IP en UMTS ofrece la separación de la identidad de acceso a radio y a red de datos. Así la autenticación de servidor de AAA / FA / HA es independiente de la autenticación de IGSN / HLR. Aunque pueden aparecer juntos, IGSN y FA disponen de dos interfaces lógicas independientes para los dos sistemas de seguridad. Los servidores de AAA pueden o no formar parte de la red UMTS.



(*) El operador de UMTS particular puede ofrecerlo como servicio outsourcing

Figura 64. UE asociado al Dominio particular del operador de UMTS

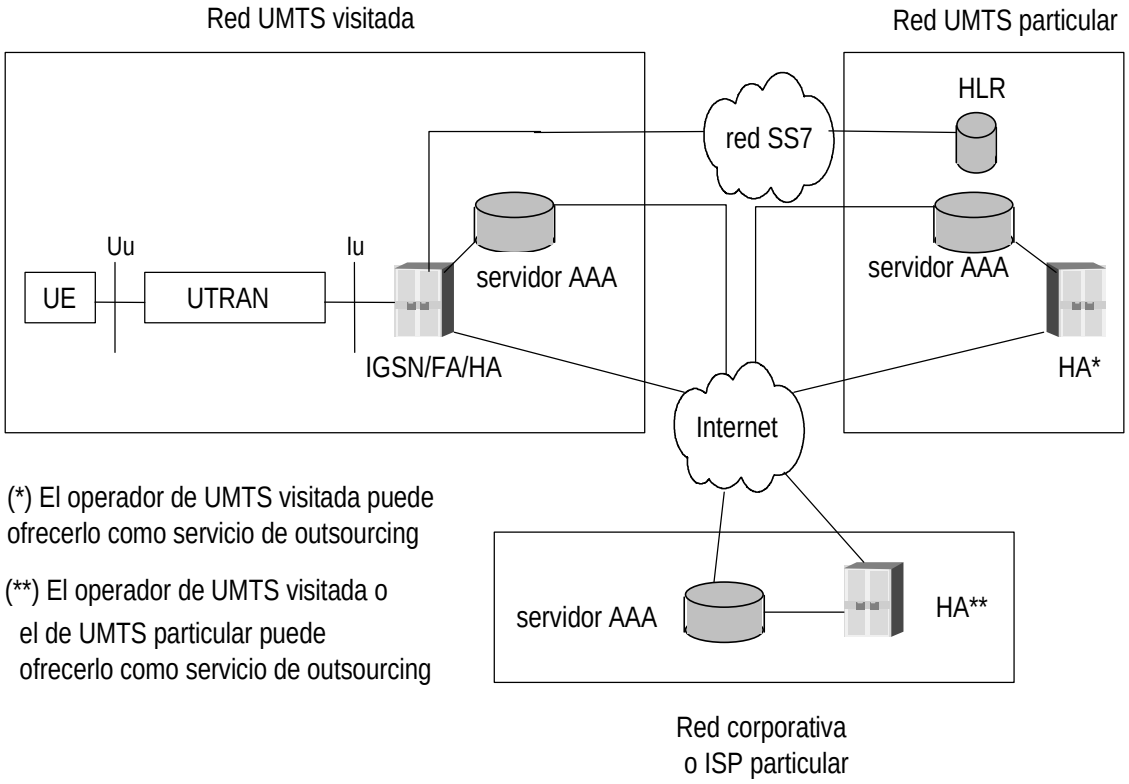


Figura 65. UE no asociado al Dominio particular del operador de UMTS

Estos procedimientos todavía no han sido definidos para IPv6, pero se espera que sean similares a los definidos para IPv4

14.2.3 Uso de IPsec

Las conexiones permanentes de IPsec establecidas y gestionadas por IGSN, permiten que la información de señalización se transmita de forma segura. La información de señalización se transmite en modo transporte.

IGSN puede tener direcciones IP específicas dedicadas exclusivamente a señalización.

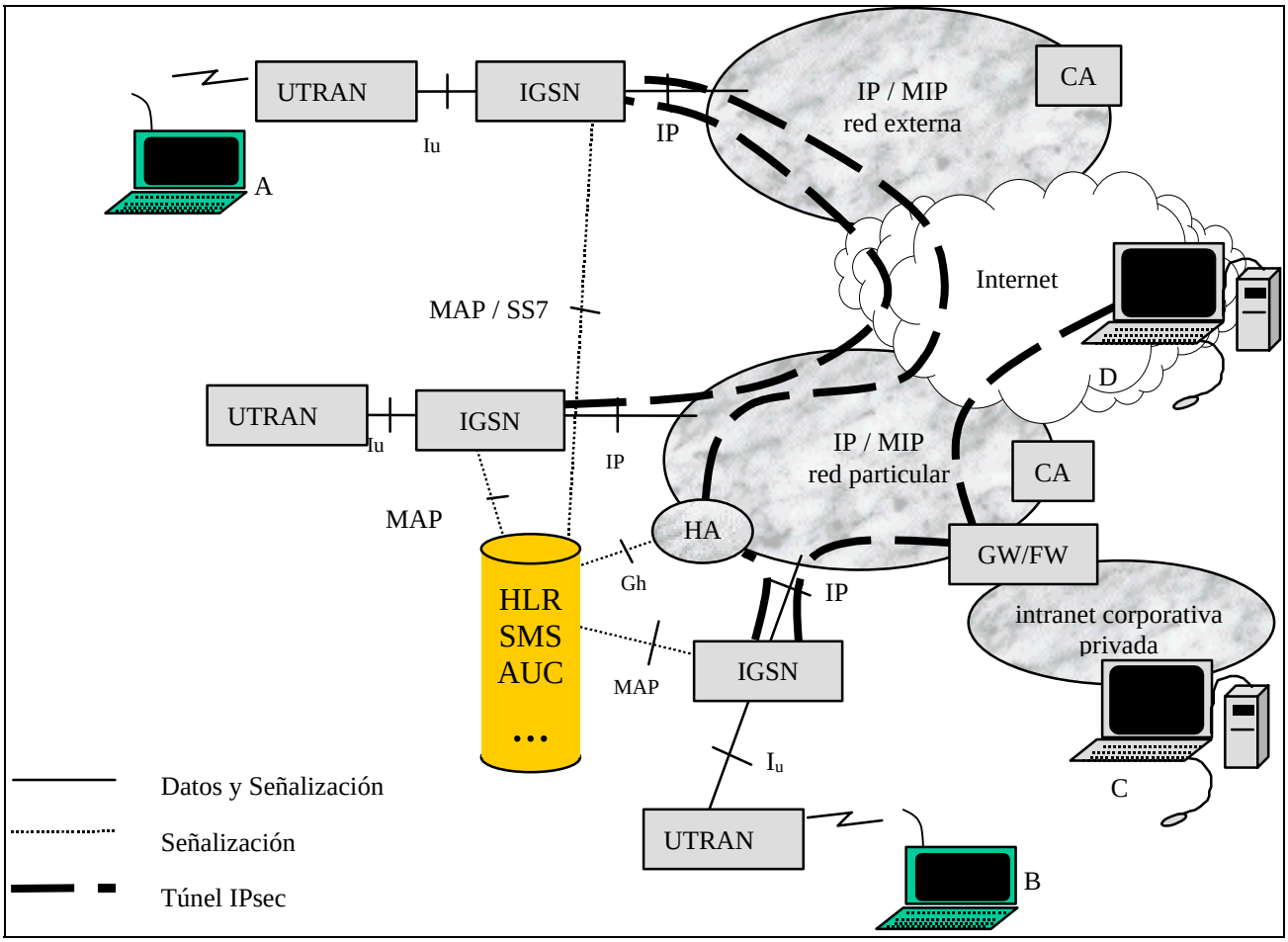


Figura 66. IPsec para conexión con intranet corporativa privada

14.2.3.1 Encriptación de MIP

En IPv4 sólo la autenticación es obligatoria, la encriptación es a pesar de ello aconsejable.

14.2.3.2 Autenticación a nivel de IP

HA al recibir una petición de registro puede comprobar si MS está correctamente autentificado en UTRAN, aún así, esto no es suficiente para saber quién está realizando la petición sin una autenticación a nivel de IP. Por ejemplo, un intruso se registra en UTRAN de forma correcta y recibe su COA correspondiente pero no la comunica a HA. Posteriormente un usuario legítimo se registra en UTRAN e intenta registrarse a su vez, en HA con su COA, si en este momento el intruso intercepta este mensaje y modifica la COA puede sustituir al usuario legítimo. En IPv4 es obligatorio que todas las implementaciones utilicen MD5 con clave de 128 bits, sin excluir otros métodos. En la tarjeta SIM de GSM también existe una clave Ki de 128 bits pero dado que ésta solo se conoce en AUC, no puede utilizarse para MIP y debemos usar claves diferentes para autenticar los mensajes de MIP.

Existen dos propuestas de autenticación, la primera consiste en el uso de claves públicas / privadas, si todos los usuarios conocen la clave pública de su HA y las claves públicas de todos los usuarios están almacenadas, por ejemplo, en HLR siendo éste accesible para HA, entonces se puede mantener un intercambio de mensajes MIP autentificado. La segunda propuesta consiste en la utilización de claves públicas de un tercer elemento de confianza combinado con certificados digitales, esta proposición presenta varias ventajas, una de ellas es que dos IGSN de dominio IP de CN diferentes, pueden utilizar certificados digitales como método de autenticación sin que se conozcan previamente, otra ventaja es que la incorporación de una nueva IGSN sólo implica la actualización del CA.

14.2.3.3 Seguridad en IPv6

En IPv6 por cada mensaje de MIP generado por ME, éste debe establecer una nueva conexión de IPsec con el HA o utilizar una existente no expirada. IPv6 gestiona de forma nativa la autenticación (y la encriptación).

15Anexo 6: Red de Acceso a Radio Terrestre de UMTS (UTRAN)

En este apartado se describe el subsistema de UTRAN, arquitectura, funcionalidad e interfaces.

Las características principales del diseño de UTRAN son la separación lógica de las funciones de la CN y de transporte, así como la separación de la información de señalización y la de transporte de datos. Otro de los puntos a tener en cuenta es que UTRAN realiza el control completo del servicio de movilidad de las conexiones RRC.

En la figura siguiente puede verse la arquitectura simplificada de UMTS junto con los puntos de referencia y las interfaces asociadas a UTRAN.

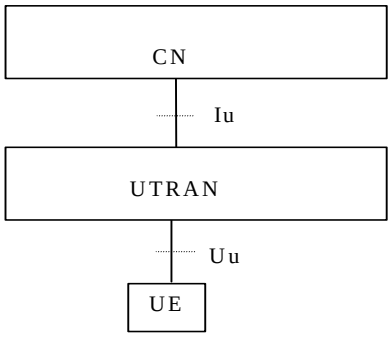


Figura 67. Arquitectura simplificada de UMTS

15.1 Arquitectura General de UTRAN

UTRAN consiste en un conjunto de subsistemas de Red de Radio (RNS) conectados con la CN a través de Iu. A su vez un RNS consiste en un Controlador de Red de Radio (RNC) y uno o más Nodos B, que se conectan con el RNC por la interfaz de Iub y donde cada uno de ellos es responsable de un conjunto de celdas.

En la UTRAN los RNCs del RNS pueden estar interconectados a través de la interfaz de Iur. Tanto la interfaz de Iu como Iur son interfaces lógicas.

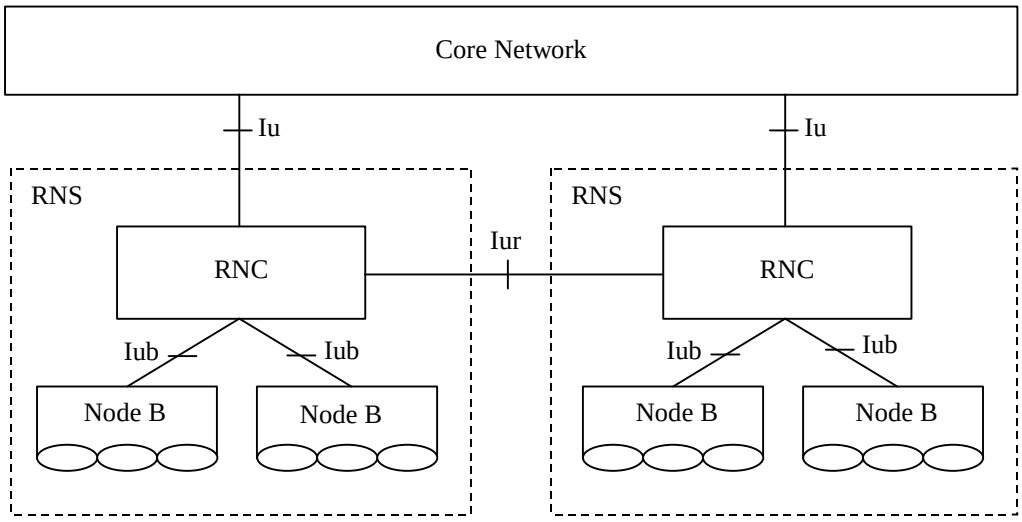


Figura 68. Arquitectura de UTRAN

15.2 Arquitectura de protocolos

Los protocolos de la interfaz de Iu y Uu pueden clasificarse en protocolos del plano de usuario, aquellos que implementan el servicio de canal lógico de acceso a radio actual, y en protocolos del plano de control, aquellos que gestionan los canales lógicos de acceso a radio y las conexiones entre el UE y la red.

15.2.1 Protocolos del plano de usuario

El Estrato de Acceso proporciona el servicio de canales lógicos de acceso a radio entre SAP y SAP.

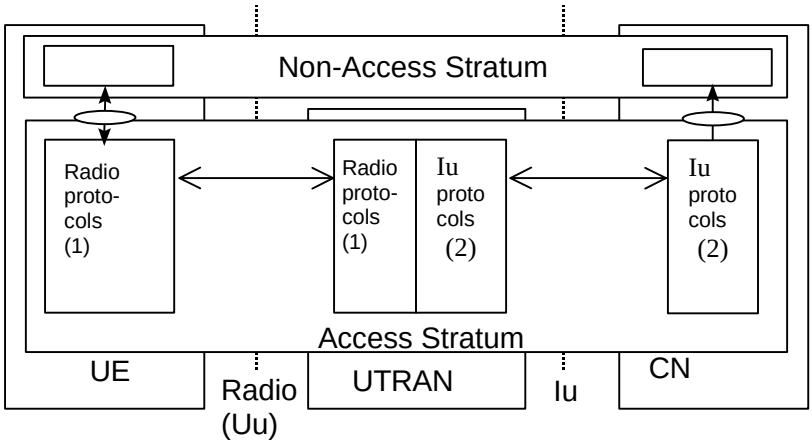


Figura 69. Plano de Usuario de Iu y Uu

15.2.2 Protocolos del plano de control

En la siguiente figura pueden verse los protocolos utilizados en el plano de control para Iu y Uu.

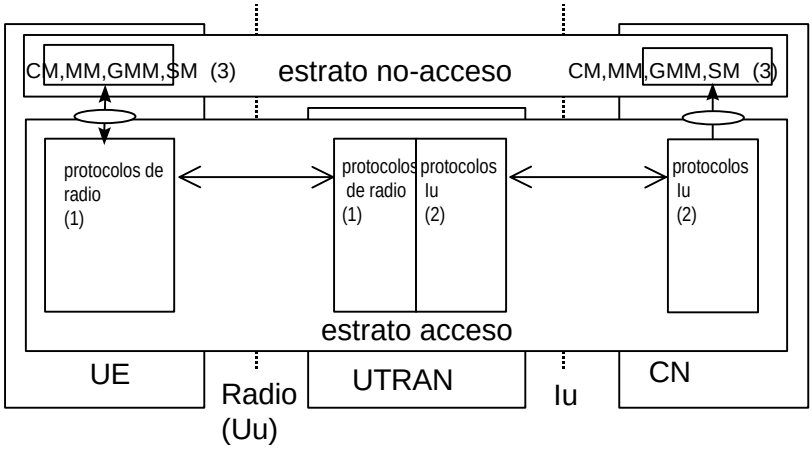


Figura 70. Plano de control para Iu y Uu

15.3 Funciones de UTRAN

Las principales funciones realizadas por UTRAN son:

- Funciones relativas al control de acceso del sistema
    - Control de Admisión
    - Control de Congestión
    - Distribución de información del sistema
- Cifrado y Descrifrado del canal de radio
- Funciones relativas a movilidad
    - Gestión
    - Reasignación de SRNS
- Funciones relativas a la gestión y control de los recursos de radio
    - Configuración y operación de los recursos de radio
    - Seguimiento del entorno de radio
    - Control de multiplexación / demultiplexación de datos
    - Control de canales lógicos
    - Asignación / Anulación de Canales Lógicos

- Funciones de protocolos de radio
- Función de Distribución de CN para mensajes no pertenecientes al Estrato de Acceso

- Funciones relativas a diseminación

15.4 Interfaces de UTRAN

En la figura presentada a continuación puede observarse el modelo general de interfaces de UTRAN, la estructura se basa en el principio de independencia lógica entre niveles y planos.

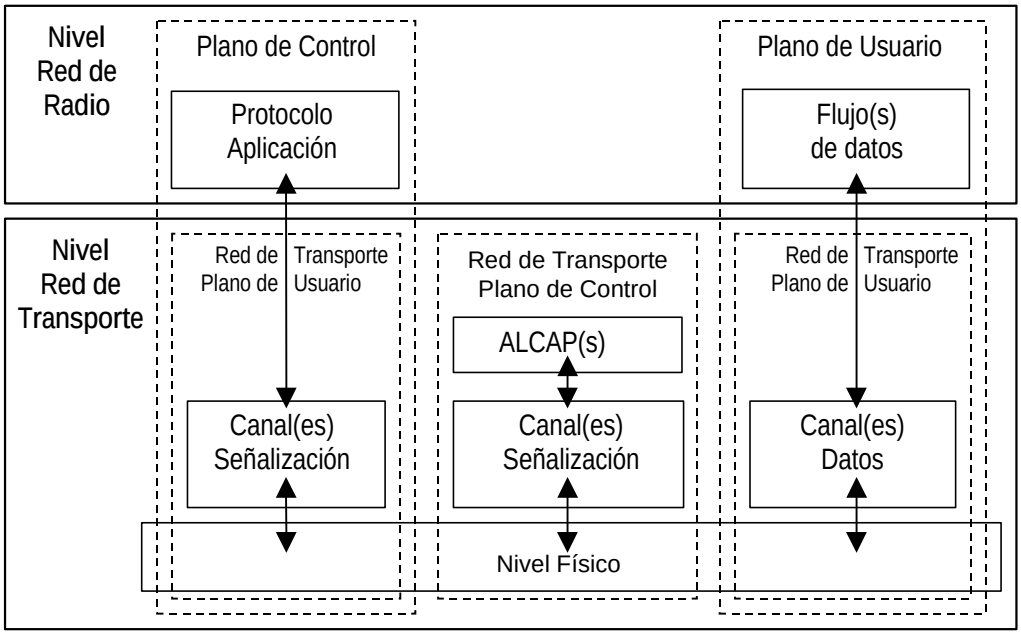


Figura 71. Modelo de Protocolos utilizados en las interfaces de UTRAN

Niveles Horizontales

La estructura del protocolo se basa en dos niveles, Nivel de Red de Radio y Nivel de Red de Transporte. Todos los puntos relativos a UTRAN, sólo son visibles a nivel de Red de Radio ya que el Nivel de Red de Transporte representa tecnología de transporte estándar sin ningún requerimiento específico para UTRAN.

Planos Verticales

Plano de Control

El plano de control incluye el Protocolo de Aplicación, por ejemplo RANAP, RNSAP o NBAP, y el Canal lógico de Señalización para el transporte de mensajes del Protocolo de Aplicación.

Plano de Usuario

El plano de usuario incluye Flujo(s) de Datos y Canales lógicos de Datos para los mismos.

Plano de Control de Red de Transporte

El plano de control de red de transporte no incluye ninguna información del Nivel de Red de Radio y está completamente en el Nivel de transporte. Sí incluye el protocolo de ALCAP utilizado en la inicialización de canales lógicos para el Plano de Usuario, así como los canales lógicos necesarios para el protocolo de ALCAP.

Plano de Usuario de Red de Transporte

El plano de usuario de red de transporte incluye los canales lógicos para el plano de usuario y para la señalización del protocolo de aplicación.

15.5 Interfaz Iu

La interfaz Iu se define entre CN y UTRAN y desde el punto de vista de la interfaz, el punto de acceso a UTRAN es RNC.

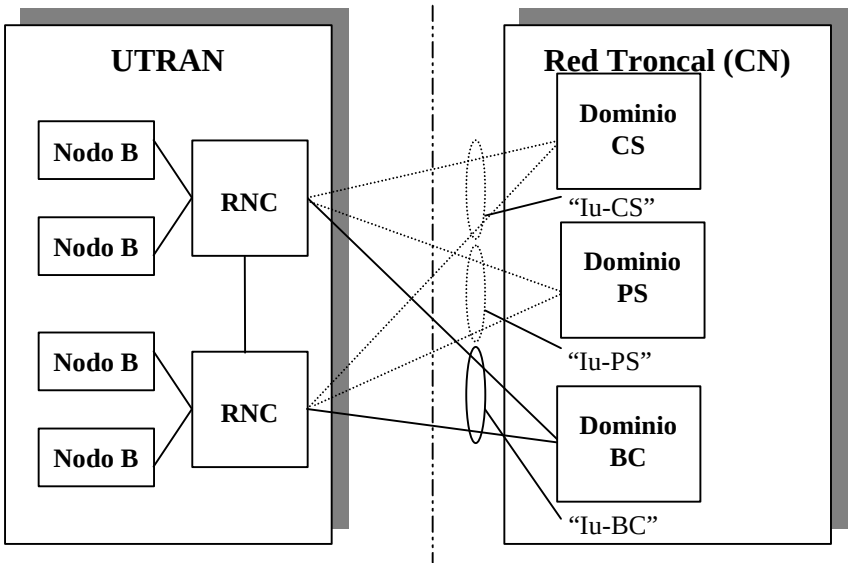


Figura 72. Arquitectura de la Interfaz Iu

Tal y como se refleja en la figura, la instancia de la interfaz Iu hacia el dominio PS se denomina Iu-PS, y la instancia hacia el dominio CS, Iu-CS. Iu-BS es el nombre que recibe la instancia hacia el dominio de diseminación. Sólo existe una Iu-CS y una Iu-PS.

Una arquitectura con CN separadas, implica que deben existir conexiones independientes tanto para la transmisión de información de señalización como para la transferencia de datos de usuario hacia los dominios de CS y PS, esto es aplicable al nivel de transporte y al nivel de radio. En arquitecturas con CN combinadas, existirán conexiones independientes en el plano de usuario para el dominio de PS y CS, aplicable tanto para nivel de transporte como el nivel de radio, y en el plano de control, existirán conexiones SCCP separadas para ambos dominios.

15.5.1 Funciones de la interfaz Iu

En la tabla presentada a continuación pueden verse las funciones definidas para la interfaz de Iu.

Función	**UTRAN**	**CN**
Funciones de Gestión RAB		
Establecer / Modificar / Eliminar RAB	X	X
Mapeo características RAB con canales lógicos Iu	X	
Mapeo características RAB con canales lógicos Uu	X	
Características RAB	X	X
Funciones de Gestión de Recursos de Radio		
Control de admisión de Recursos de Radio	X	
Información diseminación	X	X
Funciones de Gestión de conexión Iu		
Gestión de conexión de señalización Iu	X	X
Gestión VC ATM	X	X
Establecer / Eliminar AAL2	X	X
Gestión AAL5	X	X
Gestión Túneles GTP-U	X	X
Gestión TCP	X	X
Gestión de Buffer	X	
Gestión Plano de usuario Iu		
Gestión protocolo entorno plano de usuario Iu		X
Inicialización protocolo entorno plano de usuario Iu	X	
Funciones de Gestión de Movilidad		
Información de Localización	X	X
Reasignación y Cambio	X	X
Canal de avisos		X
Funciones de Seguridad		
Confidencialidad de datos		

Cifrado interfaz de radio	X	
Gestión CK		X
Confidencialidad identidad de usuario	X	X
Integridad de Datos		
Verificar Integridad	X	
Gestión de IK		X
Funciones de Acceso a Red y Servicios		
Datos de Señalización CN	X	X
Información Volumen de Datos	X	
Seguimiento UE	X	X
Información Localización	X	X
Funciones de Coordinación Iu		
Coordinación de canal de avisos	X	X

15.5.1.1 Funciones de Seguridad

Confidencialidad de datos

- Función de cifrado interfaz de radio
  A petición de la CN se activa el cifrado de los mensajes de la interfaz de radio. El cifrado puede incluir tanto datos de usuario como de señalización.

- Función de Gestión de CK
  La clave de cifrado y los algoritmos permitidos los proporciona CN pero es UTRAN quien selecciona el algoritmo a utilizar.

Integridad de datos

- Verificar integridad
  Esta función se realiza en UTRAN.

- Función de Gestión de IK
  La clave de integridad y los algoritmos permitidos los proporciona CN pero es UTRAN quien selecciona el algoritmo a utilizar.

15.5.2 Estructura de Protocolos de Iu

La señalización de Red de Radio sobre Iu consiste en la Parte de Aplicación de Red de Acceso a Radio (RANAP). Este protocolo incluye todos los mecanismos para gestionar los procesos entre CN y UTRAN así como la transmisión de forma transparente de mensajes entre CN y UE sin interpretación o procesamiento por parte de UTRAN.

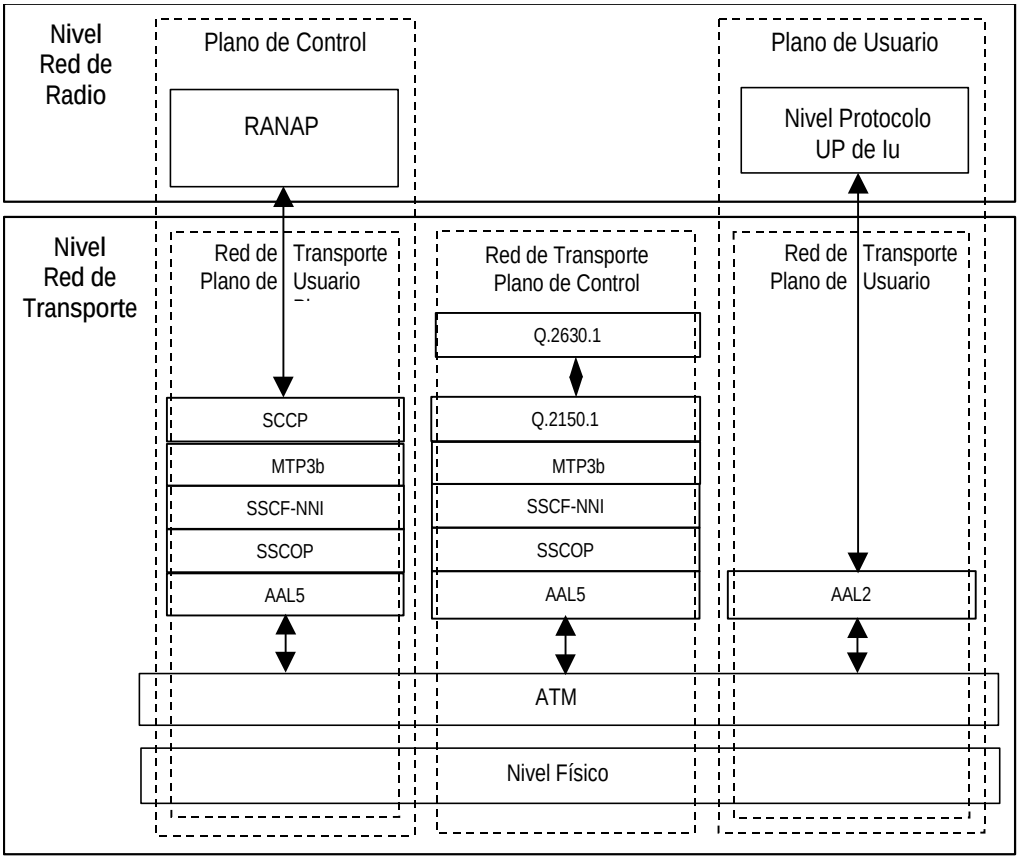


Figura 73. Estructura de Protocolos de Iu para el dominio de CS

SCCP, ofrece servicio no orientado a la conexión (clase 0), servicio orientado a la conexión (clase 2) y dentro del servicio orientado a la conexión realiza la separación y el establecimiento de las conexiones móvil por móvil.

MTP3-B, ofrece direccionamiento de mensajes, discriminación y distribución, así como gestión de conexiones de señalización.

SAAL-NNI, compuesto por SSCF, SSCOP y AAL5. SSCF mapea los requerimientos de los niveles superiores con los de SSCOP, gestiona conexiones SAAL, informa del estado de las conexiones y ofrece mecanismos para conocer el estado del procesador remoto. SSCOP presenta mecanismos para el establecimiento y eliminación de conexiones e intercambio seguro para información de señalización entre entidades de señalización. AAL5 adapta el protocolo de nivel superior a los requerimientos de ATM.

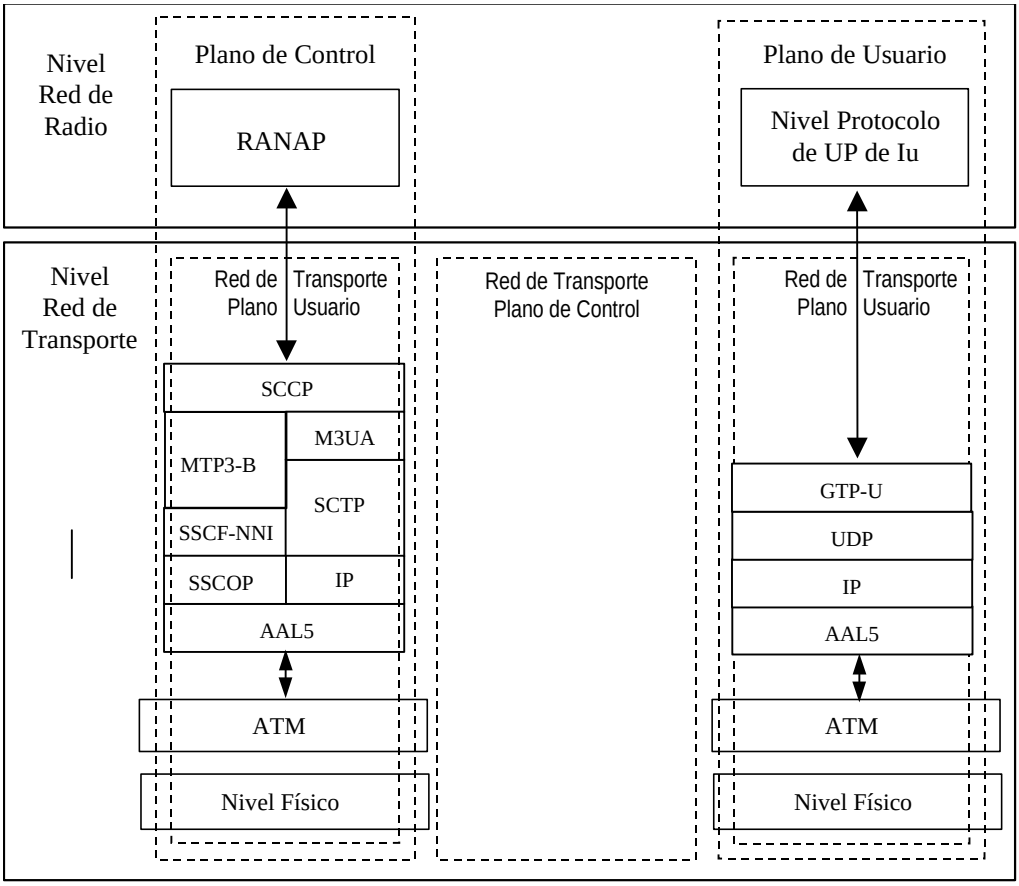


Figura 74. Estructura de protocolos de Iu para el dominio PS

SCCP, ofrece servicio no orientado a la conexión (clase 0), servicio orientado a la conexión (clase 2) y dentro del servicio orientado a la conexión realiza la separación y el establecimiento de las conexiones móvil por móvil.

MTP3-B, ofrece direccionamiento de mensajes, discriminación y distribución, así como gestión de conexiones de señalización.

SAAL-NNI, compuesto por SSCF, SSCOP y AAL5. SSCF mapea los requerimientos de los niveles superiores con los de SSCOP, gestiona conexiones SAAL, informa del estado de las conexiones y ofrece mecanismos para conocer el estado del procesador remoto. SSCOP presenta mecanismos para el establecimiento y eliminación de conexiones e intercambio seguro para información de señalización entre entidades de señalización. AAL5 adapta el protocolo de nivel superior a los requerimientos de ATM..

SCTP, se refiere al Protocolo de Transmisión de Control Simple, transmite diferentes protocolos de señalización sobre IP.

M3UA, Nivel de adaptación de SCCP a IP

15.5.3 Protocolo RANAP

El protocolo de RANAP ofrece servicios de señalización entre UTRAN y CN. Los servicios proporcionados por RANAP pueden clasificarse en tres grupos dependiendo de los Puntos de Acceso a Servicio (SAP).

Servicios de Control General

Relativos al total de la instancia de la interfaz de Iu entre RNC y el dominio lógico de CN, son accesibles en CN a través del SAP de Control General. Utilizan transporte de señalización no orientado a la conexión.

Servicios de Notificación

Relativos a un UE concreto o a todos los UEs de un área concreta y son accesibles desde CN a través del SAP de Notificación.

Servicios de Control Dedicados

Relativos a un UE y accesibles desde CN a través de un SAP de Control Dedicado. La conexión de señalización de Iu se establece con transporte de señalización orientado a la conexión.

Asimismo, RANAP ofrece dos modos diferentes para el transporte de señalización.

Servicio de transferencia de datos orientado a la conexión

Este servicio se establece en una conexión de señalización entre el dominio de RNC y CN. Es posible el establecimiento/liberación dinámica de conexiones de señalización y cada UE tiene su propia conexión de señalización.

La entrega de mensajes de RANAP se hace de forma secuencial y el protocolo de RANAP es notificado en caso de interrumpirse la conexión de señalización.

Servicio de transferencia de datos no orientado a la conexión

El protocolo de RANAP es notificado en caso de que un mensaje de RANAP no haya llegado a la entidad de RANAP destino

15.5.3.1 Funciones de RANAP

Las funciones asignadas al protocolo de RANAP son:

- Reasignación de SRNC
- Gestión de RABs
- Liberación/Petición de Liberación de todos los recursos de conexiones Iu

- Transferencia de contexto SRNS
- Control de sobre carga de la interfaz Iu
- Reinicialización de Iu
- Transferencia del ID común de UE a RNC
- Canal de avisos de usuario
- Control de la actividad del UE
- Transporte de información NAS entre UE y CN
- Control del modo de seguridad en UTRAN
- Información de Localización y Control de la información de localización
- Información de volumen de datos
- Información de situaciones de error

15.5.3.2 Procedimientos del protocolo de RANAP

En este apartado se citan los procedimientos utilizados por el protocolo de RANAP clasificados según la respuesta. Los procesos relativos a seguridad se detallarán en el siguiente apartado.

Procedimiento	Mensaje	Respuesta	Respuesta
		Con éxito	Sin éxito
Liberación Iu	IU RELEASE COMMAND	IU RELEASE COMPLETE	
Preparación Reubicación	RELOCATION REQUIRED	RELOCATION COMMAND	RELOCATION PREPARATION FAILURE
Asignación Recursos Reubicación	RELOCATION REQUEST	RELOCATION REQUEST ACKNOWLEDGE	RELOCATION FAILURE
Cancelar Reubicación	RELOCATION CANCEL	RELOCATION CANCEL ACKNOWLEDGE	
Transferencia contexto SRNS	SRNS CONTEXT TRANSFER	SRNS CONTEXT RESPONSE	
Control Modo de Seguridad	SECURITY MODE COMMAND	SECURITY MODE COMPLETE	SECURITY MODE REJECT
Listado Volumen de Datos	DATA VOLUME REPORT REQUEST	DATA VOLUME REPORT	
Diseminación Información CN	CN INFORMATION BROADCAST REQUEST	CN INFORMATION BROADCAST CONFIRM	CN INFORMATION BROADCAST REJECT
Reinicio	RESET	RESET ACKNOWLEDGE	
Recurso de Reinicio	RESET RESOURCE	RESET RESOURCE ACKNOWLEDGE	

Tabla 12. Procedimientos elementales con respuesta

Procedimiento	Mensaje
Petición liberación RAB	RAB RELEASE REQUEST
Petición Liberación Iu	IU RELEASE REQUEST
Detectar Reubicación	RELOCATION DETECT
Reubicación Completa	RELOCATION COMPLETE
Iniciación Transferencia Datos SRNS	SRNS DATA FORWARD COMMAND
Transferencia Contexto SRNS de la fuente RNC a CN	FORWARD SRNS CONTEXT
Transferencia Datos SRNS a RNC por CN	FORWARD SRNS CONTEXT
Canal de Avisos	PAGING
Identificador común	COMMON ID
Invocación Seguimiento CN	CN INVOKE TRACE
Desactivar Seguimiento	CN DEACTIVATE TRACE
Control Listado Ubicación	LOCATION REPORTING CONTROL
Listado Ubicación	LOCATION REPORT
Mensaje de UE Inicial	INITIAL UE MESSAGE
Control de Sobrecarga	OVERLOAD
Indicación de Error	ERROR INDICATION

Tabla 13. Procedimientos elementales sin respuesta

Procedimiento	Mensaje	Mensaje de Respuesta
Asignación RAB	RAB ASSIGNMENT REQUEST	RAB ASSIGNMENT RESPONSE x N (N>=1)

Tabla 14. Procedimientos con posibilidad de múltiples respuestas

15.5.3.2.1 Control de Modo de Seguridad

La finalidad de este procedimiento es permitir a CN pasar información de cifrado e integridad a UTRAN. Ésta utiliza la información para seleccionar los dispositivos de encriptación, tanto para datos de usuario como para señalización y además, le permite conocer los parámetros asociados al algoritmo de integridad. La tarea usa señalización orientada a la conexión.

CN inicia el proceso enviando a UTRAN un mensaje "Security Mode Command" especificando los posibles algoritmos de integridad y cifrado a utilizar por UTRAN. A la recepción de la instrucción, UTRAN internamente selecciona los algoritmos a usar, genera el evento para lanzar el procedimiento de la interfaz de radio y en caso necesario invoca la encriptación del dispositivo y la protección de integridad. Al finalizar este proceso de forma adecuada, UTRAN envía un "Security Mode Complete" a CN incluyendo los algoritmos de encriptación e integridad seleccionados.

El conjunto de algoritmos disponibles especificado en "Security Mode Command", debe permanecer a disposición de otras asignaciones de RAB y posibles reubicaciones internas de UTRAN.

En caso de UE con canales lógicos de acceso a radio hacia ambas CN, los datos de usuario del dominio de CS se encriptarán de acuerdo con la información recibida del dominio de CS y los del dominio de PS con la información recibida de PS. Los datos de señalización se cifrarán siempre con la última información de cifrado recibida y se aplicará la protección de integridad con la última información de integridad recibida.

En el caso de que UTRAN o UE no sean capaces de utilizar los algoritmos descritos en el mensaje "Security Mode Command" o si falla el procedimiento de Control de Seguridad de la interfaz de radio, se envía hacia CN un "Security Mode Reject" indicando el problema detectado.

15.5.3.3 Formato de Mensajes de Seguridad

15.5.3.3.1 Security Mode Command

Este mensaje es enviado por CN para activar las funciones de integridad y cifrado sobre la interfaz de radio. El canal establecido es un canal orientado a la conexión.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Tipo de Mensaje							
x.2(etc)	Información Protección de Integridad							
x.3(etc)	Información de Encriptación							
x.4(etc)	Estado de Clave							

Octeto x.2-... Información de protección de integridad

Datos relativos al procedimiento de integridad, incluye claves y algoritmos. Obligatorio

Octeto x.3-... Información de encriptación

Datos relativos al procedimiento de encriptación, incluye claves y algoritmos. Opcional

Octeto x.4-... Estado de clave

Estado actual de la clave. Obligatorio

15.5.3.3.2 Security Mode Complete

Este mensaje es enviado por RNC como respuesta de proceso finalizado con éxito. El canal establecido es orientado a la conexión.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Tipo de Mensaje							
x.2(etc)	Algoritmo de Protección de Integridad Seleccionado							
x.3(etc)	Algoritmo de Encriptación Seleccionado							
x.4(etc)	Diagnóstico							

Octeto x.2-... Algoritmo de Protección de Integridad Seleccionado

Algoritmo seleccionado por UTRAN para aplicar el servicio de integridad. Obligatorio

Octeto x.3-... Algoritmo de Encriptación Seleccionado

Algoritmo seleccionado por UTRAN para aplicar el servicio de encriptación. Opcional

Octeto x.4-... Diagnóstico

Información de proceso. Opcional

15.5.3.3.3 Security Mode Reject

Este mensaje es enviado por RNC como respuesta de proceso finalizado sin éxito. El canal establecido es orientado a la conexión.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Tipo de Mensaje							
x.2(etc)	Causa							
x.3(etc)	Diagnóstico							

Octeto x.2-... Causa

Causa de rechazo de la instrucción de Modo de Seguridad. Obligatorio

Octeto x.3-... Diagnóstico

Información de proceso. Opcional

15.5.3.3.4 Integrity Protection Information

Este elemento contiene los algoritmos y la clave para el procedimiento de integridad. Todos los campos son obligatorios.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Algoritmo de Protección de Integridad				No definido			
x.2-17	Clave de Integridad							

Octeto x.1 Algoritmo de Protección de Integridad

Valor entre 0 y 15. Actualmente sólo se utiliza el valor 0 para indicar el algoritmo UIA1.

Octeto x.2-x.17 Clave de integridad

Cadena de 128 bits

15.5.3.3.5 Encryption Information

Este elemento contiene los algoritmos y la clave para el procedimiento de encriptación. Todos los campos son obligatorios.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Algoritmo de Encriptación				No definido			
x.2-17	Clave de Encriptación							

Octeto x.1 Algoritmo de Encriptación

Valor entre 0 y 15. Actualmente sólo se utilizan dos valores,

0 No se usa encriptación
1 Algoritmo UEA1

Octeto x.2-x.17 Clave de encriptación

Cadena de 128 bits

15.5.3.3.6 Chosen Integrity Protection Algorithm

Este elemento contiene la codificación del algoritmo a utilizar por RNC, es un campo obligatorio.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Algoritmo de Protección de Integridad				No definido			

Octeto x.1 Algoritmo de Protección de Integridad

Valor entre 0 y 15. Actualmente sólo se utiliza el valor 0 para indicar el algoritmo UIA1.

15.5.3.3.7 Chosen Encyption Algorithm

Este elemento contiene el algoritmo a utilizar por RNC, el campo es obligatorio.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Algoritmo de Encriptación				No definido			

Octeto x.1 Algoritmo de Encriptación

Valor entre 0 y 15. Actualmente sólo se utilizan dos valores.

0 No se usa encriptación
1 Algoritmo UEA1

15.5.3.3.8 Message type

Identifica el mensaje a enviar. Es obligatorio para todos los mensajes.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Código de procedimiento							
x.2	Tipo de mensaje							

Octeto x.1 Código de procedimiento

Enumerado, se asume número máximo de mensajes 256, con los valores siguientes:

1. Asignación de RAB
2. Petición Abandono RAB
3. Petición Abandono Iu
4. Abandono Iu
5. Preparación Reasignación

6. Asignación de Recursos Reubicados
7. Detección Reubicación
8. Reubicación Completa
9. Cancelar Reubicación
10. Transferencia Contexto SRNS
11. Inicio Datos Dirigidos a SRNS
12. Direccionamiento de Contexto SRNS de la fuente RNC a CN
13. Direccionamiento de Contexto SRNS de CN a RNC
14. Canal de avisos
15. ID Común
16. Invocación seguimiento de CN
17. Control Modo de Seguridad
18. Control Información de Ubicación
19. Información Volumen de Datos
20. Transferencia Directa de Mensaje Inicial de UE
21. Diseminación Información de CN
22. Control Sobrecarga
23. Reinicio
24. Indicación de Error
25. Desactivar Seguimiento de CN
26. Información de Reubicación de RANAP
27. Recursos de Reinicio
28. ACK de Recursos de Reinicio

Octeto x.2 Tipo de Mensaje

Enumerado que puede tomar los siguientes valores

1. Mensaje Inicial
2. Salida con éxito
3. Salida sin éxito
4. Salida

15.5.3.3.9 Cause

Identifica la razón de un determinado evento para el protocolo de RANAP.

	Bits							
octetos	8	7	6	5	4	3	2	1
x.1	Código de causa							

Octeto x.1 Código de causa

Nivel de red de radio

Entero, dentro del rango 1-64, con los valores siguientes:

1. RAB asignado a otro usuario (1)
2. Trelocoverall expirado (2)
3. Trelocprep expirado (3)
4. Trelocomplete expirado (4)
5. Tqueing expirado (5)
6. Activación Reubicación (6)
7. Incapaz de establecer durante la Reubicación (8)
8. RNC Destino Desconocida (9)
9. Reubicación cancelada (10)
10. Reubicación con éxito (11)
11. Algoritmo de cifrado y / o de protección de integridad pedido no soportado (12)
12. Cambio Algoritmo de cifrado y / o de protección de integridad pedido no soportado (13)
13. Error en el procedimiento de la interfaz de radio (14)
14. Abandono por Razón Generada por UTRAN (15)
15. Inactividad de Usuario (16)
16. Reubiciación Crítica en Tiempo (17)
17. Petición de Clase de Tráfico no Disponible (18)
18. Valor de parámetros de RAB incorrecto (19)
19. Petición de Máxima Tasa de bit no Disponible (20)
20. Petición de Máxima Tasa de bit para DL no Disponible (33)
21. Petición de Máxima Tasa de bit para UL no Disponible (34)
22. Petición de Garantía de Tasa de Bit no Disponible (21)
23. Petición de Garantía de Tasa de Bit para DL no Disponible (35)
24. Petición de Garantía de Tasa de Bit para UL no Disponible (36)
25. Petición de Retraso de Transferencia no Conseguido (22)
26. Combinación de Parámetros de RAB incorrecta (23)
27. Condición de Parámetros de SDU violada (24)
28. Condición de Prioridad de Gestión de Tráfico violada (25)
29. Condición de Garantía de Tasa de Bit violada (26)
30. Versiones de Plano de Usuario no soportadas (27)
31. Error en UP de Iu (28)
32. Trelocalloc expirado (7)
33. Error en Reubicación en Destino CN / RNC o Sistema Destino (29)
34. ID de RAB incorrecto (30)
35. RAB no existente (31)
36. Interacción con otros procedimientos (32)
37. Error de Verificación de Integridad Repetido (37)

Nivel de red de transporte

Entero, dentro del rango 65-80, con los valores siguientes:

1. Error lógico. Asociación de Transporte de Iu desconocida (65)

Causa NAS

Entero, dentro del rango 81-96, con los valores siguientes:

1. Indicación de Inicio de Restricción de usuario (81)
2. Indicación de Fin de Restricción de usuario (82)
3. Abandono normal (83)

Causa de Protocolo

Entero, dentro del rango 97-112, con los valores siguientes:

1. Error de Sintaxis de Transferencia (97)
2. Error Semántico (98)
3. Mensaje incompatible con el estado del receptor (99)

Causas Varias

Entero, dentro del rango 113-128, con los valores siguientes:

1. Intervención O&M (113)
2. Recursos no Disponibles (114)
3. Error sin especificar (115)
4. Optimización de Red (116)

Causa no estándar

Entero con valor entre 129 y 256.

15.5.3.3.10 Criticality Diagnostics

	Bits							
octetos	8	7	6	5		3	2	
x.1-x.2	Diagnóstico de Importancia							
x.3-x.n	Diagnóstico de Importancia de Elemento de Información							

Octeto x.1-x.2 Diagnóstico de Importancia

Valoración de la importancia del error producido.

Octeto x.3-x.n Diagnóstico de Importancia de Elemento de Información

Datos relativos al error producido.

15.5.3.3.11 Criticality Diagnostics (2)

Todos los campos son opcionales.

	Bits							
octetos	8		6	5	4	3	2	1
x.1	Código de Procedimiento							
x.2	Mensaje Activador							
x.3	Respuesta							

Octeto x.1 Código de Procedimiento

Entero, con rango 0 a 255, utilizado en caso de que el mensaje sea parte del procedimiento de Indicación de Error y no como respuesta a la operación causante del error.

Octeto x.2 Mensaje Activador

Mensaje que provoca el envío de Criticality Diagnostics. Enumerado que puede tomar los siguientes valores

1. Mensaje Inicial
2. Salida con éxito
3. Salida sin éxito
4. Salida

Octeto x.3 Respuesta

Enumerado que puede tomar los siguientes valores:

1. rechazar
2. ignorar
3. notificar

15.5.3.3.12 Information Element Criticality Diagnostics

Los dos primeros campos son obligatorios y el tercero opcional. Este elemento se repite tantas veces como en número máximo de errores (valor comprendido entre 0 y 255).

	Bits							
octetos	8	7	6	5	4		2	1
x.1	Respuesta							
x.2-x.3	Identificador Elemento de Información							
x.4	Número de repetición							

Octeto x.1 Respuesta

Enumerado que puede tomar los siguientes valores:

1. rechazar
2. ignorar
3. notificar

Octeto x.2-x.3 Identificador Elemento de Información

Entero comprendido entre 0 y 65535.

Octeto x.4 Número de Repetición

Número de veces que se ha repetido el IE. Entero de rango 0 a 255.

15.5.3.3.13 Key Status

Enumerado que identifica si la clave ha sido usada o no con anterioridad.

	Bits							
octetos	8	7		5	4	3		1
x.1	Estado de la clave							

Octeto x.1 Estado de la clave

Toma por valores:

1. vieja
2. nueva

15.5.4 Interfaz de Transporte de Datos y de Señalización

15.5.4.1 Dominio de Circuitos Conmutados (CS)

En la figura presentada a continuación pueden verse los protocolos utilizados en la interfaz Iu como plano de usuario de la red de transporte para el dominio CS.

AAL-2 SAR SSCS
AAL2
ATM

Figura 75. Plano de Usuario de la Red de Transporte del dominio CS

Donde AAL.2 SAR SSCS, Subnivel de Convergencia Específico de Servicio de Reensamblaje y Segmentación se utiliza para la segmentación y el reensamblaje de SDUs de AAL2.

En la siguiente figura veremos los protocolos utilizados para el plano de control (ALCAP).

Conexión de señalización AAL2
Transporte de Señalización AAL2 Conversor para MTP3b
MTP3b
SSCF-NNI
SSCOP
AAL5
ATM

Figura 76. Plano de Control de la Red de Transporte del dominio CS

15.5.4.2 Dominio de Paquetes Conmutados (PS)

El plano de usuario para la red de transporte de la interfaz Iu se refleja en la siguiente figura.

GTP-U
UDP
IP
AAL5
ATM

Figura 77. Plano de usuario de la Red de Transporte del dominio PS

El plano de control de la red de transporte para el dominio PS, no requiere el protocolo ALCAP.

15.5.5 Protocolos del Plano de Usuario de Iu

El protocolo de UP de Iu, se ubica en el nivel Plano de Usuario de Red de Radio de Iu y se utiliza para que converjan los datos de usuario asociados a un canal lógico. Una instancia de UP de Iu se asocia a un único RAB.

La figura siguiente nos presenta la localización del protocolo de UP de Iu en UTRAN.

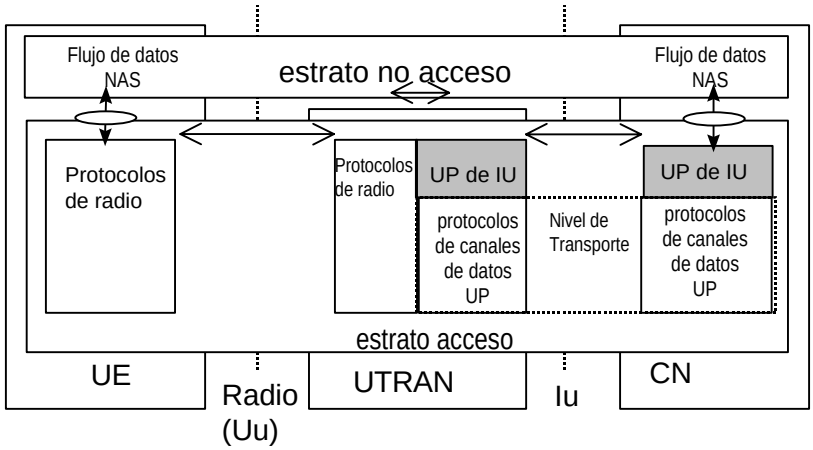


Figura 78. Ubicación de UP de Iu en UTRAN

El protocolo de Plano de Usuario de Iu tiene dos modos de operación:

- Modo Transparente (TrM)

  Para aquellos RABs que no necesitan ninguna opción especial de UP de Iu, sólo la transferencia de datos de usuario.

- Modo de Soporte para tamaño de SDU predefinido (SMpSDU)

  Para aquellos RABs que requieren alguna característica especial de UP de Iu además del transporte de datos de usuario.

CN decide en el momento del establecimiento de un RAB concreto, el tipo de transporte a utilizar.

15.5.5.1 Modo Transparente

Este modo permite la transferencia de datos sobre la interfaz de Iu de forma transparente, comunicándose la información a través del SAPs para Flujos de Datos de Estrato no de Acceso (NAS).

Las interfaces del nivel de protocolo UP de Iu en modo transparente son el nivel de red de transporte y los niveles superiores, siendo el nivel de UP de Iu, un nivel “vacío” por el cual se transmiten los datos desde el Nivel de Red hasta los niveles superiores.

Este protocolo, utiliza los servicios de los niveles de Transporte para transferir la información en la interfaz Iu.

15.5.5.2 Modo de Soporte

El modo de soporte del protocolo UP de Iu se utiliza para aquellos flujos de datos que necesitan gestión de entorno. Al igual que el modo de transporte, se comunican por SAPs de Flujo de Datos para NAS.

El modo de soporte proporciona sus servicios a niveles superiores de UP a través de un SAP Dedicado para la Transferencia de Información.

Este protocolo, utiliza los servicios de los niveles de Transporte para transferir la información en la interfaz Iu.

15.5.6 Interfaz Iur

Iur es la interfaz que representa la conexión lógica existente entre dos RNCs en UTRAN. Iur utiliza el protocolo SCCP para el intercambio de mensajes de señalización entre RNCs y define la función de usuario de Parte de Aplicación de Subsistemas de Red de Radio (RNSAP). RNSAP utiliza una conexión de señalización por DRNC y UE, donde cada UE tiene una o más conexiones de radio activas para la transferencia de mensajes de nivel 3.

15.5.6.1 Funciones de la interfaz Iur

Las principales funciones llevadas a cabo por la interfaz de Iur son:

- Gestión de Transporte de Red
- Gestión de Tráfico de Canales de Transporte Comunes
- Gestión de Tráfico de Canales de Transporte Dedicados
- Gestión de Tráfico de Canales de Transporte Compartidos en sentido descendente
- Información de medidas para objetos de medida comunes y dedicados

15.5.6.2 Protocolos de Iur

En la interfaz Iur, existe una clara separación entre el Nivel de Red de Radio y el nivel de Transporte, como puede observarse en la siguiente figura.

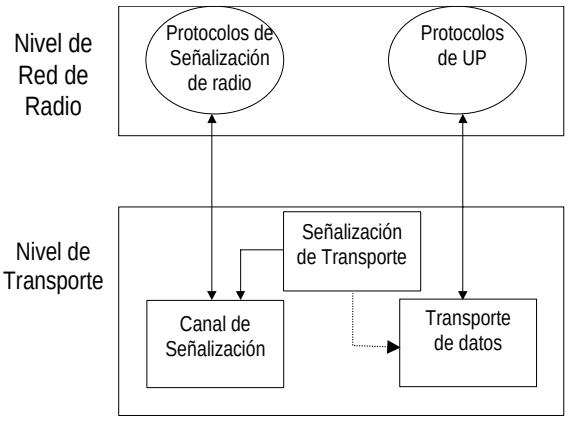


Figura 79. Separación de los protocolos de Red y Transporte en Iur

La arquitectura de protocolos de Iur está formada por dos niveles funcionales,

- Nivel de Red de Radio

  Define los procesos relativos a la interacción entre dos RNCs dentro de una PLMN. Este nivel se basa en el Plano de Control de Red de Radio y el Plano de usuario de Red de Radio.

- Nivel de Transporte

  Define los procesos de establecimiento de conexiones físicas entre dos RNCs de una misma PLMN.

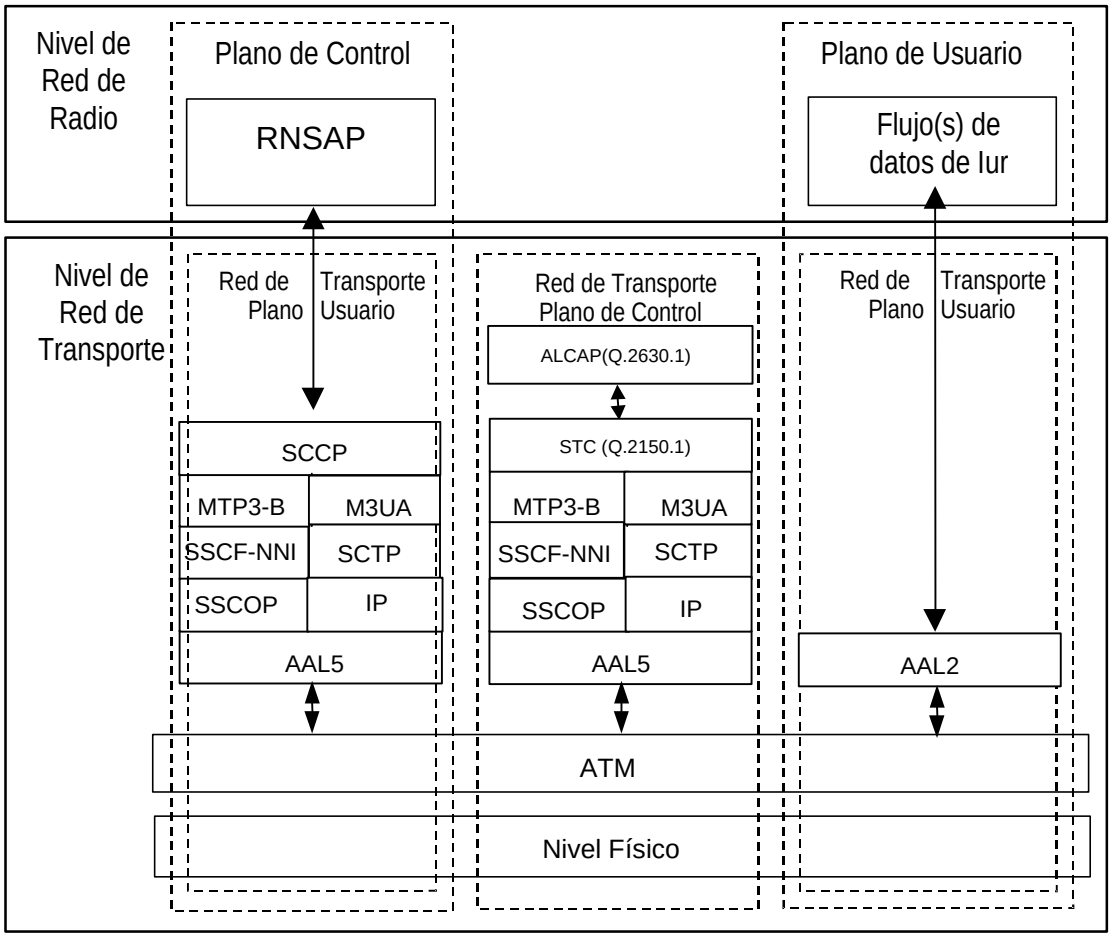


Figura 80. Estructura de protocolos de la interfaz Iur

15.5.6.2.1 RNSAP

RNSAP es el protocolo del plano de control para el nivel de Transporte. Ofrece los servicios de:

- Procedimientos de Movilidad Básica RNSAP
- Procedimientos DCH de RNSAP
- Procedimientos de Canal de Transporte Común RNSAP
- Procedimientos Generales RNSAP

Los procedimientos de Movilidad, como su nombre indican, se utilizan para gestionar la movilidad en UTRAN. Los procesos de DCH se encargan de la gestión de tráfico DCH entre RNCs, el uso de estos mecanismos sólo es posible si este módulo se usa en una Iur específica. Los procedimientos de Canal de Transporte Común sirven para controlar los flujos de datos de canal de transporte común sobre Iur y finalmente, los procesos Generales son aquellos no relativos a un UE concreto.

Además de estos procedimientos, RNSAP ofrece dos modos de servicio.

- Servicios de transferencia de datos orientado a la conexión

Este servicio se establece en una conexión de señalización entre RNCs. Es posible el establecimiento/liberación dinámica de conexiones de señalización y cada UE tiene su propia conexión de señalización.

La entrega de mensajes de RNSAP se hace de forma secuencial y el protocolo de RNSAP es notificado en caso de interrumpirse la conexión de señalización.

- Servicio no orientado a la conexión

El protocolo de RNSAP es notificado en caso de que un mensaje no llegue a la entidad RNSAP destino.

16Anexo 7: GPRS en UMTS

En esta sección se describen los Servicios de Radio Generales de Paquetes, su funcionalidad y arquitectura.

El dominio de paquetes utiliza una técnica de transmisión de paquetes de alta y baja velocidad así como señalización. PS mantiene una estricta separación entre el subsistema de radio y el de red a fin de permitir reutilizar el subsistema de red con diferentes tecnologías de acceso a radio.

El Nodo de Soporte de Servicios GPRS (SGSN) se cuida de la ubicación de MS individuales y de la funciones de seguridad y control de acceso. HLR contiene la información de los suscriptores y SMS-GMSC y SMS-IWMSC soportan la transmisión de SMS vía SGSN. Opcionalmente, MSC/VLR puede diseñarse para permitir una coordinación más eficiente de servicios y funcionalidades del dominio PS y CS. Para acceder a los servicios de PS, MS debe como primer paso dar a conocer su presencia en la red mediante su unión a GPRS y posteriormente, a fin de recibir y enviar datos PS, debe activar el contexto de Protocolo de Datos por Paquete que desea utilizar. Este proceso permite que MS sea reconocido por el correspondiente GGSN y que pueda comenzar el intercambio con redes de datos externas.

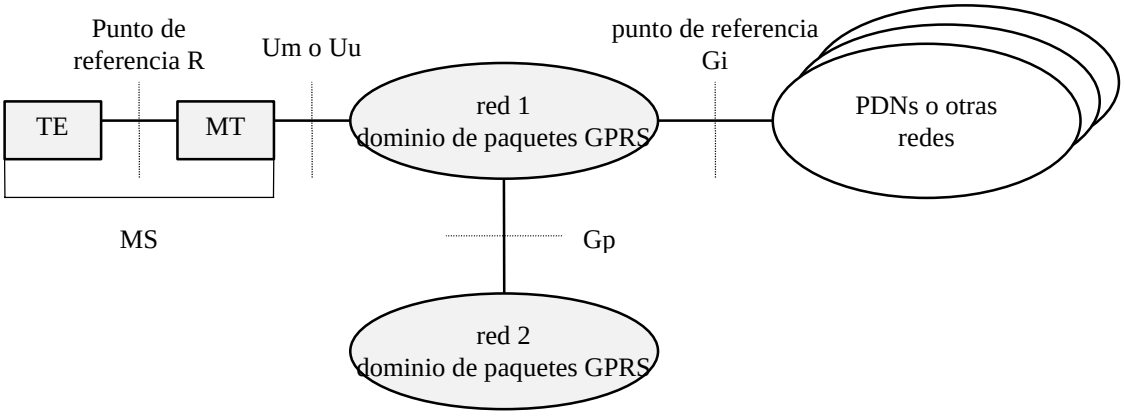


Figura 81. Interfaces de Acceso al Dominio de PS y Puntos de Referencia

16.1 Funcionalidad de GPRS

Las funcionalidades de alto nivel asociadas a GPRS son:

- Control de Acceso
- Direccionamiento de paquetes y funciones de transferencia
- Gestión de Movilidad para el dominio PS,
- Gestión de Recursos de Red de Radio
- Funciones de Gestión de Red

16.1.1 Control de Acceso

El acceso a la red puede iniciarse tanto desde la parte móvil como desde la parte fija de la red. La interfaz de red fija puede soportar múltiples protocolos de acceso a redes de datos externas, por ejemplo IP. Se incluyen en esta funcionalidad los servicios de :

- Registro

  Es el mecanismo por el cual un Identificador de Usuario móvil se asocia con la dirección (o direcciones) y el protocolo (o protocolos) de datos por paquete del usuario, dentro de la PLMN y también, con el punto (o puntos) de acceso del usuario hacia la red PDP externa. La asociación puede ser estática o dinámica.

- Autorización y Autenticación

  Esta función ejecuta la identificación y la autenticación del demandante del servicio así como, la validación del tipo de servicio requerido para asegurar que el usuario está autorizado para el uso de los servicios concretos de la red. La función de autenticación se ejecuta en asociación con las funciones de Gestión de Movilidad.

- Control de Admisión

  La finalidad de esta función es estimar los recursos de la red requeridos para proporcionar la calidad de servicio pedida, determinar si están disponibles y reservarlos. El control de admisión se ejecuta en asociación con las funciones de Gestión de Recursos de Radio para estimar los requerimientos de recursos de radio de cada celda.

- Filtro de Mensajes

  La función realiza el filtro de aquellos mensajes no autorizado s o no solicitados.

- Adaptación de Paquetes del Terminal

  Esta función transforma los paquetes recibidos / transmitidos del / para el equipamiento de terminal en un formato adecuado para su transmisión por el dominio PS de la red.

– Recolección de Datos de Tasas

  Esta función recoge la información necesaria para gestionar las suscripciones y / o las tasas de tráfico.

16.1.2 Direccionamiento de Paquetes y Funciones de Transmisión

Dentro de esta funcionalidad se incluye los servicios de:

– Direccionamiento y envío de un nodo al siguiente según la ruta marcada
– Traducción y mapeo de direcciones
– Encapsulación
– Túnel
– Compresión
– Servidor de Dominio de nombres
– Cifrado

16.2 Arquitectura Lógica del dominio PS de la CN

La funcionalidad de la Red Troncal para el dominio PS se implementa en dos nodos de red, el Nodo de Soporte de Servicios GPRS (SGSN) y el Nodo de soporte GPRS Pasarela (GGSN). Las interfaces entre los componentes de la PLMN se observan en la siguiente figura:

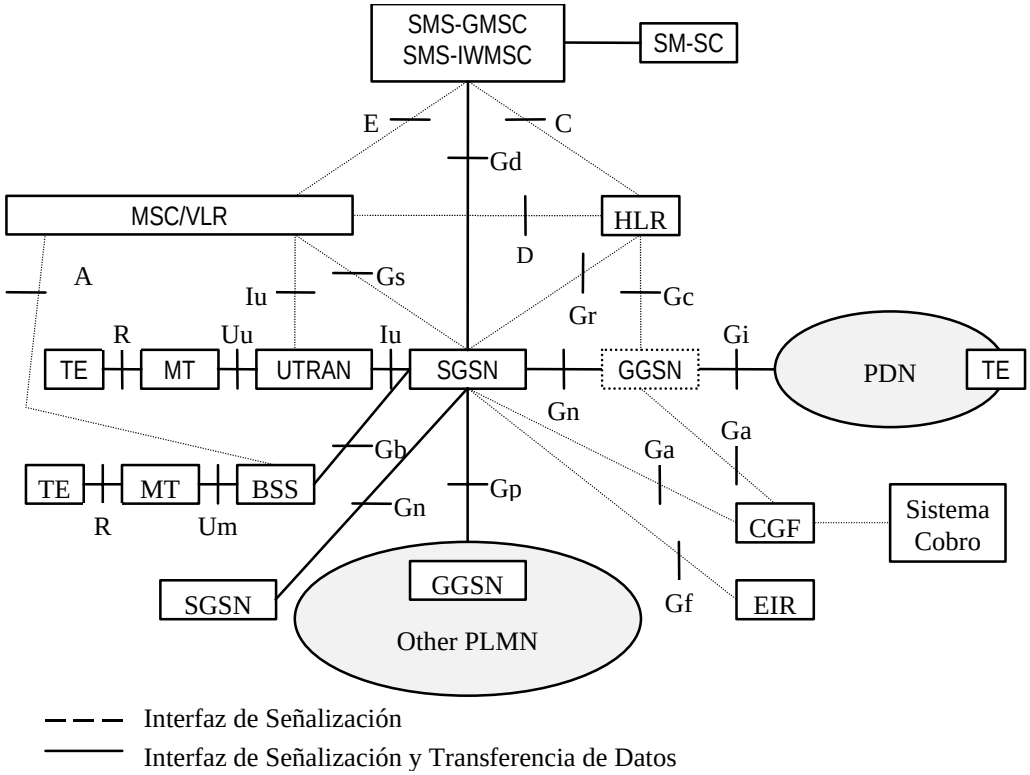


Figura 82. Diseño general de la arquitectura lógica del dominio PS

16.2.1 Nodos de la Red Troncal del dominio PS

El Nodo de soporte GPRS (GGSN) contiene los elementos necesarios para ofrecer la funcionalidad GPRS para UMTS (y/o GSM). Dentro de una misma PLMN pueden coexistir más de uno nodo GGSN.

GGSN es el nodo en el cual la red PS comprueba la dirección PDP. También contiene información de direccionamiento para usuarios PS, esta información se utiliza para traspasar las N-PDUS por túnel hasta el punto de acceso de MS actual. GGSN puede pedir información de ubicación a HLR por la interfaz opcional Gc.

SGSN es el nodo que da servicios a MS y a la vez soporta GPRS. Al anexarse a PS, el nodo SGSN establece el contexto de gestión de movilidad que contiene información perteneciente, por ejemplo, a movilidad y seguridad de MS. En el proceso de Activación del Contexto PDP, SGSN establece un contexto PDP que utilizará en el direccionamiento con el GGSN del usuario.

Las funcionalidades de SGSN y GGSN pueden combinarse en el mismo nodo físico o pueden residir en diferentes nodos. SGSN y GGSN contienen funcionalidad de direccionamiento, IP u otra, y pueden estar interconectados con routers IP En el caso de que SGSN y GGSN residan en PLMNs diferentes, se relacionan a través de la interfaz Gp que ofrece la funcionalidad de la

interfaz Gn más la funcionalidad de seguridad necesaria para la comunicación entre PLMNs. Las funciones de seguridad se basan en los acuerdos entre operadores.

SGSN puede enviar información de ubicación a MSC / VLR a través de la interfaz opcional Gs y puede recibir peticiones de canal de avisos de éste por la misma interfaz. Para el tema del control opcional de CAMEL, SGSN utiliza las interfaces con GSM-SCF.

16.2.1.1 HLR

HLR contiene datos de suscripción del dominio de paquetes e información de direccionamiento. Es accesible desde SGSN por la interfaz Gr y desde GGSN por la interfaz Gc.

16.2.1.2 SMS-GMSC y SMS-IWMSC

SMS-GMSC y SMS-IWMSC se conectan a SGSN por la interfaz Gd para permitir a SGSN ofrecer el servicio de SMS.

16.2.1.3 Estaciones Móviles

Una estación móvil UMTS puede operar en uno de los siguientes modos:

Modo PS/CS

MS se adhiere a ambos dominios y es capaz de operar simultáneamente con servicios PS y CS.

Modo PS

MS se adhiere sólo al dominio PS y sólo puede operar con servicios PS.

Modo CS

MS se adhiere sólo al dominio CS y sólo puede operar con servicios CS.

16.2.2 Planos de Usuario y de Control

16.2.2.1 Plano de usuario MS- GGSN

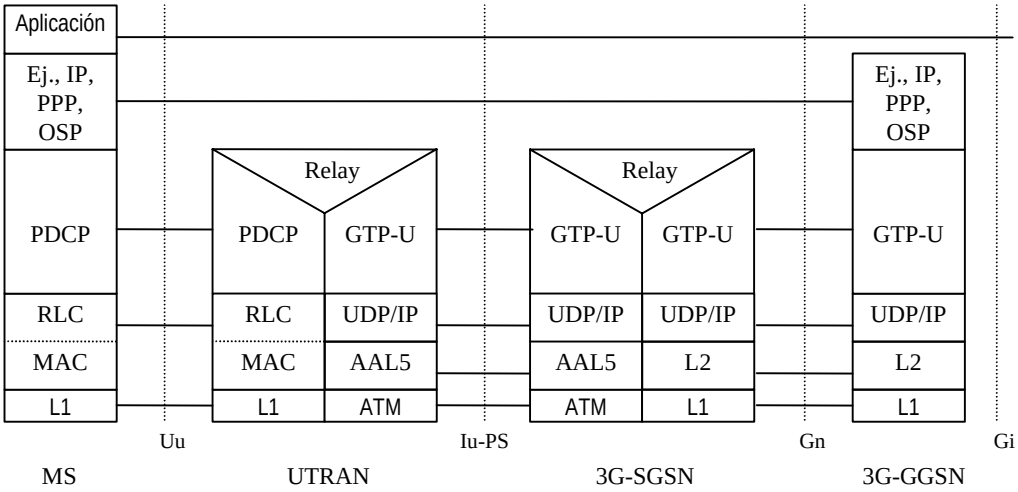


Figura 83: Plano de usuario para UMTS

Leyenda:

Protocolo de Convergencia de Paquetes de Datos (PDCP)
Esta funcionalidad de transmisión mapea las características de niveles altos a las características de los protocolos de la interfaz de radio. PDCP soporta por ejemplo, IPv4, PPP,IPv6 y OSP.

Protocolo de Túnel GPRS para plano de usuario (GTP-U)
Este protocolo transmite por túnel los datos de usuario entre UTRAN y SGSN, así como entre GSN y la red externa. Todas las PDUs de PDP deben encapsularse mediante GTP.

UDP/IP
Protocolos de red utilizados para el direccionamiento de datos de usuario y de señalización de control.

Modo de Transmisión Asíncrono (ATM)
La información a transmitir se divide en celdas de tamaño fijo (53 octetos), se multiplexa y se transmite.

Nivel 5 de Adaptación ATM (AAL5)
Este protocolo ofrece soporte para servicios orientados a la conexión de tráfico variable y para servicios de datos no orientados a la conexión.

Control de Conexión de Radio (RLC)

RLC ofrece control de conexión lógica sobre la interfaz de radio. Pueden existir múltiples conexiones RLC por cada MS, siendo cada conexión reconocida por el identificador de canal lógico.

Control de Acceso al Medio (MAC)
El protocolo de MAC controla la señalización de los procedimientos de acceso (petición y permiso) al canal de radio.

16.2.2.2 Plano de control

El plano de control esta formado por los protocolos definidos para gestionar y soportar las funciones de usuario. Servicios ofrecidos por el plano de control serían:

- control de las conexiones de acceso al dominio PS,
- control de los atributos de una conexión establecida,
- control del direccionamiento de una conexión establecida a fin de soportar la movilidad de usuario y,
- control de la asignación de recursos de la red para satisfacer las demandas de los usuarios.

16.2.2.2.1 MS - SGSN

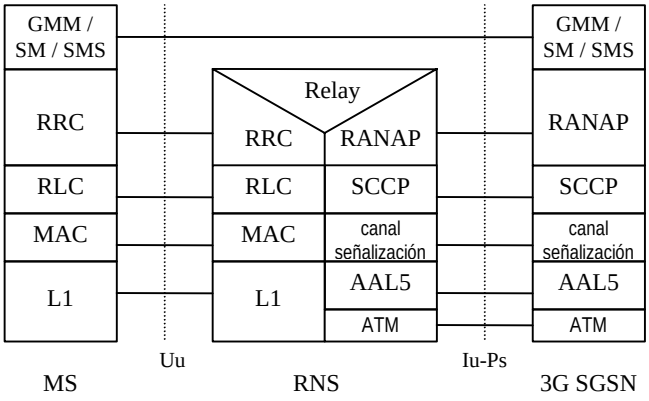


Figura 84: Plano de control MS- SGSN

Leyenda:

Gestión de Sesiones y Gestión de Movilidad UMTS (GMM/SM)
GMM soporta funciones de gestión de movilidad como unión al dominio, dejar el dominio, seguridad y cambio del área de direccionamiento. SM soporta el contexto de activación / desactivación de PDP.

SMS soporta el servicio de mensaje corto originado / terminado por el móvil.

Protocolo de Aplicación de Red de Acceso de Radio (RANAP)

Este procolo encapsula y transporta señalización de alto nivel y gestiona la señalización entre SGSN y UTRAN. También gestiona las conexiones GTP en la interfaz Iu

Control de Conexión de Radio (RLC)
RLC ofrece control de conexión lógica sobre la interfaz de radio para la transmisión de mensajes de señalización de alto nivel y SMS.

16.2.2.2.2 SGSN - HLR

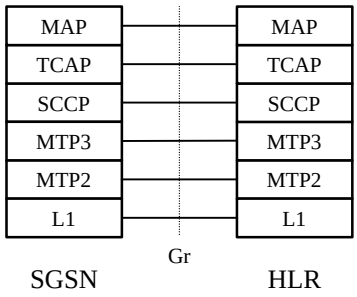


Figura 85:Plano de control SGSN - HLR

Leyenda:

Parte de Aplicación Móvil (MAP)
Este protocolo soporta el intercambio de señalización con HLR.

TCAP, SCCP, MTP3 y MTP2
Son los mismos protocolos que los utilizados para el dominio de CS por MAP. Ofrecen servicio no orientado a la conexión, direccionamiento de mensajes, discriminación, etc.

16.2.2.2.3 SGSN – MSC / VLR

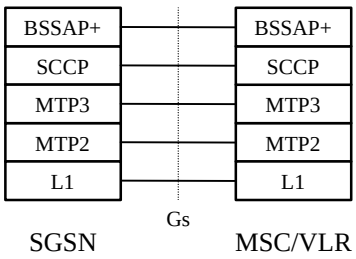


Figura 86: Plano de control SGSN – MSC/VLR

Leyenda:

Parte de Aplicación del Sistema de Estación Base + (BSSAP+)
Subconjunto de procedimientos BSSAP que soporta la señalización entre SGSN y MSC / VLR.

16.2.2.2.4 SGSN - EIR

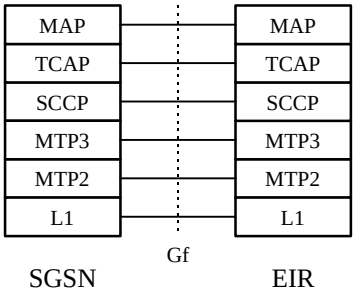


Figura 87: Plano de control SGSN - EIR

Leyenda:

Parte de Aplicación Móvil (MAP)
Protocolo que mantiene la señalización entre SGSN y EIR.

16.2.2.2.5 SGSN – SMS-GMSC o SMS-IWMSC

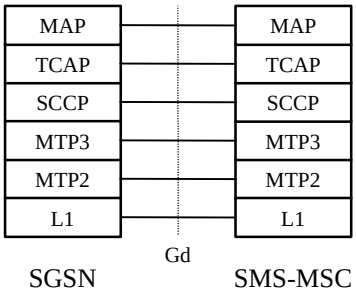


Figura 88: Plano de control SGSN – SMS-GMSC o SMS-IWMSC

Leyenda:

Parte de Aplicación Móvil (MAP)
Este protocolo soporta la señalización entre SGSN y SMS-GMSC o SMS-IWMSC.

16.2.2.2.6 GSN- GSN

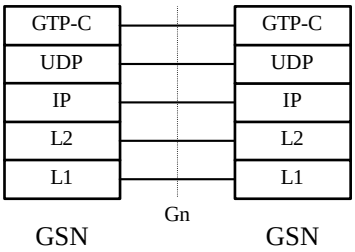


Figura 89: Plano de control GSN - GSN

Leyenda

Protocolo de Túnel GPRS para el plano de control (GTP-C)
Transfiere mensajes de señalización por túnel entre SGSN y GGSN, y entre SGSNs.

Protocolo de Datagrama de Usuario (UDP)
Transfiere mensajes de señalización entre GSNs.

16.2.2.2.7 GGSN- HLR

Este camino de señalización opcional permite el intercambio de información de señalización entre GGSN y HLR. Existen dos alternativas de implementación de este camino.

16.2.2.2.8 Señalización GGSN – HLR basada en MAP

Si se instala una interfaz SS7 en GGSN, el protocolo de MAP puede utilizarse entre GGSN y HLR.

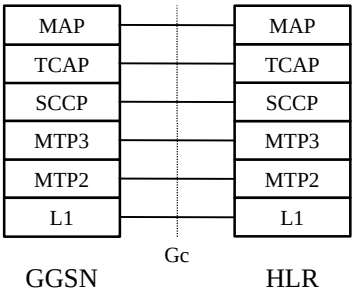


Figura 90: Plano de control GGSN – HLR utilizando MAP

Leyenda:

Parte de Aplicación Móvil (MAP)
Este protocolo soporta el intercambio de señalización entre GGSN y HLR.

16.2.2.2.9 Señalización GGSN – HLR basada en GTP y MAP

Si no se instala una interfaz SS7 en GGSN, cualquier interfaz SS7 instalada en la misma PLMN que GGSN puede utilizarse como convertidor del protocolo GTP a MAP para permitir la señalización GGSN y HLR

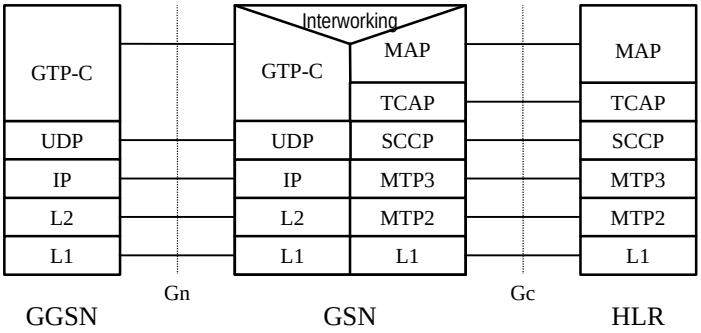


Figura 91: Plano de control GGSN-HLR utilizando GTP y MAP

Leyenda:

Protocolo de Túnel GPRS para el plano de control (GTP-C)
Transfiere mensajes de señalización por túnel entre GGSN y el convertidor de protocolo GSN

Interrelación
Ofrece relación entre GTP y MAP para la señalización de GGSN – HLR.

16.3 Funcionalidad de Gestión de Movilidad

16.3.1 Interacción entre SGSN y MSC/VLR

Los procesos descritos en este apartado son soportados siempre que la interfaz opcional Gs esté instalada.

Para coordinar los procesos de MM de MS adheridos a GPRS y a IMSI, se crea una asociación entre SGSN y MSC/VLR. Esta asociación tiene como fin la gestión de relación entre ambos elementos y se crea cuando VLR almacena el código asociado a SGSN y éste a su vez guarda el código asociado a VLR.

Las acciones posibles con SGSN-VLR son:

- Adherencia/Abandono a/de IMSI a través de SGSN.
  Es posible realizar combinaciones de adherencias a GPRS/IMSI o abandonos GPRS/IMSI permitiendo ahorrar recursos de radio.

- Coordinación de actualización LA / RA incluyendo las actualizaciones periódicas.
  MS envía una actualización combinada RA / LA a SGSN quien transmite la actualización de LA a VLR.

- Canal de avisos de conexión CS vía SGSN

- Procedimientos de alerta para servicios no pertenecientes al dominio PS

- Procedimiento de identificación

- Procedimiento de Información de MM

16.3.1.1 Administración de Asociación SGSN-MSC / VLR

La asociación se crea al ejecutar las siguientes acciones:

- Adherencia combinada a GPRS / IMSI
- Adherencia a GPRS cuando MS ya está adherido a IMSI
- Actualización combinada RA / LA cuando MS se adhiere a IMSI y ya está en GPRS
- Actualización combinada de RA / LA cuando cambia la adherencia a IMSI o GPRS de modo de operación

La asociación tiene como elemento iniciador a SGSN, quien envía un mensaje BSSAP+ para un MS concreto de VLR. Para obtener el número de VLR, SGSN convierte el RAI actual en un número VLR mediante una tabla. Si durante el proceso de conexión CS, se lanza la adherencia a GPRS entonces, después del abandono de la conexión, la asociación se inicia con una actualización RA / LA combinada.

La asociación sólo se actualiza cuando MS cambia de VLR o cuando MS cambia de SGSN, nunca durante una conexión CS.

SGSN-MSC / VLR se elimina al abandonar IMSI o GPRS. Si MSC / VLR recibe una actualización de LA proveniente de la interfaz A o Iu y existe una asociación para ese terminal, ésta se elimina sin notificarlo a SGSN. En el caso de ser SGSN quien recibe una actualización de RA, actúa de la misma manera eliminando la asociación sin notificarlo a MSC / VLR.

16.3.1.2 Actualización combinada RA / LA

Si MS está adherido tanto a GPRS como a IMSI, la actualización de LA / RA se hace de forma coordinada para reducir el número de recursos empleados en la operación, siempre que el modo de operación de la red lo permita.

El proceso se inicia desde MS enviando un mensaje “Routeing Area Update Request” a SGSN, debe tenerse en cuenta que la actualización de LA está incluida en la actualización de RA. SGSN envía la actualización de LA a MSC / VLR quien opcionalmente contestará a MS con un nuevo VLR vía SGSN.

16.3.1.3 Canal de avisos de CS

Los canales de avisos de servicios de circuitos conmutados se hace a través de SGSN, siempre que MS esté adherido a GPRS e IMSI y que el modo de operación de red lo permita.

16.3.1.4 Alerta para servicios no GPRS

MSC/VLR puede realizar una petición a SGSN para obtener información de la actividad de un MS específico, en este caso MSC/VLR envía un mensaje BSSAP+ "Alert Request" (IMSI) a SGSN donde MS es el nodo actual adherido a GPRS.

16.3.1.5 Procedimiento de Información MS

Si VLR reconoce a un MS como adherido a IMSI y a GPRS, VLR puede ejecutar el proceso de petición de información de MS vía SGSN.

Si SGSN dispone de los datos requeridos por VLR, contesta con esta información sin reclamar a MS el envío de los datos. En la siguiente figura puede verse un esquema del proceso seguido.

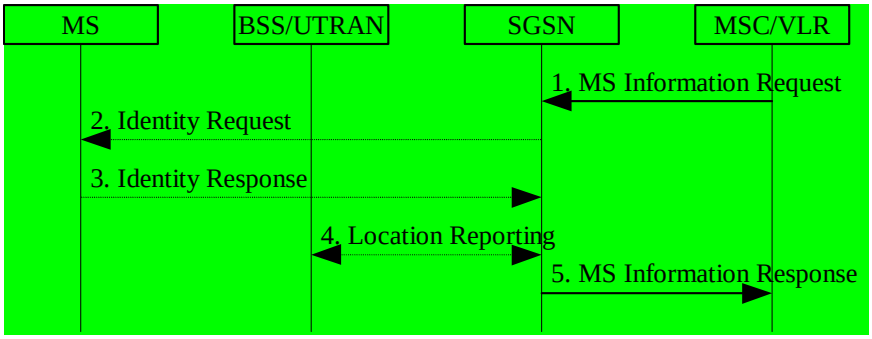


Figura 92. Procedimiento de Información de MS

1) MSC/VLR envía la petición "MS Information Request" (IMSI, Tipo de Información) a SGSN.
2) Si la información es desconocida para SGSN transmite la petición a MS.
3) MS responde con "Identity Response" (Identidad).
4) Si existe una conexión Iu para MS, SGSN utilizará el procedimiento de "Location Reporting" para obtener la Identidad del Área de Servicio.
5) SGSN responde a MSC/VLR con un "MS Information Response" (IMSI, Información) con la información requerida.

16.3.1.6 Procedimiento de Información de MM

Si VLR reconoce a un MS como adherido a GPRS e IMSI, VLR puede ejecutar el proceso de "MM Information" vía SGSN. Este proceso se utiliza para comunicar a MS datos como el nombre de la red o la zona de tiempo local del móvil.

En el esquema siguiente puede observarse el proceso.

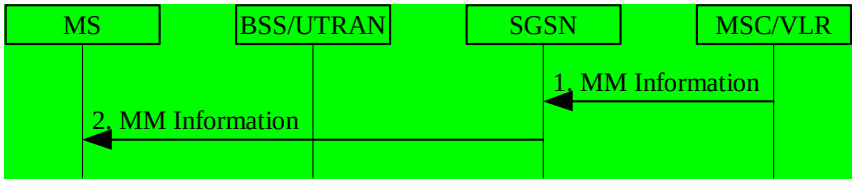


Figura 93. Procedimiento de Información MM

1) SGSN recibe el mensaje "MM Information" (IMSI, Información) de MSC / VLR.
2) SGSN transmite el mensaje a MS.

16.3.2 Procedimientos GMM

La gestión de movilidad implica funciones y acciones diversas como pueden ser:

- Funciones de Adherencia GPRS

  Funciones que permiten el acceso a servicios GRPS.

- Funciones de Abandono de GPRS

  Funciones que permiten a MS comunicar a SGSN su decisión de no acceder más a servicios GPRS, o a SGSN transmitir a MS la no disponibilidad de servicios GPRS.

- Funciones de Purgado

  Funciones que permiten a SGSN comunicar a HLR que ha eliminado los contextos de PDP y MM para un MS concreto.

- Funciones de Seguridad

  Funciones que permiten establecer y gestionar una política de seguridad.

- Funciones de Gestión de Ubicación

Funciones de control de la ubicación de MS.

- Funciones de Gestión de Suscriptores

  Funciones que permiten informar a los nodos de los cambios producidos en la suscripción PS para un suscriptor PS concreto.

- Procedimientos de Petición de Servicio

  Funciones para realizar una petición de una conexión segura y/o para reservar recursos para contextos PDP activos.

16.3.3 Funciones de Seguridad

Las funciones de seguridad:

1. Impiden el uso no autorizado de servicios del dominio PS (autenticación de MS por la red y validación de la petición de servicio)

2. Ofrecen confidencialidad de la identidad de usuario (identificación temporal y cifrado)

3. Ofrecen confidencialidad de datos de señalización y de usuario (cifrado)

4. Ofrecen para el acceso de radio UMTS, integridad de datos y autenticación del origen de datos de señalización (integridad)

5. Ofrecen para el suscriptor UMTS, autenticación de la red por el MS

16.3.3.1 Autenticación

La autenticación UMTS implica autenticación mutua, de MS por la red y de la red por MS. También implica el establecimiento de nuevas claves de cifrado (CK) y fijar una clave de integridad (IK) entre MS y SGSN.

16.3.3.1.1 Autenticación del Suscriptor de UMTS (USIM)

El proceso de autenticación ejecutado por SGSN realiza la autenticación mutua y establece las claves de seguridad. Los quintetos de autenticación se almacenan en SGSN.

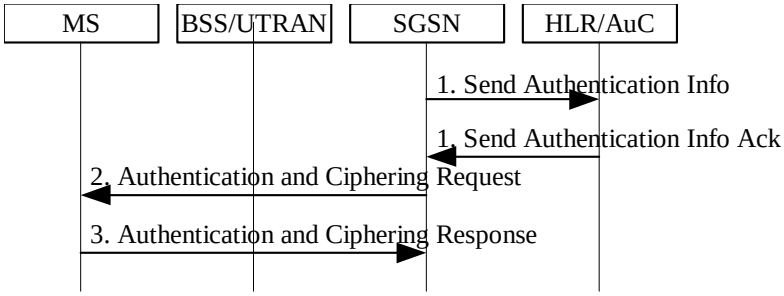


Figura 94: Procedimiento de autenticación de USIM

1) Si SGSN no tiene quintetos de vectores de autenticación previamente grabados, transmite un mensaje de "Send Authentication Info" (IMSI) a HLR. Al recibir el mensaje, HLR/AuC responde con un mensaje de "Send Authentication Info Ack" incluyendo una cadena ordenada de quintetos. Cada quinteto contiene RAND, CRES,AUTN,CK e IK.
2) SGSN selecciona el siguiente quinteto y transmite los valores de RAND y AUTN, del quinteto seleccionado, a MS en el mensaje "Authentication and Ciphering Request" (RAND, AUTN,CSKN). SGSN selecciona un número de secuencia de clave de cifrado, CKSN, y lo incluye en el mensaje.
3) A la recepción del mensaje, el USIM verifica AUTN y, si acepta el valor de AUTN, calcula la firma de RAND y RES. Si el USIM considera que la autenticación es correcta entonces MS devuelve el mensaje "Authentication and Ciphering Response" (RES) a SGSN. El USIM calcula una nueva clave de cifrado, CK, y una nueva clave de integridad (IK). Si por el contrario, el USIM considera incorrecta la autenticación envía el mensaje "Authentication and Ciphering Failure".

16.3.3.2 Confidencialidad

16.3.3.2.1 Confidencialidad de la Identidad de Usuario

La Identidad Temporal de Red de Radio (RNTI) identifica a un usuario entre MS y UTRAN. La relación entre RNTI e IMSI sólo es conocida por MS y por UTRAN. El usuario entre MS y SGSN se identifica por un P-TMSI, siendo la relación entre el P-TMSI y el IMSI sólo conocida por el MS y el SGSN.

16.3.3.2.2 Firma P-TMSI

Opcionalmente se envía una firma P-TMSI en los mensajes, entre SGSN y MS, Aceptar Adherencia y Aceptar Modificación de Área de Direccionamiento.

Si la Firma P-TMSI se ha enviado a MS, éste incluirá la Firma en los siguientes mensajes de Petición de Modificación de Área de Direccionamiento, Petición de Abandono de dominio y Petición de Adherencia con la finalidad de comprobar la identidad. Al recibir la Firma P-TMSI, SGSN la compara con la firma almacenada en SGSN, si los valores no coinciden puede utilizar las funciones de seguridad para autentificar a MS. Si la red soporta el mecanismo de cifrado, SGSN enviará la Firma cifrada a MS.

Los mensajes de Petición de Modificación de Área de Direccionamiento y Petición de Adherencia enviados por MS no están cifrados.

16.3.3.2.3 Procedimiento de Reasignación de P-TMSI

SGSN puede reasignar P-TMSI en cualquier momento y la reasignación puede producirse por el procedimiento de Reasignación de P-TMSI o puede estar incluida en los procedimientos de Adherencia o Modificación del Área de Direccionamiento

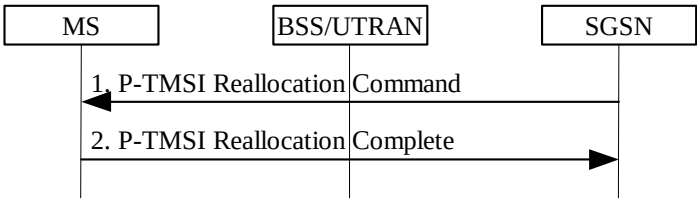


Figura 95: Procedimiento de reasignación de P-TMSI

1) SGSN envía a MS un mensaje “P-TMSI Reallocation Command” (nuevo P-TMSI, Firma P-TMSI,RAI). La Firma P-TMSI es un parámetro opcional que MS devolverá a SGSN en el siguiente procedimiento de Adherencia o Modificación Área de Direccionamiento.
2) MS devuelve a SGSN el mensaje “P-TMSI Reallocation Complete”.

16.3.3.3 Confidencialidad de Señalización SM / GMM y Datos de Usuario

El ámbito del mecanismo de cifrado incluye desde la función de cifrado en UTRAN a la función de cifrado en MS. El cifrado se ejecuta con el Algoritmo de Encriptación de UMTS (UEA), donde la Clave de Cifrado (CK) es un parámetro de entrada. El inicio del cifrado se controla por el procedimiento del contexto de seguridad

16.3.3.3.1 Procedimiento de Comprobación de la Identidad

En la siguiente figura se muestra un gráfico del procedimiento utilizado:

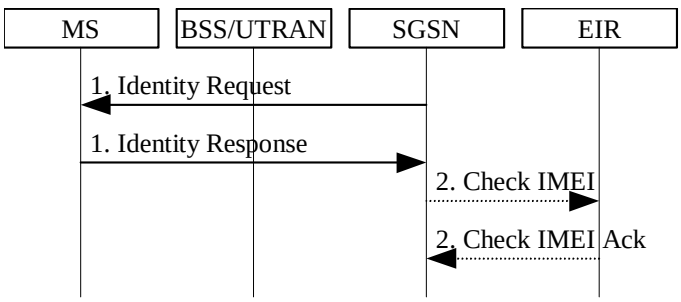


Figura 96: Procedimiento de Comprobación de la Identidad

Leyenda:

1)SGSN envía un mensaje “Identity Request” (Tipo Identidad) a MS que responde con “Identity Response” (Identidad Móvil).
2) Si SGSN decide verificar el valor de IMEI con EIR, envía un mensaje “Check IMEI” (IMEI) a EIR, el cual le responde con un mensaje “Check IMEI Ack” (IMEI).

16.3.3.4 Integridad de Datos

El mecanismo de integridad de datos se ejecuta entre MS y UTRAN y sólo es aplicable a la información de señalización de radio. Este proceso se realiza con el algoritmo de integridad de UMTS (UIA) que tiene como parámetro de entrada la clave de integridad (IK).

16.3.4 Procedimiento de Petición de servicio

El procedimiento de petición de servicio se utiliza para requerir el establecimiento de una conexión segura con SGSN. También puede ser utilizado para reservar recursos para contextos PDP activos.

16.3.4.1 Petición de Servicio Iniciada por MS

MS envía un mensaje de Petición de Servicio a SGSN a fin de establecer una conexión de señalización con el dominio PS para señalización de un nivel superior o para reservar recursos para el contexto PDP activo. Después de recibir este mensaje, SGSN puede autenticar o ejecutar el procedimiento de seguridad.

Posteriormente al establecimiento de una conexión de señalización segura con SGSN, MS puede comenzar a transmitir mensajes de señalización o SGSN puede empezar a reservar recursos para el contexto PDP, dependiendo del servicio pedido en el mensaje de Petición de Servicio.

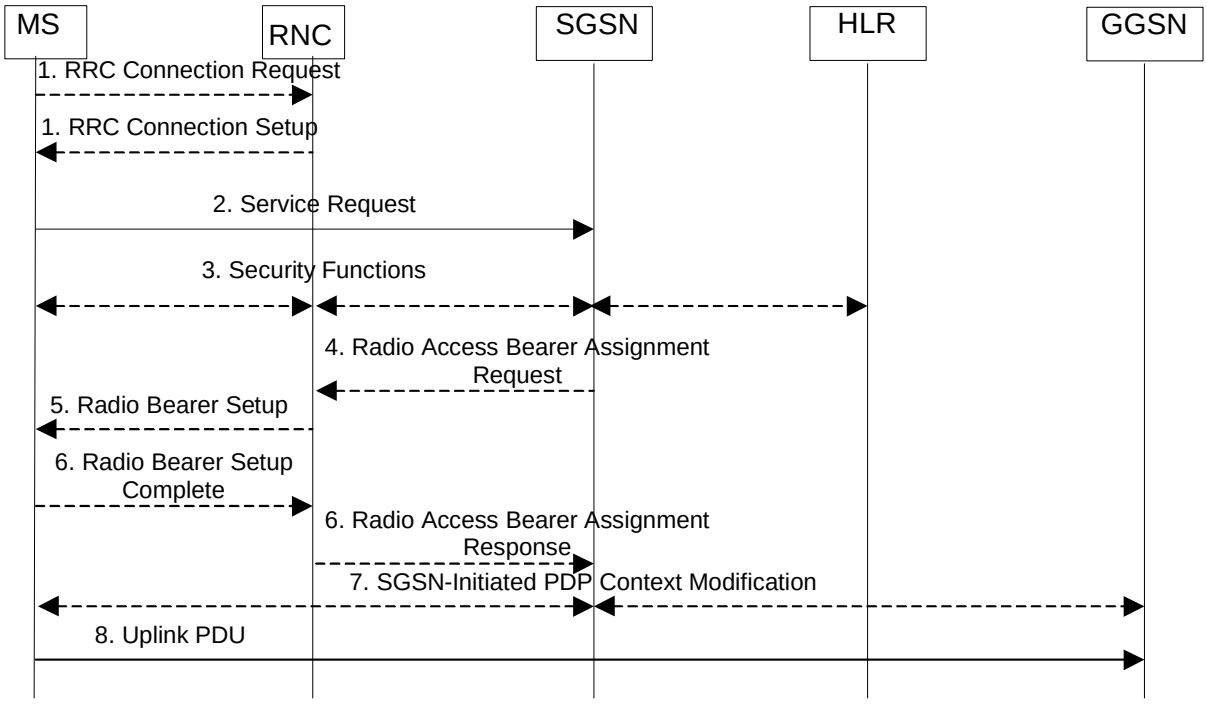


Figura 97: Petición de Servicio iniciada por MS

Leyenda:

1) MS establece una conexión RRC
2) MS envía un mensaje “Service Request” (P-TMSI,RAI,CKSN,Tipo de Servicio) a SGSN, éste ejecuta el proceso de autenticación.
3) En el caso de que el estado de inicio del proceso de MS fuera PMM-IDLE, SGSN puede lanzar las funciones de seguridad.
4) Si el Tipo de Servicio era datos en vez de señalización, SGSN envía un mensaje “Radio Access Bearer Assignment Request” para reestablecer los parámetros para los contextos PDP activados.
5) RNC indica a MS la nueva Identidad de Radio establecida y el correspondiente ID RAB
6) SRNC responde con un mensaje “Radio Access Bearer Assignment Response”. La interfaz de Iu establece el túnel GTP. En el caso de existir problemas de QoS, puede repetirse el proceso desde el paso 4).
7) Por cada RAB establecida con una QoS actualizada, SGSN inicia el contexto PDP.
8) MS envía un paquete de desconexión.

Si el Tipo de Servicio es señalización, MS sabe que la petición de servicio ha sido recibida correctamente por SGSN cuando recibe un mensaje de Comando de Control Modo Seguridad de RRC. En el caso de Tipo de Servicio es datos, MS recibe un mensaje Inicializar Parámetros de Radio del RNC.

16.3.4.2 Petición de servicio iniciada por la red

Cuando SGSN recibe un paquete de un MS es estado PMM-IDLE, envía una petición de canal de aviso a UTRAN quien provoca la Petición de Servicio en MS.

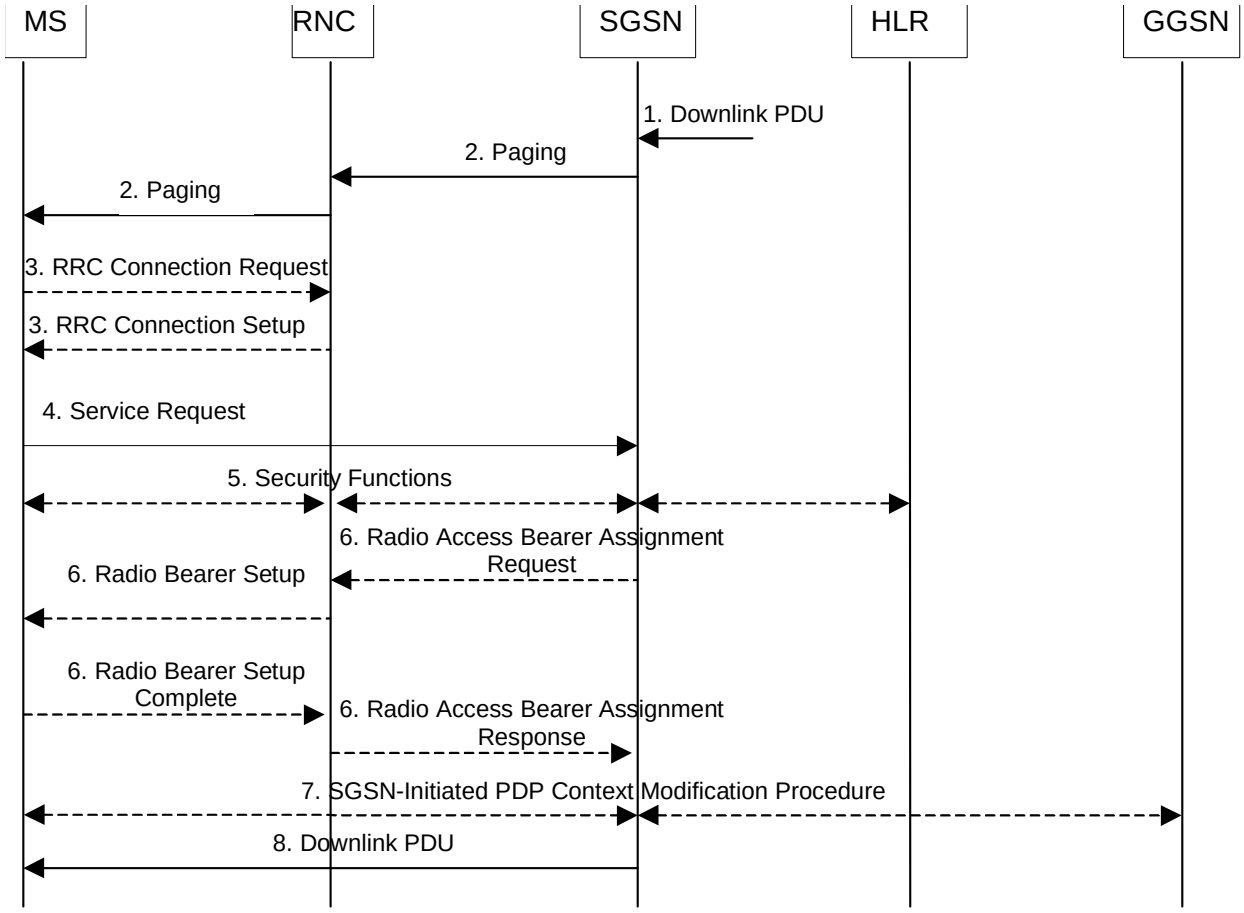


Figura 98: Petición de Servicio iniciada por la red

Leyenda:

1) SGSN recibe una PDU (por ejemplo del contexto PDP) de un MS es estado PMM-IDLE
2) SGSN envía un mensaje de "Paging" a RNC quien a su vez lo envía a MS.
3) MS establece una conexión RRC, si no existía.
4) MS envía un mensaje "Service Request" (P-TMSI,RAI,CKSN,Tipo de Servicio) a SGSN definiendo el tipo de servicio como respuesta de canal de aviso. El mensaje "Service Request" se transmitirá en un mensaje "RRC Direct Transfer" y en el mensaje "RANAP Initial MS" en la interfaz de Iu. En este momento, SGSN puede ejecutar el proceso de autenticación.

5) En el caso de que el estado de inicio del proceso de MS fuera PMM-IDLE, SGSN puede ejecutar el procedimiento de modo de seguridad.
6) Si los recursos del contexto PDP se han modificado, SGSN envía un mensaje "Radio Access Bearer Assignment Request" a RNC, quien a su vez envía un "Radio Bearer Setup" a MS. MS envía la respuesta a RNC y éste a SGSN, para notificarle que los parámetros y el túnel GTP ya se han sido establecidos entre MS y RNC.
7) Por cada RAB modificado, SGSN inicia el procedimiento de "Context Modification Procedure".
8) SGSN envía el paquete descendente.

Si el Tipo de Servicio es respuesta página, MS sabe que la petición de servicio se ha sido recibida correctamente por SGSN, cuando recibe un mensaje de Comando de Control Modo Seguridad de RRC

16.3.5 Funcionalidad de Gestión de Recursos de Radio

En la figura siguiente podemos observar la máquina de estados de RRC. El estado RRC describe el estado de MS en UTRAN.

La máquina de estados existe como dos entidades paralelas sincronizadas, una en UTRAN y otra en MS.

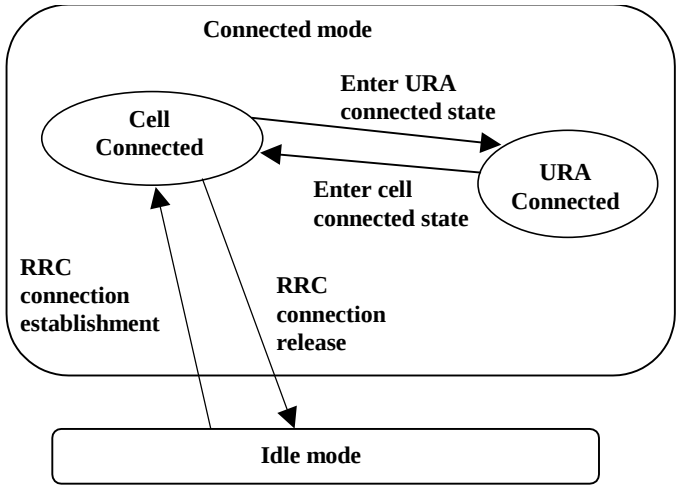


Figura 99: Máquina de estados RRC

Leyenda:

RRC "Idle mode"
En este estado no existen conexiones establecidas entre MS y UTRAN. No se transmite señalización alguna entre ellos, excepto la información del sistema.

MS puede recibir mensajes de canal de avisos con una identificación de CN en el PCH. UTRAN no guarda ninguna información de MS.

RRC "Connected Mode"
En el Modo Conectado, los estados principales son celda conectada ,"Cell Connected", y conectado a URA, "URA Connected". En este modo un RNC está actuando como servidor RNC y existe una conexión entre MS y SRNC. Cuando la posición de MS se conoce a nivel de celda, estamos en el estado "Cell Connected". Si la posición de MS se conoce a nivel de URA, se denomina estado "URA Connected". En este estado no se utilizan recursos de radio dedicados.

16.3.5.1 Canal de avisos iniciado por CN

El nodo de CN sólo efectúa una Petición de Canal de aviso a MS en estado CMM-IDLE o PMM-IDLE. Para cada Petición de Canal de aviso recibida, RNC determina si MS tiene establecida una conexión o no.

Si no existe un contexto definido, se ejecuta un proceso de canal de aviso PCH normal, el mensaje se transfiere al canal de aviso e incluye la identidad del canal de MS recibida de CN y un indicador de tipo de dominio de la CN. Si existe un contexto, se transfiere un mensaje "Paging" de CN utilizando la conexión RRC existente. El mensaje también incluye el tipo de dominio de la CN.

16.3.5.1.1 Paginación PS iniciada por SGSN sin Conexión RRC para CS

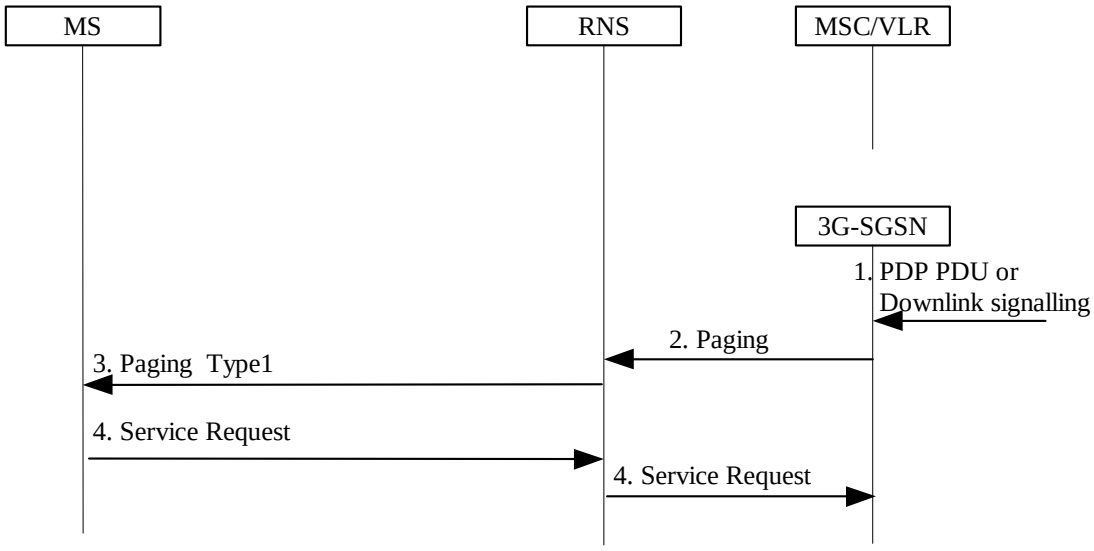


Figura 100: Canal de avisos de PS sin conexión RRC para CS

Leyenda:

1) SGSN recibe una PDU PDP o señalización de un MS en estado "PMM Idle".

2) SGSN envía un mensaje “Paging” (IMSI,P-TMSI,Área,Indicador Dominio CN) de RANAP, a cada RNS perteneciente al área de direccionamiento en la cual está ubicado MS.
3) RNS controla si MS tiene establecida alguna conexión RRC o no.
4) La petición de canal de avisos provoca los procesos de Petición Servicio en el MS.

16.3.5.1.2 Canal de avisos de PS iniciado por SGSN con conexión RRC para CS

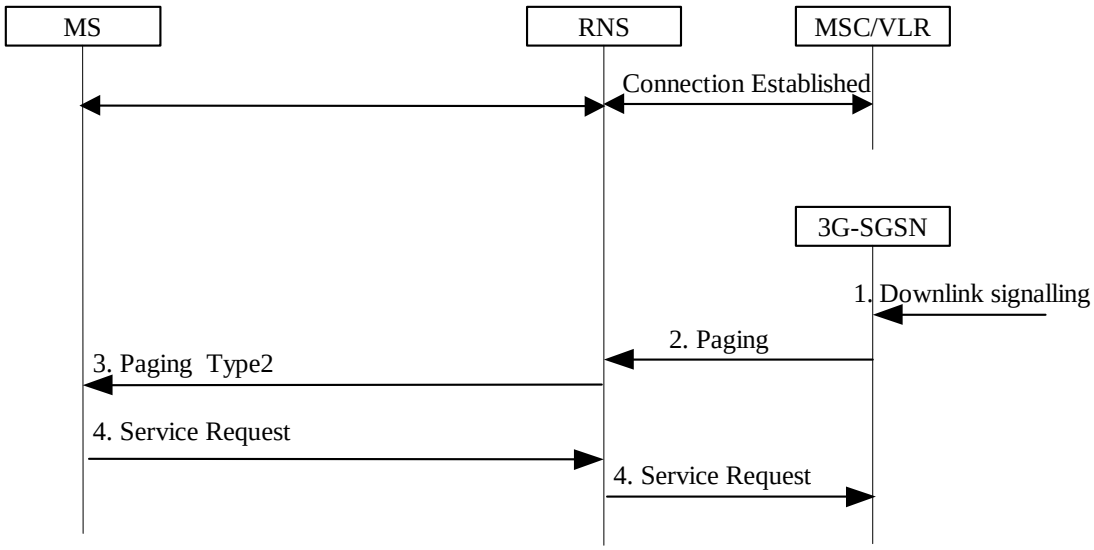


Figura 101: Canal de avisos de PS con conexión RRC para CS

Leyenda:

1) SGSN recibe señalización de un MS en estado “PMM Idle”.
2) SGSN envía un mensaje “Paging” (IMSI,P-TMSI,Área,Indicador Dominio CN) de RANAP, a cada RNS perteneciente al área de direccionamiento en la cual está ubicado MS.
3) RNS controla si MS tiene establecida alguna conexión RRC o no. En este caso, al existir la conexión, RNS envía un “Paging Type RRC 2” (ID dominio CN) a MS en la conexión RRC existente.
4) La petición de canal de avisos provoca los procesos de Petición Servicio en el MS.

16.3.5.2 Canal de avisos iniciado por UTRAN

Si el estado de RRC de MS es conectado a URA, RNC realiza el proceso de establecimiento de canal de avisos antes de cualquier transmisión descendente hacia MS. El procedimiento utilizado modificará el estado de RRC a Celda Conectada para permitir a RNC la transmisión de datos o mensajes de señalización al recurso de radio. La respuesta de MS es el mensaje de Actualización Celda que modifica el estado del RRC a Celda Conectada.

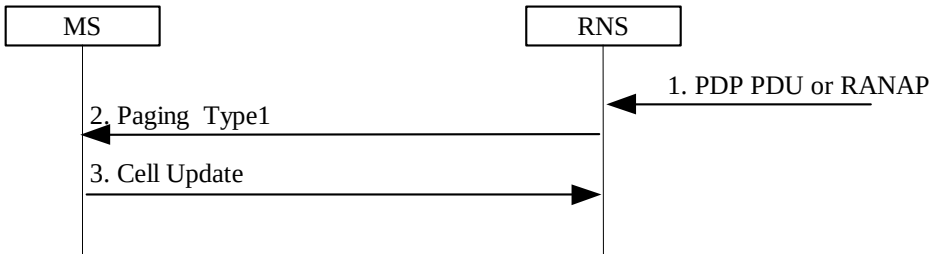


Figura 102: Procedimiento de canal de avisos de URA

Leyenda:

1) RNS recibe una PDU PDP para un MS con estado de RRC conectado a URA.
2) RNS envía un mensaje “Paging Type1” en cada celda perteneciente al área de direccionamiento de la UTRAN donde reside MS.
3) La petición de canal de avisos provoca el proceso de” Cell Update” en MS.

17Anexo 8: Tecnología WAP

La tecnología WAP aparece en el mercado como resultado del desarrollo de la tecnología WWW orientado a la tecnología sin cables. Las características principales del protocolo de WAP son :

- Independencia de cualquier dispositivo
- Independencia de la interfaz de radio
- Interoperabilidad entre sus componentes
- Acceso a Internet de tecnología sin cable

El modelo de programación WAP toma como punto de partida los estándares existentes en WWW, definiendo un lenguaje de programación WML y WMLScript basado en XML.

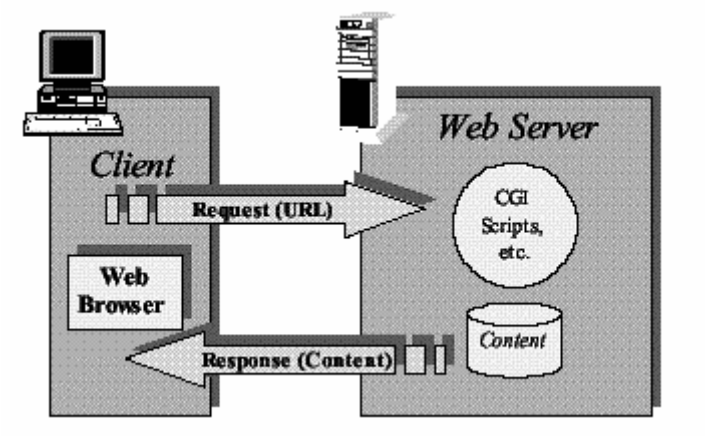


Figura 103. Modelo de Programación WWW

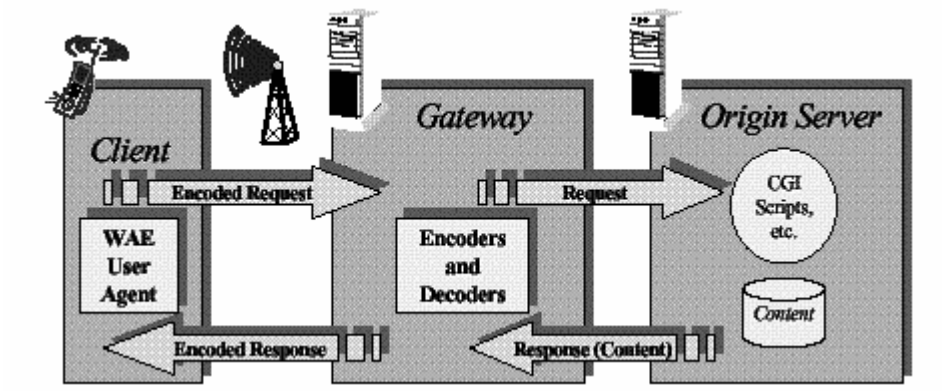


Figura 104. Modelo de programación WAP

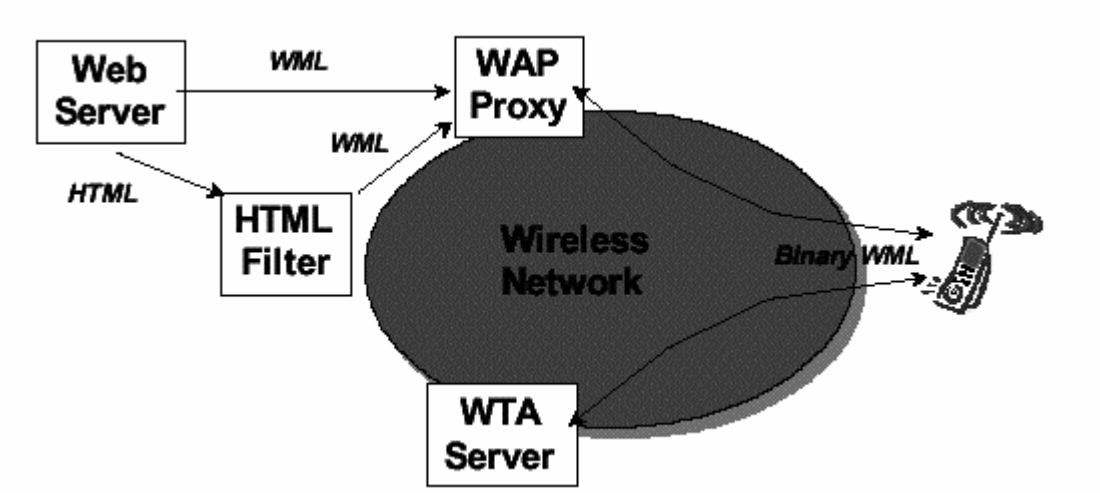


Figura 105. Ejemplo de red WAP

17.1 Arquitectura de protocolos

Los puntos más destacables de esta arquitectura son en primer lugar, la seguridad extremo a extremo entre elementos de protocolo WAP, y en segundo lugar la posibilidad de que otros servicios y aplicaciones independientes de WAP utilicen sus servicios a través de interfaces. Las aplicaciones externas pueden acceder directamente a los niveles de sesión, transacción, seguridad y transporte. Ver figura.

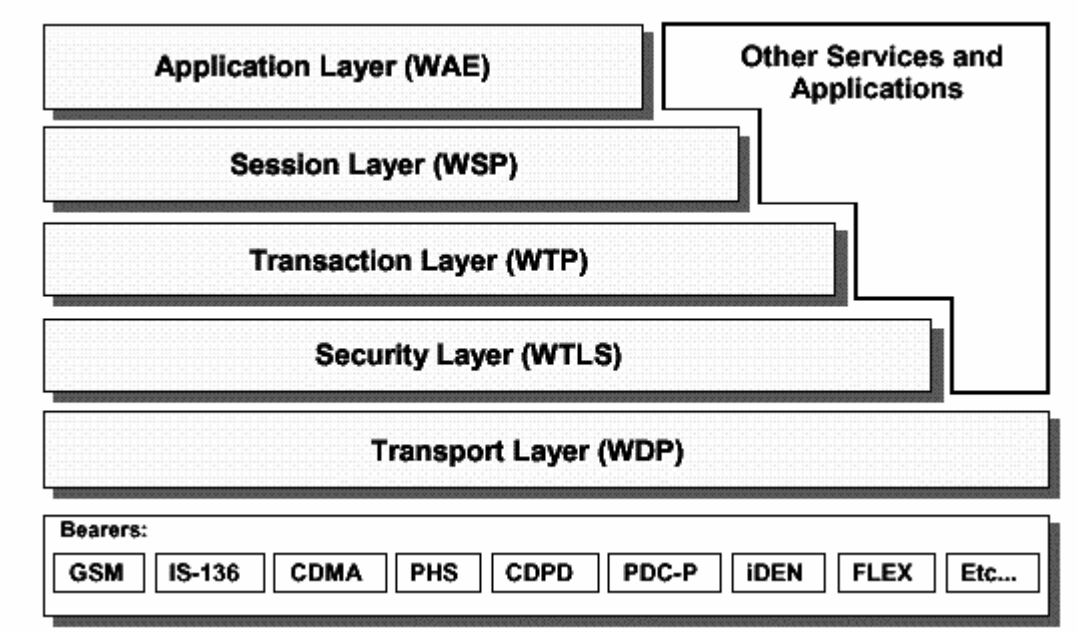


Figura 106. Modelo de arquitectura WAP

17.1.1 Nivel de Aplicación (WAE)

El nivel de aplicación, es un entorno de aplicación de propósito general basado en una combinación de WWW y tecnologías de telefonía móvil. Incluye un entorno de micro-buscador con funcionalidad WML, WMLScript, formatos (datos, imágenes, registro de listín telefónico,...), etc.

17.1.2 Nivel de Sesión (WSP)

El nivel de Sesión ofrece una interfaz con dos tipos de servicios de sesión. El primero está orientado a la conexión y opera sobre el nivel de transporte (WTP) y el segundo no está orientado a la conexión y opera sobre un nivel de datagrama (WDP). En ambos casos el uso de nivel de seguridad es opcional.

Este nivel se caracteriza por:

- Adoptar la funcionalidad de HTTP 1.1
- Permitir sesiones de larga duración
- Permitir la "suspensión" y "reinicio" de sesiones
- Permitir el envío de datos desde el servidor (iniciando éste el proceso)
- Permitir la negociación de características del protocolo

17.1.3 Nivel de Transporte (WTP)

El nivel de transporte trabaja sobre el nivel de datagrama y ofrece un protocolo de transacción orientado a la conexión. WTP opera tanto sobre un nivel de datagrama seguro como inseguro y ofrece:

- Tres tipos de servicios de transacción:
  - Transacciones de petición, de un paso, no fiables
  - Transacciones de petición, de un paso, fiables
  - Transacciones de petición con respuesta, de dos pasos, fiables
- Concatenación de PDUs y postposición de mensajes ACK
- Transacciones asíncronas
- Opcionalmente, fiabilidad usuario a usuario
- Opcionalmente, datos fuera de banda en mensajes ACK

17.1.4 Nivel de Seguridad (WTLS)

El nivel de seguridad se basa en TLS, en versiones anteriores conocido como SSL, optimizado para el uso en canales de comunicación de banda estrecha. Los servicios que ofrece son:

- Integridad de datos
- Confidencialidad
- Autenticación
- Protección contra la negación de servicio

WTLS también puede utilizarse para la protección de comunicaciones entre terminales. Además las aplicaciones pueden seleccionar la activación / desactivación de cualquiera de las funcionalidades de WTLS dependiendo de sus requerimientos y de las características de la red.

17.1.5 Nivel de Datagrama (WDP)

El nivel de datagrama ofrece una interfaz común a los niveles superiores independientemente de los canales de comunicación del nivel inferior.

Para redes IP se utiliza el protocolo UDP como nivel de datagrama ya que ofrece la misma funcionalidad y es un protocolo ampliamente difundido.

17.2 WTLS

WTLS es el nivel de seguridad definido para tecnología WAP. Este nivel, se caracteriza por ser accesible desde aplicaciones y servicios independientes de WAP, a partir de unas interfaces definidas.

Basado en el protocolo TLS, esta optimizado para el uso sobre canales de comunicación de banda estrecha. Los servicios que ofrece WTLS son:

- Integridad de datos
- Confidencialidad
- Autenticación
- Protección contra negación de servicios

WTLS ofrece una interfaz de servicio de transporte segura y una interfaz de gestión de conexiones seguras. Todos los procesos se realizan mediante primitivas de servicio ya estandarizadas.

Las aplicaciones seleccionan aquellos servicios de WTLS que desean ejecutar, dependiendo de sus requerimientos de seguridad y de las características de la red de nivel inferior.

17.2.1 Gestión de conexiones WTLS

La gestión de conexiones WTLS permite al cliente conectarse con un servidor y fijar las opciones del protocolo a utilizar. La negociación puede incluir los parámetros de seguridad, intercambio de claves y autenticación.

17.2.2 Protocolo de Registros WTLS

En el nivel de WTLS se define el Protocolo de Registros de WTLS, este protocolo recoge los mensajes a enviar, opcionalmente comprime los datos, aplica un MAC, encripta y finalmente transmite el resultado. En el caso de recepción de datos realiza el proceso inverso, desencripta, verifica y descomprime el mensaje antes de distribuirlo a los clientes de nivel superior.

La información llega a este nivel en bloques, no vacíos, de longitud máxima 2^{16}-1. A diferencia de TLS, el nivel de registro no fragmenta la información y es tarea del nivel de transporte realizar este proceso

Dentro del protocolo de registros de WTLS se definen cuatro protocolos, el protocolo de cambio de especificación de cifrado, el protocolo de sincronización, el protocolo de alerta y el protocolo de datos de aplicación.

17.2.2.1 Protocolo de sincronización

El protocolo de sincronización permite a entidades acordar los parámetros de seguridad, autenticarse y transmitirse los errores producidos. Es el protocolo responsable de la negociación de sesiones seguras.

Al inicio de la comunicación entre un servidor y un cliente WTLS, se fija una versión de protocolo, se seleccionan los algoritmos criptográficos, opcionalmente se autentican y utilizan las técnicas de encriptación con clave pública para generar una clave compartida.

17.2.2.2 Protocolo de cambio de especificación de cifrado

Este protocolo consiste en un único mensaje cuya finalidad es notificar a la otra entidad la transición entre algoritmos de cifrado.

17.2.2.3 Protocolo de alerta

El protocolo de alerta consiste en la transmisión de determinados mensajes que llevan asociados el nivel de error, en el caso de error grave implican la finalización inmediata de la conexión segura.