



**ESCUELA SUPERIOR POLITECNICA DEL LITORAL**  
**Facultad de Ingeniería en Electricidad y Computación**

**" DISEÑO E IMPLEMENTACION DE UN SISTEMA DE  
ANTIFRAUDE CELULAR "**

**PROYECTO DE GRADUACION**

Previa a la Obtención del Título de:  
**INGENIERO EN ELECTRICIDAD**

ESPECIALIZACION  
**ELECTRONICA**

PRESENTADO POR:

*Ximena Artieda Garzón*  
*David Castro Carrasco*  
*Jimmy Rodríguez Galán*

GUAYAQUIL - ECUADOR

**AÑO**

**1 9 9 9**

# AGRADECIMIENTO

ING. VICENTE

SALTOS

Director del Tópico de graduación, por su ayuda y colaboración para la realización de este trabajo.

# DEDICATORIA

A NUESTRO

DIOS

A NUESTROS

PADRES

A NUESTROS

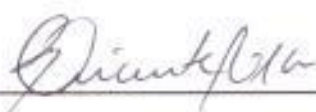
HERMANOS Y

AMIGOS

# TRIBUNAL DE GRADUACION



Ing. Carlos Monsalve A.  
DECANO DE LA FIEC



Ing. Vicente Saltos B.  
DIRECTOR DE TESIS



Ing. Washington Medina  
VOCAL



Ing. Boris Ramos.  
VOCAL

# DECLARACION EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado, nos corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITECNICA DEL LITORAL”



Jimmy Rodríguez G.



David Castro C.



Blanca Ximena Artieda. G.

## RESUMEN

El presente proyecto establece la solución al grave problema del fraude celular en redes inalámbricas, ya que hasta ahora está ampliamente aceptado y reportado por toda la industria telefónica mundial, incluyendo las operadoras de tanto redes inalámbricas a nivel celular y analógico.

El propósito de esta tesis es proveer a las operadoras de PORTA y BELLSOUTH, un sistema de autenticación celular para evitar la clonación de teléfonos celulares que tanto daño hace a las operadoras celulares y a los subscriptores. Esperamos que con este aporte podamos subsanar el problema del fraude celular y que las entidades públicas o privadas ahonden esfuerzos para aportar con un capital económico para implementar este sistema de autenticación.

El proyecto de esta tesis involucra cuatro capítulos específicos:

- El fraude en el ámbito mundial, en el cual se especifica el impacto que tiene el fraude en las redes operadoras analógicas y digitales siendo las primeras autenticadas o no autenticadas.
- La presencia de la autenticación, como un recurso para combatir el fraude en las redes inalámbricas. Aquí se discutirá los diferentes elementos de la autenticación celular (MSC, HLR, VLR, Centro de Autenticación, etc..) y además se hablará del proceso de autenticación y los estándares de los cuales se basa.
- El diseño e implementación de un sistema de autenticación, es decir de un sistema

de seguridad que sea capaz de prevenir el fraude y de proveer autenticación a teléfonos válidos.

- Un estudio de costos y mercadeo para tener una idea de cómo se llevará un plan de tarificación de llamadas celulares, a su vez se llevara una lista de costos para la implementación del sistema de autenticación y del impacto que pueda tener este sistema en el mercado celular.

## ÍNDICE GENERAL

	Pág.
RESUMEN .....	VI
ÍNDICE GENERAL.....	VIII
ÍNDICE DE FIGURAS.....	XIV
ÍNDICE DE TABLAS.....	XVI
ABREVIATURAS.....	XVII
INTRODUCCIÓN.....	1
<b>1. FRAUDE</b> .....	<b>2</b>
1.1 Introducción al fraude.....	2
1.2 Evolución del fraude inalámbrico.....	6
1.3 Tipos de fraude.....	9
1.3.1 Fraude Técnico .....	12
1.3.2 Fraude por Prepago.....	18
1.3.3 Fraude por Suscripción .....	19
1.3.4 Fraude Clandestino.....	25
1.3.5. Negociando o revendiendo el fraude.....	27



1.3.6. Fraude en los equipos (microteléfonos).....	28
1.3.7 Ingeniería social y amistad fraudista.....	29
1.4 El Impacto del fraude.....	31
1.4.1 Perdidas Financieras.....	31
1.4.2 Marketing.....	32
1.4.3 Relaciones de clientes.....	32
1.4.4 Percepciones del accionista.....	32
1.5 Herramientas para combatir el fraude.....	33
1.5.1 Métodos de detección.....	34
1.5.2 Métodos de prevención.....	35
<b>II. AUTENTICACIÓN CELULAR.....</b>	<b>47</b>
2.1 Introducción y elementos básicos de autenticación.....	47
2.1.1 Entidades Funcionales de Red.....	50
2.2 Centro de autenticación.....	53
2.3 Proceso de autenticación.....	54
2.3.1 Autenticación en el acceso.....	64
2.3.2 Autenticación en la Registración de la llamada.....	68
2.3.3 Autenticación en la originación de una llamada.....	71

2.3.4 Escenarios de Autenticación.....	74
2.3.5 Interface Aérea.....	85
2.3.6 Consideración del RAND.....	90
2.3.7 Mensajes de Autenticación.....	91
2.4 Proceso del Unique Challenge.....	94
2.5 Proceso de Actualización del SSD.....	95
2.5.1 Actualización del SSD iniciada durante el acceso del móvil.....	99
2.5.2 Actualización Manual del SSD para un móvil.....	106
2.5.3 Actualización Manual del SSD para un móvil no disponible.....	109
2.6 Fallas de Autenticación.....	114
2.6.1 Error del AUTHR en la registraci3n y originaci3n...	114
2.6.2 Falla del RANDC en la Registraci3n y Originaci3n.....	122
2.7 Móviles Autenticables.....	132

### **III. DISEÑO Y SIMULACION DEL SISTEMA**

<b>DE AUTENTICACION.....</b>	<b>134</b>
3.1 Objetivo.....	134

3.2 Operaciones del Centro de Autenticación.....	135
3.3 Configuraciones del Centro de Autenticación.....	137
3.3.1 Dos regiones de cobertura con un solo centro de autenticación externo.....	140
3.3.2 Dos regiones de cobertura con dos centros de autenticación externos propios.....	141
3.3.3 Dos regiones de cobertura con sus centros de autenticación internos respectivamente.....	143
3.3.4 Dos regiones de cobertura con un centro de autenticación integrado en una de ellas.....	144
3.4 Planificación del Sistema de Autenticación.....	146
3.4.1 Objetivos de la Planificación.....	146
3.4.2 Metodología.....	148
3.5 Tratamiento del sistema de autenticación.....	156
3.5.1 Procesamiento del registro de datos de las llamadas.....	158
3.5.2 Perfiles del usuario.....	159
3.5.3 Alarmas.....	159
3.5.4 Entradas y salidas de datos.....	161

3.5.5 Funciones de Negocios.....	163
3.5.6 Interfaces del Usuario.....	165
3.5.7 Reportes.....	166
3.5.8 Comercialización del usuario.....	168
3.6 Beneficios del sistema de autenticación.....	170
3.7 Provisionamiento del sistema de autenticación.....	172
3.7.1 Administración de las Claves de Autenticación.....	172
3.7.2 Generación de las claves de Autenticación.....	174
3.7.3 Creación y Mantenimiento de la Base de Datos del Centro de Autenticación.....	175
3.7.4 Administración de las rutas del HLR.....	180
3.8 Hardware y software requeridos en el sistema de autenticación.....	180
3.8.1 Hardware en el Centro de Autenticación.....	180
3.8.2 Software en el Centro de Autenticación.....	181
3.8.3 Hardware en el sistema de administración de la clave de autenticación.....	182
3.8.4 Software del Sistema de Administración de Seguridad de la Clave de Autenticación.....	184

3.8.5 Hardware de la interface de programación del	
A-key.....	184
<b>IV ANALISIS COMERCIAL.....</b>	<b>186</b>
4.1 Planes de tarificación de llamadas celulares.....	186
4.2 Costos de implementación de un sistema de autenticación	
vs RF Fingerprinting.....	199
4.2.1 Comparación de las Técnicas.....	199
4.2.2 Análisis Comparativo.....	202
4.2.3 Costos estimados de autenticación	
y RF Fingerprinting.....	204
4.3 Costos de hardware y software del centro	
de autenticación.....	210
4.4 Costos de hardware y software del sistema de administración	
del la clave de autenticación.....	211
4.5 Impacto estimado del sistema de autenticación.....	212
<b>V CONCLUSIONES.....</b>	<b>213</b>
<b>VI RECOMENDACIONES.....</b>	<b>216</b>
APÉNDICES.....	219
BIBLIOGRAFÍA.....	348

## INDICE DE FIGURAS

Fig. 1.1	Principio de la Clonación.....	14
Fig. 1.2	Clonación Profesional.....	15
Fig. 1.3	Tumbling.....	16
Fig. 1.4	Arquitectura RF Fingerprinting.....	38
Fig. 1.5	RF Fingerprinting y Roaming.....	39
Fig. 2.1	Arquitectura de Red de un AC Externo.....	50
Fig. 2.2	Arquitectura de Red de un AC Interno.....	51
Fig. 2.3	Arquitectura del Sistema de Autenticación.....	56
Fig. 2.4	Registración en el Acceso Inicial del Sistema.....	65
Fig. 2.5	Autenticación en la Registración del AC.....	69
Fig. 2.6	Autenticación en la Registración del Móvil.....	70
Fig. 2.7	Autenticación en la Originación del Móvil.....	72
Fig. 2.8	Autenticación en la Originación del AC.....	73
Fig. 2.9	Registración Inicial Exitosa.....	76
Fig. 2.10	Originación Exitosa sin entrada VLR.....	79
Fig. 2.11	Originación Exitosa con entrada VLR (SSD no compartido).....	82
Fig. 2.12	Originación Exitosa con entrada VLR (SSD compartido).....	84
Fig. 2.13	Actualización del SSD en el Acceso del Móvil.....	105
Fig. 2.14	Actualización del SSD para un Móvil.....	109
Fig. 2.15	Actualización del SSD para un Móvil no Disponible.....	113
Fig. 2.16	Error del AUTHR en la Registración.....	117
Fig. 2.17	Error del AUTHR en la Originación.....	122
Fig. 2.18	Registración en la Celda Adyacente y el RANDC no igual a cero .	129
Fig. 2.19	Originación de la Celda Adyacente y el RANDC no igual a cero .	132
Fig. 3.1	Arquitectura Interna del Sistema con un AC Externo.....	139
Fig. 3.2	Arquitectura del Sistema con un AC Interno.....	140
Fig. 3.3	Dos Regiones de Cobertura con un solo AC Externo.....	142
Fig. 3.4	Dos Regiones de Cobertura con dos AC Externos propios.....	143
Fig. 3.5	Dos Regiones de Cobertura con sus AC Internos.....	145
Fig. 3.6	Dos Regiones de Cobertura con un AC integrado en una de ellas	146
Fig. 3.7	Cronograma de Actividades para la Planificación del Sistema de Autenticación.....	150
Fig. 3.8	Hardware en el Sistema de Autenticación.....	183
Fig. 3.9	Hardware en el Sistema de Administración de la Clave de Autenticación.....	185
Fig. 3.10	Interface de Programación del A-key.....	194
Fig. A.1	Estructura del modelo IS41 C	
Fig. A.2	Solicitud de Autenticación	
Fig. A.3	Autenticación Directiva	
Fig. A.4	Base Station Challenge	
Fig. A.5	Reporte del Status de Autenticación.	

- Fig. A.6 Reporte de la Falla de Autenticación
- Fig. A.7 Reporte del Estatus de Seguridad.
- Fig. A.8 Registración Inicial con Autenticación en el Canal de Radio.
- Fig. A.9 Origenación con Autenticación en el Canal de Radio.
- Fig. A.10 Terminación con Autenticación en el Canal de Radio.
- Fig. A.11 Autenticación en el Canal de Voz.
- Fig. A.12 VLR iniciado con Unique Challenge.
- Fig. A.13 Actualización del SSD con SSD Compartido.
- Fig. A.14 Estructura de los slots del canal DCCH.
- Fig. A.15 Capas de la Interface IS 136
- Fig. A.16 Trama de slots de datos del IS 136
- Fig. A.17 Configuración de los canales IS 136
- Fig. A.18 Canal de control analógico (ACC) versus la consumpción corriente de la batería en el DCCH.
- Fig. A.19 Mensajería de teleservicio con IS-41.
- Fig. A.20 Sistema de microcelda privado dentro de una macrocelda pública con IS 136
- Fig. A.21 Estructuras de celdas jerárquicas en IS 136
- Fig. A.22 Distribuciones de los canales IS 136.
- Fig. A.23 Componentes del SMS en IS 91 a
- Fig. A.24 Mensajería IS 91 a
- Fig. A.25 Trama de Datos del Estándar IS 54B
- Fig. B.1 Elementos del Algoritmo CAVE
- Fig. B.2 Algoritmo CAVE
- Fig. B.3 Pseudo código para verificación del A-Key
- Fig. B.4 Generación del SSD\_A y SSD\_B
- Fig. B.5 Pseudo código para actualizar el SSD
- Fig. B.6 Carga Inicial del CAVE para cálculos del AUTH / AUTHU
- Fig. B.7 Cálculo del AUTHER y AUTHU
- Fig. B.8 Pseudo código para cálculo del AUTHER
- Fig. B.9 Pseudo código para clave CMEA y generación del VPM
- Fig. B.10 Generación de la clave CMEA y de la máscara de privacidad de voz (VPM)
- Fig. B.11 Generación detallada de la clave CMEA y VPM
- Fig. C.1 Pseudo código para t-box
- Fig. C.2 Pseudo código del Algoritmo CMEA

## INDICE DE TABLAS

Tabla 2.1	Interfaces aéreas Soportadas en el MSC.....	86
Tabla 2.2	Teléfonos Celulares Autenticables.....	133
Tabla 3.1	Información de la Base de Datos del AC por Móvil.....	181
Tabla 4.1	Plan 1.....	190
Tabla 4.2	Plan 2.....	191
Tabla 4.3	Plan 3.....	192
Tabla 4.4	Plan 4.....	193
Tabla 4.5	Plan 5.....	194
Tabla 4.6	Plan Oficina.....	195
Tabla 4.7	Plan Empresarial.....	196
Tabla 4.8	Plan Permanente.....	197
Tabla 4.9	Plan Permanente Plus.....	198
Tabla 4.10	Plan Negocio.....	199
Tabla 4.11	Plan Grupal.....	200
Tabla 4.12	Flujo de Caja.....	205
Tabla 4.13	Costos de Móviles y Unidades RFU.....	207
Tabla 4.14	Balance estimado del Sistema de Autenticación.....	208
Tabla 4.15	Costos de Autenticación y RF Fingerprinting.....	210
Tabla 4.16	Costos de Hardware y Software del Centro de Autenticación.....	212
Tabla 4.17	Costos de Hardware y Software del Sistema de Administración La Clave de Autenticación.....	213
Tabla A.1	Puntos de Referencia de la interface IS-41C	
Tabla A.2	Canales lógicos del IS 136	
Tabla A.3	Especificaciones de la Interface aérea IS 54B	
Tabla B.1	Tabla del Algoritmo CAVE	
Tabla B.2	Tabla CAVE en ASCII	



## ABREVIATURAS

<b>AAV</b>	Versión del Algoritmo de Autenticación
<b>AC</b>	Centro de Autenticación
<b>ACCH</b>	Canal de Control Analógico.
<b>AFREPORT</b>	Reporte de Fallas de Autenticación.
<b>AG</b>	Comando de Generación del A-key
<b>AGEN</b>	Comando de Generación manual del A-key en el AC.
<b>A-KEY</b>	Clave de Autenticación
<b>AMPS</b>	Servicio Telefónico Móvil Avanzado
<b>ASREPORT</b>	Reporte del Status de Autenticación.
<b>AUTH</b>	Parámetro de Autenticación
<b>AUTHBS</b>	Salida del CAVE para procedimiento BSCHALL
<b>AUTHDIR</b>	Autenticación Directiva
<b>AUTHR</b>	Parámetro resultante de Autenticación
<b>AUTHREQ</b>	Solicitud de Autenticación
<b>AUTHU</b>	Respuesta del CAVE para procedimiento Unique Challenge
<b>BSC</b>	Estación Base Controladora
<b>BSCHALL</b>	Mensaje de la Estación Base para procedimiento Unique Challenge
<b>CAVE</b>	Algoritmo de Autenticación Celular y Encripción de Voz
<b>CCS7</b>	Señalización de Canal Común # 7
<b>CDMA</b>	Acceso Múltiple por División de Código
<b>DB-25</b>	Puerto de conexión de 25 pines
<b>DCCH</b>	Canal de Control Digital
<b>DEC SS7</b>	Software de Señalización # 7
<b>DEL</b>	Comando para cambiar la Base de Datos de Autenticación
<b>DOR</b>	Originación Denegada
<b>DTM</b>	Terminación Denegada
<b>ESN</b>	Número Serial Electrónico
<b>FBCCH</b>	Canal de Control de Retransmisión Rápida
<b>FCCH</b>	Canal de Control Delantero
<b>GSM</b>	Estandar Global para Móviles
<b>HLR</b>	Registro Localizador Local
<b>IS-41</b>	Estándar Interino IS-41
<b>IS-54B</b>	Estándar Interino IS-54 Rev. B
<b>IS-91</b>	Estándar Interino IS-91
<b>IS-95</b>	Estándar Interino IS-95
<b>IS-136</b>	Estándar Interino IS-136
<b>IVA</b>	Impuesto al valor agregado
<b>MIN</b>	Número de Identificación del Móvil

<b>MS</b>	Estación Móvil
<b>MSC</b>	Centro de Conmutación Móvil
<b>MSC-A</b>	Centro de Conmutación Móvil Región A
<b>MSC-B</b>	Centro de Conmutación Móvil Región B
<b>NRVR</b>	Anulador del Restablecimiento de Verificación Roaming
<b>OMT</b>	Tren de Mensajes Delantero
<b>PIN</b>	Número de Identificación Personal
<b>PRS</b>	Tasa de Servicio Premio
<b>RAND</b>	Número Aleatorio
<b>RANDC</b>	Parámetro de Confirmación Aleatoria Challenge
<b>RANDSSD</b>	Valor Aleatorio para Confirmación del SSD
<b>RANDU</b>	Variable Aleatoria del Unique Challenge
<b>REGAUTH</b>	Registro de Autenticación
<b>REGNOT</b>	Registro de Notificación
<b>RF</b>	Radio Frecuencia
<b>RRU</b>	Unidad de Radio Frecuencia
<b>RS232</b>	Interface de Datos de 32 pines
<b>RST</b>	Comando para Borrarr información Dinámica del Móvil
<b>RVR</b>	Restablecimiento de Verificaciói del Roaming
<b>SCC</b>	Sistema Central de Control
<b>SPINA</b>	Número de Identificación Personal de Acceso al Subscriptor
<b>SSD</b>	Dato Secreto Compartido
<b>TC</b>	Tabla de Control
<b>TCAP</b>	Parte de Aplicación de Capacidad de Transacción
<b>TDMA</b>	Acceso Múltiple por División de Tiempo
<b>TIA</b>	Asociación de Industrias en Telecomunicaciones
<b>TRU</b>	Unidades de Radio Tranceiver
<b>V.35</b>	Protocolo de Comunicación de 35 pines
<b>VCH</b>	Canal de Voz
<b>VLR</b>	Registro Localizador Visitante
<b>X.25</b>	Protocolo de Enlace de Datos

## INTRODUCCION

El presente trabajo es un "Diseño e Implementación de un Sistema de Autenticación Celular" (SAC), el cual detectará la presencia de fraude celular o el hurtamiento de teléfonos celulares y a su vez darle una seguridad a las registraciones y originaciones de llamadas celulares. También se realizara la simulación de una llamada telefónica celular de tal forma que se ingrese el número telefónico mediante teclado en la computadora y bajo un ambiente de programación que usaremos (lenguaje C), se autenticará un teléfono celular y en la pantalla de la computadora se visualizará la señalización de los diferentes mensajes de autenticación mediante el protocolo IS-41C.

La tecnología del Sistema de Autenticación Celular en cuestión estará basado bajo los sistemas de multiplexación existentes en el Ecuador (TDMA, AMPS). Aunque dicho sistema puede dar servicio a redes NAMPS y CDMA.

Entre otras bondades del sistema de autenticación celular que se implementará, serán:

- Soporte para líneas telefónicas.
- Soporte para llamadas celulares.
- Soporte a llamadas Inalámbricas Local Loop.
- Soporte para tecnología analógica.
- Soporte para tecnología digital.

## CAPITULO I

### FRAUDE

#### **1.1 INTRODUCCION AL FRAUDE**

Este es un bosquejo de los más comunes aspectos del fraude, el cual está perjudicando tanto a las operadoras fijos y operadoras móviles quienes dan servicio con una conexión directa e indirecta a la red. El infractor es ingenioso y práctico, y frecuentemente encuentra una vía para estafar el servicio a los usuarios de la red pública o inalámbrica celular, para nuestro medio sería la red pública de Pacifictel y las operadoras celulares como son PORTA y BELLSOUTH. Estas son muchas variaciones de cada uno de los temas identificados, consecuentemente todos los aspectos de fraude son también numerosos de mencionar.

El fraude es una industria multibillonaria, la cual afecta a toda la red pública

telefónica. Los fraudistas que se dedican a este negocio, no solamente son motivados por el dinero, sino también necesitan del anonimato para otros crímenes, o a veces el desafío de estafar al sistema.

Como una consecuencia directa, el fraude resulta de las pérdidas de inversiones y de costos significativos adicionales para las operadoras, de tal forma que se reducen sus ganancias. Indirectamente, el fraude también impactará a las operadoras a través de la erosión de sus centros de consumo masivo celular, es decir, los clientes legítimos incorrectamente tarifados (cuando su teléfono celular es clonado, se verán obligados a terminar con el servicio que estuvo en uso; esto permite que la red de un operador abra un nuevo servicio con una red competidora en la misma geografía, síndrome conocido como "Agitamiento". De manera general todos los clientes son menos y menos deseosos para soportar el costo del fraude como una "política segura".

Una pregunta viene a la mente de las operadoras de servicio celular, la cual debe ser contestada: ¿Qué es el Fraude Celular?. El fraude es un **robo**. Cuando ciertos individuos usan las comunicaciones sin pagar por el servicio, ellos están robando el servicio de los proveedores. Desde un punto de vista práctico, no hay diferencia entre el hurtamiento de la propiedad de otro y de servicios robados. En ambos casos, algo de valor se disipa, es decir, el perpetrador pasa desapercibido.

El tamaño de las pérdidas directas de inversiones debido al fraude y lo que le

suceden a las operadoras de servicio celular, está estimado entre el 2% y 4% de los ingresos anuales que perciben las empresas de servicio celular móvil. Esto no incluye pérdidas debido a deudas.

Son de gran importancia las pérdidas que sufren las operadoras, debido a enemigos que quieren destruirlas, causando a los subscriptores una mala impresión del servicio de llamadas que reciben y con ello lleva a los subscriptores ir a otra empresa con un mejor servicio celular, lo cual prohíbe el crecimiento de negocios de toda una red operadora.

Algunas áreas son afectadas más que otras. El fraude puede ser encontrado en todas partes, sea que haya o no haya una alta densidad de subscriptores. Aunque en las áreas metropolitanas son más propensas a tasas más grandes de fraude que de menor población y también en áreas rurales.

Para poner el problema en perspectiva, considere un pequeño operador con 100 000 subscriptores el cual está tarifando en promedio 40 dólares por mes. Si el fraude aumenta al 3% del ingreso de la inversión, el proveedor no percibirá 1.2 dólares por mes por suscriptor o 120 000 dólares por mes en la inversión total. Aún si las pérdidas son limitadas a un promedio de 1 dólar por suscriptor, la inversión de pérdidas excederá 1 millón de dólares en un año, lo cual es una pérdida substancial para el pequeño operador.

Las operadoras de redes móviles enfrentan un problema adicional por el hecho de que los equipos móviles frecuentemente ofrecen una ventaja en sus servicios (tal como llamada en espera, o conversación tripartita) ya que abren una puerta para un amplio campo de fraude.

El fraude es común tanto para redes fijas como móviles de todas las tecnologías. Típicamente el más avanzado de los servicios, no se escapa a la mafia fraudista, desde el pirateaje de líneas telefónicas hasta el hurtamiento de las radio-frecuencias para servicios troncalizados. El fraude está incidiendo en los servicios de telecomunicaciones, a tal punto que el riesgo no es solamente de afuera sino frecuentemente perpetrado a propios empleados dedicados en la área técnica. Para contrarrestar el fraude, se necesita estar sujeto a una definida corporación política soportada para una apropiada implementación estratégica.

El fraude se divide en dos principales categorías, el **Fraude con fines de Lucro** en el cual el motivo es hacer dinero y el **Fraude sin fines de Lucro**, motivado para objetivos más personales. Típicamente el fraude con fines de lucro puede esperar que la división aproximada sea del 50% - 50 % entre los dos tipos. El fraude sin fines de lucro incluye, proveer un servicio de voz o datos a amigos o compatriotas sin costo alguno o para el transparente deleite del manipuleo de las defensas. En la mayoría de los casos los motivos de los perpetradores es la ganancia financiera. Esto se ha llevado acabo para inversiones fraudistas, para lo cual tenemos dos principales tipos:

Las llamadas vendidas en donde el servicio es vendido con descuento junto con las facturas que no son pagadas y la (PRS) tasa de servicio premio donde las llamadas son ilícitamente estimuladas.

## 1.2 EVOLUCION DEL FRAUDE INALAMBRICO.

La historia del fraude en la industria de las telecomunicaciones está en medio de dos líneas distintas. El fraude tradicional en líneas de redes fijas ha estado alrededor de muchas décadas. Sin embargo, fue el fraude en las recientes redes móviles que tuvieron la mayor atención inicial. Hoy en día el problema del fraude está llegando a ser bien comprendido por todos los proveedores de servicios de comunicaciones.

Con esta breve historia del fraude inalámbrico demostraremos que los fraudistas emplean métodos más sofisticados para someter al fraude de la posible prevención de operadoras inalámbricas y de los mecanismos de detección. Hay numerosas etapas que pueden ser discutidas:

- *Antes de la validación de la pre-llamada: (Simple clonación vía Tumbling).*

La validación de la pre-llamada fue una técnica usada por muchos operadoras inalámbricas; los perpetradores simplemente crearon un teléfono inalámbrico con un MIN correspondiente a un rango de operadoras de números telefónicos válidos.



Creando un falso número ESN para el microteléfono que fue construido, se pudo conocer el acceso inicial de la red que fue cedido con la primera llamada. Solamente después de que la primera llamada fuera completada, y se detecte a un subscriptor ilegítimo, la combinación del MIN/ESN fue puesta en una "lista de malos números" que sirvió para chequear contra posibles llamadas futuras.

- *Después de la validación de la pre-llamada: (Simple clonación).*

Una vez que las operadoras introdujeron la validación de la pre-llamada, un microteléfono fue requerido para presentar un MIN y ESN a la red antes de que el acceso fuera cedido. Usando una tecnología más sofisticada, los fraudistas empezaron a interceptar señales de los teléfonos celulares cuando estos estaban difundiendo el MIN y el ESN a la red para la registración de una llamada. Para la intersección de esta combinación válida de los MIN/ESN, los fraudistas usaron los radios scanners con lo cual fueron capaces de programar los teléfonos con estas combinaciones, creando clones, los cuales causarían a la red en cederles el acceso. Las llamadas de estos teléfonos clonados usualmente resultó en el subscriptor legítimo la obtención de una cuenta grande para aquellas llamadas fraudulentas.

- *Sistemas de detección por presencia de fraude.*

Cuando el problema de la clonación creció en una tasa alarmante, las operadoras desarrollaron o mandaron a pedir los sistemas de detección de fraude, los cuales

primariamente rastrearon la clonación por la búsqueda de llamadas simultáneas o dos llamadas hechas en cualquier momento en las distintas localizaciones geográficas. Esto simplemente causó que los fraudistas lleguen a ser más sofisticados de nuevo. Ellos usaron los teléfonos mágicos (se encargan de esparcir las llamadas fraudulentas alrededor de muchas combinaciones MIN/ESN válidos), reduciendo el impetu de la detección.

Otro aspecto de la moda de la clonación fue que se mudó de mercados “protegidos” por un sistema de detección a áreas más rurales. Los fraudistas para protegerse de la detección, viajaron a mercados de proveedores de tal forma que obtengan las combinaciones de los MIN/ESN válidos para clonar los teléfonos. Ellos entonces retornarían a su mercado local y harían llamadas fraudulentas. El más pequeño de los proveedores recibiría las llamadas fraudulentas en forma de llamadas roamer.

Aunque aquellos proveedores que también tuvieron sistemas de detección que podrían ser perjudiciales debido al retardo en el retorno de los registros de detalle de llamadas roaming.

- *Después de la introducción a la autenticación y a las redes digitales.*

La clonación disminuye y la suscripción por fraude se incrementa. Tanto más y más redes analógicas están introduciendo autenticación y en tanto las redes digitales

crecen, el problema ha sido una transición lejana de la clonación al fraude por suscripción. El segundo tipo de fraude antes mencionado, está llegando a ser el problema primario para muchas redes inalámbricas de hoy en día.

Muchos esfuerzos han sido agotados por la industria para autenticar el equipamiento telefónico. Sin embargo, la carencia de verificar tanto de la identidad y el crédito devaluado de los suscriptores antes de ceder el acceso a la red, ha llevado a incrementar el fraude por suscripción. El fraude por suscripción es fácil desde una perspectiva tecnológica, desde que muchas operadoras están tratando rápidamente de incrementar el tamaño de sus bases suscriptoras, están literalmente invitando a los fraudistas para entrar en su red.

El desafío de hoy en día para la prevención del fraude inalámbrico es de que los proveedores deban continuar autenticando los microteléfonos mientras que también se entrena al suscriptor. La tecnología no puede totalmente proteger a la red contra el enemigo llamado fraude.

### **1.3 TIPOS DE FRAUDE.**

Todas las redes sean estas basadas en tecnología analógica (AMPS) o en tecnología digital (GSM) son impactadas por el fraude. Las tecnologías inalámbricas y los

servicios están en constante evolución, y tal es así que las técnicas son usadas por los fraudistas. Así pues es dificultoso diseñar y bloquear una definición común de la industria de los tipos de fraude. En esta sección, las definiciones generalmente aceptadas por la industria inalámbrica y las operadoras móviles serán usadas.

En general tanto las redes de operadoras analógicas y digitales son vulnerables y expuestas al fraude. A menudo las operadoras de red creen que hay mucho menos fraude en redes digitales y que de cualquier forma la naturaleza del fraude entre redes analógicas y digitales es fundamentalmente diferente. Esto es verdad solamente en algunos casos. Una lista de los diferentes tipos de fraude se presenta aquí:

- FRAUDE TECNICO, *que consiste en hacerse pasar como un cliente legítimo o proveer un servicio no autorizado.*

El fraude técnico se divide en:

- *Clonación*
- *Tumbling*

- FRAUDE POR PREPAGO, *que consiste en el abuso de la seguridad del servicio.*

Entre las más importantes técnicas, tenemos:

- *Hurtamiento técnico para eliminar la carga*
- *Recargo fraudulento de servicio de prepago.*

- FRAUDE POR SUBSCRIPCIÓN, que consiste en obtener el servicio legítimo con motivos ilegítimos y con medios para hacerlo. Entre las más importantes técnicas, tenemos:
  - *No intentando pagar.*
  - *Hacer Roaming*
  - *Uso ilegítimo de servicios suplementarios.*
  
- FRAUDE CLANDESTINO, este fraude es perpetrado por personas dentro de la organización de la operadora. Entre las más importantes técnicas, tenemos:
  - *Teléfonos fantasmas en la red, pero que no son tarifados*
  - *Servicios de valor agregado no pagados.*
  - *Ajustes de cuenta no autorizadas.*
  
- NEGOCIANDO O REVENDIENDO CON EL FRAUDE, consiste en la explotación de los incentivos financieros. Entre las más importantes técnicas, tenemos:
  - *Falsificación de la información para comisiones ilegítimas.*
  
- FRAUDE EN LOS EQUIPOS (MICROTELEFONOS), consiste en traficar teléfonos móviles ilegítimos. Entre las más importantes técnicas, tenemos:
  - *Reciclando microteléfonos robados.*
  - *Revendiendo microteléfonos subsidiados.*
  - *Fomentando la falsificación de microteléfonos.*

- INGENIERIA SOCIAL Y AMISTAD FRAUDISTA, este tipo de fraude se realiza obteniendo acceso a la red simplemente espiando y proporcionando información. Entre las más importantes técnicas, tenemos:
  - *Haciéndose pasar como una alta autoridad, el fraudista y dando información.*
  - *Tomando ventaja de las operadoras que tienen amistades con los clientes, pretendiendo mover las cargas ilegítimas.*

### **1.3.1 FRAUDE TECNICO**

#### **1.3.1.1 CLONACION**

La clonación es el mejor medio conocido por los fraudistas telefónicos, afectando redes analógicas en particular. La clonación es la práctica de la programación de la identidad de un teléfono legítimo en otro. Los detalles de esta identidad son usualmente obtenidos ya sea por escuchar secretamente en su interconexión con la estación base o por robo de ella y lo que se trata de hacer es que las llamadas sean recargadas al propietario del teléfono legítimo.

Se han reportado múltiples casos de clonación telefónica, esto claramente multiplica y produce pérdidas económicas. La clonación móvil consiste en copiar el par MIN &

ESN de suscriptores válidos por el Canal de Control Delantero FCCH (Ver fig. 1.1). El teléfono celular es modificado para tener el mismo ESN/MIN de un suscriptor legítimo. Para obtener estos números de identificación el ladrón usa unos equipos llamados radios scanners que son vendidos por proveedores del servicio celular. Estos equipos leerán el par ESN/MIN directamente de las ondas aéreas y además de esto necesitan de una PC para reprogramar los teléfonos celulares.

Una vez reprogramados, todas las llamadas localizadas con el teléfono clonado serán cargados a la subscripción del cliente legítimo al cual fue copiado. La sospecha de fraude por clonación ocurre cuando las llamadas son hechas dentro de un breve tiempo en que se transmite la trama de las estaciones móviles con los mismos MIN/ESN.

Para evitar esto, los teléfonos son localizados geográficamente en distintas partes haciendo imposible la combinación de los MIN&ESN. Los teléfonos digitales celulares y la encriptación digital hacen mucho más difícil el hurtamiento del número ESN/MIN, pero pasará varios años antes de la conversión para que el teléfono celular este completo y protegido.

Los teléfonos clonados son vendidos por los perpetradores con una garantía de que funcionarán en un número de meses, pero si el clon es detectado por el proveedor, el fraudista lo reemplazará libre de carga en el periodo que dure la garantía.

**FIGURA 1.1**  
**PRINCIPIO DE LA CLONACION**





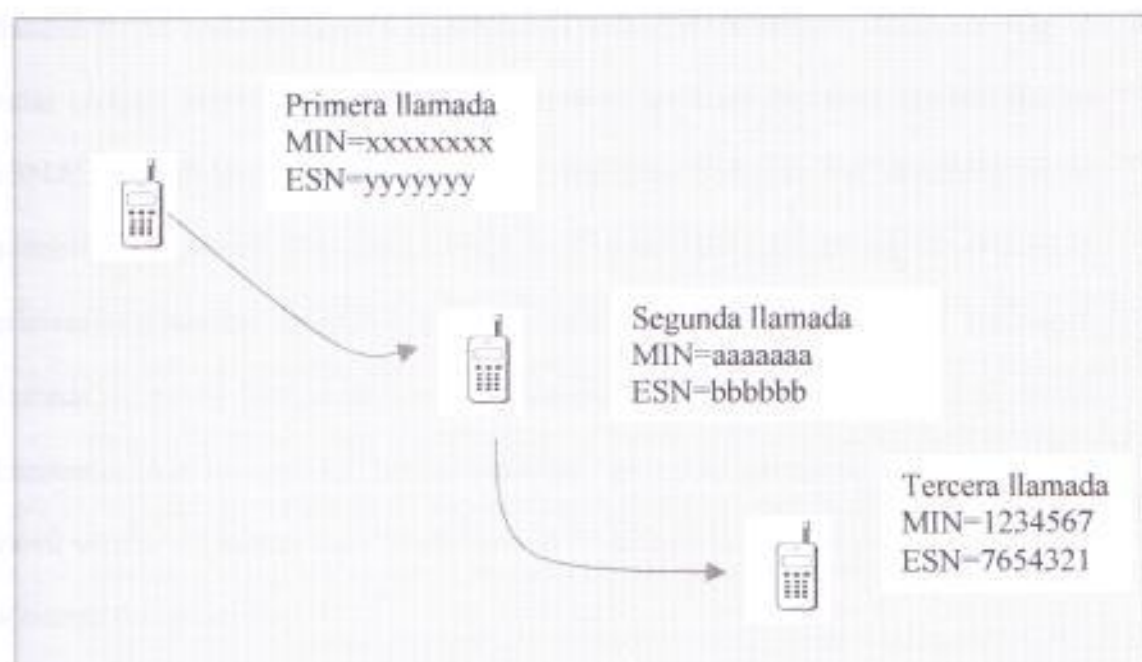
FIGURA 1.2



### 1.3.1.2 MOVILES TUMBLING

La técnica tumbling es una forma de poder perjudicar a las redes analógicas principalmente. Es una variante sofisticada de fraude por clonación. El usuario fraudulento obtiene una lista de varios números (usando scanners y capturando la información en áreas de tráfico altamente densas tales como aeropuertos). Algunos móviles pueden ser cargados con el software que permita al usuario reprogramar nuevas combinaciones después de cada llamada, usando el teclado del teléfono móvil. El cambio constante de la identidad del teléfono fraudulento debilita la colisión y la velocidad de chequeo con la que fue construido el sistema de detección, y requiere otras técnicas de detección tales como el perfil del suscriptor y otros parámetros normales de las llamadas.

FIGURA 1.3 TUMBLING



Para realizar esta actividad fraudista, se necesitan además crear programas para el aumento o cambio del MIN/ESN. El teléfono tumbador contiene un chip especial que rota a través de legítimos y falsos números pares de ESN/MIN. Ya que ellos constantemente usan diferente números de identificación, los teléfonos tumbling son extremadamente difíciles de rastrear. El uso de códigos falsos produce una debilidad a la red celular. Esto permite que la primera llamada de un nuevo ESN/MIN pase a través del sistema antes de verificar la validación del par. Estos teléfonos burlan el sistema en el sentido de que cada llamada realizada por el subscriptor con falsos números de identificación sea la primera llamada en que se especifica el par.

En lo que respecta a los teléfonos mágicos es una reciente tecnología diseñada por los fraudistas. Un teléfono mágico integra la funcionalidad de un radio escáner, un software clonado y un teléfono móvil dentro de un microteléfono. El usuario fraudulento se conecta con el teléfono móvil en una celda congestionada entonces el radio escáner escucha a la interface aérea y el software de clonación detecta los MIN&ESN válidos de los subscriptores legítimos y luego los almacena en la memoria del teléfono. Una clave simple en el teclado del teléfono mágico rellama la primera combinación del MIN&ESN de la memoria y la usa para localizar una nueva llamada. El móvil fraudulento produce una potencia de salida en RF en la misma frecuencia en la que opera el celular del subscriptor y se sobrepone a la potencia del móvil válido. El ladrón hace "flash" con el fin de que la llamada que haga se pase a la cuenta del subscriptor.

Esta tecnología es una nueva implementación de la técnica tumbling. Originalmente lanzado por los US y ahora esta difundiéndose en Europa. La presencia de los teléfonos tumbling y mágicos no se desarrollan en las redes digitales.

### **1.3.2 FRAUDE POR PREPAGO**

El servicio prepago en redes inalámbricas esta sometido al fraude técnico. Este tipo de fraude viene en tres importantes categorías.

#### **1.3.2.1 RECARGO FRAUDULENTO**

El servicio de prepago está sometido para la explotación fraudista cuando los minutos adicionales pueden ser agregados en una manera automatizada, es decir, se usa un equipo especial que pueden escribir en la cinta magnética de una tarjeta de prepago para redes analógicas. Otras maneras para recargar el servicio de prepago incluyen el uso de información de tarjetas de crédito robadas para incrementar el balance del prepago.

#### **1.3.2.2 IMPEDIMENTO DE LA DEDUCCIÓN DEL BALANCE PARA LLAMADAS CORRIENTES.**

Algunos microteléfonos tienen un código regresivo el cual impide una llamada en

progreso para tener el inicio del balance deducido de un balance prepago. Algo más interesante pero simple es lo que ha sido recientemente descubierto, esto es cuando una persona localiza una película delgada (cinta adhesiva) en la cinta magnética de una tarjeta de prepago. La película delgada permite todavía al microteléfono leer el balance corriente de la tarjeta, pero degrada la habilidad para la operación de escritura. Cuando esto ocurre, el nuevo balance (después que la llamada corriente ha sido deducida) no puede ser escrita a la cinta magnética de la tarjeta, así pues se preserva el antiguo balance.

### **1.3.2.3 ROBO O PERDIDAS DE TARJETAS DE PREPAGO**

El robo de tarjetas de prepago representa un gasto significativo para los proveedores del servicio. Este gasto puede ser minimizado por los cuidadosos procedimientos de inventarios y la respuesta rápida por la adición de los números seriales de tarjetas de prepago robadas o perdidas a una lista negra. El sistema de prepago entonces denegaría cierta tarjeta de prepago que ha sido registrada en la lista negra.

### **1.3.3 FRAUDE POR SUBSCRIPCION**

La subscripción por fraude es la presentación incorrecta de la información para obtener un servicio fraudulento, o de otra forma, no cumplir las obligaciones de un contrato del servicio.

La subscripción por fraude es un riesgo significativo para estafar a todas las redes.

Hubo numerosos casos documentados donde la identificación de tarjetas ha sido presentada para dar el servicio, y estas identificaciones fueron mas tarde declaradas como robadas o perdidas. Algunas naciones tienen identificación de tarjetas para todos los ciudadanos residentes, aunque algunas de estas tarjetas de identificación no proporcionen una barrera contra la falsificación de la identificación y por lo tanto existe un medio primario para someter al fraude por suscripción. Las tarjetas de identificación son fáciles de fabricar con información falsa, y algunas no tienen la firma o fotografía para la identificación. Adicionalmente hay algunos locales donde un residente no está requiriendo volver a su antigua tarjeta cuando él o ella se le actualice y recibe una nueva tarjeta de identificación, entonces no debe una persona volver a la identificación antigua cuando se dio un reemplazo. Esto da como resultado muchas identificaciones incorrectas para el uso del servicio sin una dirección de tarificación válida proporcionadas al operador.

Las tarjetas de suscripción de prepago son diseñadas para ayudar al suscriptor a ahorrar en el pago de un cierto número de llamadas, esto es una propuesta atractiva en la cual el suscriptor tiene una pequeña oportunidad de evitar sus pagos. Otra forma de perpetrar la suscripción de tarjeta es recargar las tarjetas del teléfono celular sin la necesidad de comprar una nueva tarjeta de prepago. La vulnerabilidad de las operadoras para la suscripción por fraude se incrementa dramáticamente como fraude de red que llega a ser más dificultosa y caro para someterse.

El fraude por suscripción ocurre cuando un suscriptor se le asigna el servicio con

una identificación falsa o con una información al cliente fraudulentamente obtenida, de tal forma que el perpetrador no paga por el servicio.

El fraude por suscripción es perpetrado usando un número de métodos. Algunos usuarios fraudulentos actualmente pagan las primeras tarifas, luego cambian su patrón de uso, entonces dejan de pagar las nuevas tarifas y continúan usando el servicio hasta que sus llamadas privilegiadas sean bloqueadas. Algunos de los métodos más frecuentados para el fraude por suscripción son mencionados aquí.

### **1.3.3.1 INFORMACIÓN INVALIDA EN LA APLICACIÓN**

Este método de suscripción por fraude es exitoso cuando un servicio proveedor ejecuta créditos insuficientes. El fraudista ingresará la información incorrecta o inadecuada en la forma de aplicación para impedir la tarificación de su llamada. El servicio es proveído antes de la verificación en que el suscriptor pueda ser tarifado. Algunas proveedoras activarán el servicio del suscriptor inmediatamente, entonces se ejecutará la identificación y el crédito mas tarde. Durante el tiempo en que toma el proveedor descubrir la información falsificada, el suscriptor ha generado parte del uso que jamás será pagado. Para algunas operadoras, esto es todavía el tipo más común de suscripción por fraude que se ha visto. Este método continuará restando importancia a muchos operadoras que tratan de engrandecer a sus suscriptores y a los procedimientos de verificación de crédito.

### 1.3.3.2 ROBO DE LA IDENTIDAD

Este método de suscripción por fraude es usado cuando un individuo se hace pasar por otro para obtener el servicio. Esto es a menudo hecho con una identificación falsificada. Esta técnica involucra la adquisición de muchas partes de información acerca de la identidad del individuo. El conocimiento acerca de la dirección del individuo, el empleo y otras características de información (tales como números de tarjetas de crédito, seguridad social o números de identificación) pueden proveer un medio convincente de la credibilidad en el impostor.

El gran peligro con respecto a una identidad robada es que una simple identificación, la verificación de la dirección y el chequeo de crédito no revelaran la representación. La dirección se validará y el crédito será exitoso (asumiendo que la persona a la cual se identifica fue usada para fraude, tiene un buen crédito). El impostor recibe el servicio y las cuentas para ese servicio son enviadas a una persona no sospechosa. Para que la situación sea aún más efectiva, el impostor, inmediatamente después de recibir el servicio, archivará un cambio en la dirección a su cuenta de tal forma que se divierta con las facturas y otros tipos de comunicación del operador a otro lugar. Como consecuencia la víctima no sospechosa no tiene idea del servicio que ha sido tomado en su nombre hasta que su crédito sea perjudicado por las cuentas de teléfono no pagadas. El robo de la identidad no es lo único para un servicio de telecomunicaciones. Las identidades son robadas con el propósito de adquirir



préstamos, compras de tarjetas de crédito y para otros fines. Una persona sufre con esto por los daños a su tarjeta de crédito o aún estará sujeto a otras penalidades porque ciertas personas fraudulentas acaban con la cuenta del suscriptor de tal forma que el usuario legítimo no pueda pagar grandes cantidades de dinero.

### **1.3.3.3 DELINCUENCIA**

Usando este método, los individuos se suscribirán al servicio, entonces serán víctimas en sus pagos o en su efecto no pagarán todo. A menudo estos individuos, después de ser bloqueadas sus llamadas reemplazarán usando otros nombres de miembros de familias o con una variación de su información corriente.

La delincuencia se presenta en dos formas, la primera después de obtener el servicio, el individuo hará tantas llamadas como sea posible hasta que ellas sean cortadas. La segunda forma es cuando el individuo pagará un número de cuentas tal que el servicio proveedor las considere como cliente de confianza y con buen historial de pago. Este estatus es a veces acompañado por servicios adicionales tales como límites de crédito altos (donde los límites de crédito son relevantes) y la habilidad para hacer llamadas normalmente no ofrecidas para nuevos suscriptores. Después de obtener este estatus, ellos harán tantas llamadas como sean posibles antes de ser cortadas. La exposición al fraude para suscriptores para operadoras es magnífica en esta forma de delincuencia hasta que tarde o temprano se compruebe la identidad del sospechoso, ya que en la actualidad ellos han aparecido como clientes buenos.

Los métodos para combatir los tipos de fraude ya mencionados en la delincuencia usualmente ocasionan una mayor investigación personal detallada, validación de dirección, evaluación de crédito y procedimientos de administración riesgosos. Se debe mantener una lista del pasado delincuencia para varios negocios y de individuos de tal forma que ayudarán a identificar a los delincuentes de los clientes que están en servicio. Estos clientes son luego requeridos para dejar un depósito, dado el uso de limitaciones de ciertos tipos de actividades de llamadas.

Las pérdidas de inversiones son típicamente detectadas después de varios ciclos de tarificación así pues se resalta la importancia de poner a prueba un sistema capaz de detectar este tipo de fraude en tiempo real.

La suscripción por fraude es perpetrada en otras dos dimensiones a través del uso principalmente en el hogar o mercado local, y también cuando se haga roaming.

#### **1.3.3.4 SUBSCRIPCIÓN DE FRAUDE LOCAL**

La suscripción de fraude local se aplica a suscriptores locales (suscriptores registrados en una red de operador y usando su infraestructura de red local nacionalmente). Esto contrasta con el fraude por suscripción roaming, el cual se aplica ya sea a suscriptores registrados en las operadoras visitando otras redes (como se permitió cuando los acuerdos por roaming están localizados entre operadoras) o a visitantes que vienen de otras redes.

### 1.3.3.5 FRAUDE POR SUBSCRIPCIÓN ROAMING

Para hablar del roaming en el uso de los teléfonos móviles, este se produce cuando el usuario pasa entre dos celdas, o cuando se pasa de una red a otra. Sin embargo, los piratas aprovechan este tiempo que transcurre en el cambio de celdas, activando cierta información entre los dos operadoras, por ejemplo un usuario puede evadir los límites de tarificación de su teléfono celular hechos en su propia red, haciendo llamadas con un alto costo cuando está haciendo roaming, es decir, cuando pasa a otra red. Es posible que se cierre su cuenta en su país de origen, pero todavía usará su teléfono en el extranjero un cierto periodo de tiempo. La transferencia rápida de información entre las operadoras, preferiblemente por EDI, es el método más efectivo para solucionar este problema.

### 1.3.4. FRAUDE CLANDESTINO

El fraude clandestino es aquel que cuando un individuo dentro de la compañía de servicio proveedor, ayuda a otras personas ya sea obteniendo información, de servicios opcionales, o equipamiento que permitirá a una persona a obtener acceso a la red. Algunos de los siguientes aspectos son indicados en el fraude clandestino:

- Entrega de la información al cliente que paga por ella con el fin de sobornar o de quebrar al proveedor del servicio.

- Creación de subscriptores quienes no tienen tarifados teléfonos fantasmas es decir, un subscriptor ha sido activado en la red, pero el sistema de tarificación no está apto para tarifar la información de esos teléfonos.
- Abuso de pruebas o cuentas de emergencia. El fraude interno puede resultar, cuando estas cuentas no son estrechamente ajustadas y no son también tarifadas. En una ocasión una operadora permite estas pruebas o cuentas emergencia para permanecer indefinidamente, y no perder el resto de estas cuentas. Cualquiera de estas cuentas que no son tarifadas, no hay frecuentemente una manera fácil para que el operador tarife estas cuentas olvidadas aún existentes.
- La entrega de características adicionales para un subscriptor en la cual el individuo no pagó o está restringido del uso del servicio.
- Infraestructura de red no autorizada.
- Evidencia removida de la información de fraude.

Las redes digitales y analógicas son igualmente vulnerables a este tipo de fraude. Las operadoras en su mayor parte no tienen razones para creer que un problema grande de fraude clandestino pueda existir. Las auditorias son hechas paso a paso entre el sistema de tarificación y los elementos de red (los cuales presentan el acceso actual a la red).

En muchas operadoras un porcentaje del registro de llamadas recibidas (llamadas fantasmas) son rechazadas por el sistema de tarificación y así pues estas llamadas no

son tarifables. Algunas de estas llamadas no tarifadas no concorderán con un cliente conocido y puede ser que el resultado de los teléfonos fantasmas, fraudulentamente accesen a la red. Otras llamadas rechazadas pueden dar algunas inconsistencias dentro de la misma red. En conclusión, *el fraude clandestino es el más direccionado a través de un grupo de políticas y procedimientos y globalmente es sensitivo a la seguridad de datos. Esto incluye la auditoría de datos y sistemas para la actividad ilegal o abusiva.*

### **1.3.5. NEGOCIANDO O REVENDIENDO EL FRAUDE**

El fraude clandestino puede o no puede incluir la confabulación de un negociador o revendedor. En este tipo de fraude las aplicaciones son aceptadas y subsiguientemente aprobadas sin la apropiada verificación de la identidad o de la información suficiente para producir una cuenta para el cliente. Para la mayoría de los negociantes un cliente que ellos asignaron, el hecho de que no pague sus cuentas no es su problema. Es el problema del operador.

Otros ejemplos más serios para negociar fraude involucra la alteración de la documentación contractual del servicio después de que el nuevo cliente deje la oficina del negociador. Después de que el aplicante haya llenado la solicitud y se haya ido el negociador altera la aplicación de tal forma que la persona aparezca como si fuera elegible para el plan tarifario o de promoción.

Una manera popular para un negociador de incrementar sus comisiones es de activar el servicio a personas no existentes en el plan de tarificación. Estos subscriptores no atraerán la atención, hasta que ellos no hagan llamadas. Después de un periodo delincencial, estos subscriptores simplemente serán desactivados y la operadora creerá que no hubo algún perjuicio. Sin embargo el negociante tendrá su comisión. Este tipo de fraude es más que un fraude procesado, pero que puede ser combatido con políticas de seguridad y procesos eficientes; y pero también usando un computador basado en sistemas de detección de fraude que un monitor de bajo uso para la subscripción.

En conclusión el negociante de fraude puede ser enfocado para negociantes que necesiten verificar información en las solicitudes y revisiones funcionales de la calidad de los subscriptores registrados o activados por el negociador. Adicionalmente los incentivos y los no incentivos pueden llevar a cabo algún beneficio y tener más subscriptores y castigar incorrectamente un número de aplicaciones fraudulentas.

### **1.3.6. FRAUDE EN LOS EQUIPOS (MICROTELEFONOS)**

Otra forma de fraude en redes analógicas y en redes de negocios es el fraude indiscriminado en los equipos para ello hay tres maneras de llevarlo a cabo:

- Reciclar equipos robados
- Revender equipos subsidiados

- Auditoría externa para la falsificación de equipos

El fraude en los equipos será detectado como parte de la clonación y suscripción por fraude. Hay archivos con “una lista negra” de micro teléfonos robados que son también usados como entrada al sistema de detección de fraude, con el propósito de generar alarmas a cualquier micro teléfono que se encuentre en la lista negra cuando este sea encontrado en uso.

### **1.3.7. INGENIERIA SOCIAL Y AMISTAD FRAUDISTA**

La ingeniería social sucede cuando un fraudista es capaz de convencer a una persona de poder acceder a la organización de un operador para revelar información requerida al fraude, o es actualmente capaz de tener un individuo o espía para hacer funciones específicas para perpetrar el fraude. Todo esto es hecho sin que la víctima conozca que ellos están ayudando a una organización con actividades de fraude. El problema con los buenos ingenieros sociales es que ellos se dejan convencer y no pueden ser capaces de darse cuenta de lo que los perpetradores quieren. Ellos también aparentarán ser amigables y actuarán como si ellos hayan trabajado con la víctima anterior. Cuando los ingenieros sociales mencionan los nombres de los administradores ellos son asumidos como las víctimas a tener credibilidad.

La mejor protección contra la ingeniería social es educando a los ingenieros de las

operadoras de los posibles peligros de este tipo de fraude y comunicar los procedimientos estrictos para la liberación de información.

La amistad fraudista por otro lado es un nuevo concepto de algunos proveedores. Esto es cuando un suscriptor reclama por las llamadas las cuales él no ha hecho, y a la espera de que el proveedor las borre de la cuenta de tarificación. Si el proveedor es incapaz de determinar de que dichas llamadas no fueron hechas por el suscriptor entonces el proveedor a veces cambiará las cargas para promover las relaciones de buenos clientes. La amistad fraudista se incrementa con la carencia de confianza en la habilidad del proveedor para asegurar a la red y proveer tarificación adecuada.

Algunos proveedores confían en el historial de cuentas pasadas para ayudarles a tener una idea de las llamadas demandadas. Si la factura demandada es significativamente más que aquella que se tasó en los cuatro o cinco últimos meses y no hay evidencia de que este incremento sea el resultado del uso del suscriptor, entonces muchos operadoras confiarán en la honestidad del suscriptor, y modificarán la cuenta a un nivel más característico. Hay ciertamente un riesgo de que alguno de los suscriptores tomen ventaja de esto.

En el presente momento la amistad fraudista no es un factor en algún operador cuando se compare algunos otros tipos de fraude, pero representa un símbolo de debilidad en la credibilidad del proveedor.



## **1.4.- EL IMPACTO DEL FRAUDE**

El fraude negativamente impacta a una compañía telefónica en cuatro maneras:

### **1.4.1 PERDIDAS FINANCIERAS.**

Las pérdidas financieras pueden ser altamente impredecibles. De acuerdo a las estimaciones de industrias aceptadas un proveedor de red fija puede experimentar pérdidas arriba del 3% de las inversiones de red anual debido a la dependencia del fraude. Para redes móviles, esta figura puede ser más grande todavía estamos hablando del 5% de las inversiones. Donde las llamadas internacionales son involucradas, sería inevitable el caso las pérdidas del fraude de manera significativa, entonces si esto es así también se producirá una fuga sustancial de dinero para la compañía. No habría inversiones tomadas para cubrir estos costos. Esto tiene un efecto significativo e impredecible en los márgenes de operación y crucialmente llevaría la atención de los miembros de la compañía a tomar alguna solución. El impacto que lleva a todas las compañías ya sea móviles o fijas puede ser ya sea en menor o mayor grado (20% al 30%).

Los factores los cuales afectan la magnitud de la exposición financiera incluyen localización geográfica, madurez del operador o nuevos operadores que traten de ser vistos como blancos fáciles, comprensibilidad de algunas medidas y servicios de portafolio ofrecidos.

## **1.4.2 MARKETING**

La vulnerabilidad al fraude puede obligar a un carrier a ofrecer el más óptimo de los servicios que su red puede ser técnicamente capaz de soportar. Por ejemplo, muchas dudas al ofrecer los servicios de fax o voz que permiten marcación "out dialling" (mandar faxes o mensajes de correo de voz a usuarios especificados) aún se pensó que esto daría ventajas competitivas. La protección del fraude puede también ser un punto de venta positivo para clientes de negocios particularmente cuando se hace la venta contra un carrier en cuestión.

## **1.4.3 RELACIONES DE CLIENTES**

El fraude es un puente que relaciona a los clientes. El fraude a menudo impacta a las cuentas de los clientes finales y los lleva a una posible discusión. La percepción de los clientes es afectada adversivamente si el servicio es visto para ser pobremente protegido o sin reacción alguna al fraude. Increíblemente esto se mantiene como verdadero si el fraude es originado en el pensamiento de los clientes. El resultado es una pérdida ventajosa y competitiva.

## **1.4.4 PERCEPCIONES DEL ACCIONISTA**

La confianza del accionista puede ser debilitada, ya que podría la compañía ser una

victima de un fraude mayor. La persecución de los fraudistas invariablemente genera publicidad, la cual puede ser positiva o negativa dependiendo de cuan rápidamente y efectivamente ellos sean detectados. Adicionalmente el fraude afecta el funcionamiento financiero de la compañía mientras que los costos son incrementados; para lo cual ninguna inversión es tomada en cuenta tanto como se incrementa el porcentaje de una mala deuda.

Esto directamente impacta el fondo de las redes de telecomunicaciones. Para nuevos operadoras ellos hacen un tratamiento del problema aunque sea con demora pero con el fin de dar una perspectiva positiva al asunto, mientras las compañías sean más maduras, esto será un punto a favor para las redes de telecomunicaciones.

## **1.5.- HERRAMIENTAS PARA COMBATIR EL FRAUDE**

Pues para combatir el fraude tenemos algunas de las vías que los proveedores utilizan contra éste, tal es el caso de la Detección y la Prevención, ya que todavía no se conoce un método de corrección de fraude. En primer lugar tenemos que aplicar los métodos de detección como son por software, los sistemas FraudBuster y las características del PIN. Y en segundo lugar tenemos los métodos de prevención como son el RF Fingerprinting y la Autenticación.

## **1.5.1.- METODOS DE DETECCION**

### **1.5.1.1 SOFTWARE DE DETECCION POR LA MODIFICACION DE ESN.**

Este software detecta el fraude de modificación de ESN para originación y terminación de llamadas de un roamer transiente. Permite primero hacer la primera llamada, y detiene la siguiente llamada si el ESN es repetido o si se detecta algún patrón. Si el móvil modifica nuevamente su ESN, esta habilitado para continuar haciendo nuevas llamadas gratis. El proveedor del servicio puede bloquear las llamadas y/o emitir un log. Cuando un par ESN/MIN coinciden, hay dos posibles consecuencias:

- Un log es generado y la llamada es grabada
- Un log es generado y la llamada es permitida para completarse.

### **1.5.1.2 SISTEMAS DE DETECCION DE FRAUDE (FRAUDBUSTER)**

Provee a los carriers celulares con una plataforma residente en la red, la cual detecta clonaje, mala subscripción y fraude por modificación del ESN. Crea un perfil histórico

de uso para cada suscriptor, identifica un patrón de uso anormal que es una muestra indicadora de actividad fraudulenta; alerta inmediatamente al operador de red de un posible fraude. Además detecta nuevos tipos de fraude como vayan ocurriendo.

**1.5.1.2.1 PIN DE ACCESO DEL SUBSCRIPTOR.-** Provee capacidad de bloqueo de teléfonos basados en la red. El usuario digita un número predeterminado más su pin asignado y da SEND para bloquear su teléfono, y hace lo mismo para desbloquearlo. La operadora de la red podría causar que el móvil se desbloquee automáticamente bajo específicas circunstancias, como por ejemplo cuando esta haciendo roaming. Es transparente al sistema servidor cuando se soporta revisiones de IS-41 A o posteriores.

## **1.5.2.- METODOS DE PREVENCION**

Para prevenir el fraude, antes de que la llamada sea procesada es necesario conocer las siguientes propiedades:

- RF Fingerprinting
- Proceso de Autenticación
- Restablecimiento de la Verificación del Roamer (RVR)
- PIN de Acceso para el Suscriptor (SPINA)

Cada una de las propiedades mencionadas, usan un método diferente para ayudar al proveedor del servicio a prevenir el fraude celular.

### **1.5.2.1 RF FINGERPRINTING (RF HUELLA DIGITAL).-** Examina

el patrón de ondas de radio frecuencia RF emitidas por la estación móvil. Está comprobado en tecnología militar y se basa en la teoría de que cada estación móvil emite un único patrón de onda, de tal forma que monitorea un equipo instalado en cada celda. Los patrones móviles válidos deben ser captados por el sistema. Se valida los móviles comparando los patrones de onda emitidos con los archivos de patrones de onda de RF de los móviles válidos.

En RF Fingerprinting, las características únicas de la energía de radio frecuencia de un teléfono celular que transmite, son usadas para establecer la identidad de la persona que llama. Cada teléfono tiene una única huella de RF. La señal del teléfono celular es medida, la huella de la RF es calculada, y luego comparada a la huella legítima del teléfono. El tamaño de la huella RF promedio es de 2000 bits hasta que varíe de un vendedor a otro vendedor. Una huella de un microteléfono variará, basado en la temperatura, en la relación S/N, interferencia, y con ello se dará un margen de error.

Cuando un carrier implementa el RF Fingerprinting, el primer uso del teléfono es ser rastreado y almacenado para compararlo con todos los usos futuros. Se cree que un teléfono clonado puede ser inicialmente rastreado, y los consumidores descubrirán que desde el primer momento en que se produzcan la clonación ellos tratarán de usar su teléfono legítimo, y será rechazado como un clon.

Una arquitectura RF Fingerprinting consiste de dos componentes principales: una unidad de radio frecuencia (RFU) en cada sitio de celda y un sistema centro de control (SCC) en cada mercado. (ver figura). El RFU se monta en el equipo bastidor llamado rack de la celda para lo cual debe monitorear el canal de control reverso (RCC) para todas las señales de los teléfonos celulares, incluyendo originación de llamadas, registraciones, y respuestas page.

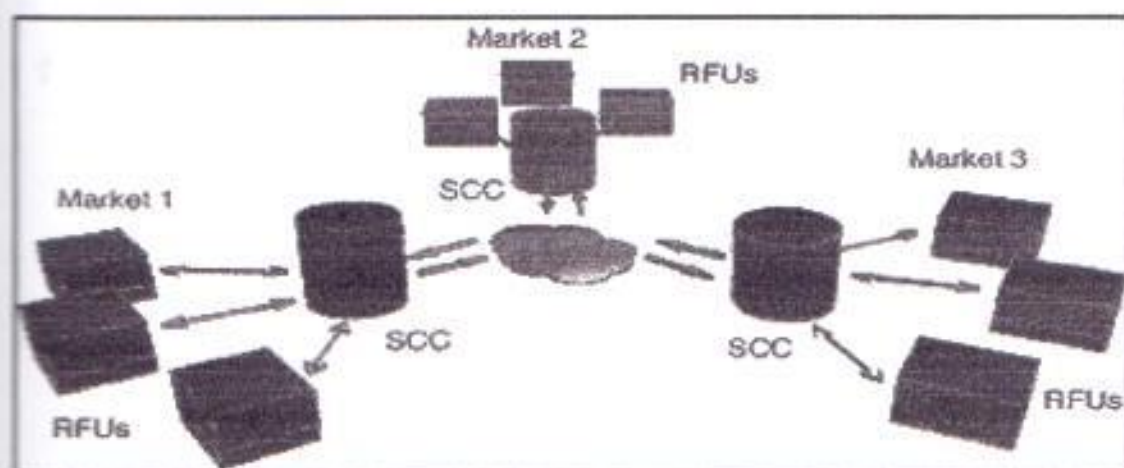
El RFU calcula la huella RF para cada teléfono y almacena cada huella para la actualización de la base de datos distribuida del sistema. Para las originaciones de llamadas, el RFU chequea la huella de la llamada contra una base de datos amplia para determinar si la llamada se origina desde un teléfono de un suscriptor o desde un clon. Esto toma menos que un segundo.

Si la llamada es fraudulenta, la unidad RF elimina la llamada. El SCC periódicamente carga nuevas huellas desde los RFUs y usa este dato para actualizar su base de datos maestra RF fingerprinting.

Puesto que el SCC comparte las huellas actualizadas de radio frecuencia con todos los sitios de celda, cada RFU tiene la última información a través del mercado. El SCC también provee el control administrativo en el sistema entero y se interconecta con el carrier para generar reportes e intercambio de datos con otras herramientas de control de fraude.

FIGURA 1.4

## ARQUITECTURA RF FINGERPRINTING

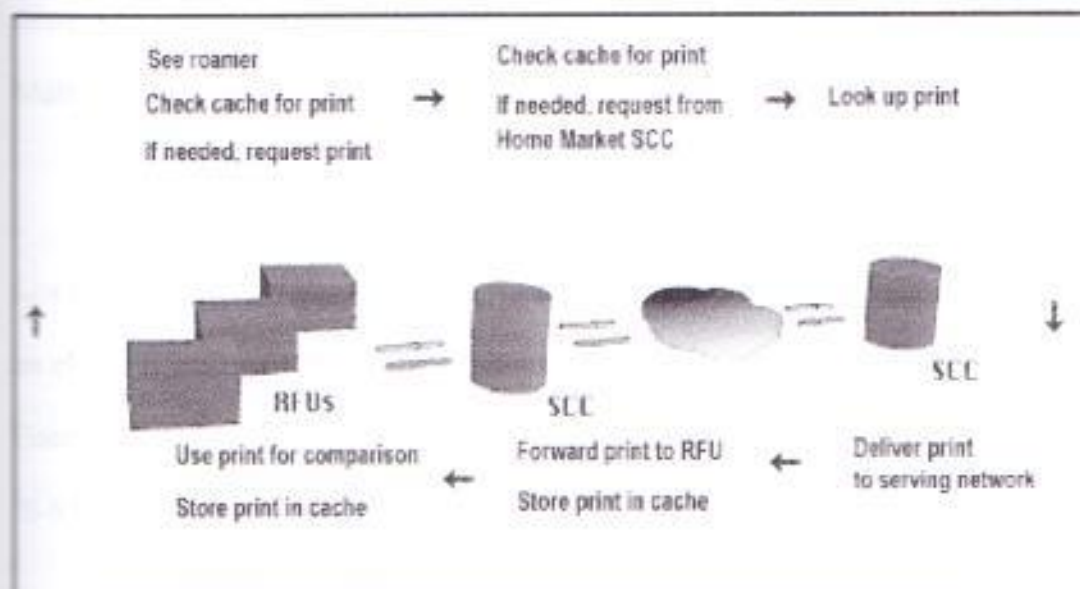


El RF Fingerprinting permite ya sea compartir las huellas entre mercados o protección roaming en permanencia aislada. Al compartir la información del RF fingerprinting, el SCC interroga a los mercados locales SCC por la huella en tiempo real. Las huellas digitales independientes del RF de la detección Roamer que hace roaming en los teléfonos, pueden también conducir al análisis del comportamiento para detectar fraude por roaming.



FIGURA 1.5

## RF FINGERPRINTING Y ROAMING



Cabe recalcar que este sistema es caro debido a que hay que colocar un equipo de monitoreo en cada celda.

**1.5.2.2 AUTENTICACION.-** Es el método más seguro y utilizado, ya que provee el procedimiento de respuesta llamado Unique Challenge, además ve a futuro la solución de combatir el fraude celular. Este sistema previene pérdidas de ingresos evitando la clonación celular, provee de la validación pre-llamada de la estación móvil. Puede ocurrir en varios accesos como: en registraci3n, durante originaci3n de la llamada, durante la terminaci3n de la llamada y en cualquier tiempo usando el procedimiento antes mencionado.

La autenticación incluye el mecanismo para generar, distribuir y manejar el SSD, y cada componente es indispensable para la implementación exitosa de la autenticación. El acceso de autenticación esta disponible por Acceso Múltiple por División de tiempo (TDMA), el Servicio Telefónico Móvil Analógico (AMPS) y Acceso Múltiple por División de Código (CDMA).

Los mensajes de autenticación usan los estándares de IS-41. El estándar está basado en el algoritmo cryptográfico de la TIA llamado Cellular Authentication and Voice Encryption (CAVE). El protocolo de autenticación IS-54 es usado por los estándares IS-91, IS-95 e IS-136.

La autenticación también provee un mecanismo al proveedor de servicio para verificar la identidad de un móvil en los siguientes sistemas de acceso: registro, originación y en flash. Los abonados validos disfrutaran los beneficios de la autenticación, la cual los protege del fraude llevando a un incremento en la satisfacción del cliente.

Usa una clave de autenticación A-Key para encriptación, se almacena tanto en el centro de autenticación como en la estación móvil. No se la puede transmitir en el aire. Provee plataformas de voz con capacidades de privacidad.

### 1.5.2.3 RESTABLECIMIENTO DE LA VERIFICACIÓN DEL ROAMER

El Restablecimiento de Verificación del Roamer (RVR) identifica un medio para rutear un roaming subscriber en un mercado de alto fraude para su Centro de Autenticación. El RVR provee una forma de validar al subscriber y reduce las pérdidas financieras causadas por un móvil clonado.

Hoy en día, el fraude ha crecido a proporciones épicas en muchos mercados inalámbricos. Un método de manejo para este fraude es por la negativa de privilegios roaming por la portadora local para estos números fraudulentos. Halando estos números, como así lo realiza este método, no solamente bloquea el roamer fraudulento, sino que también niega el acceso roamer del móvil válido para otros mercados.

El RVR provee dos componentes iniciales usados para combatir las pérdidas incrementadas incurridas por proveedores de servicio debido al fraude. Los "altos fraudes" son definidos por proveedores de servicio individual. Además para los rangos específicos, el servicio proveedor puede agrupar rangos de altos fraudes no contiguos por el asignamiento de un número de grupo fraude. Con esto, el número de grupo puede ser empleado para definir una área particular, tanto como para definir una región geográfica.

El Restablecimiento de la Verificación del Roamer (RVR) provee un mecanismo para reducir pérdidas financieras debido a las cargas incurridas por suscriptores móviles clonados quienes hacen roaming en áreas conocidas para tener altas instancias de fraude. El RVR bloquea establecimientos y opcionalmente terminaciones de llamadas para un suscriptor pirata por el posicionamiento de restricciones de llamadas en el VLR de una Originación de Denegada (DOR) y Terminación Denegada (DTM). Una vez denegado, el RVR permite al suscriptor ser restablecido para un tiempo límite (el mínimo tiempo límite es 15 minutos). Mientras no haya tiempo límite máximo responsable se pondrá este perfil, que está limitado a un tiempo bien pequeño de 15 minutos. El ruteamiento para el restablecimiento de las llamadas son puestos en la pre-traslación de emergencia y no son sujetos a procedimientos RVR. Esta característica también provee una opción HLR, Anulador RVR (ORVRP), el cual permanentemente libra al suscriptor de las restricciones de llamadas del RVR.

El proceso RVR provee para un restablecimiento suave del acceso roamer en mercados visitados para el móvil válido para un tiempo limitado. Sobre la primera originación en un mercado manipulador de fraude, el suscriptor es instruido para colgar y marcar #711 para el ruteamiento de un centro de autenticación.

Una segunda opción podría ser marcar #611 para el ruteamiento del móvil a un centro de servicio al cliente para dar instrucciones adicionales.

Otra opción para el servicio proveedor es rutear estas llamadas directamente al centro de servicio consumidor.

El RVR bloqueara todos los establecimientos de llamadas que son pretendidas previo al restablecimiento. Además para la Originación Denegada (DOR), algunas portadoras pueden seleccionar a terminaciones denegadas (DTM) al RVR roamer bloqueado. Las salidas del RVR, registra lo que el portador usa para compilar las estadísticas del RVR o detectar actividad de fraude.

#### **1.5.2.4 PIN DE ACCESO SUBSCRIPTOR**

El PIN de Acceso Subscriptor (SPINA) permite a un subscriptor controlar si su estación móvil esta permitida para acceder a la red por el uso de un Número de Identificación Personal como una identidad de subscriptor. Esta característica puede ser usada por el subscriptor y por el proveedor de servicio para prevenir el uso desautorizado de su estación móvil o uso fraudulento por un clon.

El SPINA permite a un suscriptor móvil a restringir el origen de una llamada (bloquea el teléfono) por la aplicación de un código de identificación personal de 4 a 8 dígitos de su estación móvil. La activación del SPINA no inhibirá la presentación de llamadas entrantes al subscriptor de estación móvil. Las llamadas originadas de la

estación móvil serán restringidas excepto por aquellas que son definidas como de emergencia.

El SPINA permitirá que el móvil sea bloqueado automáticamente sin la necesidad de que el usuario tenga que entrar algún tipo de código personal de su estación móvil (auto activación) cuando el se encuentre en un alto mercado de fraude. El SPINA también permitirá al usuario a desbloquear automáticamente, cuando pase de un alto mercado de fraude a un mercado mas bajo. El SPINA también es conocido como: barrido de control de código y bloqueo telefónico.

Note: Cuando las referencias están aquí como estación móvil, implica una estación física, la actual implementación es basada en la identificación de las combinaciones ESN/MIN de la estación móvil. No obstante un clon perpetrador de la estación base deberá tener un PIN para poder originar un servicio de ESN/MIN con la activación de SPINA. SPINA no provee un método absoluto para la prevención de la clonación de una estación base.

#### **1.5.2.4.1 Operaciones SPINA.**

Los subscriptores de acceso PIN permiten subscriptores MSC temporarios que desactivan todas las llamadas, las llamadas internacionales que son basadas en el

HLR también son desactivadas. Mientras las diferentes variables de SPINA funcionan como se explicara a continuación:

#### **1.5.2.4.1.1 SPINA denyall**

Cuando se activa SPINA denyall, todas las llamadas de emergencia se originan por la pre-traslación, y la desactivación del SPINA bloqueará un móvil. Con esta opción (El indicador IS-41 de origen =2 funciona como una opción DOR), y cuando SPINA denyall esta inactivo el móvil puede realizar cualquier tipo de llamada basado en sus archivos.

#### **1.5.2.4.1.2 SPINA denytoll**

Cuando se activa SPINA denytoll, todas las llamadas no utilizadas pueden ser completadas, bloqueando el móvil con la opción (indicador IS-41 de origen=3, solo para llamadas locales), y cuando SPINA denytoll se desactiva, el móvil puede realizar todo tipo de llamadas basado en sus archivos.

#### **1.5.2.4.1.3 SPINA denyintl**

Cuando se activa SPINA denyintl, todas las llamadas no internacionales, pueden ser completadas con un bloqueo al móvil con la siguiente opción (indicador IS-41 de

origen=6, para llamadas que no son internacionales), y cuando SPINA denyintl se desactiva, el móvil puede realizar cualquier tipo de llamada basada en sus archivos.

Cuando cualquiera de las opciones del SPINA se activan, no inhibirá las terminaciones móviles o llamadas deliberadas.



## CAPITULO II

### AUTENTICACIÓN CELULAR

#### 2.1 INTRODUCCION Y ELEMENTOS BASICOS DE AUTENTICACION

La autenticación es el proceso en el cual la información es intercambiada entre una estación móvil (Mobile Station) MS y un Centro de Autenticación de tal forma que se pueda confirmar la identidad de un MS y prohibir el acceso al sistema de cualquier MS ilegal. El proceso de autenticación puede ser iniciado por todo móvil que pueda ser autenticable. Una identificación exitosa de un móvil significa que el MS y el AC poseen una copia idéntica de una clave de autenticación.

En un sistema de acceso, el MS ejecuta el algoritmo de encriptación para generar un parámetro de autenticación. El parámetro resultante de la autenticación es transmitido en el enlace de radio y ciertos enlaces de red al AC. El AC entonces ejecuta el

algoritmo de encriptación en la misma forma como el MS. El AC compara su parámetro resultante de la autenticación con el parámetro de autenticación transmitido al AC. Si el resultado del parámetro generado en el MS concuerda con el parámetro generado en el AC, el sistema de acceso permite la llamada, y el MS es considerado auténtico.

La autenticación provee la autenticidad de un móvil en los siguientes accesos del sistema:

- Registración
- Originación
- Flash para conferencia tripartita o transferencia de llamada.

La autenticación provee la funcionalidad para ejecutar:

- El Unique Challenge en un móvil
- La actualización del Share Secret Data en un móvil a través de un canal de voz (VCH)
- El Unique Challenge cuando se inicia ya sea en el Centro de Autenticación o en el Centro de Conmutación Móvil.

La autenticación provee un método de validación de prellamada de las estaciones móviles que no requieren de la intervención del usuario. La autenticación puede ocurrir en la registración inicial de una llamada, en la originación de la llamada y en

cualquier momento durante la llamada usando los procedimientos del Unique Challenge. La autenticación esta basada en el share secret data (SSD) que es reconocida por el Centro de Autenticación (AC) y la Estación Móvil (MS). El share secret data esta basado en la clave de Autenticación (A-key) que es jamas transmitida en el aire.

La funcionalidad de la autenticación es soportada en celdas con sistemas TDMA y BTS (CDMA) por medio de la Unidad de Radio Transceiver (TRU) y el servicio que esta soportado para todos los canales de control y de trafico CDMA. Las celdas que reúnen estos requerimientos se denominan **celdas con capacidad de autenticación**.

Los mensajes de la red de autenticación usan los estándares IS-41C. Este estándar esta basado en el Algoritmo criptográfico de la TIA denominado Autenticación Celular y Encriptación de Voz (CAVE). El protocolo de autenticación a nivel celular usa los estándares IS-54B, IS-91, IS-95, IS-136, y ANSI J-STD-008 que es la interface aérea. Las interfaces IS-54B, IS-91, IS-136 se las puede revisar en el Apéndice A de la tesis.

También tenemos la autenticación en sistemas CDMA la cual provee las modificaciones necesarias de la tabla de control para soportar una configuración Dual-BSC (Estación Base Controladora) en un sistema MSC con CDMA antifraude.

### 2.1.1 ENTIDADES FUNCIONALES DE RED:

El proceso de autenticación incluye más que nada el uso del protocolo de autenticación. La autenticación también incluye los mecanismos para la generación, distribución y manejo del dato secreto de autenticación. Las siguientes entidades funcionales son necesarias para implementar la autenticación en un sistema MSC. El primero de ellos es cuando el centro de autenticación esta fuera de la red de autenticación (ver fig. 2.1) y el segundo cuando el centro de autenticación esta incorporado al sistema de la red de autenticación (ver fig. 2.2)

**FIGURA 2.1**  
**ARQUITECTURA DE RED DE UN AC EXTERNO**

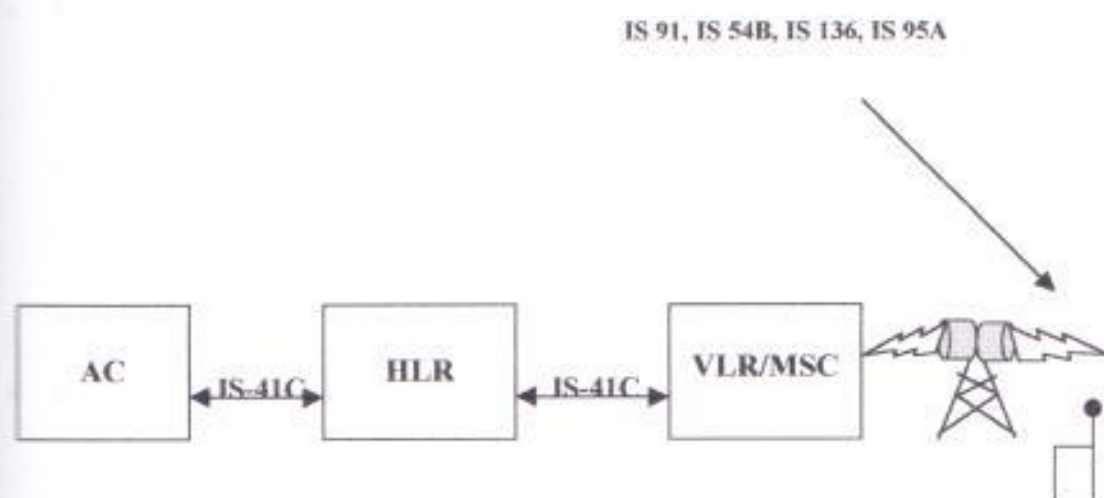
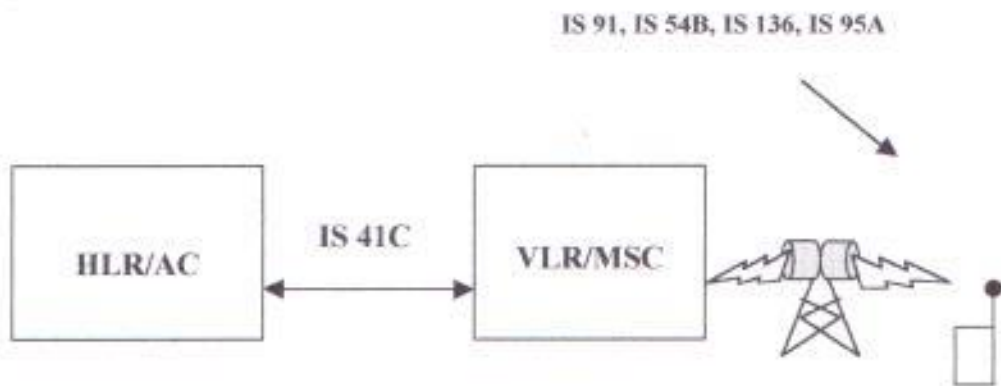


FIGURA 2.2

## ARQUITECTURA DE RED DE UN AC INTERNO



- **Centro de Autenticación (AC):** Esta identidad mantiene los datos por suscriptor y ejecuta las funciones de autenticación y privacidad. EL AC trabaja en compañía con el MSC local y esta íntimamente enlazado al HLR es decir que todas las comunicaciones internas del MSC al AC se las hace via HLR.
- **Registro de Localización Local (HLR):** Esta unidad soporta todas las comunicaciones entre el AC y otras entidades de red. El HLR contiene toda la información del perfil del celular asociado con un suscriptor, y puede o no puede ser integrado al AC.
- **Registro de Localización Visitante (VLR):** Esta unidad almacena la información del suscriptor que esta haciendo roaming, la cual es obtenida del sistema local del suscriptor para su registro. El VLR, puede tomar muchas de

las responsabilidades del AC con el propósito de reducir el tráfico de mensajes de comunicación con el AC en un acceso móvil. Esto es posible gracias al concepto de SSD compartido. Cuando el VLR contiene el SSD, este puede realizar la validación de autenticación de un móvil. Para realizar estas funciones de autenticación el VLR debe tener el SSD del móvil y tener la habilidad de correr el algoritmo CAVE.

- **Centro de Conmutación Móvil (MSC):** Esta unidad es el cerebro del sistema celular ya que enruta las llamadas celulares a su destino. Entre sus funciones está la de manejar el establecimiento de las llamadas, procesamiento de las llamadas, registración de las llamadas, parámetros y medidas asociadas con la autenticación y comunicaciones con la estación base. El MSC-S tiene muchas responsabilidades en proveer un sistema capaz de autenticar. Este determina si un móvil debe generar parámetros de autenticación anteriormente al acceso al sistema mientras también provee alguno de los parámetros de entrada que el móvil necesita con el propósito de autenticarse.
- **Estación Base (BS):** Es la que soporta el protocolo de interface entre el MSC y la estación móvil.
- **Estación Móvil (MS):** Esta unidad terminal soporta dos formas de autenticación: el Global y el Unique Challenge. Los estándares corrientes de la TIA que va

soportar la estación móvil son el IS-91(analógico), IS-54B (TDMA/ACCH) IS-136(TDMA/DCCH), Y el IS-95A(CDMA).

- **Red de Señalización IS-41:** soporta el protocolo de autenticación para IS 41C.

## 2.2 CENTRO DE AUTENTICACION

El objetivo primario de esta entidad funcional es permitir que la red se proteja a si misma de los móviles no autorizados, asegurándose de que sólo los móviles válidos tengan acceso a los servicios de red. Estas propiedades se las implementan en el Centro de Autenticación.

El Centro de Autenticación es la entidad de red del estándar IS-41 que confirma la identidad del móvil. El AC es la entidad lógica en una red celular necesaria para la autenticación.

Entre las responsabilidades del AC tenemos las siguientes:

- Mantener una base de datos de la información de autenticación de los móviles.
- Dar acceso a móviles autenticables. El AC recibe los mensajes AUTHREQ en varios sistemas de acceso y verifica la autenticidad del móvil haciendo uso del algoritmo CAVE.

- Manejar las fallas en la autenticación. Si el AC detecta fallas mientras se procesa el AUTHREQ o es notificado de algún problema por medio del mensaje AFREPORT este tiene que reaccionar de acuerdo a como se lo haya configurado para manejar un tipo específico de fallas.
- Actualizar el SSD de los móviles. El AC puede iniciar una actualización de SSD inmediata hacia el móvil, haciendo uso del mensaje AUTHDIR o esperando por el siguiente acceso al sistema y ahí actualizar el SSD.
- Procesar los mensajes IS-41 de BSCHALL. El AC calcula el mensaje de respuesta apropiado para este mensaje cuando es interrogado por la estación base.
- Procesa los mensajes IS-41 de ASREPORT. Cada vez que el AC requiere que el MSC/VLR realice alguna transacción de autenticación, por ejemplo una actualización de SSD, el sistema servidor envía un ASREPORT al AC para informarle de los resultados.

### 2.3 PROCESO DE AUTENTICACION

El proceso de autenticación esta basado en el algoritmo criptográfico CAVE (Cellular Authentication and Voice Encryption). Solamente la estación móvil y el AC conocen el A-Key. El hecho de que el proceso sea transparente al usuario es una característica clave de autenticación. El SSD, cuyo valor es derivado del A-key, y el valor proporcionado del AC, es usado para procesar los valores de autenticación que son transmitidos en el aire. Esto proporciona una capa de protección contra la



interceptación del A-Key durante el proceso de distribución de la clave. El SSD, el cual también necesita solamente ser conocido por el MS y el AC, y el A-key son los datos cruciales en los cuales la autenticación depende.

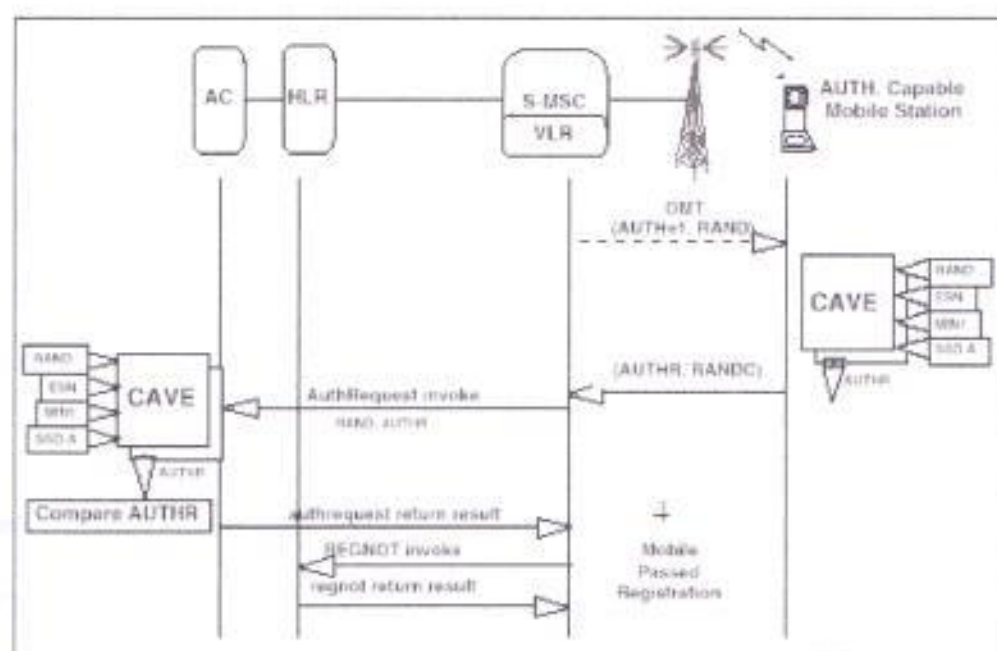
Hay cinco diferentes intercambios de autenticación; Registración, Originación, Terminación, Unique Challenge y la actualización del SSD. La estación móvil inicia los intercambios de la registración, originación y terminación. El AC inicia la actualización del SSD y la respuesta única (Unique Challenge).

Los valores de autenticación procesados en los intercambios de autenticación no son procesados directamente desde el A-key, pero más bien desde el SSD. El SSD por si mismo es procesado desde el A-key, ESN y un valor aleatorio escogido por el AC. La estación móvil procesa el SSD solamente en la recepción de la actualización del SSD desde el AC y verificando el orden con el AC.

Para los intercambios iniciados en la estación móvil, el MS basa sus procesamientos en un AC transmitido el número aleatorio (RAND) y transmite el número aleatorio y el valor de autenticación. El AC ejecuta el mismo procesamiento con el número aleatorio y compara el resultado al valor de autenticación transmitido. Si ellos son iguales, la estación móvil es verificada. En los intercambios iniciados en el AC, el AC selecciona un número aleatorio y procesa un valor esperado de autenticación. Este se envía al MS el número aleatorio solamente y el MS responde con su propio valor

de autenticación procesado. Si los valores de autenticación de los MSs concuerdan con los valores de autenticación del AC esperados, el MS es verificado.

**FIGURA 2.3**  
**ARQUITECTURA DEL SISTEMA DE AUTENTICACIÓN**



Veamos algunos términos que actúan en la autenticación celular:

- **Clave de Autenticación (A-key):** Esta clave confidencial tiene 20 dígitos la cual es conocida y almacenada solamente por el móvil y el AC autorizado. El A-key es almacenado en la memoria de seguridad e identificación permanente del móvil. El A-key es la esencia de la autenticación y de la Encriptación de voz. Por razones de seguridad esta clave no es transmitida en el radio enlace y tampoco es

mostrada en la pantalla del móvil. Para tener aun más seguridad en la clave de autenticación una forma encriptada de la clave conocida como SSD (Share Secret Data) es generada usando el algoritmo CAVE. El valor de esta clave puede ser cambiada solamente por solicitud del AC y provee una variable de entrada al algoritmo CAVE. El proceso de actualización o generación del SSD es en el mismo momento en que la clave A-key es usada como entrada al algoritmo CAVE.

- **CAVE :** El Algoritmo Cellular Authentication and Voice Encryption (CAVE) es el corazón de la autenticación y encriptación. Este es usado para calcular el parámetro de autenticación en el móvil y en el centro de autenticación. Para mayor información acerca de este algoritmo, ver el apéndice B
- **Share Secret Data (SSD) :** Es un patrón de 128 bits almacenados en la memoria semipermanente del móvil. El SSD es generado del A-key por la ejecución del algoritmo CAVE tanto en el móvil como en el Centro de Autenticación. Al igual que el A-key esta información no es transmitida por el radio enlace. El SSD es dividido en dos grupos de 64 bits: el SSDA utilizado para procedimientos de autenticación y el SSDB usado como una criptovariante para la Encriptación de Mensaje de Señalización y Privacidad de Voz

La generación del SSD ayuda los procesos de autenticación y de encriptación en dos aspectos. Primero da prioridad a la seguridad del proceso de autenticación, es decir el

SSD oculta al A-key de la exposición directa y provee de una variable de entrada al algoritmo CAVE, complicando el posible manipuleo reversible de la clave de autenticación para la encriptación de datos. Segundo, existe el concepto de la formación del SSD con el VLR. Esto significa que el SSD permite al VLR almacenar el valor corriente del SSD y generar los parámetros de autenticación desde este SSD formado, principalmente el SSD formado optimiza la mensajería que pueda suceder entre el sistema servidor y el Centro de Autenticación para los procesos de autenticación y encriptación. Cuando el SSD esta compartido, el centro de autenticación es requerido solamente para iniciar las actualizaciones de los SSD y reacciona contra posibles fallas de autenticación.

Todos los otros procesos de autenticación y de encriptación pueden ser ejecutados por la unidad de switch MSC/VLR usando el valor SSD compartido.

- **RAND:** Random Challenge memory, RAND (reside en el móvil) es un valor de 32 bits pasado al móvil en el canal de control y que sirve para generar la respuesta de autenticación (AUTHR) para el procedimiento Global Challenge y que puede tomar mas de 4 millones de posibles valores. El móvil lee el valor RAND en el canal de control y usa este valor con el SSD y otros parámetros como entrada para el algoritmo CAVE para la generación del AUTHR. Con esta variable se retransmite el mensaje de parámetros de acceso en el FBCCH (Fast Broadcast Control Channel) Canal de Control de retransmisión Rápida y en el DCCH (Canal

de Control Digital). Además se puede hacer la retransmisión del Tren de Mensajes (OMT) en el ACCH. El RANDC es el más significativo de los 8 bits del RAND. Este mismo valor RAND es conocido por el MSC, y es usado como entrada para ejecutar el algoritmo CAVE en el AC para la generación de los resultados de autenticación. El RAND en el MSC es enviado al AC en los mensajes de red.

Con el propósito de asegurar que el AC y el móvil están usando el mismo RAND para calcular el parámetro de autenticación resultante, el móvil envía un parámetro de Random Challenge Confirmation (RANDC) en el mensaje de acceso al sistema. El RANDC son los 8 bits más significantes del valor de RAND que el móvil leyó en la información del canal de control. Cuando el switch recibe un mensaje de acceso al sistema, este debe determinar a partir del RANDC cual es el valor de RAND que el móvil usa para calcular el resultado de autenticación. Entonces el switch envía el mismo RAND al AC para el cálculo del AUTHR. Si el switch no puede encontrar el RANDC, este considera una falla en el proceso de autenticación.

- **RANDBS** : Es un valor aleatorio de 32 bits usado en vez del valor RAND generado por la Estación Móvil. Específicamente para estaciones base Challenge.
- **RANDU** : Es un valor aleatorio de 24 bits usado en vez del RAND generado ya sea por el Centro de Autenticación o por el MSC siempre y cuando el SSD este formado. Específicamente par un procedimiento Unique Challenge.

- **RANDSSD:** Es un valor aleatorio de 56 bits usado en vez del RAND generado por el Centro de Autenticación. Específicamente se lo usa para la actualización del SSD.
- **Proceso de Actualización del RAND:** Este proceso consiste en que periódicamente, el MSC genera un nuevo RAND y actualiza los canales de control del sistema antifraude.
- **AUTH:** El mensaje AUTH determina si el móvil está intentando acceder a un sistema de autenticación en un sistema de acceso. El elemento de información AUTH en el Canal de Control para una interfase aérea específica, puede proveer una indicación de la habilidad del sistema para soportar la autenticación. Cuando el campo pertinente en el Canal de Control OMT (Tren de Mensajes de Delantero) indica que los parámetros de autenticación son requeridos, el móvil para autenticarse, necesita generar un resultado de autenticación (AUTHR) previo a cualquier acceso del sistema. Cuando la información en el canal de control indica que los parámetros de autenticación no son requeridos, entonces el móvil no necesita generar el AUTHR y el móvil es todavía capaz de acceder al sistema.
- **AUTHR:** Es una salida única de 18 bits del Algoritmo CAVE para registrar y originar llamadas.

- **AUTHU:** Es una salida única del algoritmo CAVE para el procedimiento Unique Challenge.
  
- **AUTHBS:** Es una salida única de 18 bits del Algoritmo CAVE para la Estación Base Challenge.
  
- **Procedimientos de Autenticación Challenge:** Hay dos formas de Autenticación que vamos a usar en nuestro sistema antifraude, los cuales están supeditados a los protocolos: IS-91 (analógico), IS-54B (TDMA/ACCH), IS-136 (TDMA/DCCH), IS-95 (CDMA). Estos protocolos son los puentes de comunicaciones entre el sistema antifraude y las estaciones móviles, estos a su vez están soportados con los procesos de autenticación denominados: Autenticación Global Challenge y Autenticación Unica Challenge.
  
- ⇒ **Global Challenge:** Cuando la autenticación "Global Challenge" esta activa, un número aleatorio (RAND) y el AUTHU=1 es transmitido, los móviles capaces de autenticarse son esperados para transmitir en el canal de control delantero. Las estaciones móviles capaces de la autenticación son entonces esperados para incluir una respuesta de autenticación, llamada AUTHR, con todo intento de acceso (originación y registración). El cálculo del AUTHR es hecho por el Algoritmo CAVE. Si el SSD es formado entonces el Centro de Autenticación o el

VLR también procesan el AUTHR y se lo compara al valor proveído por el MS.

Si los valores son iguales, la autenticación es exitosa.

⇒ **Unique Challenge:** El Unique Challenge es otro tipo de autenticación. Si el SSD es formado, el Centro de Autenticación o el VLR generan una variable aleatoria Challenge, denominada RANDU, y la estación móvil es explícitamente "desafiado" para autenticarse así mismo. La estación móvil calcula su respuesta, denominada AUTHU y lo retorna al Centro de Autenticación o al VLR donde es comparado con la respuesta esperada. El cálculo del AUTHU es hecho por el algoritmo CAVE usando el RANDU. El Unique Challenge puede llevarse a cabo en los canales de control o de voz/tráfico, cuando el móvil ejecuta Flash o falla debido al error del RANDC.

- La operación es iniciada por un Centro de Autenticación. Esta operación es iniciada por el servidor MSC/VLR.
- *Estación Base de Desafío (BASE STATION CHALLENGE)* - La operación del BSCHALL es usada para solicitar una respuesta a una orden BSCHALL recibida de un móvil. Esta operación es iniciada por el Servidor MSC/VLR.

• **Mensajes de Autenticación relacionados con el IS-41 Rev. C.**

Las capacidades del intersistema de autenticación están basadas en las operaciones de autenticación y procedimientos expuestos en el protocolo IS-41C. La siguiente lista



de mensajes identifica las operaciones de autenticación que soportará nuestro sistema MSC.

- *Autenticación Directiva (AUTHDIR)*
- *Autenticación de Reporte de falla (AFREPORT)*
- *Solicitud de Autenticación (AUTHREQ)*
- *Reporte del Status de Autenticación (ASREPORT).*

El sistema MSC que se implemente en nuestra tesis no provee soporte para las siguientes operaciones de autenticación:

- *Autenticación Directiva Delantera*
- *Solicitud de conteo*
- *Solicitud de variable aleatoria.*

Estas operaciones no se realizan en IS-41C ya que no son operaciones del intersistema de autenticación. Estas se las usan en los Centros de Autenticación y de los VLRs con protocolo TSB-51.

• **Mensajes de Autenticación relacionados con la interface aérea:**

La siguiente información nos permite ver los mensajes de autenticación que soporta el sistema antifraude en la interface aérea:

- *Orden de Desafío Unico*
- *Orden de Desafío de la Estación Base*
- *Orden de Actualización del SSD.*

A continuación se describirá el proceso de autenticación de un móvil en los siguientes accesos del sistema: registraci3n, originaci3n y flash. La autenticaci3n en todos los accesos del sistema, en celdas con capacidad de autenticaci3n, previene el cl3neo de m3viles celulares del acceso del sistema, as3 pues se produce la eliminaci3n del fraude celular causado por personas dedicadas a la clonaci3n de los m3viles.

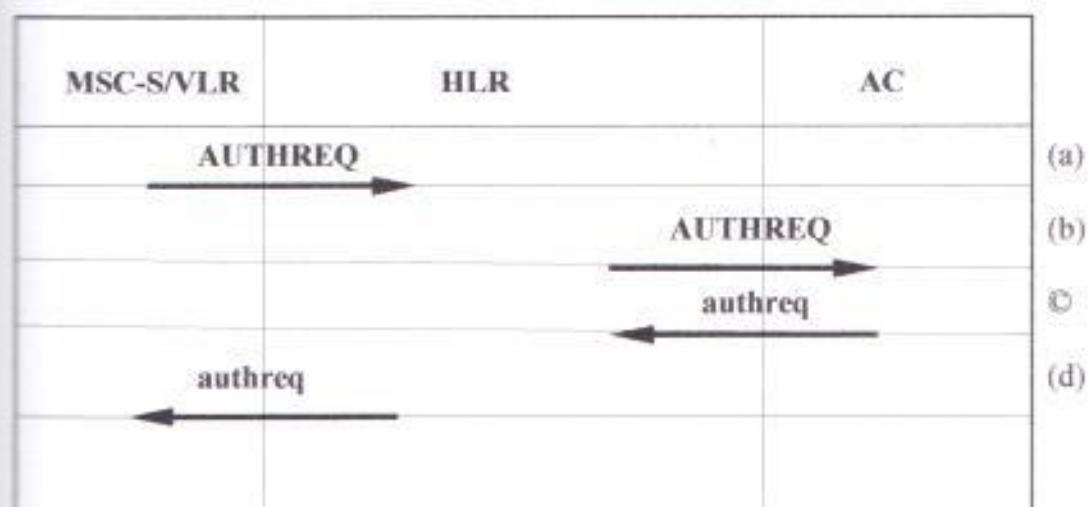
Dentro de cada acceso hay informaci3n en la cual se detalla condiciones de error y respuestas espec3ficas para un escenario de autenticaci3n.

### **2.3.1 AUTENTICACI3N EN EL ACCESO**

Cuando un m3vil accesa a una red celular donde es requerido para ejecutar la autenticaci3n, la autenticaci3n puede ya sea ser ejecutada en el AC o en el MSC/VLR si el SSD es compartido. Como un ejemplo de esto, el siguiente flujo de se1ales muestra el proceso de autenticaci3n para un m3vil registr3ndose en un nuevo sistema.

FIGURA 2.4

## REGISTRACION EN EL ACCESO INICIAL DEL SISTEMA



- a. El móvil se registra por primera vez en un nuevo sistema. El sistema servidor necesita ejecutar la autenticación pero no tiene el valor del SSD para el móvil, así que envía un Authentication Request al HLR del móvil.
- b. El HLR envía el Authentication Request al AC.
- c. Usando el SSD y otro dato de autenticación para el mensaje y el perfil del móvil en el AC, el CAVE está procesando para generar el AUTHR. Si el AUTHR procesado por el AC concuerda con el AUTHR en el Authentication Request entonces el móvil es auténtico. Si ellos no concuerdan entonces el móvil es potencialmente un intruso. Para una respuesta:

- Si el AC quiere denegar el servicio entonces enviara un Authentication Response conteniendo el parámetro de acceso denegado.
- Si el AC quiere permitir el servicio entonces enviará de regreso un Authentication Response vacío.
- Si el AC quiere compartir el SSD, entonces el AC incluirá el SSD en el Authentication Response.

4 El HLR envía el Authentication Response al MSC/VLR.

Cuando el SSD es compartido, el AC está requiriendo el acceso inicial para un móvil ya que el sistema servidor no tiene el SSD de ese móvil.

El proceso radica en:

- El AC recibe un AUTHREQ para el acceso del sistema.
- EL AC ejecuta la autenticación inicial.
- El AC retorna el SSD para los móviles auténticos.

Subsiguiente a compartir el SSD, el próximo acceso del AC para ese móvil será solamente cuando la autenticación falle en el sistema servidor (notificado mediante

un AFREPORT) o cuando el SSD haya sido removido por el sistema servidor (notificado por mediante un AUTHREQ).

En el caso donde el SSD no sea compartido, el AC es requerido para ejecutar la autenticación en cada sistema de acceso autenticable, por ejemplo un AUTHREQ es recibido en cada sistema de acceso autenticado.

El procesamiento para la recepción de un AUTHREQ es:

- Verificar el MIN/ESN en el AUTHREQ contra el MIN/ESN en la base de datos del AC.
- Recoger la información necesaria del mensaje basado en el sistema de acceso.
- Ejecutar la operación específica del CAVE para esa solicitud. Para la registración, originación y terminación, el CAVE es llevado a cabo para una comparación. Para hacer flash y alguna operación no especificada, el CAVE procede a generar el AUTHU.
- Reportar al sistema servidor que otra operación hay que hacer si fuera necesario.

### 2.3.2 AUTENTICACIÓN EN LA REGISTRACIÓN DE LA LLAMADA

Esta actividad de autenticación provee la seguridad para la registración inicial del móvil en el MSC de servicio. Una vez que el móvil se ha registrado satisfactoriamente en un sistema antifraude, todos sus intentos subsiguientes de registro de llamadas no son autenticados. La autenticación en el registro inicial es importante ya que evita la localización actual del móvil en el HLR, debido a que existen intentos de registración de llamadas celulares fraudulentas. De esa forma el HLR contendrá la localización de los móviles validados y autenticables. Esto mejora la probabilidad de cobertura del sistema antifraude para con los móviles cuando la finalización de la llamada es llevada a cabo.

Cuando un móvil quiere enviar una solicitud de registro a un sistema antifraude y la información del canal de control indica que AUTH=1, entonces el móvil reconoce que debe generar un valor AUTHR. Los valores del AUTHR y el RANDC junto con otros parámetros de registración son enviados al MSC en el mensaje de registración. Al recibir en el MSC el valor del RANDC, esta entidad compara dicho valor con el RANDC local. Si los RANDCs son iguales entonces el MSC envía la Solicitud de Autenticación al AC/HLR para ejecutar la autenticación. De otra forma el MSC solicita al Centro de Autenticación el inicio del procedimiento del Unique Challenge para el móvil. En la verificación de los parámetros de autenticación o del

procedimiento satisfactoriamente completo del Unique Challenge, el Centro de Autenticación informa al MSC para permitir el acceso. Entonces el MSC envía la solicitud de registraci3n del m3vil al HLR.

En la figura 2.5 y 2.6 se observan la autenticaci3n en la registraci3n de una llamada.

**FIGURA 2.5**

**AUTENTICACION EN LA REGISTRACION DEL AC**

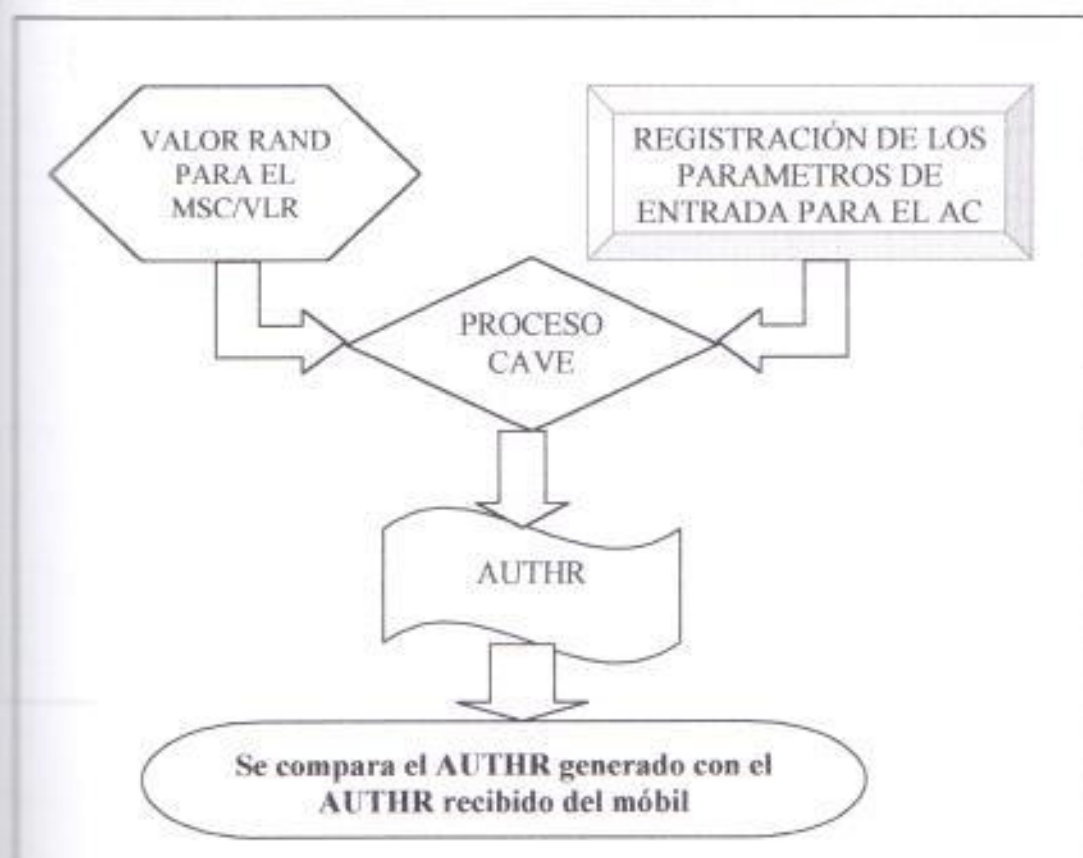
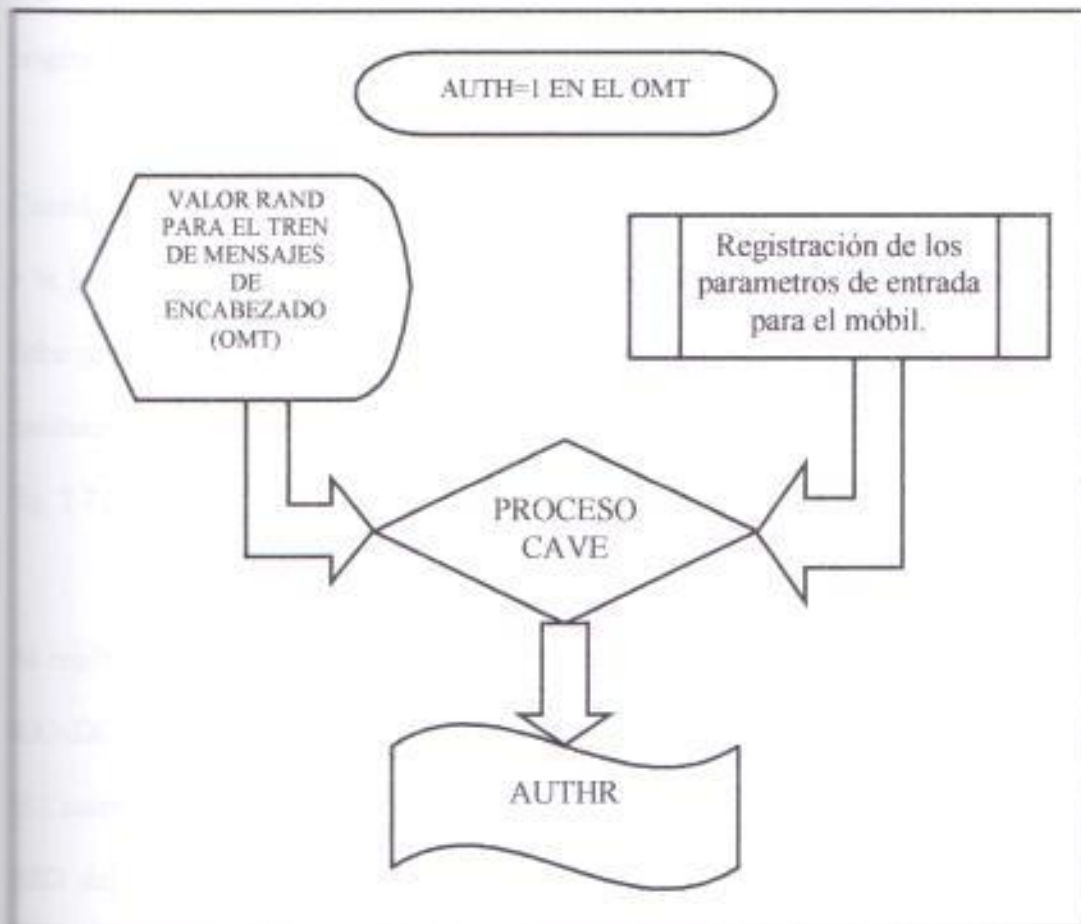


FIGURA 2.6

## AUTENTICACION EN LA REGISTRACION DEL MÓVIL





### 2.3.3 AUTENTICACIÓN EN LA ORIGINACIÓN DE UNA LLAMADA.

Esta habilidad de autenticación, soporta la autenticidad de un móvil durante una originación de una llamada. La autenticación en la originación es importante para la seguridad del sistema dado que una mayoría de llamadas fraudulentas empiecen con originaciones móviles.

Cuando un móvil accesa un sistema a través de un intento de originación de llamadas, y la información del canal de control indica que AUTH=1, El móvil reconoce que debe generar el valor AUTHR. Los valores del AUTHR y el RANDC junto con otros parámetros de originación son enviados al MSC en el mensaje de originación. (Ver fig. 2.7)

Al recibir en el MSC el valor del RANDC, esta entidad compara dicho valor con el RANDC local. Si los RANDCs son iguales entonces la acción del MSC depende de si el Centro de Autenticación ya ha formado el SSD del móvil con el MSC/VLR. Si el SSD del móvil está disponible en el MSC/VLR, entonces se procede a correr el algoritmo CAVE localmente y se compara sus resultados a los que se recibió del móvil.(Ver fig. 2.8) De otra forma el MSC envía una Solicitud de Autenticación al ACHLR para ejecutar la autenticación. Si la autenticación no es satisfactoria, el MSC no establece la llamada.

FIGURA 2.7

## AUTENTICACIÓN EN LA ORIGINACION DEL MÓVIL

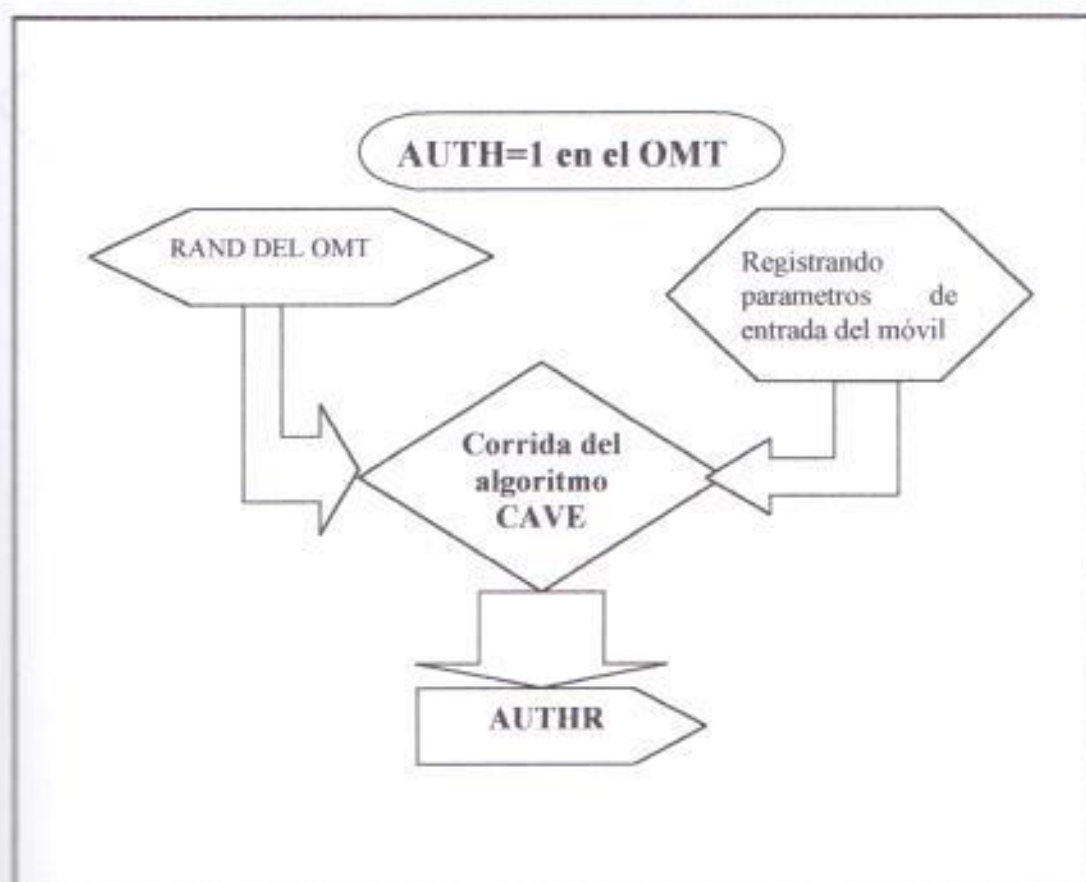
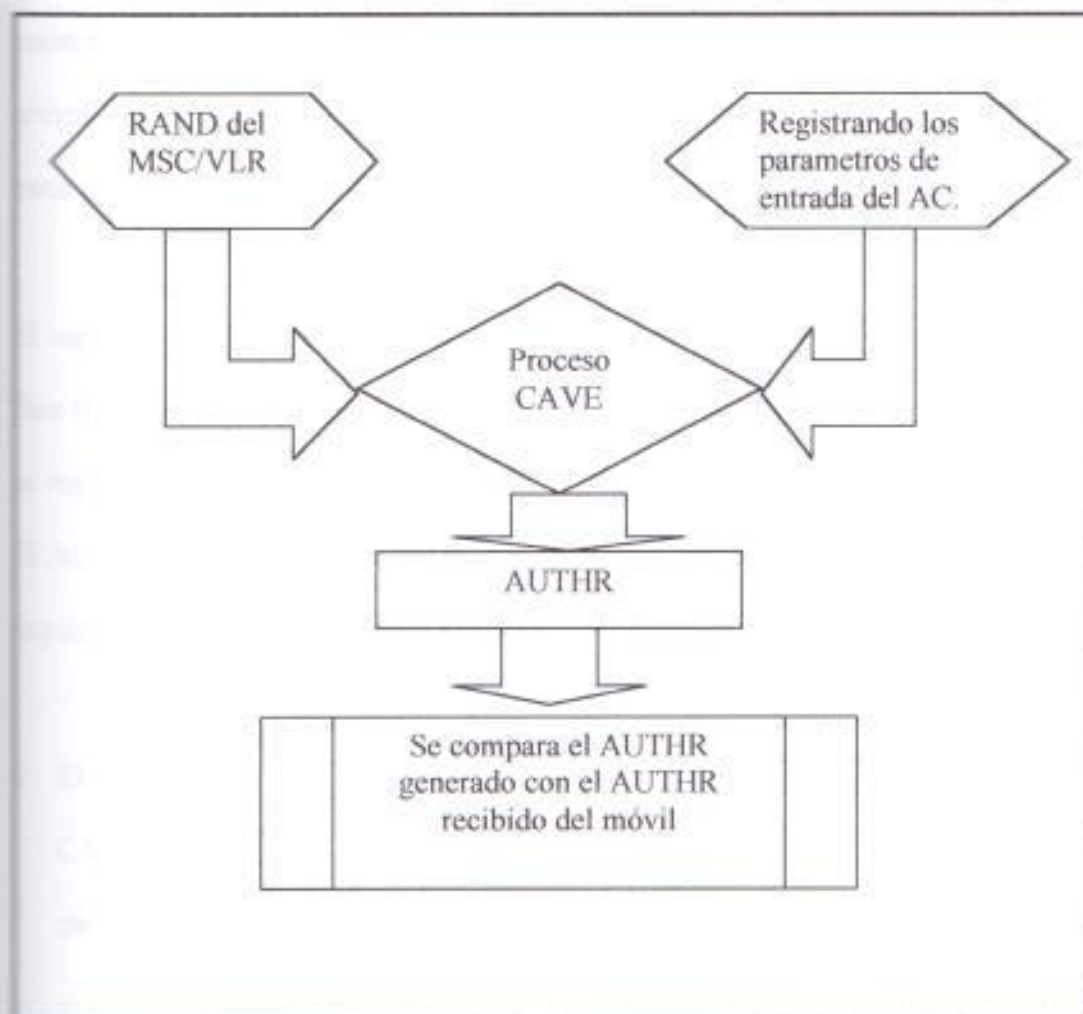


FIGURA 2.8

## AUTENTICACIÓN EN LA ORIGINACION DEL AC



## 2.3.4 ESCENARIOS DE AUTENTICACIÓN

### 2.3.4.1 AUTENTICACIÓN EN REGISTRO

La autenticación en un acceso inicial al sistema es también conocida como la autenticación en el primer registro. La autenticación en el primer registro es vital para mantener la correcta información de localización para un móvil en el HLR para prevenir el envío de mensajes REGNOT (Registration Notification) de IS-41 por parte de móviles fraudulentos.

El siguiente flujo de mensajes (ver fig.2.7), se refiere a “un registro inicial exitoso”. Esta figura muestra el proceso seguido para una autenticación exitosa de un móvil en su registro inicial.

El AUTH=1 y el RAND son transmitidos sobre el canal de control indicando que se requiere autenticación para todo el acceso al sistema.

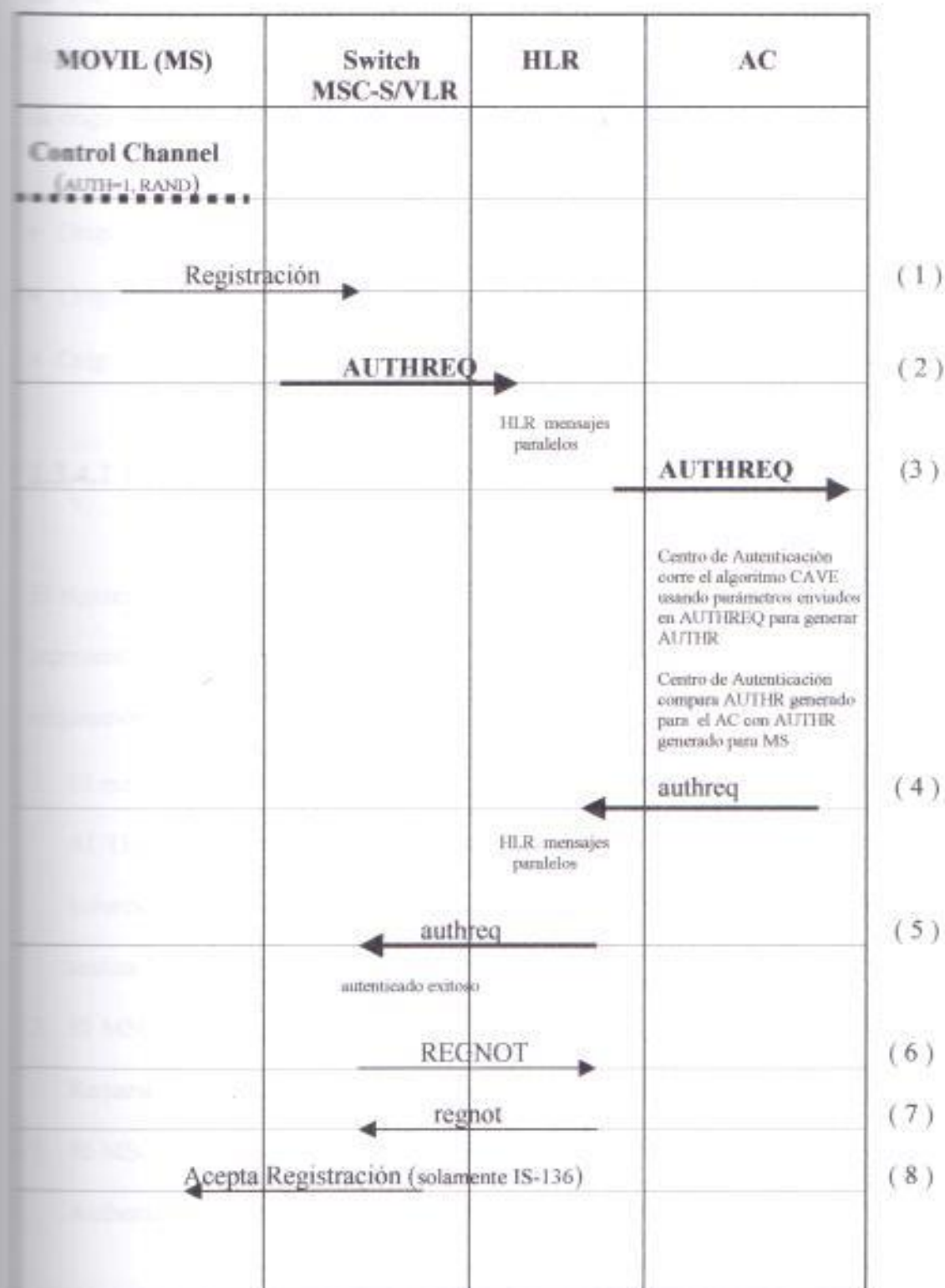
1. El móvil lee el valor del RAND desde el canal de control y ejecuta el algoritmo CAVE para generar el AUTHR. El AUTHR y el RANDC son enviados en el mensaje de registro hacia el switch
2. Cuando el switch recibe el mensaje de registro, este determina a partir del valor del RANDC, que valor de RAND usó el móvil para calcular el AUTHR. El switch compara el valor del RANDC y el del RAND almacenado en el switch. La

comparación pasa, y el switch envía un mensaje de requerimiento de autenticación conteniendo los valores de AUTHR y RAND a los móviles HLR.

3. El HLR reenvía el mensaje de requerimiento de autenticación a el Centro de autenticación (AC).
4. El AC ejecuta el algoritmo CAVE para generar el AUTHR. Este compara su AUTHR con el AUTHR generado por el móvil. El resultado de la comparación es enviado de vuelta al HLR en un mensaje de respuesta al authentication request.
5. El HLR reenvía el mensaje de authentication request response de regreso al MSC.
6. Cuando el switch recibe el mensaje de respuesta del authentication request, este determina si la autenticación fue exitosa y envía un mensaje de notificación de registro hacia el HLR del móvil.
7. El HLR confirma el mensaje de registro con un mensaje de respuesta al restration notification.
8. Si la interface de aire es IS-136 DCCH, el switch un mensaje de aceptación de registro al móvil.

FIGURA 2.9

## REGISTRACION INICIAL EXITOSA



### 2.3.4.2 AUTENTICACIÓN SOBRE ORIGINACIÓN

La autenticación sobre originación es importante desde que la mayoría de las llamadas fraudulentas son de móviles originando llamadas. Los siguientes escenarios de originación son discutidos mas adelante:

- Originación sin entrada VLR
- Originación con entrada VLR, pero con SSD no compartido
- Originación con entrada VLR, y con SSD compartido.

#### 2.3.4.2.1 ORIGINACION SIN ENTRADA VLR

El siguiente flujo de mensajes "Originación exitosa sin entrada VLR" (Ver fig.2.8), representa el proceso seguido por una autenticación exitosa de un móvil en una originación.

1. El móvil lee el valor de RAND sobre el canal de control y lo usa para calcular el AUTHR. El mensaje de originación es generado por el móvil conteniendo los valores de AUTHR y RANDC. El MSC recibe el mensaje de originación y realiza la validación del AUTHR y el RANDC.
2. El MSC pide el perfil del móvil mediante el envío del mensaje de Qualification Request hacia el HLR del móvil.
3. El MSC pide la información de autenticación del móvil enviando un mensaje de Authentication Request a el HLR del móvil. El MSC traduce los dígitos y

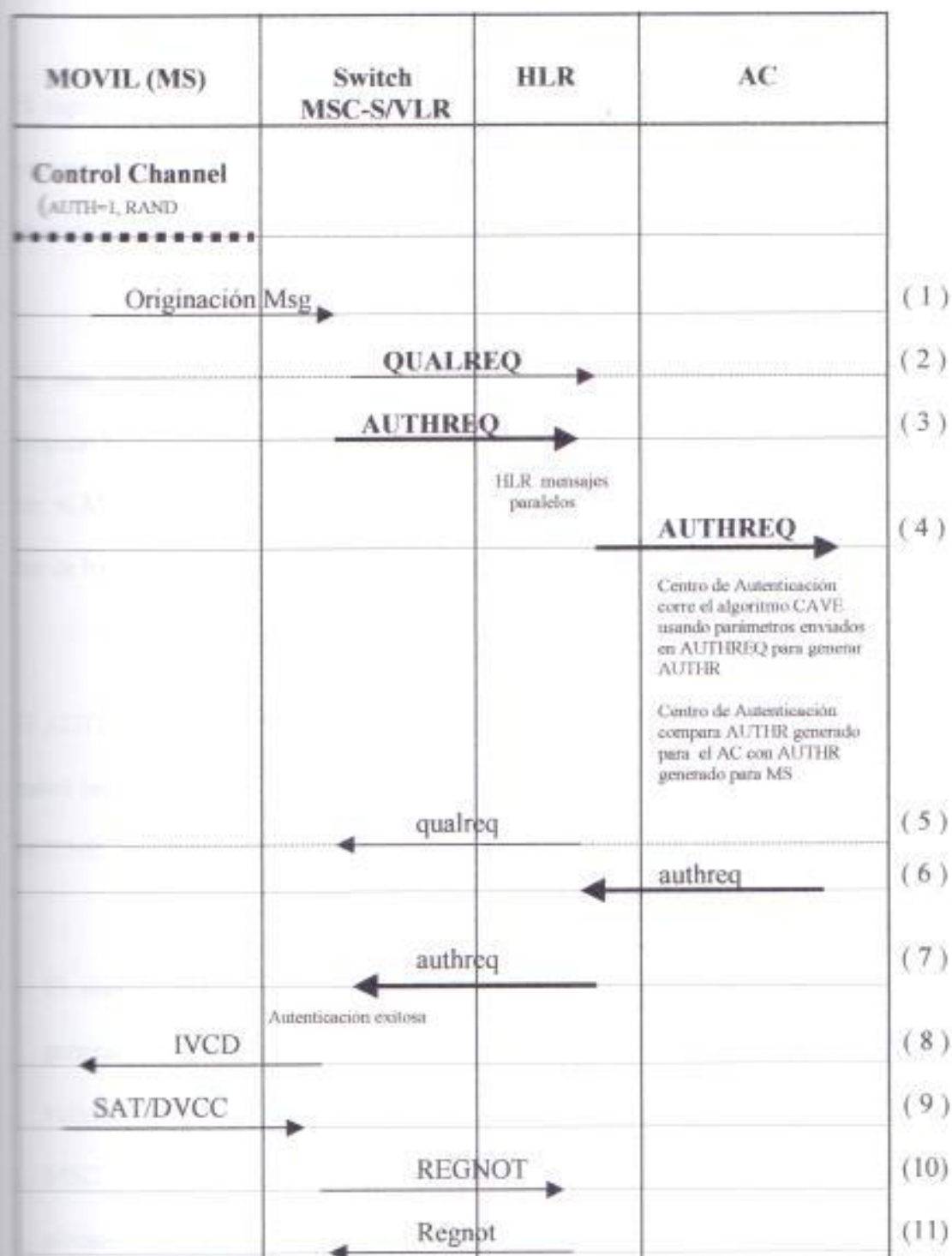
retardos enviando el mensaje IVCD mientras los mensajes de Authentication Response y Qualification Response son recibidos.

4. El HLR rutea el Authentication Request al Centro de Autenticación. Cuando el Centro de Autenticación recibe el Autenticación Request, este realiza la validación del MIN/ESN. Este usa el tipo de acceso al sistema para determinar que tipo de llamada será autenticada. El AC envía un requerimiento al algoritmo CAVE para generar el AUTHR. El AC compara el AUTHR generado por el móvil con el AUTHR generado por el AC.
5. El MSC recibe el mensaje de Qualification Response, actualiza el perfil del móvil, y espera por el mensaje de Authentication Response. Si el Qualification Response falla, entonces la llamada se cae sin esperar el Authentication Response.
6. El AC envía el resultado de la comparación del AUTHR al HLR en el mensaje de Authentication Response.
7. El HLR rutea el mensaje de Authentication Response de regreso al MSC.
8. El MSC recibe el Authentication Response. La información en este mensaje indica que el AUTHR paso la comparación. El MSC envía al móvil el mensaje IVCD solo después de que los mensajes Authentication y Qualification Responses han sido recibidos.
9. El móvil responde al mensaje IVCD con SAT/DVCC.
10. El HLR confirma el mensaje de registro con el mensaje de Registration Notification Response.
11. El HLR manda el mensaje REGNOT al SWITCH para originar la llamada.



FIGURA 2.10

## ORIGINACION EXITOSA SIN ENTRADA VLR



### 2.3.4.2.2 ORIGINACION EXITOSA CON ENTRADA VLR PRESENTE Y SSD NO COMPARTIDO

El siguiente flujo de mensajes "Originación Exitosa con entrada VLR (SSD no esta compartido)" representa el proceso que sigue una autenticación exitosa de un móvil en originación con una entrada de VLR pero sin SSD compartido.

En este caso, la llamada procede después de que el mensaje de Authentication Request ha sido enviado al AC/HLR. Cuando el Authentication Response es recibido por el MSC, se determina si la autenticación ha fallado y si la llamada se la debe de dar de baja. Si el móvil ha sido autenticado con éxito, la llamada no es interrumpida.

El AUTH=1 y RAND son transmitidos sobre el canal de control. Si el AUTH=1, el móvil lee el valor de RAND desde el canal de control para ser usado para generar el AUTHR.

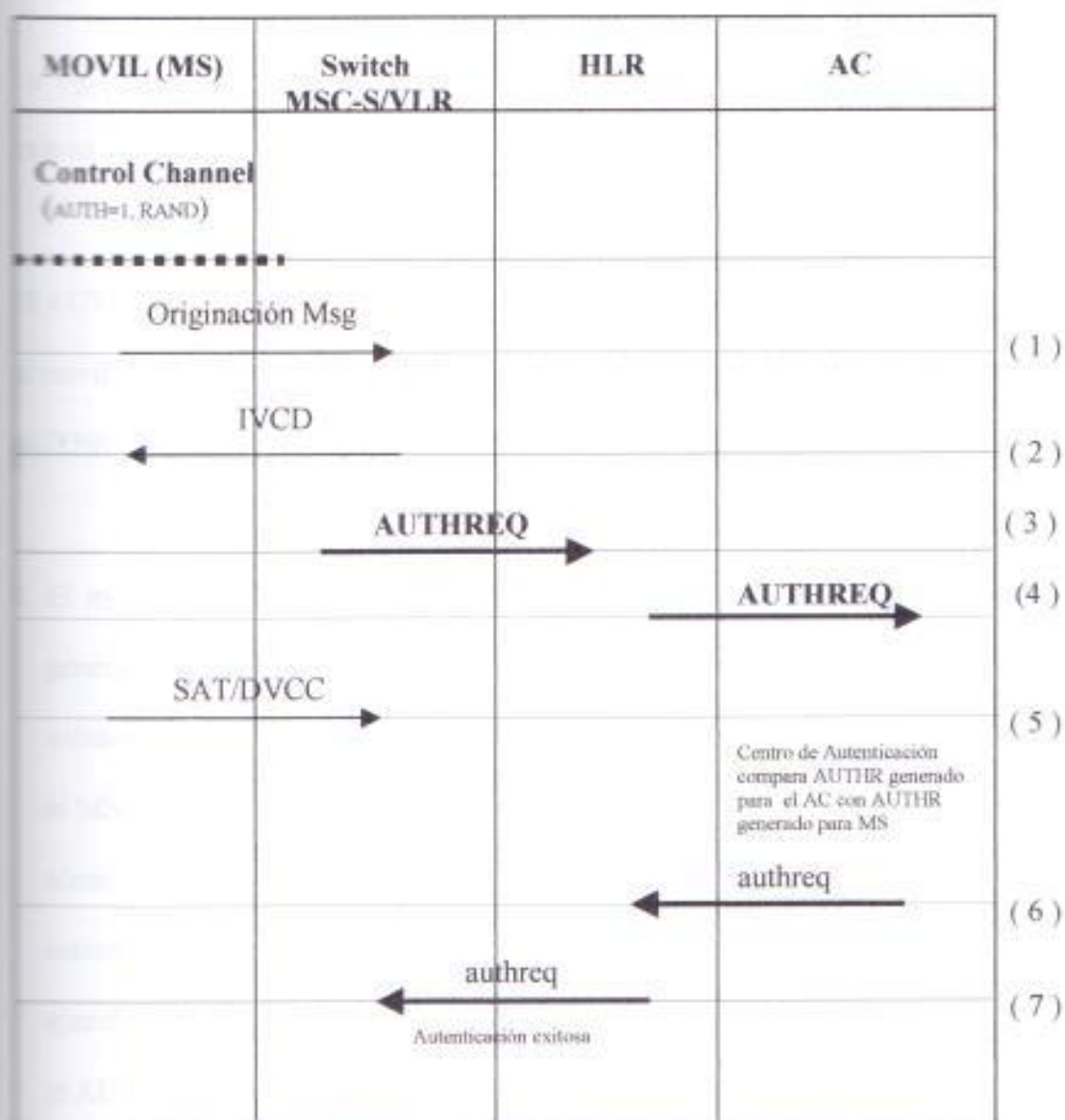
1. El móvil genera el mensaje de originación conteniendo el valor de AUTHR generado. Cuando el MSC recibe el mensaje de originación, este realiza la validación del MIN/ESN y EL RANDC. Si una entrada VLR válida existe, el MSC determina que el móvil es capaz de autenticar desde la información almacenada en la entrada VLR.

2. El MSC determina que el SSD no es compartido por la ausencia de un valor SSD asociado con la entrada VLR del móvil. El proceso de llamada continua.
3. Un mensaje de Authentication Request es enviado al HLR del móvil.
4. El HLR reenvía el Authentication Request al AC. Cuando el AC recibe el Authentication Request, este realiza la validación del MIN/ESN. Este usa el parámetro de capacidad del sistema para determinar que tipo de llamada ha sido autenticada. El AC envía un requerimiento al algoritmo CAVE para generar el AUTHR. El AC compara el AUTHR generado por el móvil con el AUTHR generado por el AC.
5. SAT/DVCC es usado por el móvil en respuesta al mensaje IVCD.
6. El AC envía el resultado de la comparación del AUTHR hacia el HLR en un mensaje de respuesta de autenticación (Authentication Response message).
7. El HLR reenvía el Authentication Response al MSC servidor. Cuando el Authentication Response es recibido por el MSC indicando que la autenticación ha sido positiva, el MSC permite que la llamada continúe.

Si la originación contiene un requerimiento de alguna propiedad, este requerimiento será enrutado antes de que la autenticación se complete.

FIGURA 2.11

**ORIGINACION EXITOSA CON ENTRADA VLR (SSD no compartido)**



### 2.3.4.2.3 ORIGINACIÓN CON ENTRADA VLR SSD COMPARTIDO.

Para una originación normal, una llamada procede después de se hace un requerimiento para correr el CAVE. Cuando la respuesta del CAVE es recibida, se determina si la autenticación fallo para dar de baja a la llamada. Si el móvil se autenticó correctamente, no se interrumpe la llamada.

La siguiente figura representa el flujo de mensajes seguidos para una autenticación exitosa de un móvil en originación, con entrada VLR y SSD compartido.

El AUTH=1 y RAND son transmitidos sobre el canal de control. Cuando AUTH=1, el móvil lee el valor del RAND del canal de control que va a ser usado para generar el AUTHR.

1. El móvil genera el mensaje de originación conteniendo el valor de AUTHR generado. Cuando el MSC recibe el mensaje de originación, este realiza la validación del MIN/ESN y el RANDC. Si una entrada validada existe en el VLR, el MSC determina que el móvil es capaz de autenticarse a partir de la información almacenada en el VLR. El MSC determina que el SSD es compartido por la entrada SSD en el VLR asociada a la entrada del móvil en el VLR, y por tanto ejecuta el CAVE desde el MSC. Si el AUTHR generado por el móvil coincide con el AUTHR generado por el MSC, el móvil se autentifica.

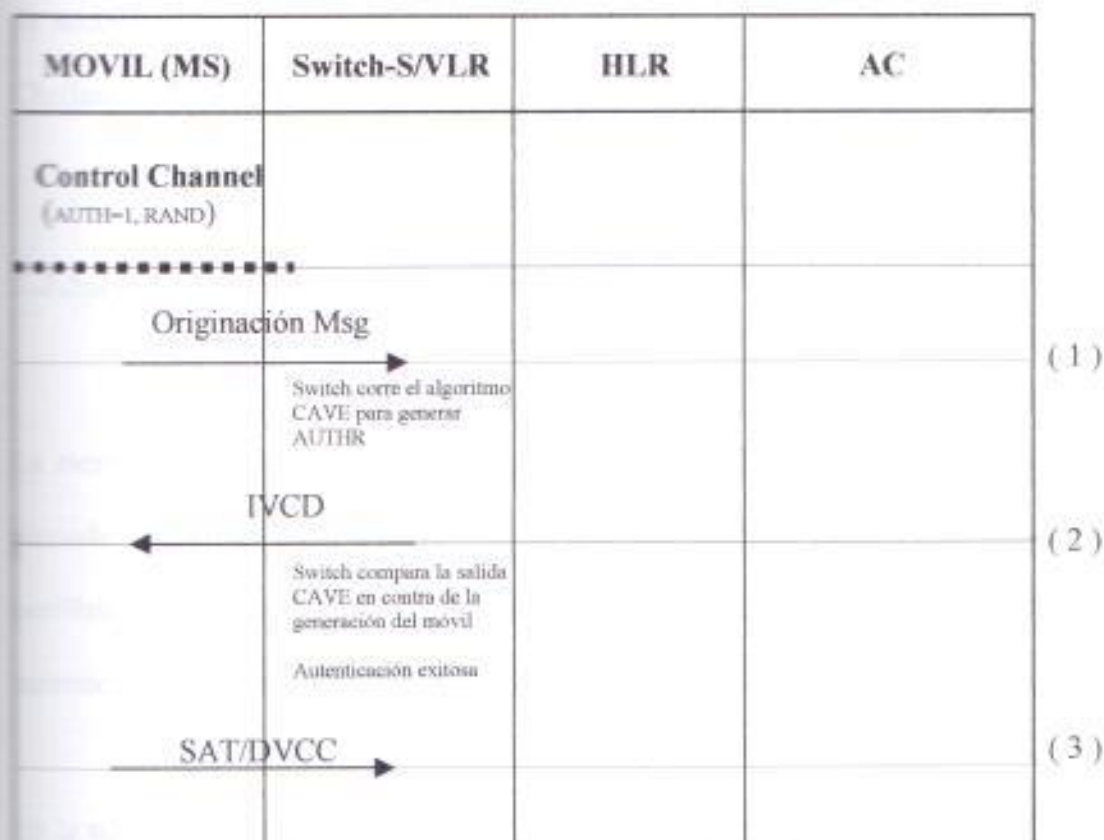
2. El proceso de la llamada corre paralelo con la autenticación, por lo tanto el mensaje ICVD puede ser enviado al móvil antes de la autenticación se complete.

3. El móvil responde con el mensaje SAT/DVCC.

Si la originación contiene un requerimiento de alguna propiedad, este requerimiento será enrutado sin esperar que se complete la autenticación.

FIGURA 2.12

**ORIGINACION EXITOSA CON ENTRADA VLR (SSD compartido)**



## **2.3.5 INTERFACE AÉREA**

### **2.3.5.1 VISIÓN**

Para proveer un entendimiento completo del sistema de autenticación, en nuestra tesis proveeremos información sobre las interfaces aéreas soportadas y su contenido específico de autenticación, y una breve descripción de los mensajes relacionados con la autenticación.

Lo restante es información referente al proceso de autenticación para diferentes tipos de acceso y los procesos de actualización del SSD y funcionamiento del Unique Challenge en un móvil.

### **2.3.5.2 MENSAJERÍA DE LA ESTACIÓN MÓVIL**

La mensajería de autenticación a la estación móvil puede ser ejecutada fuera de una llamada celular o durante varias etapas de una llamada celular. Las entidades periféricas involucradas en esta mensajería está basada en el tipo del móvil. La autenticación es soportada en AMPS, TDMA y CDMA.

En la siguiente tabla mostramos las interfaces que soporta el sistema de conmutación:

Tabla 2.1

## INTERFACES AÉREAS SOPORTADAS EN EL MSC

Interface Aerea	Tipos de Radio	Funciones de Autenticación
IS-95 A	Canal de Acceso	Autenticación en la originación y registración, Unique Challenge
	Canal Paging	Se transmite el AUTH y el número aleatorio RAND, se inicia el Unique Challenge.
	Canal de Tráfico	Autenticación en flash, Unique Challenge, Actualización del SSD.
IS-136	Canal de Control Digital	Se transmite AUTH y el RAND. Se autentifica en originación y registración, se inicia el Unique Challenge.
IS-54 B, IS-91 A, IS-136 A	Canal de Control Analógico	Se transmite el AUTH y el RAND. Se autentifica en originación y registración, se inicia el Unique Challenge
	Canal de Voz Analógico Canal de Tráfico Digital	Autenticación en flash, se inicia el procedimiento Unique Challenge y se actualiza el SSD.



### **2.3.5.3 IDENTIFICACIÓN DEL CANAL DE CONTROL DE LA AUTENTICACIÓN.**

El procedimiento Global Challenge es una manera de informar a la estación móvil que la autenticación es requerida cuando se está accediendo al sistema. Lo que sigue es una breve descripción de los parámetros de autenticación necesarios seguidos de una explicación de cómo estos parámetros están comunicados al móvil.

### **2.3.5.4 PARAMETROS DE AUTENTICACIÓN.**

Hay dos parámetros que son usados para soportar el proceso de autenticación Global Challenge, estos son el AUTHU y el RAND. El parámetro AUTHU provee una indicación de si el proceso global challenge es activado o desactivado en el MSC/VLR. Sobre la capacidad del global challenge, el móvil debe generar un AUTHR previo a algún sistema de acceso. Cuando el proceso Global Challenge está incapacitado, el móvil no es requerido para generar el AUTHR y es capaz de acceder al sistema.

En lo que respecta al RAND, cuando el proceso Global Challenge está incapacitado, entonces el valor del RAND es usado como una de las entradas al algoritmo CAVE para procesar el AUTHR.

## 23.5.5 PARÁMETROS DE AUTENTICACIÓN EN EL CANAL DE CONTROL ANALÓGICO

Los parámetros de Autenticación son comunicados para móviles AMPS/TDMA via el Tipo de Mensajes de Encabezado del Canal de Control (CCH OMT). El CCH OMT es una combinación de varios mensajes son enviados al Canal de Control Delantero Analógico. (CCH)

El parametro AUTH en el CCH OMT esta definido como parte del Mensaje Encabezador del Paramtero del Sistema (SPOM).

El parametro RAND en el CCH OMT esta definido como parte del Mensaje Encabezador de Acción Aleatoria Global Challenge (GAOM).

El valor aleatorio challenge A GAOM contiene los 16 bits mas significativos de los 32 bits del RAND (RANDI\_A). El valor aleatorio Random Challenge B GAOM contiene los 16 bits menos significantes de los 32 bits del número RAND(RANDI\_B).

### **2.3.5.6 PARAMETROS DE AUTENTICACIÓN EN EL CANAL DE CONTROL DIGITAL (DCCH).**

Los parámetros de autenticación son comunicados a los móviles con el canal DCCH a través del Canal de Control para Difusión Rápida (Fast Broadcast Control Channel). El F-BCCH es un canal lógico para transportación del sistema generico relacionado a la información.

Tanto los parámetros AUTH y RAND en el F-BCCH estan definidos como parte del mensaje de Parametros de Acceso. El bit 1 del AUTH y el bit 32 del número aleatorio RAND son campos gobernantes del mensaje.

### **2.3.5.7 PARAMETROS DE AUTENTICACIÓN EN CDMA.**

Los parámetros de autenticación estan comunicados a los móviles del CDMA a través del canal de Paginación (Paging). El canal de Paginación es usado para enviar la información de control a un móvil que no ha sido asignado a un Canal de Tráfico.

Tanto los parámetros del AUTH y el RAND en el canal Paging estan definidos como parte del mensaje de Parametros de Acceso. Cuando el bit 2 del AUTH es puesto a

"01", el sistema incluye un bit 32 del RAND en el mensaje a ser usado por el móvil para la autenticación. Para algunos otros valores, el sistema omite el campo RAND en el mensaje.

## **2.3.6 CONSIDERACIÓN DEL RAND.**

En la subsiguiente información describiremos el proceso para actualizar el RAND y la frecuencia del RAND en el Canal de Control OMT.

### **2.3.6.1 PROCESO DE ACTUALIZACIÓN DEL RAND.**

Periódicamente, el MSC genera un nuevo RAND y actualiza los canales de control del sistema. El valor del RAND puede ser también manualmente actualizado a través del comando 'RANDUP'. Esta funcionalidad provee la conmutación para poner al día el RAND para la autenticación de TDMA/AMPS siempre que sea necesario.

### **2.3.6.2 FRECUENCIA DEL RAND EN EL CANAL CCH OMT.**

Corrientemente un gran número de estaciones móviles de la EIA-553 (AMPS) no complica al estandar EIA-553 en relación al canal CCH OMT. De acuerdo al estandar, el móvil con EIA-553 es requerido para ignorar parámetros extraños en el OMT. Sin embargo este no es el caso con muchos móviles del EIA-553

corrientemente en uso. Estos móviles intentan leer estos parametros del IS-54B en el OMT en lugar de codificar o de inhabilitar información en el OMT. Este proceso continua y el móvil jamas recibirá el servicio.

El MSC varia la frecuencia de los parametros del IS-54B en el OMT con el proposito de proveer el servicio para aquellos móviles con estandar EIA-553. Sin embargo los parametros del IS-54B deberian también ser incluidos muy a menudo para cubrir móviles que confían en esos parametros.

## **2.3.7 MENSAJES DE AUTENTICACIÓN**

En las siguientes líneas proveeremos una breve vistazo de la autenticación relacionada con los mensajes que son usados en las siguientes secciones.

### **2.3.7.1 AUTENTICACIÓN RELACIONADA CON LOS MENSAJES IS-41 REVISIÓN C.**

Las capacidades de establecimiento de una red intersistemas de la autenticación están basadas en las operaciones de autenticación y procedimientos subrayados en IS-41C. La siguiente lista identifica las operaciones de autenticación soportados por el MSC y se los describe de la siguiente forma:

- *Autenticación Directiva (AUTHDIR)*- La operación AUTHDIR es usada para modificar uno de los parametros de autenticación del móvil (por ejemplo la actualización del SSD) o solicitar la autenticación de un móvil con capacidad de autenticación. Esta operación es iniciada por un Centro de Autenticación con un MSC/VLR de servicio de un móvil.
- *Reporte de Falla de Autenticación (AFREPORT)*- La operación AFREPORT es usada para reportar una falla de autenticación para un móvil. Esta operación es iniciada por el MSC/VLR en servicio con el Centro de Autenticación correspondiente al móvil.
- *Solicitud de Autenticación (AUTHREQ)*- La operación del AUTHREQ es usada para solicitar la autenticación de un móvil con capacidad de autenticarse. Esta operación es iniciada por el MSC/VLR con el Centro de Autenticación correspondiente al móvil.
- *Reporte de Estatus de Autenticación (ASREPORT)*- La operación ASREPORT es usada para reportar en la salida de una operación de autenticación iniciada por un Centro de Autenticación. Esta operación es iniciada por el MSC/VLR servidor con el Centro de Autenticación correspondiente al móvil.
- *Desafío de la Estación Base (BSCHALL)*- La operación BSCHALL es usada para solicitar una respuesta a una Orden de desafío de la Estación Base recibida de un móvil. Esta operación es iniciada por el MSC/VLR con el Centro de Autenticación correspondiente al móvil.

La autenticación no provee soporte para las siguientes operaciones:

- Autenticación Directiva Delantera
- Solicitud de Conteo.
- Solicitud de Variable Aleatoria.

### 2.3.7.2 MENSAJES DE AUTENTICACIÓN RELACIONADOS CON LA INTERFACE AÉREA.

La siguiente información enlista los mensajes soportados en el MSC sobre la interface aérea y se describe de la siguiente manera:

- *Orden de Desafío Unico.*- Este mensaje es enviado al móvil para iniciar un Desafío Unico y causa en el móvil la corrida del algoritmo de autenticación. El móvil responde a este mensaje una Orden de Confirmación de Desafío Unico el cual contiene la autenticación de las salidas del algoritmo de autenticación.
- *Orden de Desafío de la Estación Base.*- Este mensaje es enviado del móvil al MSC/VLR y contiene el RANDBS para ser usado como entrada al algoritmo de autenticación. El MSC/VLR responde a este mensaje con una Orden de Confirmación de Desafío de la Estación Base la cual contiene la autenticación de las salidas del algoritmo de autenticación.
- *Orden de Actualización del SSD.*- Este mensaje es enviado al móvil para iniciar un procedimiento de Actualización del SSD y causa en el móvil la corrida del algoritmo de autenticación. El móvil responde a este mensaje después de

completar el proceso de Desafío de la Estación Base (BSCHALL), con una Orden de Confirmación de la Actualización del SSD la cual contiene una indicación del éxito o fracaso del procedimiento de actualización del SSD.

## 2.4 PROCESO DEL UNIQUE CHALLENGE

El Unique Challenge es otro método para la autenticación del móvil. Puede ser iniciado por el Centro de Autenticación o el MSC/VLR si el SSD es compartido.

El Unique Challenge es usado en los siguientes escenarios:

- Durante el proceso de actualización del SSD. Después de que el SSD es actualizado en un móvil, un Unique Challenge es inmediatamente iniciado para verificar que el SSD fue correctamente actualizado en el móvil.
- En respuesta a una falla. Si una falla es detectada, el Centro de Autenticación puede ser configurado para iniciar un Unique Challenge para autenticar el móvil.
- En respuesta a un acceso al sistema. Los Unique Challenge son usados para autenticar móviles que están haciendo flash y en sistemas de accesos no especificados.

El proceso del Unique challenge usa una variable aleatoria única (RANDU) y ejecuta el CAVE para generar un parámetro de resultado de autenticación para el Unique



**Challenge (AUTHU).** El sistema servidor entonces le pregunta el móvil para ver si se puede generar el AUTHU con el mismo valor del RANDU. La comparación de los AUTHUs determina si el móvil es auténtico o no.

## 2.5 PROCESO DE ACTUALIZACION DEL SSD.

El proceso de autenticación el cual genera y actualiza un SSD de un móvil es el escenario más intensivo en el procesamiento de la autenticación. Este es necesario para asegurar tanto que el AC y el móvil tengan el mismo valor SSD cuando el proceso sea completado. El proceso longitudinalmente también asegura que un móvil fraudulento no sea erróneamente actualizado con un nuevo SSD. El proceso actual del SSD es siempre iniciado desde el Centro de Autenticación, sin tomar en cuenta de que si el SSD corriente sea compartido o no. Los valores de la bandera AUTH para los móviles con IS 54 e IS 136 no inciden en la decisión para llevar a cabo el proceso de actualización del SSD en esos móviles. El MSC puede recibir la Orden del SSD actual desde el AC mediante los siguientes mensajes:

- Authentication Directive Invoke
- Authentication Request Resonse
- Authentication Status Report
- Authentication Failure Report Response.

Una vez que el MSC ha procesado la orden, se envía de regreso un Authentication Status Report conteniendo un parámetro llamado SSD Update Report (SSDURPT) y un parámetro llamado Unique Challenge Report (UCHALRPT).

El parámetro SSDURPT indica la salida de la operación para la actualización del SSD. Esta operación puede contener uno de los siguientes valores:

- Actualización del SSD no atendido, es decir, que el MSC no es capaz de completar o de empezar una operación para actualizar el SSD, esto es debido a que el móvil está siendo apuntado, está haciendo hand off a otro sistema.
- Actualización del SSD no contestado, es decir, que el MSC tiene un tiempo de espera para un Base Station Challenge o una continuación de actualización para el SSD.
- Actualización del SSD exitosa, es decir que el MSC ha recibido una confirmación actual del SSD con un código de retorno exitoso.
- Actualización del SSD fracasada, es decir, que el MSC ha recibido una confirmación del SSD actual con un código de retorno erróneo.

El estándar IS 41 C requiere que un SSD actual sea siempre seguido por la ejecución de un Unique Challenge para confirmar el nuevo valor del SSD del móvil. El parámetro UCHALRPT indica la salida de la operación del Unique Challenge. Esta operación contiene uno de los siguientes valores:

- Unique Challenge no intentado, es decir, que el MSC no es capaz de completar o de iniciar la parte del Unique Challenge de la operación de actualización del SSD debido a un problema del sistema.
- Unique Challenge no contestado, es decir, que el MSC tiene un tiempo de espera para la confirmación del Unique Challenge.
- Unique Challenge exitoso, es decir, que el MSC ha recibido una confirmación del Unique Challenge y el AUTHU generado por el móvil comparado con el AUTHU generado ya sea en el Centro de Autenticación o en el MSC.
- Unique Challenge fracasada, es decir, que el MSC ha recibido una confirmación Unique Challenge, y el AUTHU generado por el móvil no se lo compara generado ya sea en el Centro de Autenticación o en el MSC.

En nuestro sistema de autenticación, la actualización del SSD es conducida en los canales de voz solamente. Si la solicitud de la actualización del SSD es recibida desde el Centro de Autenticación, y el móvil no está haciendo una llamada, entonces la celda en la cual se encuentra el móvil es capaz de autenticarlo en ese momento. El MSC envía de regreso un Authentication Status Report junto con los parámetros del SSDURPT y el UCHALRPT puestos como no intentados. También si el móvil pierde la llamada en cierto momento durante el proceso de actualización del SSD, es resto de la actualización del SSD es abortado, y el Status corriente de la actualización del SSD y el Unique Challenge es reportado al Centro de Autenticación. Además, si un móvil hace flash durante el proceso de actualización del SSD, la actualización del

SSD será abortada para permitir que la autenticación para la solicitud de hacer flash tome lugar.

El Centro de Autenticación puede decidir que hacer sobre la actualización del SSD en uno de los siguientes aspectos:

- Ingreso de una clave de autenticación en el móvil y en Centro de Autenticación.
- La expiración del intervalo de actualización del SSD para el móvil,
- Un procedimiento administrativo para fijar los problemas del SSD con un móvil.

Una vez que el Centro de Autenticación decida que hacer con la actualización del SSD para un móvil, este puede enviar los parámetros de actualización al MSC/VLR en uno de los siguientes métodos:

- Si el SSD es compartido corrientemente con un MSC/VLR, el Centro de Autenticación puede revocar el SSD corriente tal que un mensaje de autenticación será enviado al Centro de Autenticación en el próximo sistema de acceso del móvil. El Centro de Autenticación puede procesar el mensaje y lo puede incluir en los parámetros de actualización del SSD en la respuesta.
- Sin esperar por el acceso del móvil, el Centro de Autenticación puede inmediatamente enviar los parámetros de actualización del SSD en el mensaje AUTHDIR.

## 2.5.1 ACTUALIZACION DEL SSD INICIADA DURANTE EL ACCESO DEL MOVIL

La fig. 2.13 es un ejemplo de una actualización del SSD iniciada durante el acceso del móvil.

1. Si el Centro de Autenticación está compartiendo el SSD con el sistema servidor MSC/VLR del móvil, el Centro de Autenticación envía un Authentication Directive Request al HLR del móvil. El mensaje contiene la instrucción para revocar el SSD corriente almacenado en el VLR del móvil. Esto es necesario para asegurar que el Centro de Autenticación sea informado del próximo sistema de acceso del móvil.
2. El HLR envía el Authentication Directive al sistema servidor MSC/VLR.
3. El MSC/VLR envía de regreso una respuesta llamada Authentication Directive Response al HLR indicando que el mensaje ha sido aceptado.
4. El HLR rutea la respuesta del Authentication Directive Response de regreso al Centro de Autenticación. En este punto, la operación de actualización del SSD es suspendida hasta que el móvil identificado pueda acceder de nuevo al sistema. Hay que notar que el próximo sistema de acceso autenticable puede ser una registración, una originación, o un flash. Hay que notar además que el MSC no

puede ejecutar la actualización del SSD durante el acceso de registración, ya que el móvil no está en un canal de voz. El MSC enviará el ASREPORT junto con los parámetros del Status puestos en "no procurado" en ese caso.

5. En este escenario, el móvil envía en un mensaje de originación al sistema servidor MSC/VLR. Otros accesos posibles pueden ser registración y flash en este escenario.
6. Durante la recepción del mensaje de originación, el MSC envía el IVCD al móvil y Authentication Request es enviado al Centro de Autenticación. El MSC empieza un tiempo denominado ACBOUND para esperar un Authentication Response.
7. El HLR rutea el Authentication Request al Centro de Autenticación.
8. El mensaje SAT/DVCC viene del móvil.
9. El Centro de Autenticación opcionalmente autentica al móvil, y envía de regreso el Authentication Response conteniendo los siguientes parámetros de actualización del SSD como son: RANDSSD y el SSD ( si el Centro de Autenticación opta por compartir el SSD).

- 11. El HLR rutea el Authentication Response al sistema servidor MSC/VLR.
- 12. Durante la recepción del parámetro de actualización del SSD en el Authentication Response, el MSC aclara el tiempo ACBOUND. Luego el MSC chequea si el móvil identificado está involucrado en una llamada dentro de una celda con capacidad de autenticación. En este caso lo está. El MSC envía una orden de actualización del SSD conteniendo el RANDSSD para el móvil. Si el móvil no está haciendo una llamada, el MSC envía de regreso un Authentication Status Report con los parámetros SSDURPT= puesto en 'no intentado' y el UCHALRPT= 'no intentado'.
- 13. Durante la recepción de la orden de actualización del SSD, el móvil ejecuta el CAVE para computar el SSD pendiente. El Cave selecciona un RANDBS, en el Base Station Challenge Order para el sistema servidor MSC. El móvil entonces computa el AUTHBS usando el RANDBS.
- 14. Si el MSC tiene un SSD de un móvil y puede ejecutar el CAVE, entonces el CAVE computa el AUTHBS usando el RANDBS recibido desde el móvil. Si el MSC no tiene un SSD de un móvil o no puede correr el CAVE, entonces envía el RANDBS en el mensaje BSCHALL al HLR y empieza tiempo BSCT.

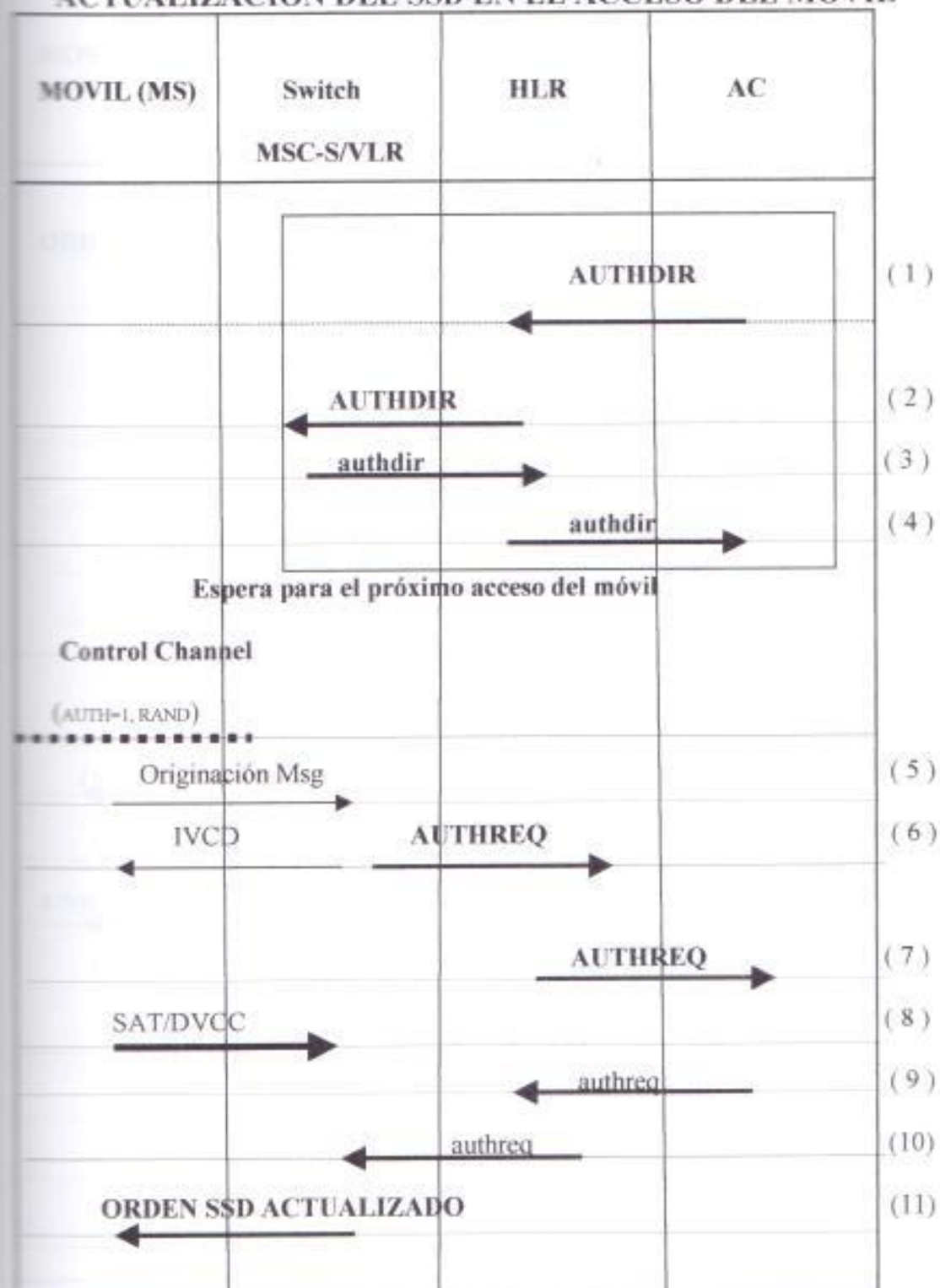
14. El HLR rutea el mensaje BSCHALL al Centro de Autenticación. El AC ejecuta el CAVE para computar el AUTHBS.
15. El AC envía de regreso un AUTHBS en el mensaje de respuesta BSCHALL Response al HLR.
16. El HLR rutea el BSCHALL Response al sistema servidor MSC/VLR. El MSC/VLR aclara el tiempo BSCT.
17. El sistema servidor envía de regreso el AUTHBS en un Base Station Challenge Confirmation al móvil.
18. El móvil luego compara el valor del AUTHBS recibido desde el MSC con el generado hace poco. Se asume que la comparación pasa en este caso. El móvil almacena el SSD pendiente como SSD corriente y retorna su proceso "éxito" en la confirmación de la actualización del SSD al sistema servidor MSC. Si la comparación ha fallado, el móvil tendría que haber enviado un "failed" en la Confirmación de la actualización del SSD al sistema servidor MSC y mandar ha enviar el SSD pendiente.



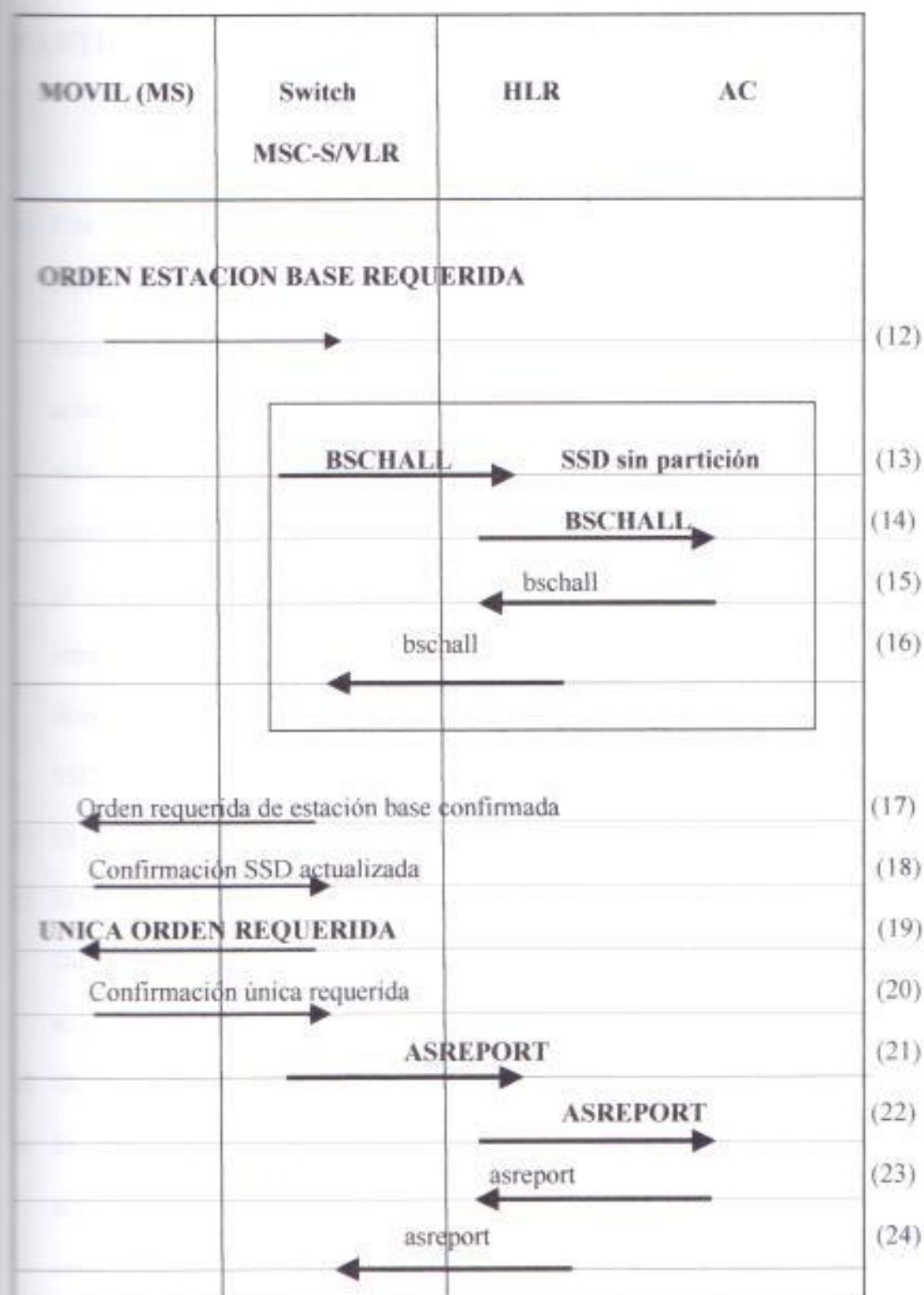
19. Si los parámetros del RANDU y el AUTHU no fueron recibidos desde el Centro de Autenticación, el MSC genera el RANDU y computa el AUTHU. El MSC envía el RANDU en una orden Unique Challenge al móvil.
20. Durante la recepción la Confirmación del Unique Challenge desde el móvil, el MSC compara los valores del AUTHU. En este caso, la comparación si pasa.
21. El MSC inicia un tiempo ACBOUND y envía de regreso un Authentication Status Report al HLR del móvil con los parámetros SSDURPT = 'exitoso' y el UCHALRPT= 'exitoso' todo esto para señalar la operación completamente exitosa para la actualización del SSD. Si la comparación del AUTHU ha fallado, entonces el MSC envía el ASREPORT al HLR, con los parámetros SSDURPT = 'exitoso' y el UCHALRPT= fallado.
22. El HLR rutea el Reporte del Status de Autenticación al AC.
23. El AC puede compartir el nuevo valor del SSD en la Respuesta de Reporte del Estatus de Autenticación hacia el MSC/VLR servidor del móvil.
24. El HLR rutea la respuesta del Reporte del Status de Autenticación al MSC/VLR. Una vez que el sistema servidor MSC/VLR reciba la respuesta, este borra el temporizador ACBOUND y almacena el nuevo SSD.

FIGURA 2.13

## ACTUALIZACION DEL SSD EN EL ACCESO DEL MOVIL



(continuación)



## 2.5.2 ACTUALIZACION MANUAL DEL SSD PARA UN MOVIL PARTICULAR

- a) Una solicitud de Autenticación Directiva (AUTHDIR) es enviada al HLR del móvil. Este mensaje contiene instrucciones para revocar el SSD corriente almacenado en el VLR del móvil. Este mensaje también incluye parámetros de actualización del SSD (RANDSSD, SSD, RANDU, AUTHU) necesarios para actualizar el SSD del móvil. El anterior SSD es revocado con el propósito de garantizar que el AC sea informado del próximo sistema de acceso del móvil con el propósito de retenerlo en caso de una falla. Todos los parámetros de actualización del SSD son almacenados en caso de que el móvil no este disponible, y la entrada sea marcada como necesaria de una actualización del SSD.
- b) El HLR transmite el AUTHDIR al sistema servidor MSC/VLR.
- c) El sistema servidor MSC/VLR envia de regreso una Respuesta de Autenticación Directiva (authdir) al HLR, indicando que el mensaje directivo ha sido aceptado y se inicia el proceso de Actualización del SSD del móvil.
- d) EL HLR rutea de regreso la respuesta (authdir) al AC.
- e) El mensaje Base Station Challenge (BSCHALL) es parte del proceso de actualización del SSD. Si el MSC no esta compartiendo el SSD, entonces el MSC envia el mensaje (BSCHALL) al AC. Si el MSC es capaz de correr el algoritmo

CAVE entonces el SSD enviado en el AUTHDIR podría ser usado para el proceso (BSCHALL), de tal forma que se elimine el mensaje Base Station Challenge.

- ⑤ El HLR rutea el Base Station Challenge al AC.
- ⑥ El AC recibe el Base Station Challenge y corre el algoritmo CAVE para calcular el AUTHBS y retornar ese valor en el mensaje de retorno (bschall).
- ⑦ El HLR rutea la respuesta del (bschall) al sistema servidor MSC/VLR. El MSC envía el Base Station Challenge al móvil. Cuando el MSC recibe una confirmación positiva del móvil, el MSC ejecuta un Unique Challenge en el móvil.
- ⑧ El MSC envía un reporte de Actualización del SSD (ASREPORT) y el reporte del Unique Challenge al AC.
- ⑨ El AC evalúa el valor de los dos reportes. Si ellos indican que la actualización del SSD fue exitosa, el AC resetea el número de fallas de actualización del SSD a cero y marca la entrada como no necesaria para la actualización del SSD.

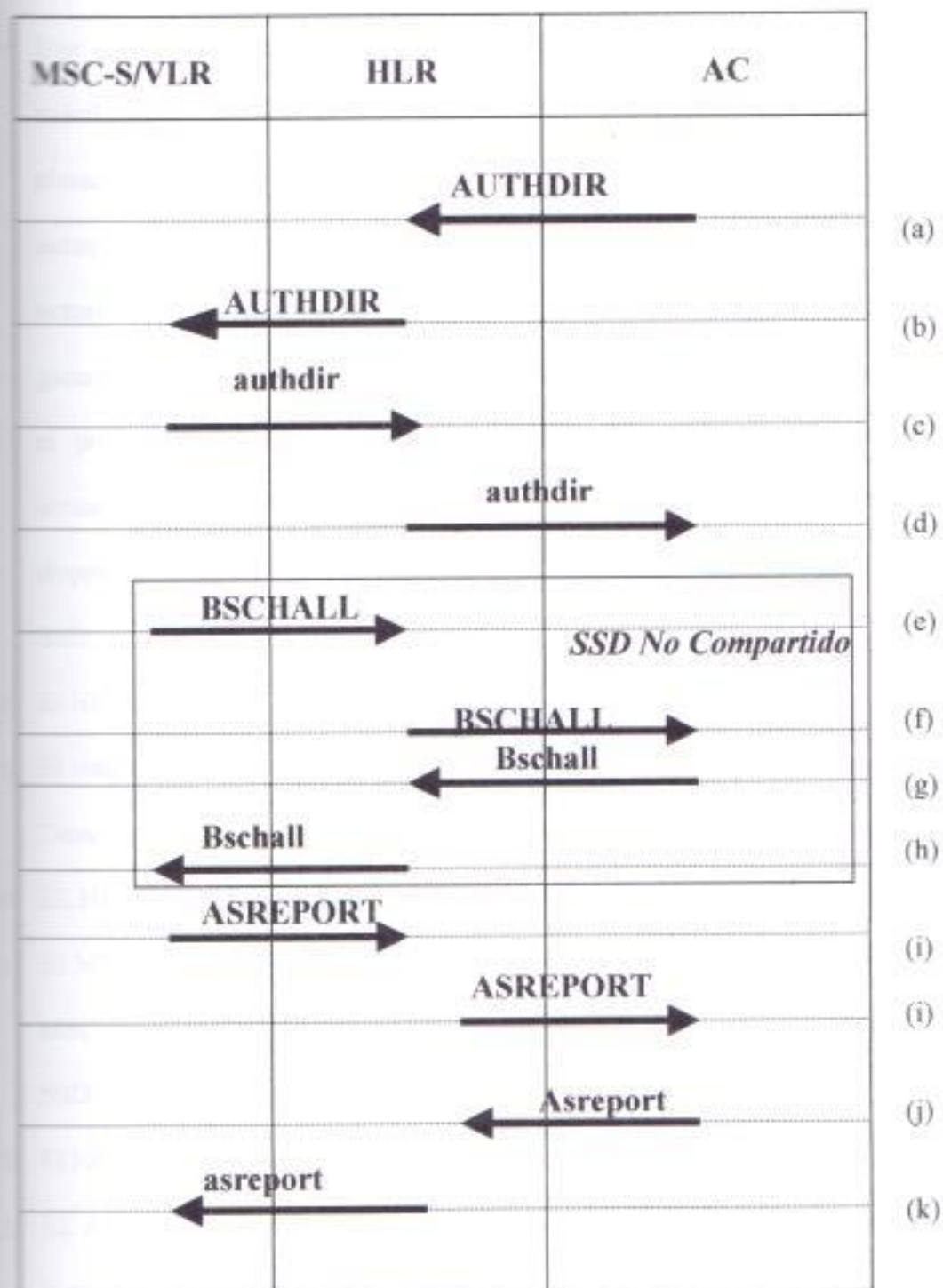
Si los reportes indican que la Actualización del SSD fue un fracaso, entonces el contador de fallas de actualización del SSD es incrementado.

El AC envía entonces un Reporte del Status de Autenticación (asreport) "vacío" al HLR.

- ⑩ El HLR rutea la respuesta Authentication Status Report al sistema servidor MSC/VLR.

FIGURA 2.14

## ACTUALIZACION DEL SSD PARA UN MOVIL



### 2.5.3 ACTUALIZACION MANUAL DEL SSD A UN MOVIL PARTICULAR NO DISPONIBLE

- a) Una solicitud de Autenticación Directiva (AUTHDIR) es enviada al HLR del móvil. Este mensaje contiene instrucciones para revocar el SSD corriente almacenado en el VLR del móvil. Este mensaje también incluye parámetros de actualización del SSD (RANDSSD, SSD, RANDU, AUTHU) necesarios para actualizar el SSD del móvil. El anterior SSD es revocado con el propósito de garantizar que el AC sea informado del próximo sistema de acceso del móvil con el propósito de retenerlo en caso de una falla. Todos los parámetros de actualización del SSD son almacenados en caso de que el móvil no este disponible, y la entrada sea marcada como necesaria de una actualización del SSD.
- b) El HLR transmite el AUTHDIR al sistema servidor MSC/VLR.
- c) El sistema servidor MSC/VLR envia de regreso una Respuesta de Autentidación Directiva (authdir) al HLR, indicando que el mensaje directivo ha sido aceptado.
- d) EL HLR rutea de regreso la respuesta (authdir) al AC.
- e) El MSC es incapaz de ejecutar la actualización del SSD en el móvil así que el MSC envia el mensaje ASREPORT al HLR indicando que la actualización del SSD no se encontró en el parámetro del reporte de Actualización del SSD.
- f) El HLR rutea el reporte del Status de Autenticación al AC.
- g) EL AC lee la respuesta del (asreport) de la actualización del SSD no encontrado y lo envia de regreso como un resultado vacío al HLR.

- ④ EL HLR rutea la respuesta del (asreport) al sistema servidor MSC/VLR.\*
- ⑤ Cuando el móvil accesa al sistema, una Solicitud de Autenticación es enviada al AC para autenticar al móvil.
- ⑥ El HLR rutea el Authentication Request al AC.
- ⑦ El AC primero determina si necesita autenticar el móvil. Si el estado del SSD del móvil es puesto como [inicial] entonces la autenticación no está corriendo por este acceso, aunque un SSD actual sea atendido. De otra forma, el AC corre el CAVE para calcular un valor AUTHR para el móvil y luego lo comparará con el AUTHR recibido. En este caso, la comparación pasa. El móvil es permitido para proceder con el sistema de acceso, y el AC envía de regreso una respuesta de autenticación, conteniendo los siguientes parámetros de actualización del SSD: RANDSSD y el SSD (si el AC escoje para compartir el SSD con el VLR y el VLR indica a través del parámetro de la capacidad del sistema que es capaz de correr el CAVE), or el RANDSSD, RANDU y el AUTHU (si el AC no escoje compartir el SSD).
- ⑧ El HLR rutea la respuesta de Autenticación al sistema servidor MSC/VLR.
- ⑨ Si el MSC no está compartiendo el SSD, entonces el MSC envía un mensaje BSCHALL al AC.
- ⑩ El HLR rutea el BSCHALL al AC.

---

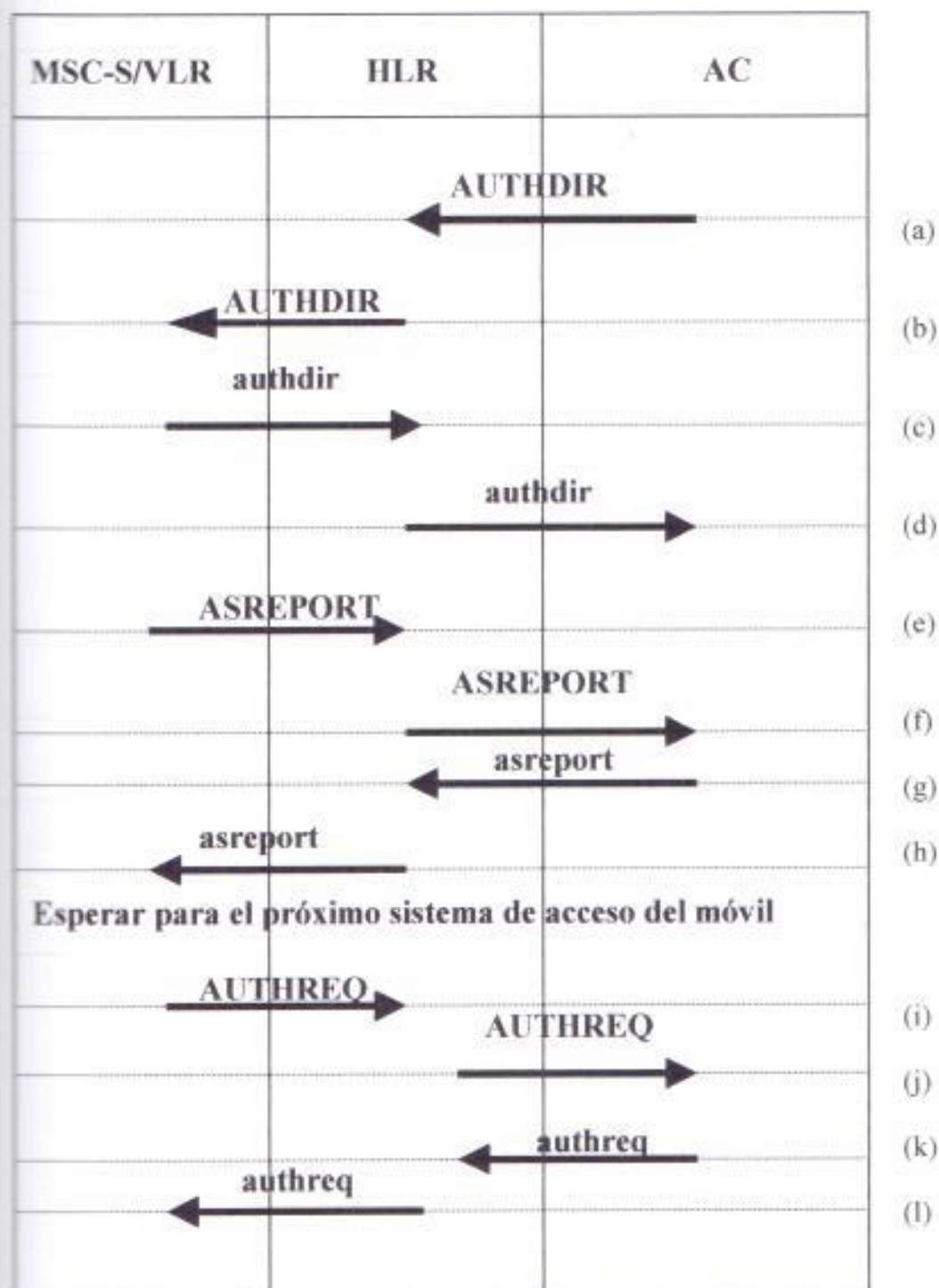
\*Nota: En este punto, la operación de Actualización del SSD no fue intentada. El MSC accederá al AC en el próximo acceso del móvil. El próximo sistema de acceso autenticable puede ser registración, terminación, originación, o flash.



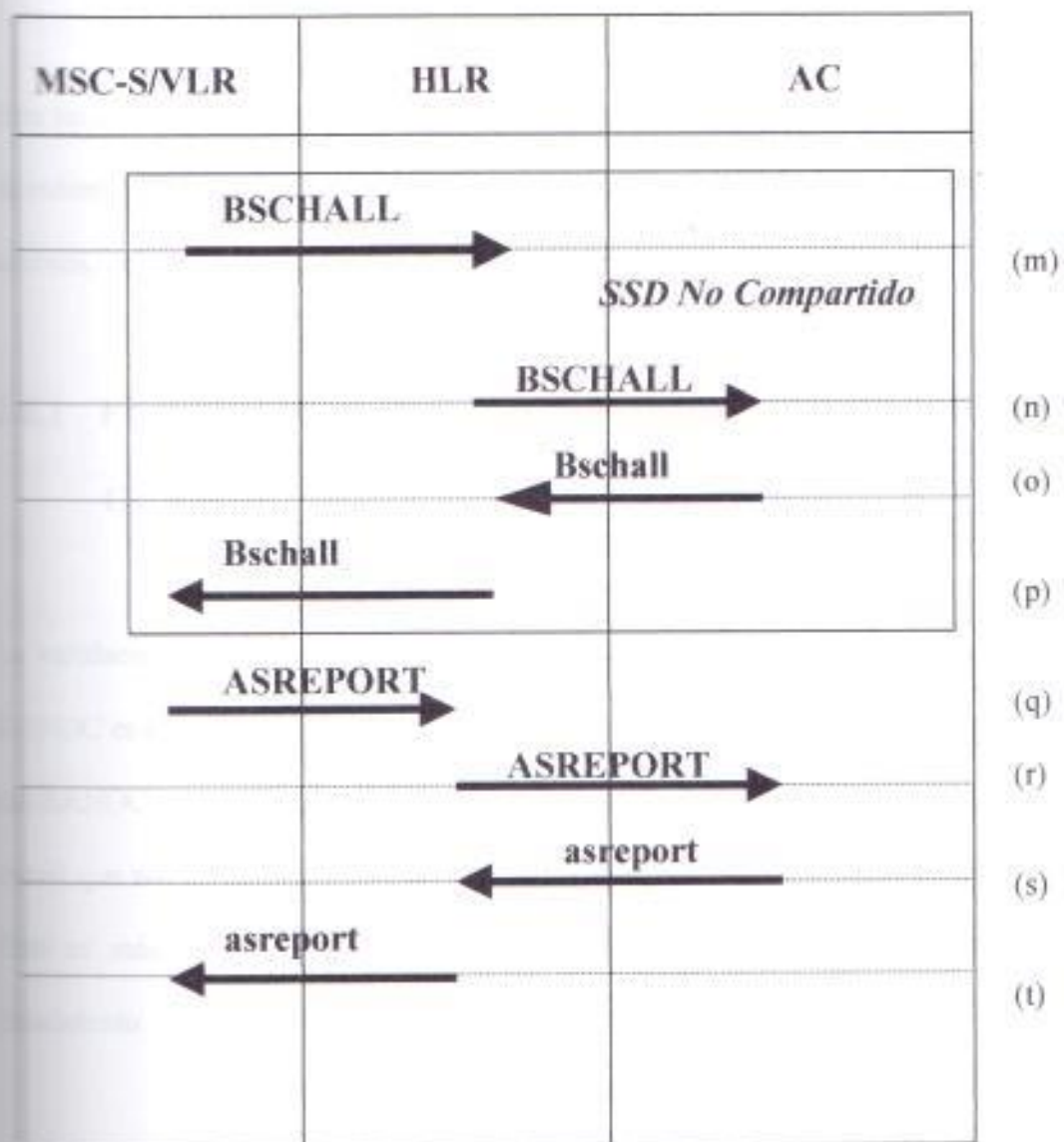
- 4) El AC recibe el Base Station Challenge y procede a correr el algoritmo CAVE para calcular el AUTHBS y regresa ese valor en el Base Station Challenge y retorna el mensaje BSCHALL al HLR
- 5) El HLR rutea la respuesta del BSCHALL al sistema servidor MSC/VLR. Cuando el MSC recibe una confirmación positiva del móvil, el MSC ejecuta un procedimiento Unique Challenge en el móvil.
- 6) El MSC envía el reporte de Actualización del SSD y el reporte del Unique Challenge al HLR en el mensaje ASREPORT.
- 7) El HLR rutea el ASREPORT al AC.
- 8) El AC evalúa el valor de los dos reportes. Si ellos indican que la actualización del SSD fue exitosa, el AC resetea el número de fallas de actualización del SSD a cero y marca la entrada como no necesaria para la actualización del SSD. Si los reportes indican que la Actualización del SSD fue un fracaso, entonces el contador de fallas de actualización del SSD es incrementado. El AC envía entonces un Reporte del Status de Autenticación (ASREPORT) "vacio" al HLR.
- 9) El HLR rutea el mensaje de respuesta ASREPORT al sistema servidor MSC/VLR.

FIGURA 2.15

## ACTUALIZACION DEL SSD PARA UN MOVIL NO DISPONIBLE



## ACTUALIZACION DEL SSD PARA UN MOVIL NO DISPONIBLE (Cont.)



## 2.6 FALLAS DE AUTENTICACION.

Esta sección cubre la administración de las fallas de autenticación en el MSC sistema de autenticación, incluyendo la administración de errores del sistema para sistemas de accesos, unique challenge y actualización del SSD en el MSC/VLR.

### 2.6.1 ERROR DEL AUTHR EN LA REGISTRACIÓN Y ORIGINACIÓN.

La validación del valor del AUTHR solamente toma lugar si la comparación del RANDC es exitoso. Así pues un error del AUTHR es una falla mas seria que un error del RANDC. Sin embargo es posible que un error del RANDC podría pasar, pero el móvil que usó el valor del RAND incorrecto y así pues se generó un AUTHR malo. Esto es más plausible que el móvil tenga un valor SSD malo o el móvil sea fraudulento.

#### 2.6.1.1 REGISTRACIÓN

La autenticación es ejecutada solamente durante la registración inicial en una celda con capacidad de autenticación, en la cual, el sistema no tiene un VLR entrante. Así que la comparación del AUTHR esta siempre ejecutada en el Centro de Autenticación y el AC envíe de regreso la acción en el Authentication Request Response.

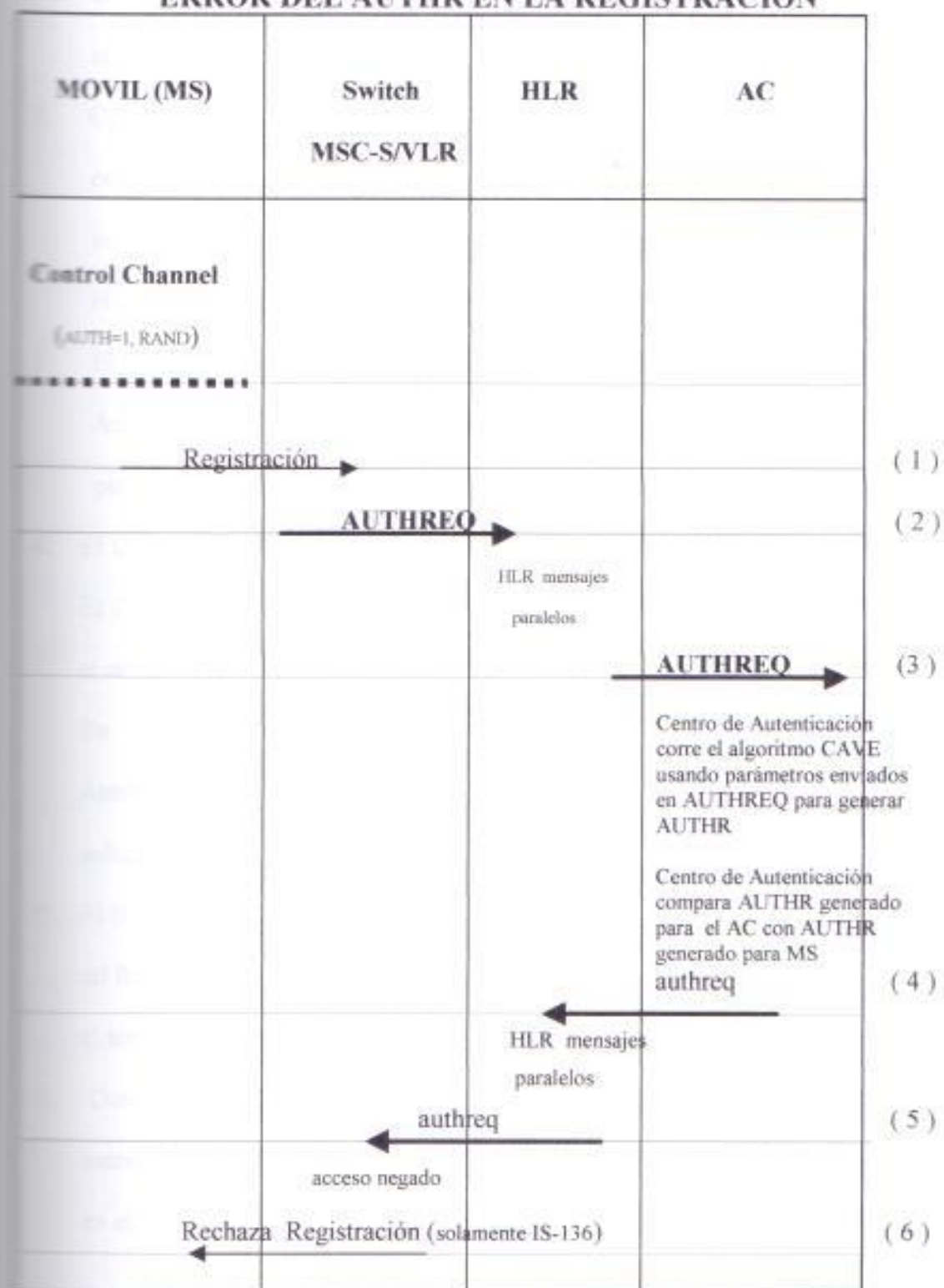
Si el AC envía de regreso el parámetro de "acceso denegado" en la respuesta, entonces el MSC/VLR no enviara el REGNOT al HLR.

También el MSC envia el mensaje de Registration Reject al móvil si la interface aérea es el canal de control digital con Initial Registration en el protocolo IS 136.

La fig. 2.16 muestra el escenario referente a la falla de autenticación en registraci3n inicial (AUTHR err3neo). Hay que tomar en cuenta que el AUTH = 1 y el RAND son transmitidos en el canal de control, indicando que la autenticaci3n es requerida en todos los accesos del sistema.

FIGURA 2.16

## ERROR DEL AUTHR EN LA REGISTRACION



1. El móvil lee el valor del RAND desde el canal de control y ejecuta el algoritmo CAVE para generar el AUTHR. El AUTHR y el RANDC son enviados en el mensaje de registraci3n al MSC.
2. Cuando el MSC recibe el mensaje de registraci3n, el MSC valida el RANDC con el valor del RAND almacenado en el MSC. El MSC envia un mensaje de solicitud de autenticaci3n conteniendo los valores del AUTHR y el RAND al HLR del móvil. El temporizador de ACBOUND es puesto en el MSC/VLR.
3. El HLR hace tandem con la solicitud de autenticaci3n hacia el Centro de Autenticaci3n. El HLR posiciona un temporizador ACBOUND para esperar por el mensaje de respuesta de autenticaci3n.
4. El Centro de Autenticaci3n corre el algoritmo CAVE para generar el AUTHR. El Centro de Autenticaci3n compara este AUTHR con el AUTHR generado por el móvil.

En este escenario, la comparaci3n del AUTHR falla y en Centro de Autenticaci3n incluye el parámetro de acceso denegado en la respuesta de solicitud de autenticaci3n al HLR.

5. El HLR hace tandem con el mensaje de respuesta de solicitud de autenticaci3n de tal forma que lo manda de regreso al sistema servidor del MSC. El HLR cancela el temporizador ACBOUND.
6. Cuando el MSC recibe el acceso denegado en la respuesta de solicitud de autenticaci3n, el MSC aborta la transacci3n de registraci3n. Si a interface aérea es el IS 136, entonces el MSC envia un escape de registraci3n con la debida

solicitud de una "falla de autenticación" al móvil. En este momento el temporizador ACBOUND es cancelado.

### 2.6.1.2 ORIGINACIÓN

Semejante a la registración, el error del AUTHR para la originación puede ser detectado en el Centro de Autenticación ( cuando el SSD no sea compartido) o en el MSC/VLR (cuando el SSD sea compartido). Cuando un AUTHR erróneo es detectado en el MSC, un Reporte de Falla de autenticación (AFREPORT) es enviado al Centro de Autenticación. El MSC esperará por el mensaje de respuesta de Reporte de Falla de autenticación desde el Centro de Autenticación antes de que tome alguna acción. La fig. 2.5.1.2 contiene el mensaje en el caso de un SSD compartido.

Si el SSD no es compartido, el MSC envía un mensaje Authentication Request al Centro de Autenticación del móvil. El Centro de Autenticación detecta el error del AUTHR y se reporta la acción en el mensaje Authentication Response. El MSC recibe el mensaje de respuesta y descarga la llamada si el parámetro de acceso denegado fue presentado en el mensaje.

El AUTH = 1 y el RAND son transmitidos en el canal de control. Hasta que el AUTH = 1, el móvil lee el valor del RAND desde el canal de control para ser usado y



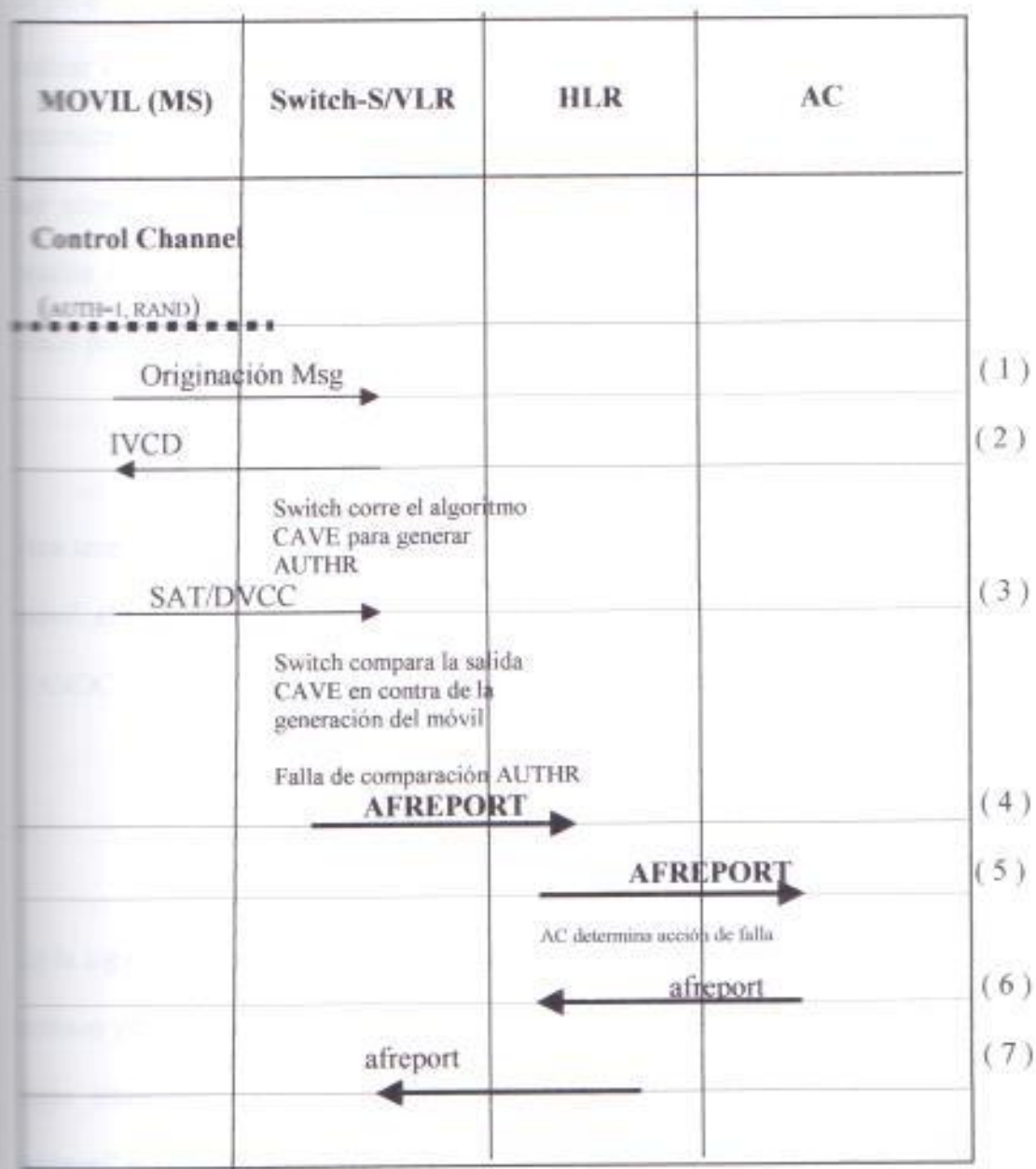
no poder generar el AUTHR. El móvil genera el mensaje de originación e incluye el valor del AUTHR en el mensaje.

1. Cuando el MSC recibe el mensaje de originación, ejecuta la validación del MIN/ESN y el RANDC. Hasta que un VLR válido ya exista, el MSC determina que el móvil es capaz de ser autenticado desde la información almacenada en el VLR entrante. El MSC determina que el SSD sea compartido por la presencia de un valor SSD asociado con el VLR entrante del móvil y corra el algoritmo CAVE desde el MSC.
2. El IVCD es enviado al móvil de forma paralela para la autenticación del móvil.
3. El mensaje SAT/DVCC es recibido en respuesta al mensaje IVCD y puede ser recibido en cualquier momento después de que el mensaje IVCD sea enviado. El AUTHR generado por el móvil fracasó en el intento de comparar el AUTHR generado por el MSC.
4. Hasta que la comparación del AUTHR sea un fracaso, el MSC envía un mensaje Authentication Failure Report conteniendo la información de falla al HLR. Aquí se presenta el tiempo AFRT para esperar la respuesta.

5. El HLR rutea el mensaje al Centro de Autenticación y posiciona un temporizador AFRT.
6. El Centro de Autenticación determina que acción tomar, basada en información de falla dentro del mensaje Authentication Failure Report. Un mensaje de respuesta Authentication Failure Report es enviado al HLR conteniendo dicha acción.
7. El HLR rutea el mensaje al MSC y cancela el temporizador AFRT. Si la llamada ha sido ruteada, el MSC descargará la llamada. Si la llamada no ha sido ruteada, el MSC no permitirá el acceso al sistema.

FIGURA 2.17

## ERROR DEL AUTHR EN LA ORIGINACION



## 2.6.2 FALLA DEL RANDC EN LA REGISTRACIÓN Y ORIGINACIÓN

El parámetro RANDC son los ocho bits más significativos del RAND. Es usado para indicar cual RAND debe ser usado por un móvil para procesar una respuesta de autenticación. Cuando un móvil o una celda la cual es adyacente a las celdas servidas por otros MSCs, trata de acceder a un sistema el cual requiere autenticación, es posible que el móvil haya levantado el RAND de un sistema adyacente y lo haya usado para ese RAND, para generar el AUTHR.

Para tener seguridad de que el valor correcto del RAND sea usado para autenticar el móvil, el sistema servidor tiene que ser capaz de manejar las situaciones erróneas del RANDC.

En la siguiente sección se describe como el MSC verifica si es un verdadero RANDC erróneo para situaciones ambiguas que mencionaremos más adelante. En todas las otras situaciones, un mensaje Authentication Failure Report, con el "RANDC erróneo" es enviado al Centro de Autenticación del móvil.

### 2.6.2.1 CELDA ADYACENTE Y EL RANDC NO IGUAL A CERO

Cuando el MSC detecta un RANDC erróneo, si el móvil está en una celda adyacente y el RANDC recibido es un valor diferente de cero, el MSC tiene las dos siguientes opciones: Enviar un RANDREQ a sistemas adyacentes para tener el RAND apropiado, o iniciar el Unique Challenge al móvil. Es importante que este escenario de un RANDC erróneo diferente de cero recibido desde el móvil en la celda adyacente, debería solamente ocurrir para móviles en el canal de control analógico, debido al hecho de que el RAND no puede ser transmitido en cada OMT en el canal de control analógico. Para móviles que soporta IS 136 con celdas CDMA con canal de control digital, mientras estos móviles sean requeridos para leer los parámetros desde el DCCH/canal pagen, este escenario, no debería ocurrir. Hasta que el RANDREQ no sea soportado en el sistema de autenticación, el MSC tiene que iniciar el Unique Challenge para autenticar el móvil. Si el SSD es compartido, el VLR puede iniciar el Unique Challenge en el móvil. De otra forma, el MSC enviará un Authentication Request con el parámetro llamado tipo de acceso del sistema para que sea puesto de una manera no especificada al Centro de Autenticación y forzar a esta entidad para que responda con un Unique Challenge.

Basado en los resultados del Unique Challenge, si el SSD no es compartido, el MSC envía un Authentication Status Report al Centro de Autenticación con el parámetro

Unique Challenge Report (UCHALRPT). El parámetro UCHALRPT indica la salida del Unique Challenge iniciado por el Centro de Autenticación o por el MSC/VLR.

Este parámetro puede contener los siguientes valores:

- Unique Challenge no intentado: la operación no es intentada debido a operaciones del sistema.
- Unique Challenge sin respuesta: ninguna respuesta es recibida desde el móvil,
- Unique Challenge exitoso: es decir, que la comparación del AUTHU ha sido exitosa
- Unique Challenge fallado: quiere decir que la comparación del AUTHU a fracasado.

Si el SSD es compartido y el Unique Challenge ha fallado, el MSC envía un Authentication Failure Report (Reporte de falla de autenticación) al Centro de Autenticación para reportar la falla de Autenticación.

• **Registración.**- Hasta que solamente las registraciones iniciales sean autenticadas, no hay un VLR entrante para el móvil, tal que el SSD compartido no sea posible.

1. Si el AUTH = 1 es transmitido en el OMT. Hasta que el AUTH siga siendo igual a 1 el móvil lee el valor del RAND desde el OMT para ser usado, de tal forma que se genere el AUTH.

2. El móvil envía el mensaje de registro conteniendo el mensaje de registro del AUTHR generado tan bien como el RANDC para el MSC. El MSC entonces valida el RANDC recibido. En este caso un RANDC erróneo es detectado. El MSC decide ejecutar un Unique Challenge en el móvil.
3. Este escenario en la interfase aérea es el AMPS /TDMA y el móvil está en la celda adyacente. Si la interfase aérea es el canal de control digital DCCH/TDMA o la celda no es una celda adyacente, entonces el reporte de falla de autenticación con el tipo de reporte puesto como "RANDC erróneo" es enviado.  
El AFREPORT es enviado puesto que el RANDC erróneo no debería ocurrir para estas interfaces aéreas o en las celdas. El MSC envía una solicitud de autenticación al Centro de Autenticación del móvil con el sistema de acceso puesto "no especificado" para solicitar al Centro de Autenticación, y poder iniciar el Unique Challenge en la respuesta.
4. El HLR posiciona el temporizador ACBOUND y rutea el mensaje de solicitud de autenticación al Centro de Autenticación. Durante la recepción del mensaje, el Centro de Autenticación corre el CAVE para generar el AUTH.
5. El Centro de Autenticación envía una respuesta de Autenticación al HLR con los parámetros del Unique Challenge.
6. El HLR actualiza el temporizador ACBOUND y rutea el mensaje de respuesta de autenticación al MSC. Cuando el mensaje es recibido por el MSC, el MSC para el temporizador del ACBOUND.

7. El MSC envía la orden del Unique Challenge a la celda en la cual el móvil trató de registrarse en la celda y en las celdas adyacentes. Si el MSC recibe los parámetros del Unique Challenge en la respuesta AFREPORT para un móvil DCCH, el MSC envía la salida de registraci3n al móvil con congesti3n tal que la raz3n de falla con un tiempo de re-registraci3n de un minuto. El MSC envía al móvil en modo libre en el cual es capaz de recibir otros mensajes. Durante el tiempo libre, el MSC re-envía la orden del Unique challenge una vez más. Si el MSC recibe los parámetros del Unique Challenge en la respuesta AFREPORT para una estaci3n móvil en modo CDMA, el MSC ejecuta el Unique Challenge en el móvil CDMA por el envío de la orden del Unique Challenge a todas las celdas en el sistema. La orden del Unique Challenge es enviada solamente una vez.
8. Durante la recepci3n de la orden del Unique challenge, el móvil computa el AUTHU y envía una confirmaci3n de la orden del Unique challenge con el AUTHU al sistema servidor MSC. Cuando el MSC recibe la confirmaci3n de la orden del Unique Challenge, se compara los valores del AUTHU. En este caso la comparaci3n si tiene éxito. Con una operaci3n exitosa del Unique Challenge en el móvil, el mensaje REGNOT para el HLR y el ASREPORT para el Centro de Autenticaci3n son enviados en paralelo. Esto reduce de gran manera el retardo de registraci3n de un móvil auténtico en el HLR.
9. El MSC luego pone un temporizador ACBOUND y envía un reporte del status de autenticaci3n al HLR.

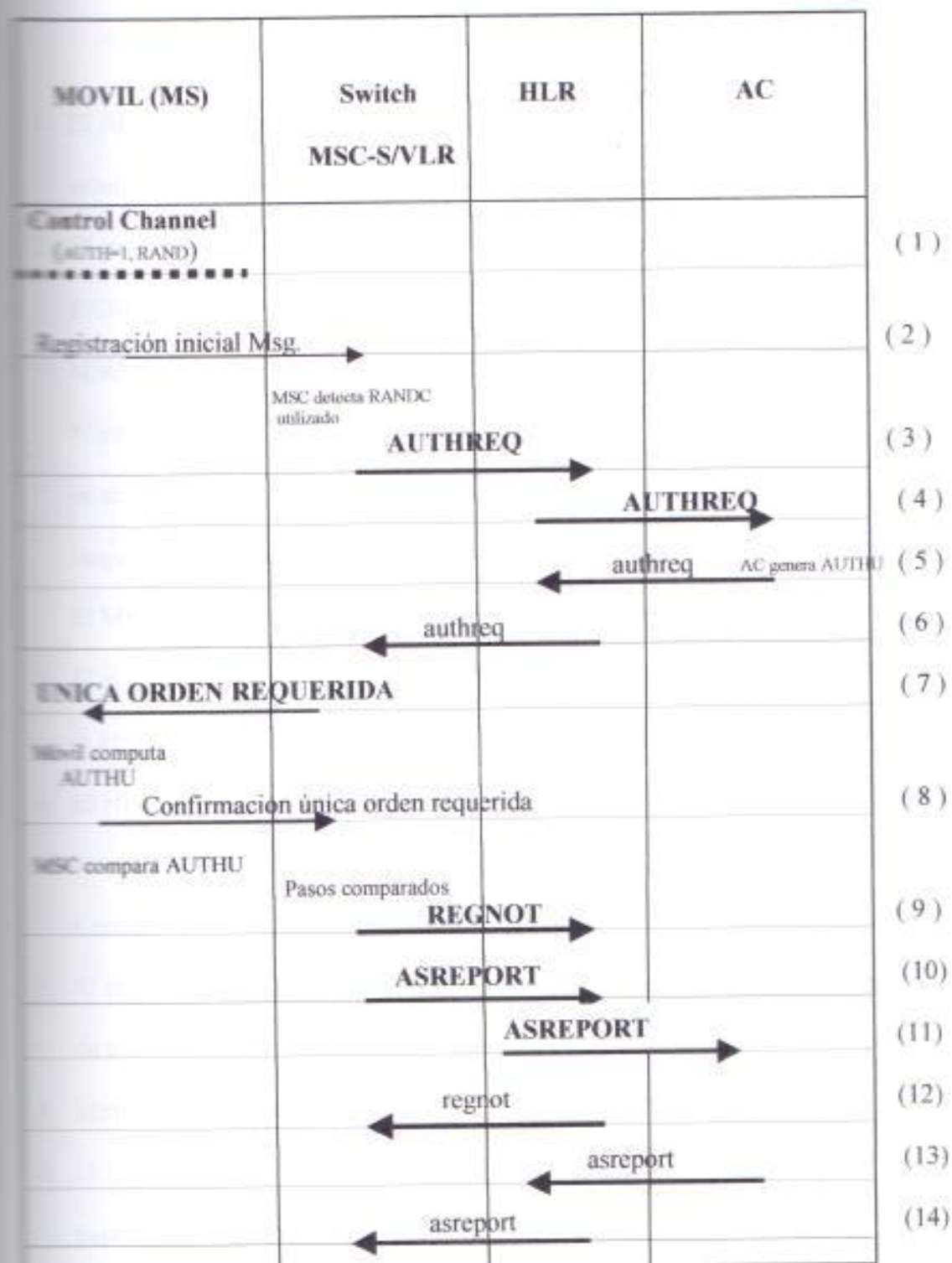


10. El HLR posiciona el temporizador ACBOUND y rutea el reporte del estatus de autenticación al Centro de Autenticación.
11. El centro de Autenticación envía una respuesta del reporte del status de autenticación al MSC.
12. El HLR actualiza el temporizador del ACBOUND y rutea la respuesta de reporte del status de autenticación al MSC. Durante la recepción el mensaje, el MSC servidor actualiza el temporizador ACBOUND y no toma acción alguna hasta que la autenticación haya pasado.
13. Cuando el MSC recibe la respuesta de autenticación, determina que la autenticación fue un éxito y envía un mensaje de notificación a los móviles en el HLR. En este momento el temporizador ACBOUND es cancelado.
14. El HLR confirma el mensaje de registración con una respuesta de notificación para la registración.

---

Si el Unique Challenge fracasa o el móvil no responde a la orden del Unique Challenge, el MSC/VLR envía un mensaje ASREPORT indicando el resultado. Más comúnmente el Centro de Autenticación especificará la negación del acceso del móvil en el mensaje de respuesta. El MSC abortará el proceso de registración en este caso.

**FIGURA 2.18**  
**REGISTRACIÓN EN LA CELDA ADYACENTE Y EL RANDC NO**  
**IGUAL A CERO**



- **Originación.**- Semejante al mensaje de registraci3n inicial, el SSD compartido es posible en el flujo de mensaje de originaci3n.

1. El AUTH = 1 es transmitido en el OMT hasta que el AUTH = 1 sea verdad, el m3vil lee el valor del RAND desde el OMT para ser usado y generar el AUTHR.
2. El m3vil en la celda adyacente envia el mensaje de originaci3n conteniendo el RANDC y el valor generado del AUTHR al centro de autenticaci3n. Cuando el MSC recibe el mensaje de originaci3n, ejecuta la validaci3n del MIN/ESN. Mientras un VLR entrante v3lido ya exista, el MSC determina el m3vil es capaz de ser autenticable desde la informaci3n almacenada en el VLR entrante. El MSC luego valida el RANDC recibido. En este caso, un RANDC err3neo es detectado. El MSC decide ejecutar un Unique Challenge en el m3vil.
3. Si el SSD no es compartido, el MSC/VLR posiciona el temporizador ACBOUND y envia una solicitud de autenticaci3n al HLR del m3vil.
4. El HLR posiciona el temporizador ACBOUND y rutea el mensaje de solicitud de autenticaci3n al Centro de Autenticaci3n. Durante la recepci3n del mensaje, el Centro de Autenticaci3n corre el algoritmo CAVE para generar el AUTHU.
5. El establecimiento de la llamada contin3a esperando por el mensaje de respuesta de autenticaci3n.
6. Idem en el punto 5.
7. El Centro de Autenticaci3n recibe una respuesta de autenticaci3n al HLR con los par3metros del Unique Challenge.

8. El HLR actualiza el temporizador ACBOUND y rutea el mensaje de respuesta de autenticación al MSC.

Como el mensaje recibido por el MSC, entonces el MSC para el temporizador ACBOUND.

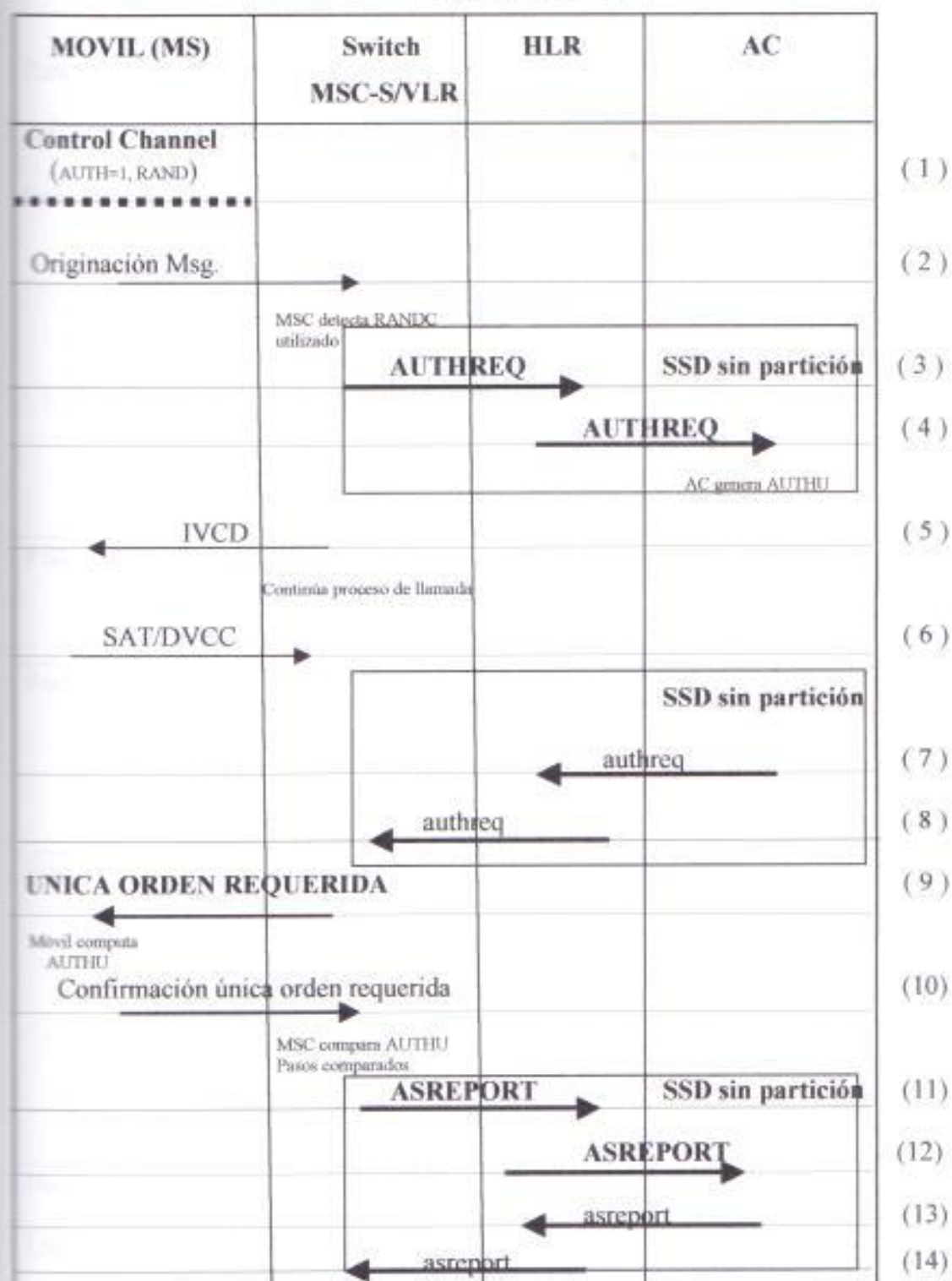
9. El MSC envía una orden del Unique Challenge al móvil.
10. Durante la recepción de la orden del Unique Challenge, el móvil procesa el AUTHU y envía una orden de confirmación del Unique Challenge con el AUTHU al sistema servidor MSC.

Cuando el MSC recibe la orden de confirmación del Unique Challenge, compara los valores del AUTHU. En este caso la comparación tiene éxito.

11. El MSC entonces posiciona un temporizador ACBOUND y envía un Reporte del Status de autenticación al HLR.
12. El HLR posiciona el temporizador ACBOUND y rutea el Reporte del Status de autenticación al Centro de Autenticación.
13. El Centro de Autenticación envía una respuesta del Reporte del Status de autenticación al MSC.
14. El HLR actualiza el temporizador ACBOUND y rutea la respuesta del Reporte del Status de autenticación al MSC.

Durante la recepción del mensaje el MSC servidor actualiza el temporizador ACBOUND y no toma acción alguna hasta que la autenticación haya pasado.

**FIGURA 2.19**  
**ORIGINACIÓN DE LA CELDA ADYACENTE Y EL RANDC NO**  
**IGUAL A CERO**



## 2.7 MOVILES AUTENTICABLES

Para finalizar este capítulo de autenticación es necesario conocer que móviles son autenticables para que tanto la operadora celular y el proveedor conozcan las bondades del sistema en cuestión.

**Tabla 2.2**

### TELEFONOS CELULARES AUTENTICABLES

PROVEEDOR	PRODUCTOS AUTENTICABLES	PROGRAMA A-KEY VIA EXTERNA PUERTO/DATOS	PROVEE ESPECIFICACION PROGRAMADA
Audiovox	MVX401, 405, 406, 430, 460, 465, 530, 560, 800A, 350A, BC66A, SP96A, CTX3600A, PRT9100AU	Algunos productos	podría cooperar con el cliente
Ericsson	AH600, SERIES, AF738, AH210, AH220, AH230, AH238, AH310, AH320, CT500, CT510, CT550, CT750, CT800, Productos posteriores a Mayo 96	si	si
Hughes	todos	no	No
Lucent	AT&T 3740, 3810A, 3812A,	si	no

	LUCENT, 6735, 6820, 6840		
Matsushita / Panasonic	H63, H64, H65, H66, PH55	Solo a través de la Red de Servicio Panasonic	Validable para cualquier compañía bajo NDA
Mitsubishi	AH129, AH131	DNR	DNR
Motorola	Todos EE3, todos los productos actualmente embarcados	si	si
NEC	Talk Time 800 series, TT900	si	Para key agentes autorizados
<b>PROVEEDOR</b>	<b>PRODUCTOS AUTENTICABLES</b>	<b>PROGRAMA A-KEY VIA EXTERNA PUERTO/DATOS</b>	<b>PROVEE ESPECIFICACION PROGRAMADA</b>
Nokia	Todos bajo producción incluyendo el 100AU, 232AU, 2120, 2160, 2190	si	no
OKI	Todos los análogos OP' 1400 series	si	Validable para reconocidas compañías y bajo NDA
Philips Consumer Comunicaciones	TA-610 (Amps)	si	no
Qualcomm	Todos los productos	no conocido	no conocido
Sony	Análogos 777888 series, CMRX100, CMD500, 600	no conocido	no conocido
Uniden	PCD1000, PCD2000	si	si

## CAPITULO III

### DISEÑO Y SIMULACION DEL SISTEMA DE AUTENTICACION

#### **3.1 OBJETIVO**

El objetivo de nuestro diseño de un Centro de Autenticación celular será darle una seguridad y eficiencia a las operadoras celulares, de tal forma que sus clientes no se sientan afectados debido a la presencia de personas dedicadas al fraude telefónico que tratan de clonar los teléfonos celulares o de cualquier otra manera, de dejar en la quiebra a las compañías telefónicas públicas y celulares. Además en nuestro diseño



haremos dos recomendaciones para configurar las operadoras antes mencionadas, la una será un Centro de Autenticación Interno a la red celular y la otra será la de un Centro de Autenticación Externo a la red celular.

Pues de todo lo dicho anteriormente las características del Centro de Autenticación Celular son las de detectar la presencia de teléfonos celulares no autorizados, mantener la autenticación de los datos de un móvil, ejecutar la validación de los móviles, proveer información de autenticación al MSC servidor cuando sea necesario y tener acciones de control en cualquier falla de autenticación. Estas características para la implementación de nuestro Centro de Autenticación deben ser complementadas por un sistema de señalización IS-41 revisión C de tal forma que confirme la identidad del móvil. El Centro de Autenticación será una nueva identidad lógica en la red celular, que trabajará sobre este protocolo.

### 3.2 OPERACIONES DEL CENTRO DE AUTENTICACIÓN

Para detallar un poco más, el Centro de Autenticación tendrá la responsabilidad de:

- Mantener una base de datos de la información de autenticación del móvil.
- Accesos de la validación de acceso móvil. El Centro de Autenticación recibe los mensajes AUTHREQs en varios requerimientos de accesos al sistema y verificar la autenticidad de ese móvil con el uso del algoritmo CAVE.

- Manejar posibles fallas de autenticación. Si el Centro de Autenticación detecta una falla mientras se procese el AUTHREQ o sea notificado de un problema mediante un mensaje AFREPORT entonces este mensaje debe reaccionar de acuerdo a la forma en que haya sido configurado el Centro de Autenticación para manejar fallas.
- Actualizar el SSD del móvil. El Centro de Autenticación puede iniciar una actualización inmediata a un móvil mediante un AUTHDIR o esperar que el próximo acceso del Centro de Autenticación y actualice el SSD en ese punto por la inclusión de los parámetros del SSD actual en un mensaje de respuesta regresando al MSC/VLR.
- Los mensajes BSCHALL del proceso IS-41. El Centro de Autenticación calcula el resultado Base Station Challenge apropiado cuando sea solicitado por el sistema servidor.
- Los mensajes ASREPORT del proceso IS-41. Cualquier momento el Centro de Autenticación solicita el MSC/VLR para ejecutar una transacción de autenticación, por ejemplo un actual SSD o Unique Challenge, el sistema servidor envía un ASREPORT al Centro de Autenticación para informar el resultado de la información del Centro de Autenticación.

### 3.3 CONFIGURACIONES DEL CENTRO DE AUTENTICACIÓN

En esta sección daremos a conocer las posibles configuraciones de los Centros de Autenticación que serán necesarias para nuestra tesis. Para lo cual tomaremos como interface protocolaria de red, al estándar IS-41 revisión C, dentro de la red celular.

Como ya se mencionó el Centro de Autenticación se responsabilizará del mantenimiento de la base de datos en la cual se encuentra información de validación de los móviles, además que se generaran los mensajes del estándar IS-41 C de las identidades funcionales de red como son el MSC, HLR, VLR y el AC.

El Centro de Autenticación puede ser instalado externamente al switch de la empresa portadora o bien internamente, por medio de enlaces IS-41, en los siguientes gráficos en donde se explica mejor la estructura:

El Centro de Autenticación estará provisionado con el hardware y software requerido que nosotros lo enunciaremos más adelante en este capítulo, y daremos a conocer los beneficios del sistema de autenticación que queremos implementar.

FIGURA 3.1

### ARQUITECTURA INTERNA DEL SISTEMA CON UN AC EXTERNO

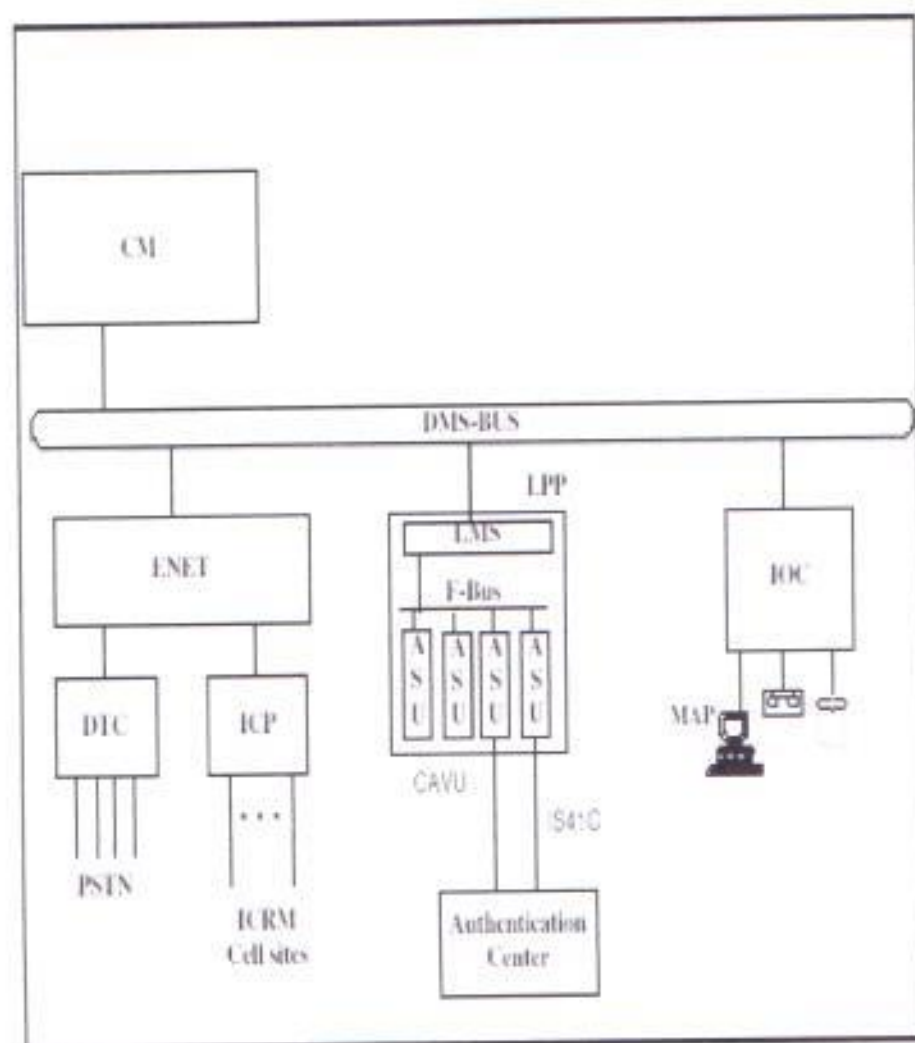
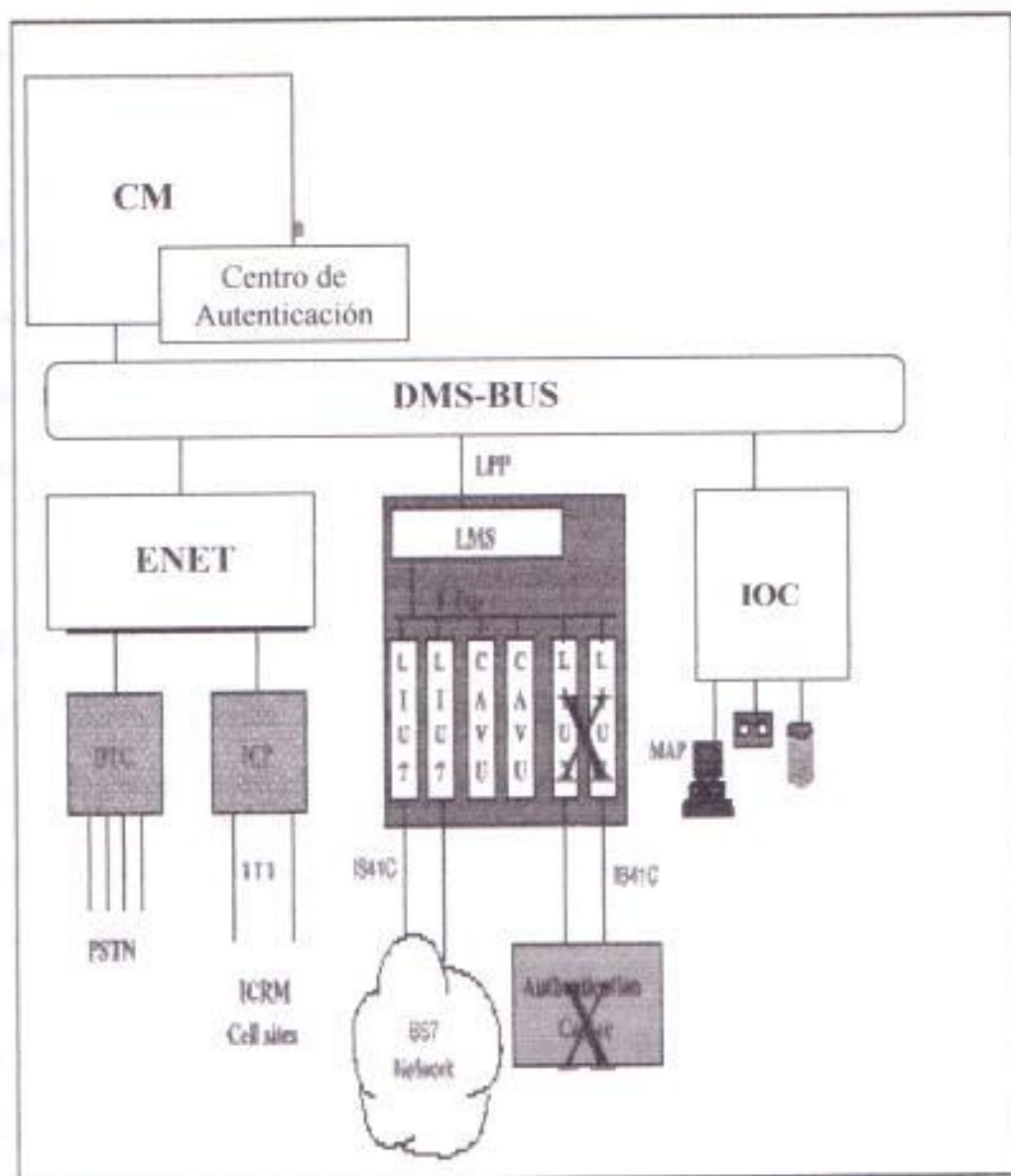


FIGURA 3.2

## ARQUITECTURA DEL SISTEMA CON UN AC INTERNO



### 3.3.1 DOS REGIONES DE COBERTURA CON UN SOLO CENTRO DE AUTENTICACIÓN EXTERNO.

En este escenario de autenticación tenemos a dos regiones de cobertura denominada MSC-A y MSC-B los cuales se enlazan a un Centro de Autenticación común en donde se encuentra la base de datos de ambas regiones.

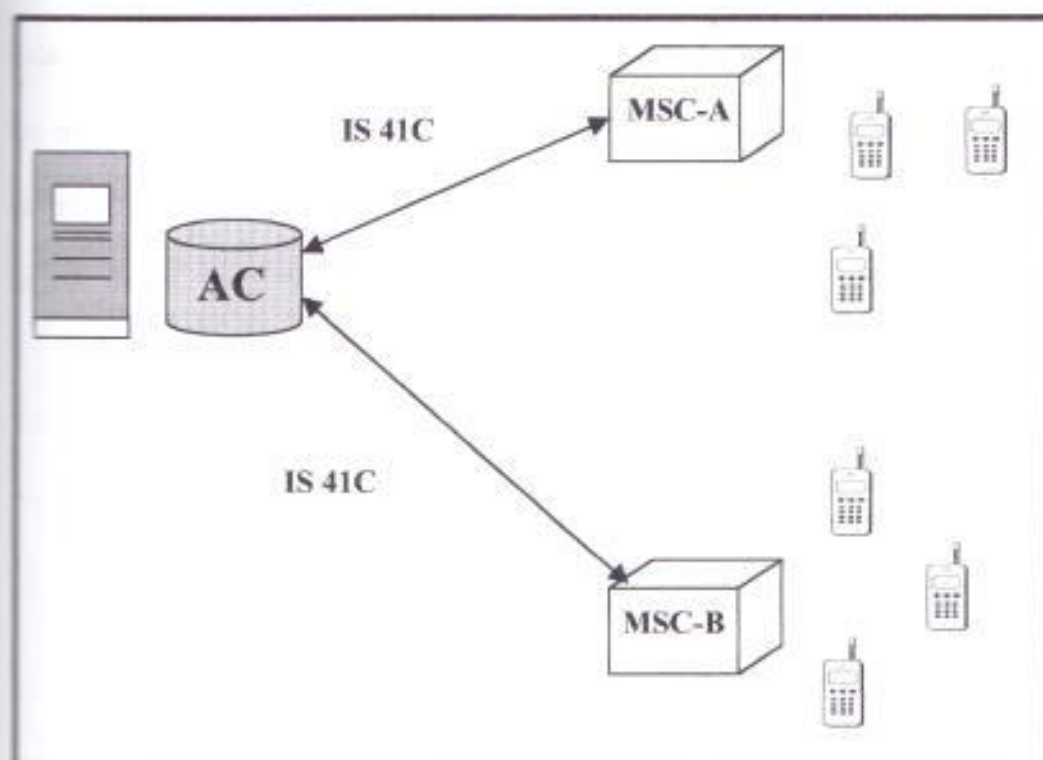
Ambas regiones de cobertura están enlazadas con el Centro de Autenticación a través de dos enlaces directos y dedicados con protocolo IS41C. Cabe destacar que el Centro de autenticación es del tipo externo, dicho de otro modo no necesariamente esta dentro del switch.

Los abonados de la región MSC-A serán autenticados a través de su propio switch por los enlaces IS41C que este tiene con el centro de autenticación. También los abonados de la región MSC-B serán autenticados a través del switch de su misma región por los enlaces IS-41 que este tiene con el Centro de Autenticación.

Como ventaja de este escenario es que al usar un solo Centro de Autenticación se optimiza la red por que la llamada de un usuario roamer no debe de pasar a través de mas de un switch para ser autenticado como sucede en otros escenarios.

FIGURA 3.3

### DOS REGIONES DE COBERTURA CON UN SOLO CENTRO DE AUTENTICACIÓN EXTERNO



### 3.3.2 DOS REGIONES DE COBERTURA CON DOS CENTROS DE AUTENTICACIÓN EXTERNOS PROPIOS.

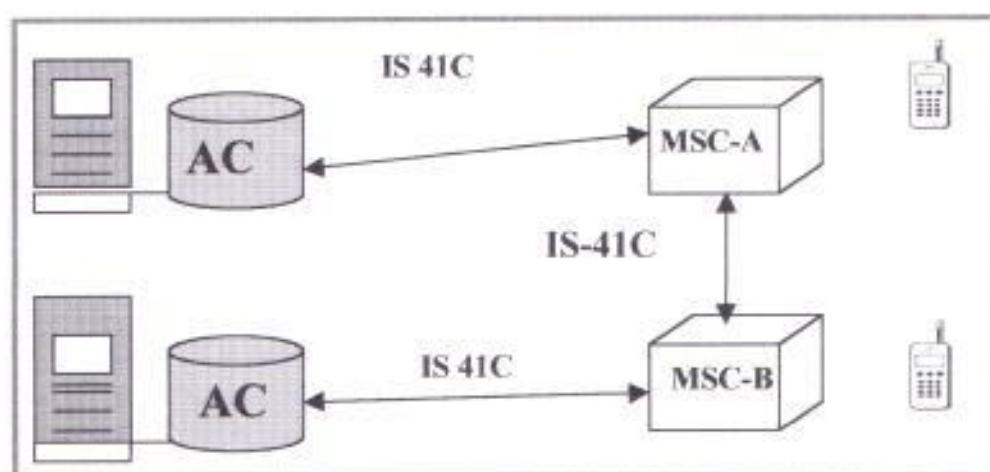
En este escenario de autenticación tenemos a dos regiones de cobertura denominadas MSC-A y MSC-B las cuales tienen su propio centro de Autenticación cada una. En este escenario los abonados de cada una de las regiones se autentican en su propio centro de autenticación a través de su respectivo MSC, gracias a un enlace IS41C que

hay entre los AC y los MSC respectivos. Los móviles se comunican al MSC a través de la interface aérea de las estaciones base con los respectivos protocolos como son IS136, IS54B e IS91.

Este tipo de escenario obliga a que haya un enlace IS-41 entre las dos regiones, para que los usuarios roamer puedan autenticarse en su propio AC. Esta es la desventaja que encontramos en este tipo de escenario. También si el usuario es un roamer se suma un retardo por que primero tiene que pasar por el MSC servidor para poder autenticarse.

FIGURA 3.4

**DOS REGIONES DE COBERTURA CON DOS CENTROS DE AUTENTICACIÓN EXTERNOS PROPIOS.**





### 3.3.3 DOS REGIONES DE COBERTURA CON SUS CENTROS DE AUTENTICACIÓN INTERNOS RESPECTIVAMENTE

En este escenario de autenticación tenemos a dos regiones de cobertura denominadas MSC-A y MSC-B las cuales tienen sus centros de autenticación internos.

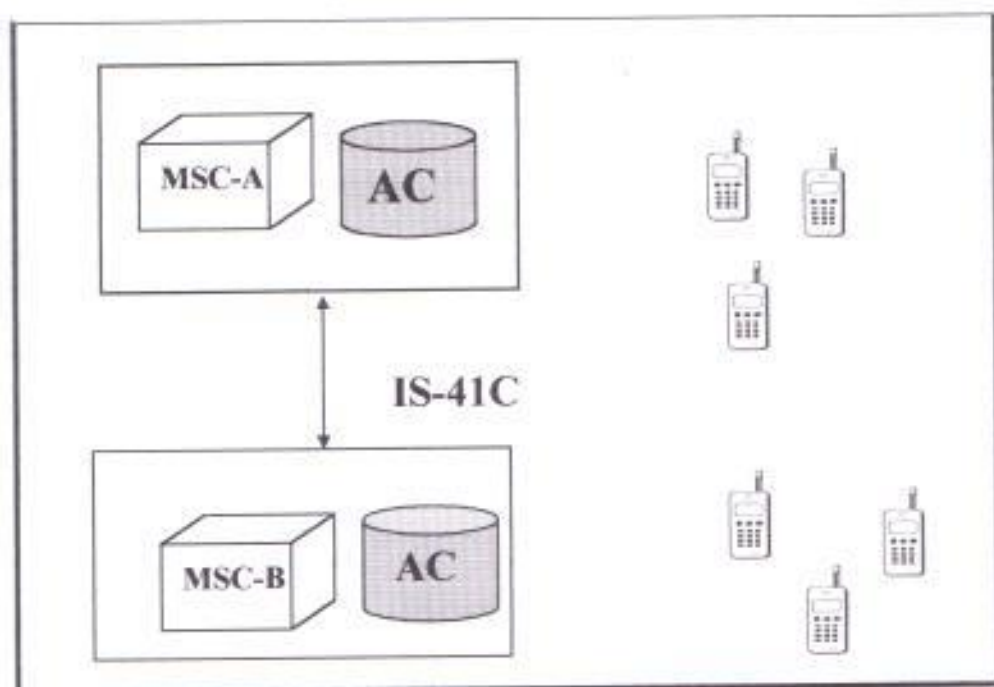
En este escenario los usuarios que hagan roaming pueden autenticarse de manera satisfactoria dentro de sus respectivos Centros de autenticación pero sin la necesidad de que el proceso de autenticación se retarde ya que tanto el MSC y el Centro de Autenticación se encuentran integrados en un mismo nodo de red.

En este escenario se optimiza aún más la red de señalización IS 41C ya que podemos apreciar, solo necesitamos de dos nodos de red, lo cual hace más factible la comunicación entre la red y los usuarios.

No cabe duda que en esta configuración hay una íntima conexión entre los dos sistemas, ya que la información de la base de datos puede actualizarse, y tanto los procedimientos de actualización del SSD y el Unique Challenge son válidos, puesto que los SSD's de las dos regiones son compartidos.

FIGURA 3.5

**DOS REGIONES DE COBERTURA CON SUS CENTROS DE AUTENTICACIÓN INTERNOS RESPECTIVAMENTE.**



**3.3.4 DOS REGIONES DE COBERTURA CON UN CENTRO DE AUTENTICACIÓN INTEGRADO EN UNA DE ELLAS.**

En este escenario de autenticación tenemos a dos regiones de cobertura denominadas MSC-A y MSC-B las cuales tienen la particularidad de que hay un solo centro de autenticación en la primera región mencionada. Para proceder a la autenticación los suscriptores de la región MSC-A podrán tener acceso en su área de cobertura pero cuando los suscriptores de la región MSC-B hagan roaming ellos necesitarán

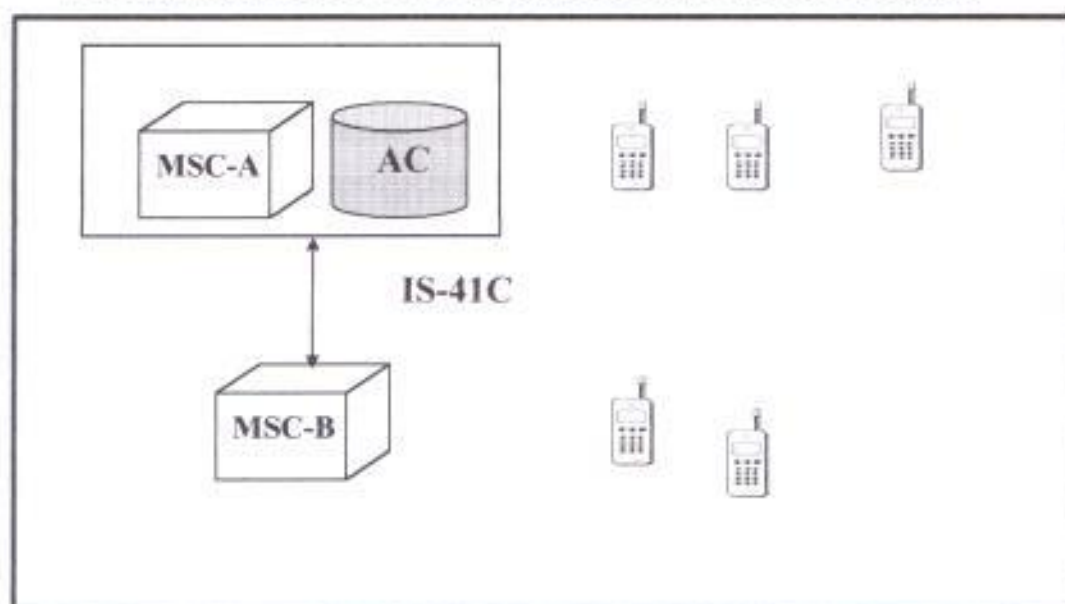
registrarse en el MSC de su región y luego mediante el enlace IS 41C la información de sus llamadas serán validadas al Centro de Autenticación de la región MSC-B.

No obstante existen en esta configuración dos puntos que hay que recalcar:

- El tiempo que tarda el proceso de autenticación en validar el teléfono celular del suscriptor que haga roaming será un poco más largo que cualquier otro escenario de autenticación ya visto.
- El enlace IS 41C entre las dos regiones debe ser el apropiado para que no haya congestión de tráfico en la señalización.

FIGURA 3.6

**DOS REGIONES DE COBERTURA CON UN CENTRO DE AUTENTICACIÓN INTEGRADO EN UNA DE ELLAS**



## 3.4 PLANIFICACIÓN DEL SISTEMA DE AUTENTICACIÓN

### 3.4.1 OBJETIVOS DE LA PLANIFICACIÓN

Nuestro sistema de autenticación necesita ser planificado para solucionar la presencia del fraude, consistiendo de una investigación minuciosa para darle servicios a la red y proyectarla como un producto de detección de fraude. La planificación de los Centros de Autenticación en redes ya diseñadas tienen tres metas importantes.

1. **Asistir al operador de red para minimizar pérdidas y costos de operación debido al fraude.** Esto es llevado a cabo por la extensión de cobertura, es decir detectar muchos tipos de fraude, precisando la detección, habilitando respuestas rápidas y proveyendo la administración de cualquier tipo de casos.
2. **Establecer protección rápida, confiable y predecible.** Esto es llevado a cabo por el uso de herramientas comprobadas, un equipo de implementación experimentado, y una metodología de trabajo que sea exitosa.
3. **Sustentar la protección que muestre cambios en el medio ambiente de negocios y conocer las técnicas usadas por los perpetradores fraudistas.** Esto es llevado a cabo por la habilidad que tenga el operador de confeccionar la solución del negocio celular y la naturaleza de los cambios de fraude, con el fin de graduar la base del

subscriber a medida que esta crezca, y tener una obligación a largo plazo para la evolución continua de la esencia del producto que en este caso sería el Centro de Autenticación.

Después de entender las metas de la planificación debemos mencionar que técnicas se pueden implementar:

- Programas basados en computadoras que fueron desarrollados con el propósito de automatizar el proceso de autenticación para manejar grandes volúmenes de registros de llamadas de datos, así pues aumentando la eficiencia de un analista que haya trabajado en ambientes de fraude, quien previamente haya trabajado con sistemas semiautomáticos y este basado en investigaciones sobre grandes volúmenes de datos.
- Se requerirá de sistemas expertos que sean usados con el propósito de darle inteligencia al sistema de autenticación y correlacionar la información del AC, reduciendo los millones de registros de llamadas de datos en miles de alarmas y solamente en centenas de casos.
- Interconectar e integrar los sistemas de negocios de varias operadoras celulares, para permitir la interacción cercana en tiempo real, de tal forma que se reduzca los ciclos de procesamiento de varias semanas o días.

### 3.4.2 METODOLOGÍA

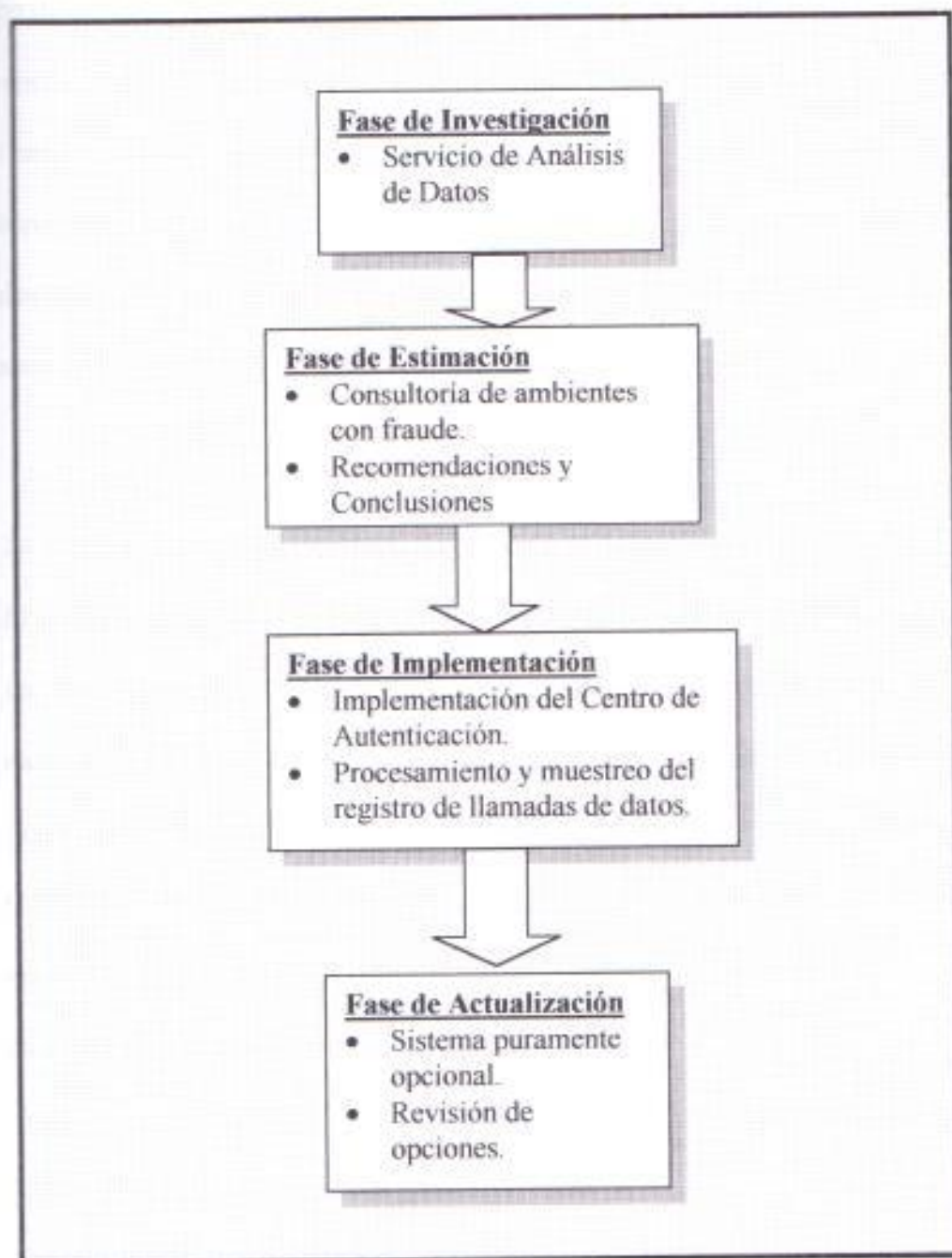
La metodología de trabajo para nuestra planificación será un proceso paso a paso para minimizar el impacto del uso fraudulento de la red. Para esta metodología se requieren de cuatro etapas, estas son:

- **Investigación**
- **Estimación**
- **Instalación y entrenamiento.**
- **Actualización**

El propósito de la metodología se contempla en dos puntos:

- Comprender la necesidad de los operadores celulares con el propósito de que el sistema se ajuste a los recursos apropiados y técnicas para la identificación y reducción de fraude.
- Ayudar a los operadores celulares, con el fin de entrenarlos y educarlos para que ellos no caigan en tentativas fraudistas que existan en el medio.

FIGURA 3.7

**CRONOGRAMA DE ACTIVIDADES PARA LA PLANIFICACION DEL SISTEMA DE AUTENTICACION**

### 3.4.2.1 FASE 1: Investigación

Durante la fase I se discute el fraude con el operador celular. Si hay una persona o un grupo de personas cuyo trabajo principal es manejar el fraude dentro de la organización del operador celular, entonces el operador celular está enterado del trato del fraude. En este caso, a menudo, los analistas del fraude ya han sido designados y han tratado el problema del fraude. En un proceso laborioso - intensivo usando algunas herramientas locales o reportes. Durante la fase de investigación, se abarcará la siguiente información:

- La infraestructura de la red actual y el plan de crecimiento de la red.
- El impacto relativo de diferentes tipos de fraude (suscripción, técnico, etc.)
- La disponibilidad de fuentes de información (Registro de llamadas desde los switches, base de información del suscriptor, subsistema de crédito y cobranzas)
- Los servicios de valor agregado listos en uso o planificados para ser usados como Correo de voz, Servicios de Mensajes Cortos y otros sistemas de soporte de operación que puedan interconectarse con el sistema de autenticación.
- La exploración geográfica a ser considerada.
- Los perfiles ya identificados por los grupos de clientes y su importancia relativa (Negocios de usuarios, usuarios domésticos, etc.)
- La importancia de los canales de distribución (Distribuidores de servicio)



- Aspectos legales específicos del país que capacitan o previenen la implementación.

El costo de la fase 1 es mínimo: No necesita de equipos o adquisición de licencia de software que sea requerida por el operador.

Después de presentar el resultado del análisis de servicio de datos al operador, la fase de investigación es completada y empieza la fase 2.

### **3.4.2.2 FASE 2: Estimación**

Durante el estudio de estimación, es importante que el proveedor del sistema de autenticación y el proveedor decidan que se puede hacer para minimizar el fraude. Hasta que cada negocio del operador sea diferente de otros proveedores y hasta que cada operador tenga un problema de fraude diferente de otros proveedores, los resultados del estudio serán específicamente dirigido al proveedor. La información confidencial es discutida y no es expuesta a individuos fuera de la organización del operador.

La estimación es importante para clientes que ya están enterados del tema, ya que es una manera fácil para decidir que hay que hacer acerca del trato serio del fraude. Adicionalmente, las mejoras para procedimientos existentes y las políticas propuestas son a menudo discutidas, permitiendo al portador desarrollar o mejorar su estrategia

para la administración del sistema de autenticación. Esta estrategia tiene 5 áreas importantes de enfoque para el fraude: Aviso, Prevención, Detección, Equilibrio defensivo y Entrenamiento. La corrida de la estimación durante esta fase hace que sea más fácil para el operador encontrar respuestas a estas preguntas.

Esta fase es también importante porque provee al operador y a la organización de entrega con información sobre el tamaño y la potencia del sistema que es requerida más tarde durante la fase 3 y la fase 4. Basado en esta información la operadora y el operador de Sistema de Autenticación pueden hacer un plan acerca de los recursos, duración, hardware y financiar los fondos. Inicialmente, el sistema es valorado para soportar la base del subscriber corriente del proveedor, permitiendo para un valorado año de crecimiento de acuerdo a los planes de crecimiento del operador.

En esta etapa se provee las siguientes distribuciones principales:

- Encontrar propuestas en cada una de las 4 áreas de enfoque: (Aviso, Prevención, Detección, Equilibrio Defensivo, y Entrenamiento).
- Documentación de requerimientos especiales validados, incluyendo requerimiento de negocios, requerimiento del usuario, y requerimientos técnicos, para la comercialización del sistema de autenticación.

- Documento específico de integración que detalle todas las interfaces para el sistema de administración de fraude con otros sistemas, tanto como un registro de llamadas e información del subscriptor.

- Un plan de implementación alineado al ambiente específico del operador.

Todas estas propuestas estarán basadas en la información recogida al entrevistar al personal de servicios al cliente, al personal de ingeniería, tarificación, contabilidad, mercadeo, ventas, la parte de liderazgo administrativo, y la parte gerencial. También se revisará la documentación técnica (interfaces, MSC, HLRs, VLRs, Centros de Autenticación y otros sistemas de aplicación relevante), y ciertos reportes relacionados al fraude que pueden ser proveídos por el operador.

Basado en opiniones que han sido validadas con el operador y basadas en la documentación proveída por el cliente se procederá a la ejecución de la siguiente fase, que es la implementación.

### **3.4.2.3 FASE 3: Implementación.**

Basado en los resultados de la Fase 2: Estimación, el proveedor será capaz de instalar el sistema de autenticación que traerá beneficios significantes en la habilidad de la operadora celular para detectar y administrar el fraude: el sistema estará estrechamente

alineado con las funciones de detección de fraude en las situaciones que ocurra dicho problema.

Durante la fase 3 el sistema de autenticación será instalado en un lugar de amplia cobertura que soporte las celdas para dar servicio de autenticación celular esta fase necesita de tres procesos:

- **Transferir conocimientos**

Los proveedores del Sistema de Autenticación deben familiarizar a la operadora con el uso del sistema de administración de fraude de la operadora y presentarle a la operadora de cómo usarlo de una manera efectiva, ayudando en el ajuste de parámetros y adaptándolo al ambiente específico de las necesidades del usuario.

- **Construir estrategias y políticas**

El sistema de administración debe ser poderoso. Debe permitir al operador hacer un nuevo grupo de políticas y decisiones estratégicas sobre el fraude que jamás tuvieron que ser hechas antes, y optimizar los recursos del sistema.

## • Adaptar el sistema

Hasta que el sistema sea instalado para la producción del servicio celular, el sistema de autenticación tendrá algunas situaciones. Estas situaciones son el resultado de discusiones y condiciones iniciadas acordadas que fueron formuladas durante la fase de estimación. Sin embargo es una actividad normal para ajustar varios puntos que estuvieron pendientes. Los cambios que ocurran en esta fase, tanto como definir nuevos parámetros operacionales, equipos; serán adaptados a los resultados actuales de algún fraude sospechoso encontrado por el sistema. Una gran ventaja es que mientras que el sistema este siendo adaptado en un periodo de días y semanas, el fraude significativo será encontrado aunque el sistema no esté perfecto, gracias a un buen sistema de base de datos.

En esta fase se necesita las distribuciones necesarias para llevar a cabo la implementación:

- Instalar el sistema de autenticación, incluyendo las pruebas necesarias de los equipos y la señalización en los enlaces IS-41C y encontrar los requerimientos específicos del operador como se definieron en la fase de Estimación. Además anexar documentación técnica del sistema de autenticación.

- Sesión de entrenamiento a los ingenieros o a los usuarios del área técnica del operador.
- Preparar al staff de la operadora de cómo preparar reportes para darle una efectividad al sistema en operaciones diarias. Estos reportes pueden llevar a recomendaciones para cambios situacionales del sistema en el sistema de autenticación celular

#### **3.4.2.4 FASE 4: Actualización.**

Después de cumplir exitosamente la fase 3, el sistema es puesto en operación. Como un resultado del análisis y el trabajo hecho en las tres fases anteriores, la puesta del sistema en servicio requiere o no de pequeños cambios al software y así mismo en las operaciones. En esta fase se hace una post - instalación del sistema de autenticación.

### **3.5 TRATAMIENTO DEL SISTEMA DE AUTENTICACIÓN**

Después de planificar nuestro sistema de autenticación es necesario darle un tratamiento interno para conocer los perfiles de los usuarios, el procesamiento del registro de las llamadas, las alarmas del sistema, entradas y salida de datos y las funciones de negocios que tenga el sistema con las empresas.

Por otro lado el sistema de autenticación divide la detección del fraude y procesa la respuesta en estas cuatro tareas importantes:

1. Grandes volúmenes de registros de llamadas son filtradas, reducidas y organizadas para transformar los datos en información adecuada específicamente para administrar el fraude.
2. El sistema instalado tiene la inteligencia de identificar eventos que son importantes para administrar el fraude. Estos componentes de detección buscan la actividad sospechosa en el tráfico de las llamadas o dentro de la base subscriptora.
3. El sistema agrega importantes eventos dentro de casos. Un caso es una información apropiada para la administración del fraude, la cual correlaciona alarmas, registro de llamadas relacionadas, información del subscriptor y uso e información individual del perfil del subscriptor.
4. Basado en las políticas de la operadora celular, el sistema hace recomendaciones a los analistas expertos en el fraude, acerca de dar opciones para contrarrestar el fraude para cada caso.

En esta sección veremos 6 tópicos importantes para el tratamiento del sistema de autenticación:

- Procesamiento del registro de llamadas de datos.
- Perfiles del subscriptor.
- Alarmas.

- Entradas y salidas de datos
- Funciones de negocios.
- Interfaces del usuario.
- Reportes.
- Comercialización.

### **3.5.1 PROCESAMIENTO DEL REGISTRO DE DATOS DE LAS LLAMADAS.**

El sistema procesa cada uno de los registros de las llamadas de los usuarios. Cada registro de llamada va hacia un proceso de detección muy rápido para determinar si dicha llamada puede ser relacionada al fraude.

Si un registro de llamada no es sospechoso, este es guardado por el sistema de administración de fraude por un breve periodo de tiempo, como para actualizar la información.

El dato que no es relevante para propósitos de administración de fraude es filtrado en dos etapas dejando solamente al dato relacionado al fraude para el análisis detallado y su presentación para los analistas expertos.



En la primera etapa, el grupo de registros de llamadas es filtrada para producir un subgrupo para el cual los mecanismos de detección puedan generar las alarmas. En la segunda etapa el sistema de autenticación evalúa las alarmas para producir un subgrupo de datos aun más pequeño que es arreglado en los llamados casos. Cada técnica puede ser adecuada mediante parámetros que reflejan la política de negocios de la operadora y sus procesos.

### **3.5.2 PERFILES DEL USUARIO**

El sistema guarda el registro del comportamiento normal de la llamada para cada uno de los subscriptores. Cada registro de la llamada contiene información sobre como los clientes usan sus teléfonos celulares. La información acerca del comportamiento normal de las llamadas de los subscriptores puede incluir lo siguiente:

- Uso local diario
- Numero de llamadas por día
- Duración promedio de llamadas.
- Destino de la llamada.
- Llamadas mixtas.
- Tarifa promedio mensual
- Llamadas roaming.
- Llamadas internacionales roaming.

- Llamadas en espera.
- Conferencia tripartita.

### 3.5.3 ALARMAS

Las alarmas del sistema de autenticación celular son básicamente eventos automáticamente generados por el sistema para el análisis de los registros de las llamadas e información de servicios. Algunas alarmas son una indicación más fuerte de fraude. Otras alarmas pueden indicar que puede haber fraude. El sistema considera que todas las alarmas cuando se construyen un caso específico permite determinar como puede existir un fraude.

Si el sistema cree que puede haber fraude, el sistema compara la información de la llamada en el caso para el perfil del cliente. Si la información de la llamada en el caso es normal para el subscriptor, entonces el sistema puede determinar que no hubo probabilidad de fraude. La operadora puede tener millones de registros de llamadas por día, pero tendría que haber solamente miles de alarmas por día agrupadas en casos.

Además de que el sistema podría detectar los diferentes tipos de fraude, este organiza las alarmas y cualquier información en casos. Cada caso contiene toda la información relacionada con alguna sospecha de fraude para el subscriptor original. Basados en

parámetros que reflejan las políticas de negocios de la operadora, el sistema de autenticación tiene una interface que puede ser ajustada y comercializada para leer la información directamente desde los otros sistemas y aplicaciones ya operacionales. Tanto sistemas como, tarificación, cuidado del cliente y otros sistemas de soporte operacional pueden ser accesados como parte del análisis del caso.

Basado en el contenido de los casos y en las políticas de la operadora, el sistema hará recomendaciones acerca de cómo contrarrestar el fraude. Las recomendaciones son hechas basadas en las políticas del sistema de autenticación y estrategias determinadas por el proveedor. El sistema mostrará las recomendaciones a la operadora junto con toda la otra información relacionada al caso.

### **3.5.4 ENTRADAS Y SALIDAS DE DATOS**

Es necesario conocer los datos entrantes y salientes que pueda manejar el sistema de autenticación celular. La siguiente información, son las entradas que dicho sistema usa durante su procesamiento:

- Registro de llamadas normalizada: Aquí se contempla las llamadas que realizan los usuarios desde los switches; adicionalmente la información contenida es capaz de detectar el fraude.

- **Geografía de intercambio:** En este set de datos se registran las coordenadas de longitud y latitud para habilitar la velocidad de detección.
- **Datos del usuario:** Aquí se registra información básica del suscriptor, incluyendo opcionalmente información acerca de aquellos suscriptores quienes son piratas en sus piratas.
- **Alarmas externas:** Estas alarmas son generadas desde el exterior del sistema de autenticación, además se requieren de alarmas que sean generadas por el sistema de red con señalización número 7, que son para ser usadas para el análisis de detección de fraude. Similarmente tenemos las salidas generadas por el sistema de autenticación.
- **Lista de llamadas fraudulentas:** Esta es una lista específica de llamadas "marcadas" por suscriptor o ciertas llamadas marcadas como fraudulentas por la operadora. La lista de llamadas puede ser usada por el equipo de tarificación para remover tantas llamadas desde la cuenta del suscriptor.
- **Status del suscriptor:** Este es un estado que puede automáticamente o manualmente cambiar el estatus del suscriptor basadas en acciones recomendadas debido a la detección del fraude.
- **Acciones de Activación:** Son acciones específicas basadas en el tipo de fraude detectado, pueden ser directamente incorporados a los teléfonos de los suscriptores, para que cuando sean robados, se pueda suspender el servicio celular de estos.

### 3.5.5 FUNCIONES DE NEGOCIOS

Las funciones de negocios para el sistema de autenticación son específicas para las características de detección, funciones y parámetros manejados por el sistema. Las funciones de negocios son:

- Minutos de uso para diferentes intervalos de tiempo: El umbral de tiempo que puede ser puesto para diversos grupos de subscriptores. Los intervalos de tiempo definidos son tiempo del día, el día (sea este pico o no pico), semana, por mes y por llamada.
- Número de intentos de llamadas para intervalos de tiempo: El tope de los intentos de llamada puede ser puesto para diferentes grupos de clientes basado en el número de llamadas esperadas en periodos de tiempo diferentes, sobre el cual un cliente causará las alarmas a ser generadas.
- Traslape y Chequeo de colisión: Las llamadas simultáneas para un número particular de tarificación puede ser detectado.
- Rastreo de Destino Internacional: Con esta función, se produce la identificación de las llamadas internacionales hechas por un fraudista, las cuales no son consistentes con los patrones normales de las llamadas del cliente. Con esta función se categoriza las alarmas, en alarma severa, alarma inusual.

- **Rastreo de Destino Nacional:** Con esta función se identifican las llamadas nacionales hechas por un perpetrador, las cuales no son consistentes con los patrones normales de llamadas de los clientes.
- **Detección del patrón:** Con esta función se hace una comparación de la llamada o el servicio de datos contra muchos tipos de fraude dentro de un registro. Cualquier llamada al ser comparada con estos patrones de fraude, generará una alarma.
- **Chequeo de la Lista negra:** Todo registro de llamada que sean comparadas en hasta 5 listas negras definidas por la operadora son señaladas por medio de una bandera por el sistema como inicio potencialmente fraudulento.
- **Subscriptores no autorizados:** Son llamadas por las cuales ningún cliente está definido en el sistema, entonces serán marcadas como un subscriptor no autorizado. Adicionalmente, el chequeo de suspensión será ejecutado por cada categoría del servicio denominada como inicio suspendible. Cualquier tipo de llamada hecha bajo suspensión resultará en una alarma.
- **Análisis de alarma:** El análisis es ejecutado a lo largo de diferentes estados tanto como el tipo y severidad de alarmas, número de alarmas, e información del subscriptor.

- **Acciones para contrarrestar el fraude:** El sistema recomienda con cada caso de fraude que las acciones a tomar estén basadas en la agregación y el análisis de alarmas para un suscriptor individual. Estas acciones pueden ser automáticamente iniciadas, en el tiempo de creación del caso o por los analistas.
- **Perfilación del cliente:** El sistema construye y mantiene un perfil compacto para cada cliente. Este perfil es usado durante la fase de análisis. Usando esta técnica, los cambios producidos en el comportamiento de las llamadas de un suscriptor pueden ser mantenidos a horas extras. El perfil de un suscriptor no cambiara cuando el fraude sea sospechado.

### 3.5.6 INTERFACES DEL USUARIO

La siguiente información esta disponible para los analistas de fraude para propósitos de administración antifraude:

- **Lista de casos:** Esta es una lista de casos fraudulentos sospechados generados por el sistema de autenticación la cual es presentada al analista. La información resumida referente a cada caso es mostrada, incluyendo el tipo de fraude sospechado y el nivel de severidad. El analista puede restringir la lista para presentar solamente aquellos casos de interés.

- **Lista de las alarmas y del registro de llamadas:** Las alarmas generadas por un caso de fraude sospechoso es mostrado con la información referente a la información de los registros de llamadas para el subscriptor desde es tiempo en que el caso fue creado. La información detallada acerca de las alarmas y del registro de llamadas es disponible mediante esta interface.
- **Recomendaciones:** Las acciones recomendadas para corregir el caso sospechoso de fraude, son mostrados al analista de fraude. Aquellas acciones que ya han sido tomadas por el sistema son apropiadamente marcadas y el analista tendrá la oportunidad de activar estas medidas correctivas.

### 3.5.7 REPORTE

El analista a parte de recibir información referente a las alarmas y a los tipos de fraude que se originen, deberá recibir también reportes que pueden ser generados por el sistema:

- **Reporte del caso detallado:** Es la información del caso detallado referente a un subscriptor. Además se registran las listas de la información detallada para un caso abierto.
- **Reportes de casos archivados:** Esta es información referente a clientes ya confirmados y casos resueltos de fraude desde días pasados.



- **Reporte promedio de resolución de casos:** Es un resumen de resolución para casos, debidos a tipos de fraude.
- **Reporte de detalles de la resolución de casos:** Este reporte es un estatus de resolución para cada caso dentro de un tiempo específico.
- **Casos por tipo de fraude:** Este es un reporte que muestra el número de casos por cada tipo de fraude sospechoso.
- **Reporte estadístico de alarmas y casos:** Este reporte categoriza el número de alarmas por el tipo de alarmas en un periodo de tiempo específico. También categoriza las alarmas de manera que ellas relacionan casos en un periodo de tiempo específico.
- **Alarmas por tipo de alarmas:** Este es un reporte del número de alarmas de cada tipo de alarmas generadas en un intervalo de tiempo.
- **Reportes del Patrón de Registro de llamadas:** En estos reportes se detalla y se resume el procesamiento del sistema de detección para todos los patrones y por cada patrón contra los registros de datos del suscriptor.

- **Reporte del perfil del subscriptor:** Este reporte lista la salida del proceso de perfilamiento del subscriptor para cada subscriptor evaluado. Este reporte lista a los subscriptores que fueron movidos entre grupos, y resume las conclusiones de cada sesión de perfilamiento.
- **Reporte de llamadas fraudulentas:** Este reporte lista el registro de todas las llamadas marcadas como fraudulentas en un intervalo de tiempo.
- **Reporte de carga del subscriptor:** Este reporte lista el estatus de procesamiento para cargar las llamadas del subscriptor.

### 3.5.8 COMERCIALIZACIÓN DEL USUARIO

El comportamiento del sistema puede fácilmente ser adaptado o modificado por un ingeniero de la operadora en un número de diferentes maneras:

- **Grupos de trabajo:** Los grupos de trabajo pueden ser modificados para generar magnificas alarmas. Dentro de cada grupo el trabajo diario y semanal puede ser modificado por varios tipos de fraude.
- **Localizaciones:** Las localizaciones para el sistema de autenticación están hechas bajo códigos de país y códigos de área, los cuales están considerados para detectar

ya sea un alto o un bajo índice de fraude. La llamada hecha a las localizaciones que se encuentran registradas en listas, si hay fraude en ésta se generarán las alarmas.

- **Patrones:** El administrador que se encuentre a cargo de los analistas de fraude puede agregar, modificar y borrar los patrones basados en indicadores de fraude corriente o condiciones en el área del servicio proveedor. Una cierta alarma puede ser asignada para cada patrón, y el patrón puede ser capaz de especificar un tipo fraude específico.
  
- **Análisis de parámetros:** Dentro del análisis de parámetros hay que mencionar tres puntos importantes:
  1. **Tipos de Fraude:** Mientras haya tipos de fraude que el sistema pueda definir, un mecanismo es también proveído para definir nuevos tipos de fraude y poder conectar esos nuevos tipos de fraude a los casos de fraude ya registrados.
  2. **Acciones Recomendadas:** Con este parámetro permite al proveedor del servicio, por el implementar políticas corporativas y tener las guías necesarias para de tal forma responder al fraude sospechoso.
  3. **Rangos de Alarmas:** Con estos parámetros se mantiene la expectativa de los niveles de alarma usados, además el analista de fraude debe ser lo suficientemente capaz de evidenciar el fraude para crear un caso.

### 3.6 BENEFICIOS DEL SISTEMA DE AUTENTICACION

Entre los beneficios de nuestro sistema de autenticación estarán especificados en la teoría básica de la autenticación, es decir que los mecanismos para generar, distribuir y administrar los parámetros de una central o switch junto con los mensajes de señalización IS 41C deberán ser apropiados para que el proceso de autenticación sea exitoso. Entre los beneficios del sistema de autenticación, tenemos:

- Previene pérdidas de inversión para la operadora, es decir restringe el acceso no autorizado a la red a los terminales que están clonados.
- Se incrementa las oportunidades de hacer roaming, es decir elimina la necesidad de implementar servicios al cliente en mercados plagados por fraude.
- Da seguridad a los canales de voz de tal forma que sean proveídos solamente para subscriptores autorizados.
- Reduce los costos de operación, es decir con un manual necesario que se le debe proveer al analista de fraude, éste podrá detectar la actividad de fraude.
- Da satisfacción al subscriptor: Este es un beneficio de gran importancia ya que con ello atraemos más subscriptores al servicio celular de tal forma que no sean perjudicados al hacer las llamadas en sus celulares.
- Además se incrementa la libertad de hacer roaming y virtualmente se elimina las cargas no autorizadas.

- El sistema de autenticación elimina los tipos de fraude usando los diferentes métodos de autenticación como son el RF Fingerprinter, y otros más que permiten a la operadora intervenir a tiempo para localizar las llamadas fraudulentas.
- Permite dar flexibilidad al centro de autenticación para localizar las llamadas sin tener que contactar un centro de servicio al cliente para la validación y almacenamiento de llamadas de privilegios internacionales.
- Ofrece la habilidad para compartir el SSD con el sistema servidor.
- Tanto los procedimientos Global y Unique Challenges son soportados por el centro de autenticación.
- Se puede iniciar manualmente un proceso Unique Challenge que pueda ser ejecutado debido a un fraude sospechoso en una estación móvil particular.
- Se puede generar también un proceso de autenticación selectivo que puede ser iniciado en los tipos de accesos al sistema, incluyendo registración, originación, respuesta de un page.
- Se pueden generar reportes de autenticación en tiempo real es decir que el sistema es capaz de hacer una administración de seguridad completa para la red inalámbrica, incluyendo: Fraude de alto nivel al cual alerta al sistema de autenticación para que éste proceda a generar procedimientos global challenge para los diferentes intentos de llamadas, generar un proceso unique challenge ya sea para intentos de llamadas exitosos o fracasados, e intentos de actualizar el SSD.

- Provee una administración al sistema de autenticación para permitir que el servicio proveedor actualice un SSD de un subscritor o el conteo del historial de las llamadas.

### **3.7 PROVISIONAMIENTO DEL SISTEMA DE AUTENTICACIÓN**

El provisionamiento del sistema de autenticación se refiere al posicionamiento y mantenimiento del sistema de autenticación. Esta sección cubre los siguientes tópicos:

- Administración de las Claves de Autenticación
- Generación de las claves de Autenticación
- Creación y mantenimiento de la base de datos del Centro de Autenticación
- Administración de las rutas del HLR.

#### **3.7.1 ADMINISTRACIÓN DE LAS CLAVES DE AUTENTICACIÓN**

La autenticación necesita existir para proveer un mecanismo por el cual las claves de autenticación pueden ser puestas en el Centro de Autenticación. Cuando un móvil es capaz de autenticarse, este es entregado por el fabricante, entonces ya contiene una clave de autenticación. Los fabricantes son seleccionados para distribuir estas claves de autenticación al proveedor. Un requerimiento para el Centro de Autenticación es ser capaz de almacenar los datos de la pareja de los ESN y los A-key (recibidos desde el

fabricante) en el switch por un grupo de móviles hasta que el tiempo del móvil actual sea provisto en la base de datos del Centro de Autenticación con un MIN definido. Entonces cuando uno de estos móviles es ingresado en el Centro de Autenticación la clave de Autenticación para ese móvil puede automáticamente ser identificado.

El Centro de Autenticación implementa esta funcionalidad por el uso de un registro en el que constan los A-key, ESN, la versión del Algoritmo de Autenticación (AVV) y una fecha. La fecha marca el tiempo cuando una pareja ESN/A-key sea ingresada en el registro. Existe una tabla de control que permite al usuario posicionarse en un ESN particular en el registro, agregar una entrada, o borrar una entrada cuando se realice el ingreso de una entrada a través de la tabla de control, la clave de autenticación necesita ser incluida; sin embargo, una vez que haya sido ingresada en la tabla, la clave de autenticación no puede ser vista o cambiada.

El dato en esta tabla permanece hasta que un nuevo móvil sea ingresado en la base de datos del centro de autenticación y entonces habrá una entrada en el registro donde se incluyen los ESN, el A-Key y el AAV. Cuando el móvil es agregado a la base de datos del centro de autenticación, la correspondiente información de ese móvil en el registro ya antes mencionado es localizado para retener la clave de autenticación. La clave de autenticación es luego automáticamente transferida a la base de datos del Centro de Autenticación, y el ingreso en el registro es automáticamente removido.

La fecha en la cual fue agregado el móvil en el registro es proveída por el cable. El proveedor tiene la potestad de poder manejar el registro de autenticación por dos razones:

- Las parejas de los ESN y los A-Key recibidos desde el fabricante deben ser dados para uno o más móviles.
- La generación de las claves de autenticación para los móviles los cuales no han sido asignados con sus respectivos MINs.

### 3.7.2 GENERACIÓN DE LAS CLAVES DE AUTENTICACIÓN

El proveedor puede tener un teléfono en su posesión para lo cual el A-Key no es conocido o necesita ser cambiado. Para la preparación de su uso, una nueva clave de autenticación necesita ser generada y localizada en el móvil. Hay un comando disponible en el centro de autenticación que permite a la operadora celular generar un A-Key para un móvil. Si existiera el caso cuando el móvil no ha sido provisto en la base de datos del centro de autenticación se debe tener un comando que permita dar acceso con el ESN del móvil. El A-Key resultante para ese móvil que no ha sido provisto es mostrado en la pantalla y también automáticamente almacenado en el registro de autenticación.



Si una entrada ya existe en el registro de autenticación, el comando que genera la clave de autenticación será bloqueado. Eventualmente cuando este móvil es ingresado en la base de datos del centro de autenticación, la clave de autenticación puede ser retenida desde el registro de autenticación.

En la parte externa de la red, los teléfonos celulares de los usuarios serán programados electrónicamente mediante una interface entre el sistema de administración de la clave de autenticación y la estación móvil esta interface se llama Validador. Los Validadores pueden ser desarrollados por el fabricante, almacenes electrónicos, puntos de venta o centros logísticos.

### **3.7.3 CREACIÓN Y MANTENIMIENTO DE LA BASE DE DATOS DEL CENTRO DE AUTENTICACIÓN**

El principal componente del centro de autenticación es una base de datos la cual contiene la información por móvil necesaria para ejecutar la autenticación. La información es contenida en la base de datos de autenticación.

Las operaciones son disponibles usando las herramientas necesarias de la base. Para provicionar un móvil en el centro de autenticación se hace referencia al agregar un móvil en la base de datos de la autenticación. Una vez que una entrada exista para el

móvil en esta base y el A-Key este presente. Entonces el centro de autenticación esta listo para iniciar la autenticación del móvil.

El núcleo de la base de datos del centro de autenticación es contenida en una nueva base de datos de autenticación. Esta base es accesible ya sea mediante la tabla de control o a través de un comando específico proveído en el centro de autenticación. La tabla de control de un móvil puede ser agregada, borrada, y cambiada en la base de datos del centro de autenticación.

• **Resultados del ingreso de un móvil a la base de datos del Centro de Autenticación.**

Cuando una entrada es agregada en la base de datos del centro de autenticación, el registro de autenticación el registro de autenticación es buscado por un ESN dado. El registro de verificación es también buscado para verificar el MIN que tenga un HLR detallado. También hay que recalcar que cuando se ingrese una entrada, el SSD para el móvil es puesto en cero y el estado de actualización del SSD en el móvil que ingrese a la red es marcado con una bandera de actualización. Cuando la próxima solicitud de autenticación viene al centro de autenticación a este móvil una actualización del SSD es iniciada.

Si un móvil tiene una clave de autenticación un A-Key en la base de datos de la autenticación, entonces un log es generado en cada solicitud de autenticación recibida por el centro de autenticación para este MIN, para indicar a su vez que este móvil actualmente no tiene un A-Key. Este móvil es continuamente permitido el acceso al sistema hasta que la clave de autenticación este presente. Si la clave de autenticación en el móvil no es conocida, entonces el usuario necesita correr el comando que permita generar una nueva clave de autenticación o de cualquier otra forma tener la combinación del ESN y del A-Key para ese móvil.

- **Cambio y eliminación de un móvil en la base de datos del Centro de Autenticación**

Una entrada en la base de datos del centro de autenticación puede ser eliminada o cambiada usando el comando apropiado para eliminar y cambiar en la base de datos de la autenticación. El comando de reseteo es disponible en el centro de autenticación y puede ser usado para resetear alguna información dinámica del móvil la cual incluye el posicionamiento del estado actual del SSD sea que este libre, cerrado (log out); además del numero de fallas del SSD, y el número de fallas de acceso.

- **Generación manual del A-Key para los MINs en la base de datos de autenticación**

Un nuevo comando para generar manualmente el A-Key en el centro de autenticación es proveído. Usando este comando, se tienen el efecto de generar una nueva clave de autenticación aleatoria y chequear los dígitos para un móvil. Hay que recalcar que la

Una A-Key es automáticamente almacenada en una entrada del centro de autenticación para el móvil.

Si el móvil ya tiene una clave de autenticación válida este comando será bloqueado y el usuario debe remover primero su base de datos de autenticación entrante y luego agregarlo lo cual emitirá remover el A-Key existente. Lo mismo es verdad si una entrada existe en el registro de autenticación cuando el comando que genera el A-Key es usado. El comando será bloqueado hasta que la entrada sea borrada desde el registro de autenticación cuando una clave de autenticación es generada almacenada en la entrada del centro de autenticación, el SSD para el móvil es respetado a cero y el estado actual del SSD para el móvil es puesto con una bandera de actualización inicial.

Si los accesos del móvil al sistema antes que la clave de autenticación ha sido actualizada en la estación móvil, las subsiguientes actualizaciones del SSD, fracasaran. El uso de los dígitos de chequeo es resuelto por el ingreso de la clave de autenticación en el móvil. Cuando se ingrese una clave de autenticación en el móvil, el valor entrante que es usado, es la concatenación de la clave de autenticación del A-Key seguido por los dígitos de chequeo.

Es necesario conocer el reporte de datos por móvil cuando un MS ingresa al sistema. A continuación presentamos una tabla con el estatus del móvil que ingresa al sistema de autenticación.

Tabla 3.1

## INFORMACIÓN DE LA BASE DE DATOS DEL AC POR MÓVIL

Estado de los datos del móvil	Descripción
MIN	Número de Identificación Móvil
ESN	Número Serial Electrónico
A-Key Presente	Si es verdad, hay un A-key no nulo para el móvil
AAV	Versión del Algoritmo de Autenticación.
SSD Timestamp	Tiempo cuando la actualización del SSD fue exitosa
Estado Actual del SSD	Inicial, Pendiente, Libre
SSD Update Lockout	Si es verdad, el móvil esta siendo denegado el acceso debido a las fallas repetidas del SSD.
Número de Fallas del SSD	Número de fallas de Actualización del SSD desde la última actualización exitosa del SSD
Último Acceso	Tipo de los últimos accesos (Originación, Registración, Terminación, Flash, No especificado)
Último Acceso Timestamp	Tiempo en que el AC fue accedido últimamente
Número de Fallas de Acceso	Número de fallas desde el último acceso exitoso del AC

### **3.7.4 ADMINISTRACIÓN DE LAS RUTAS DEL HLR**

En las operaciones del centro de autenticación existe la necesidad de conocer la ruta para un HLR del móvil. Cuando el centro de autenticación necesite enviar un mensaje no solicitado al móvil, se necesita tener la ruta al HLR del móvil. El mecanismo para el cual el centro de autenticación conoce las rutas es mediante el uso de la tabla de verificación. En dicha tabla, el centro de autenticación puede definir una ruta para un HLR para un rango particular del MIN. El tipo de roamer para los HLRs externos será con una red roamer mientras un HLR local tendrá un tipo de roamer local.

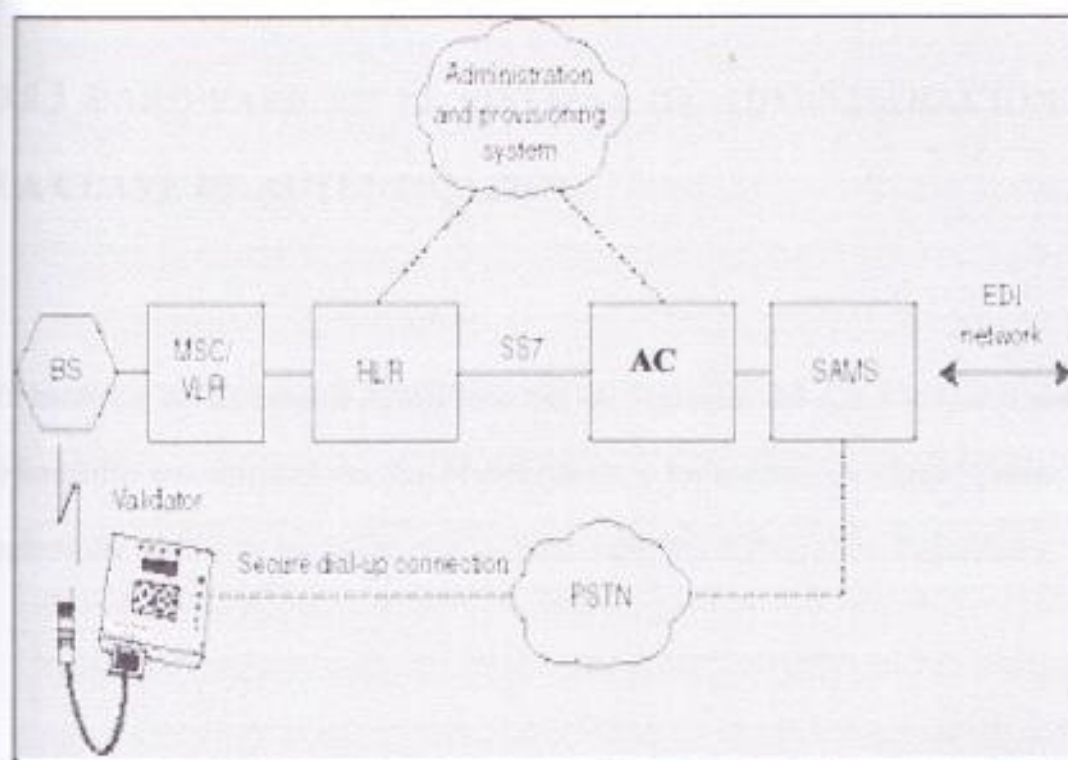
## **3.8 HARDWARE Y SOFTWARE REQUERIDOS EN EL SISTEMA DE AUTENTICACIÓN**

### **3.8.1 HARDWARE EN EL SISTEMA DE AUTENTICACIÓN**

El centro de autenticación utiliza la familia de Compaq AlphaServer como su plataforma de procesamiento en lo que se refiere a hardware. Los productos de AlphaServer 4100 usados en la configuración del Centro de Autenticación son los sistemas escalables, confiables, abiertos que entregan alto rendimiento en un precio comprable. Los sistemas de AlphaServer 4100 proveen flexibilidad de crecimiento y de configuración.

FIGURA 3.8

## HARDWARE EN EL SISTEMA DE AUTENTICACIÓN



## 3.8.2 SOFTWARE EN EL CENTRO DE AUTENTICACIÓN

El centro de autenticación requiere de bases de datos y sistemas operativos especiales para la autenticación. Estos son:

- Parte de Aplicación de Capacidades de Transacción (TCAP)
- Sistema Operativo UNIX Digital.

- Sistema de Administración de Base de Datos ORACLE.
- DECss7

### **3.8.3 HARDWARE EN EL SISTEMA DE ADMINISTRACION DE LA CLAVE DE AUTENTICACION**

El hardware del Sistema de Administración de Seguridad del A-key utiliza el sistema informático de computadores Sun Microsystems, y los modems de Cisco Systems o la batería del módem de los 3Com para las conexiones via dial-up a los Validadores.

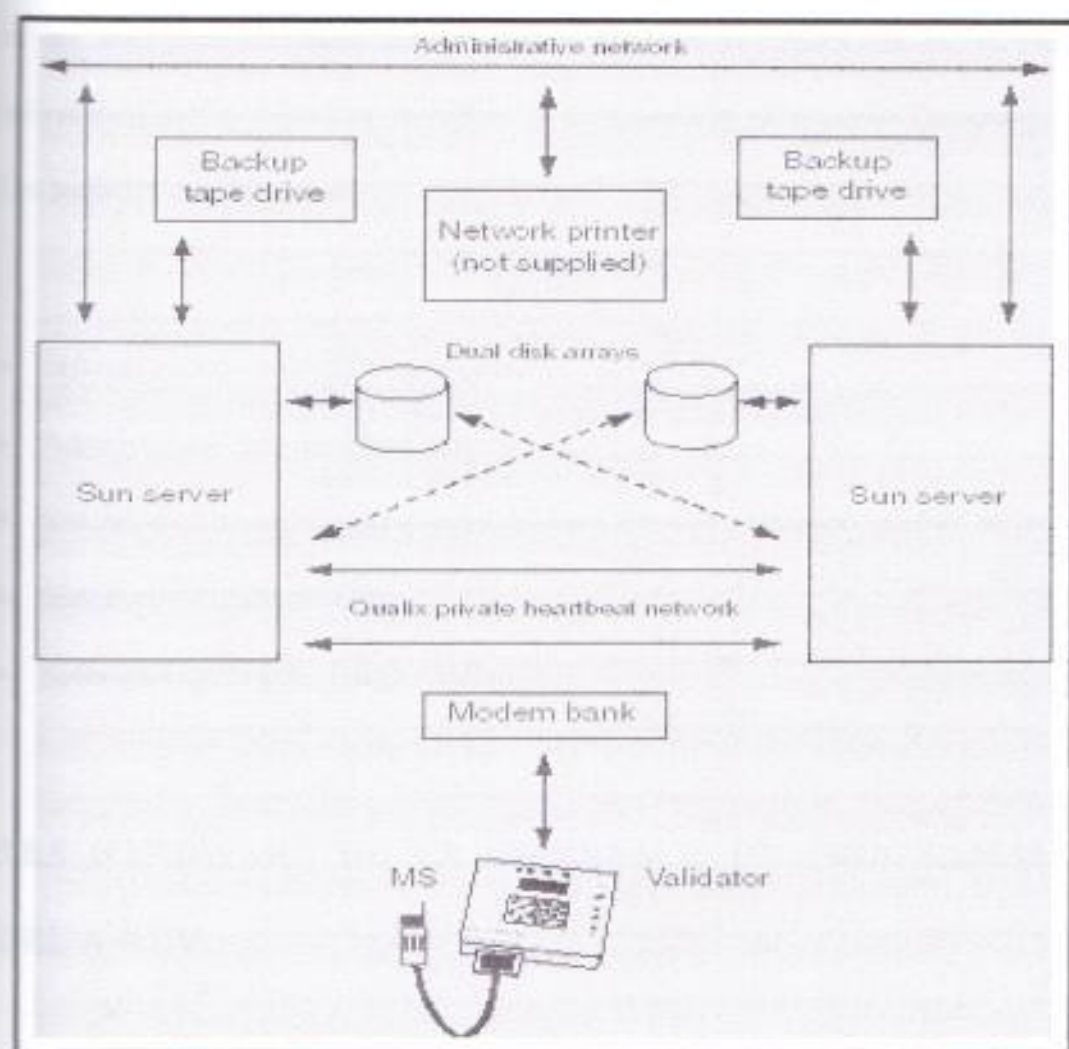
El Sistema de Administración de Seguridad del A-key se basa en una plataforma computacional llamada Sun Ultra Enterprise en el que se corre el sistema de operación Sun Solaris de UNIX y el sistema de administración de Base de Datos de Oracle.

El sistema de Administración del A-key esta disponible en la plataforma Ultra Enterprise 2 y en le Enterprise 3500, el cual es optimo para correr las aplicaciones del Sistema de Administración del A-key.



FIGURA 3.9

HARDWARE EN EL SISTEMA DE ADMINISTRACION  
DE LA CLAVE DE AUTENTICACION



### **3.8.4 SOFTWARE DEL SISTEMA DE ADMINISTRACIÓN DE SEGURIDAD DE LA CLAVE DE AUTENTICACIÓN**

El sistema de Administración de seguridad de la Clave de Autenticación requiere paquetes informáticos actuales para poner en práctica las bondades de la autenticación en las diferentes entidades de red. Estos paquetes se encuentran en el mercado informático de las diferentes empresas de computación, tales como Compaq y otros.

Los paquetes utilitarios son:

- Sistema operativo UNIX Sun Solaris.
- Administrador Sun StorEdge Volume
- Sistema de Administración de base de datos Oracle8 Enterprise, edición Relacional.
- Sistema de Archivos Veritas.
- Software Qualix HA+ (High Availability).

### **3.8.5 HARDWARE DE LA INTERFACE DE PROGRAMACIÓN DEL A-KEY**

La plataforma compacta y robusta del Validador puede ser usada en cualquiera de los teléfonos móviles que sean almacenados, programados, o vendidos. Es pequeño y

figero. La interface de los validadores, consiste de un display LCD y dos teclados para ingresar los datos de administración. Los teclados también permiten a los usuarios para interactuar con el Validador durante el proceso de programación.

El Validador tiene dos interfaces físicas:

- Un módem interno para conectividad dial-up al sistema de administración de la clave de Autenticación.
- Un puerto DB-25 para conexión a teléfonos móviles con cables de interface programación.

**FIGURA 3.10**

### **INTERFACE DE PROGRAMACIÓN DEL A-KEY**



## **CAPITULO IV**

### **ANALISIS COMERCIAL**

#### **4.1 PLANES DE TARIFACIÓN DE LLAMADAS CELULARES**

En esta sección enfocaremos los planes tarifarios celulares que servirán para darle un costo a los servicios de nuestro sistema de autenticación celular. Hay que recalcar de manera especial que estos planes tarifarios no incluyen el I.V.A.

Se recomienda que los planes tarifarios deben estar sujetos a los siguientes aspectos:

- \* Tiempo Aire Celular

\*\*\* Internet: Planes Wave y Convenientes.

\* Derecho de Inscripción para un teléfono análogo \$ 50,00.

Cientes con equipo propio no pagan Derecho de inscripción

Notas:

- Los valores no incluyen impuestos ni cargos de interconexión.
- Los valores anteriores serán facturados en sucres, de acuerdo a la cotización del dólar vigente para cada mes.
- Servicio de Noches: De 21 H00 a 7H59. Hora No Pico desde las 22H00 a 7H59 Fines de Semana y Feriados Oficiales de 00H00 a 24H00: Año Nuevo, Viernes Santo, Día del Trabajo, Batalla del Pichincha, Fundación de Guayaquil (local), 1er Grito de la Independencia, Independencia de Guayaquil, Fieles Difuntos, Independencia de Cuenca, Fundación de Quito (Local), Navidad.
- Además a 12 meses en todos los planes.
- Extensión: Una línea con equipo análogo fijo.

Tabla 4.1

Plan 1

Cuota Mensual	22,00 USD
Minutos	40
Precio Minuto (Pico)	0,39 USD
Precio Minuto (No pico)	0,05 USD
Derecho de Inscripción "	35,00 USD
Noches y F. de Semana *	15,00 USD
Noches *o F. de Semana *	10,00 USD
Celubeeper	4,00 USD
Factura Detallada	2,00 USD
Extensión Auto (T. Básica)	Incluye
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dcto)	Incluye
Porta Voz	Incluye

Tabla 4.2

Plan 2

Cuota Mensual	27,00 USD
Minutos	100
Precio Minuto (Pico)	0,38 USD
Precio Minuto (No pico)	0,05 USD
Derecho de Inscripción "	35,00 USD
Noches y F. De Semana *	15,00 USD
Noches *o F. De Semana *	10,00 USD
Celubeeper	4,00 USD
Factura Detallada	2,00 USD
extensión Auto (T. Básica)	Incluye
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dscto)	Incluye
Porta Voz	Incluye

Tabla 4.3

**Plan 3**

Cuota Mensual	15,00 USD
Minutos	15
Precio Minuto (Pico)	0,48 USD
Precio Minuto (No pico)	0,05 USD
Derecho de Inscripción "	35,00 USD
Noches y F. De Semana *	15,00 USD
Noches *o F. De Semana *	10,00 USD
Celubeeper	4,00 USD
Factura Detallada	2,00 USD
Extensión Auto (T. Básica)	Incluye
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dscto)	Incluye
Porta Voz	Incluye



Tabla 4.4

**Plan 4**

Cuota Mensual	30,00 USD
Minutos	100
Precio Minuto (Pico)	0,20 USD
Precio Minuto (No pico)	0,20 USD
Derecho de Inscripción "	35,00 USD
Noches y F. De Semana *	15,00 USD
Noches *o F. De Semana *	10,00 USD
Factura Detallada	Incluye
Extensión Auto (T. Básica)	Incluye
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dcto)	Incluye
Porta Voz	Incluye

Tabla 4.5

**Plan 5**

Cuota Mensual	35,00 USD
Minutos	140
Precio Minuto (Pico)	0,35 USD
Precio Minuto (No pico)	0,05 USD
Derecho de Inscripción "	35,00 USD
Noches y F. De Semana *	15,00 USD
Noches *o F. De Semana *	10,00 USD
Celubeeper	4,00 USD
Factura detallada	2,00 USD
Extensión Auto (T. Básica)	Incluye
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dcto)	Incluye
Porta Voz	Incluye

Tabla 4.6

**Plan Oficina**

Cuota Mensual	15,00 USD
Minutos	0
Precio Minuto (Pico)	0,15 USD
Precio Minuto (No pico)	0,05 USD
Derecho de Inscripción "	35,00 USD
Noches y F. de Semana *	15,00 USD
Noches *o F. de Semana *	10,00 USD
Factura detallada	Incluye
Extensión Auto (T. Básica)	Incluye
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dcto)	Incluye
Porta Voz	Incluye

Tabla 4.7

**Plan Empresarial**

Cuota Mensual	15,00 USD
Minutos	30
Precio Minuto (Pico)	0,15 USD
Precio Minuto (No pico)	0,12 USD
Derecho de Inscripción *	35,00 USD
Noches y F. de Semana *	15,00 USD
Noches *o F. de Semana *	10,00 USD
Factura detallada	2,00 USD
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dscto)	Incluye
Porta Voz	Incluye

Tabla 4.8

**Plan Permanente**

Cuota Mensual	15,00 USD
Minutos	0
Precio Minuto (Pico)	0,15 USD
Precio Minuto (No pico)	0,15 USD
Derecho de Inscripción "	35,00 USD
Noches y F. De Semana *	15,00 USD
Noches *o F. De Semana *	10,00 USD
Factura detallada	Incluye
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dcto)	Incluye
Porta Voz	Incluye

Tabla 4.9

**Plan Permanente Plus**

Cuota Mensual	15,00 USD
Minutos	30
Precio Minuto (Pico)	0,15 USD
Precio Minuto (No pico)	0,12 USD
Derecho de Inscripción "	35,00 USD
Noches y F. De Semana *	15,00 USD
Noches *o F. De Semana *	10,00 USD
Factura detallada	2,00 USD
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dscto)	Incluye
Porta Voz	Incluye

Tabla 4.10

Plan Negocio

Cuota Mensual	90,00 USD
Minutos	500
Precio Minuto (Pico)	0,15 USD
Precio Minuto (No pico)	0,15 USD
Derecho de Inscripción "	35,00 USD
Noches y F. De Semana *	15,00 USD
Noches *o F. De Semana *	10,00 USD
Factura detallada	Incluye
Internet 2 meses sin costo**	Incluye
Beeper (Local) Tarifa Especial	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dscto)	Incluye
Porta Voz	Incluye

Tabla 4.11

**Plan Grupal**

Cuota Mensual	50,00 USD
Minutos	400
Precio Minuto (Pico)	0,25 USD
Precio Minuto (No pico)	0,05 USD
Derecho de Inscripción "	35,00 USD
Noches y F. de Semana *	10,00 USD
Noches *o F. de Semana *	Incluye
Celubeeper	Incluye
Factura detallada	Incluye
Auto Extensión ( Tarifa Básica)	Incluye
Internet 2 meses sin costo**	Incluye
Larga Distancia Internacional	Tasa Pref.
Discado Directo Local	Incluye
Accesorios * 311 (15% Dscto)	Incluye
Porta Voz	Incluye



## 4.2 COSTOS DE IMPLEMENTACION DE UN SISTEMA DE AUTENTICACIÓN VS. RF FINGERPRINTING.

### 4.2.1 COMPARACIÓN DE LAS TÉCNICAS

Los costos específicos de la implementación de la autenticación y el RF Fingerprinting están bajo el lente de este proyecto y no están disponibles a través de restricciones propietarias. No obstante, los siguientes párrafos intentan visualizar los costos esperados de este tipo de proyectos.

Los costos primarios asociados con la autenticación son:

1. Los costos que tiene la empresa portadora en la instalación necesaria de hardware y software tanto en el centro de autenticación como en los móviles.
2. Los Costos de implementación de los equipos asociados, y
3. Costos de cliente/portador para que todos los clientes cambien o actualicen sus móviles.

Los costos primarios asociados con el RF Fingerprinting son:

1. El costo que tiene la empresa portadora en la instalación necesaria de software y hardware con el RFU (Radio Frequency Unit) y el SCC (System Control Center).
2. Costos de implementación de los equipos asociados.

Una vez que los sistemas de autenticación o RF Fingerprinting están instalados e implementados, el hurto en roaming prevalecerá hasta que no se pueda tener un sistema que incluya ambas características de autenticación y RF Fingerprinting. los posibles escenarios incluyen:

- Cloneo por medio del robo del ESN y MIN desde las ondas de radio y hacer roaming en algún mercado adyacente recibiendo servicio usando la información personal que se robo de las ondas de radio en un sistema que tiene ausencia de autenticación o RF Fingerprinting.
- Un clon entrando y recibiendo servicio en una cobertura local con un sistema de autenticación usando un teléfono analógico anterior a 1995 que no tiene capacidad de autenticación.
- Un clon entrando y recibiendo servicio en una cobertura local con una red RF Fingerprinting usando un teléfono analógico anterior a 1995 al cual anteriormente no se le ha grabado el patrón de onda.

No habrá tecnología de prevención que solucione el problema de cloncelular si alguna tecnología apropiada no es saturada y estandarizada en todos los países. Hasta ese momento, las actividades fraudulentas pueden reducirse pero no desaparecer. Si un mercado es seguro con autenticación o RF Fingerprinting y un roamer entra como un clon, el tiempo aire es pagado por el sistema de seguridad. Por esta razón muchos de los mercados como Washington DC han eliminado el acceso a los roamers.

Aunque muchos de los costos son asociados con el equipamiento para los MSC, AC, RFU y SSC, son responsabilidad de la empresa portadora, el costo de los móviles que deben ser compartidos entre el carrier y el consumidor y puede ser limitada por un factor. Las opciones del consumidor para incrementar su seguridad incluyen:

1. Mantener su teléfono analógico actual y encontrar una empresa portadora que ofrezca servicio con capacidad de RF Fingerprinting.
2. Esperar un tiempo hasta que la empresa portadora actualice su software y circuitería en los teléfonos actuales para activarlos para autenticación y
3. Comprar un móvil potencialmente mas caro, inherentemente con capacidades de autenticación.

La empresa portadora, espera siempre mantener su credibilidad y además a los clientes, es responsable de las actividades fraudulentas, y además en algunos casos, el subvencionar muchos de los teléfonos autenticables más caros. Desde que los consumidores no son responsables por los costos asociados con las actividades fraudulentas, a ellos no les parecerá grato pagar ningún monto adicional.

Hasta hace poco tiempo, pocos de los móviles soportaban autenticación y su implementación no parecía un buen costos efectivo para las empresas portadoras.

¿ Esta siendo la autenticación probada por muchos operadores en estos momentos como una respuesta a los problemas con los consumidores o en verdad es la respuesta a todo el fraude celular?

Quizás el RF Fingerprinting es la solución, o nuevamente como lo mencionamos antes, la implementación de ambas tecnologías reducirá el mercado del clonero mucho más hasta que una mejor tecnología este disponible.

#### 4.2.2 ANÁLISIS COMPARATIVO

La implementación de autenticación y RF Fingerprinting será comparada basada en los costos distribuidos, vulnerabilidades, control de fronteras y opciones tecnológicas después del compromiso, y además la transparencia hacia el consumidor de la implementación y operación.

- Costos Distribuidos: La mayoría de los autores se limitan al análisis de costo de dos items, el costo de los móviles y los costos de los RFU. La mayoría de autores basados en Asunciones, relacionan estos costos en la información publicada disponible de la industria inalámbrica.
- Costo de los Móviles: Estos costos representan el costo a la empresa portadora para actualizar los móviles que no tienen capacidad de autenticación. La empresa portadora por el general subsidiará una porción de estos costos para limitar la inversión de los consumidores. Esto puede estar entre los \$50 y \$300 dependiendo del modelo. Para este análisis asumimos un costo de \$200 por teléfono.
- RF Fingerprinting Radio Frequency Unit (RFU): Estos costos representan el costo de actualizar cada celda con RFUs. Este costo se ha estimado que este entre los

\$25000 y los \$35000 por celda. Para este análisis asumimos que el costo por celda es de \$30000.

Para el cálculo del flujo de caja y de la tasa interna de retorno usamos los siguientes datos:

**Tabla 4.12**

**FLUJO DE CAJA**

<b>DATOS:</b>	<b>COSTOS (EN \$):</b>
Inversión Inicial (\$)	1,246,000
Sistema de Autenticación	800,000
Soporte Técnico (Capacitación)	200,000
Instalaciones administrativas	150,000
Sueldo Personal ( 5 personas)	4,000
Usuarios Iniciales	300,000
<i>Adicionalmente:</i>	
Mensualmente se increm.	0.5%
Precio mensual por el servicio	2
Inc. Mensual en la facturación	1

### 4.2.3 COSTOS ESTIMADOS DE AUTENTICACIÓN Y RF FINGERPRINTING

Esta primera tabla se basa en costos estimados asumiendo que el mercado celular no esta preparado tecnológicamente para la autenticación, y sea necesario volver a actualizar los móviles de los clientes.

Se considera también nuestro mercado que es de aproximadamente unos 300.000 usuarios. Los costos de instalación de este sistema es aproximadamente de unos \$800.000 dólares, dependiendo de la casa proveedora, considerando que se deben incluir planes de soporte técnico y cursos para el personal que abarcan un costo de unos \$ 200.000 dólares, el costo efectivo de este sistema seria \$ 1'000.000. Como costos adicionales se tienen los siguientes puntos: Instalación del Centro de administración y Control del Centro de Autenticación \$ 150.000, (asumiendo que la instalación es completa, es decir desde el tipo de cableado); así llegando a un total de \$ 1'150.000.

Entre otros parámetros debemos recalcar también los gastos administrativos, entre los mas destacados tenemos los salarios de las personas a cargo del Centro de Autenticación que en promedio rodean los \$800. Para poder tener soporte las 24 h se necesitarian 4 personas que hagan turnos de 12 h cada una. Además una persona mas que se encargue de su administración, control y nuevas implementaciones. Esto

suman un total mínimo de 5 personas técnicamente calificadas. Lo que nos da un total de \$4000 en salarios técnico profesionales. En la siguiente tabla (Tabla 4.13) se especifica primero el costo total que se debe enfrentar por el cambio de tecnología para los usuarios. Y además se incluye el TIR para este proyecto.(Tabla 4.14)

**Tabla 4.13**

**COSTOS DE MOVILES Y UNIDADES RFU**

	<b>Móviles</b>	<b>RFUs</b>
Numero de consumidores Con móviles no autenticables en el mercado	300.000	
Numero de celdas en una Red analógica nacional		61
Costo Unitario	\$200	\$30.000
<b>COSTO TOTAL</b>	<b>\$ 60.000.000</b>	<b>\$ 1'830.000</b>

Tabla 4.14  
BALANCE ESTIMADO DEL SISTEMA DE AUTENTICACION  
FLUJO DE CAJA: PROYECTO SISTEMA DE AUTENTICACION

INGRESOS OPERACIONALES	DICIEMBRE	AÑO 2000											
		ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE		
CANTIDAD USUARIOS		300,000	301,500	303,008	304,523	306,045	307,575	309,113	310,659	312,212	313,773		
PRECIO SERVICIO (5)		2	3	3	3	3	3	3	3	3	3		
TOTAL INGRESOS OPERACIONALES	0	600,000	904,500	909,023	913,568	918,135	922,726	927,340	931,976	936,636	941,320		
<b>EGRESOS OPERACIONALES</b>													
SISTEMA DE AUTENTICACION		33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333		
INSTALACION DE LA ADM. - CONTROL		6250	6250	6250	6250	6250	6250	6250	6250	6250	6250		
SOPORTE TECNICO-CAPACITACION		8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333		
SUELDOS PERSONAL ADM. - TECNICO		4000	4000	4000	4000	4000	4000	4000	4000	4000	4000		
TOTAL EGRESOS OPERACIONALES	0	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916		
<b>FLUJO DE CAJA OPERACIONAL</b>	0	548,084	852,584	857,107	861,652	866,219	870,810	875,424	880,060	884,720	889,404		
<b>EGRESOS NO OPERACIONALES</b>													
INVERSION INICIAL	1,246,000												
<b>TOTAL EGRESOS NO OPERACIONALES</b>	1,246,000												
<b>FLUJO DE CAJA NO OPERACIONAL</b>	1,246,000												
<b>FLUJO DE CAJA TOTAL</b>	-1,246,000	548,084	852,584	857,107	861,652	866,219	870,810	875,424	880,060	884,720	889,404		



## AÑO 2001

NOVIEM	DICIEM	ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPT.	OCTUB	NOVIEM	DICIEM	TOTAL
318,342	316,919	318,503	320,096	321,696	323,304	324,921	326,546	328,178	329,819	331,468	333,126	334,791	336,465	7,629,582
3	3	2	3	3	3	3	3	3	3	3	3	3	3	70
946,026	950,756	637,006	960,287	965,088	969,913	974,763	979,637	984,535	989,458	994,405	999,377	1,004,374	1,009,396	22,270,244
33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	33,333	799,992
6250	6250	6250	6250	6250	6250	6250	6250	6250	6250	6250	6250	6250	6250	150000
8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	8,333	199,992
4000	4000	4000	4000	4000	4000	4000	4000	4000	4000	4000	4000	4000	4000	96000
51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	51,916	1,245,984
894,110	898,840	585,090	908,371	913,172	917,997	922,847	927,721	932,619	937,542	942,489	947,461	952,458	957,480	21,024,260
894,110	898,840	585,090	908,371	913,172	917,997	922,847	927,721	932,619	937,542	942,489	947,461	952,458	957,480	21,024,260

Hay que tomar en cuenta los siguientes parámetros para ver que tecnología es factible, ya sea autenticación o RF Fingerprinting:

- Vulnerabilidades se refieren a la facilidad de comprometerse y trabajar en esta tecnología
- Boundary Control se refiere al lugar geométrico de control relacionado con los elementos de red que manejan la tecnología de prevención de fraude. Para RF Fingerprinting, los RFUs se los coloca en cada celda, entonces este manejo es el mismo que la cobertura de todas las celdas.

En autenticación hay usualmente uno o dos centros de autenticación por cada operadora. Entonces se puede asumir que:

- Opciones tecnológicas después del compromiso se refieren a la facilidad de modificar o actualizar esta tecnología una vez que se comprometa en ella.
- Transparencia al usuario se refiere a las limitantes impuestas al usuario al implementar y usar esta tecnología.

En la siguiente tabla (Tabla 4.15) veremos los costos de autenticación y RF Fingerprinting para un mercado celular:

Tabla 4.15

## COSTOS DE AUTENTICACION Y RF FINGERPRINTING

FACTOR	AUTENTICACION	RF FINGERPRINTING
Costo de Distribution:	\$ 2 Billones (Móvil)	\$ 300 Millones (RFU) Por carrier
Vulnerabilidades	Algoritmo hackeable	Potencia arruinando la celda
Boundary Control	Centralizado - o no o dos AC Por cada empresa portadora	RFU localizados en cada celda
Una vez comprometidos, cuales son las opciones futuras dentro de esta tecnologia	-Cambiar el A-key- Incrementar la longitud del A-key	Cambiar el Móvil el nuevo patrón aumenta la sensibilidad del sistema
Implementación Transparente Hacia el Cliente	Necesitaria comprar o actualizar su teléfono celular para que Sea capaz de autenticarse	Continuaría usando el mismo teléfono
Operaciones Transparentes Hacia el Cliente	YES	YES
Habilidad de la tecnología de Migrar desde AMPS a TDMA o CDMA	YES	YES - La implementación de RF Fingerprinting sobre CDMA aun esta en Desarrollo.

La vulnerabilidad de la autenticación es hasta cierto punto posible, este tipo de algoritmo confundirá a los intrusos durante unos 20 años, según los estudios hechos por la industria inalámbrica. En cambio una potencial vulnerabilidad del RF Fingerprinting es el "power blasting" que puede ocurrir cuando un móvil se lo toda de un patrón de onda más potente y capaz de sobre-escribir el patrón de onda en el proceso de RF Fingerprinting causándole interferencia a este. La empresa portadora a través de políticas y procedimientos claros asociados con el proceso de RF Fingerprinting puede manejar considerablemente esta vulnerabilidad.

El hecho de que ambas tecnologías de prevención ofrecen excelente transparencia en las operaciones hacia el usuario, las determinaciones aplicables que quedan para discernir el mejor proyecto se reducen a cuatro factores:

- Costo de distribución
- Opciones dentro de la tecnología, una vez que se comprometa en una tecnología
- Que tan transparente es la implementación de la tecnología de prevención hacia el usuario.
- Que tan bueno es el control de Frontera

Si se comprometiera la tecnología, sería la responsabilidad de la empresa portadora aumentar la sensibilidad del patrón RF.

### 4.3 COSTOS DE HARDWARE Y SOFTWARE DEL CENTRO DE AUTENTICACIÓN

Entre los valores estimados del hardware y software para implementar el área informática del centro de autenticación celular, tenemos los siguientes equipos y programas:

**Tabla 4.16**

<b>PRODUCTO</b>	<b>VALOR</b>
Compaq AlphaServer	\$ 4.500,00
Sistema Operativo UNIX Digital.	\$ 2.500,00
Sistema de Administración de Base de Datos ORACLE	\$ 3.000,00
DECss7 (interace de software ss7)	\$ 2.000,00

#### 4.4 COSTOS DE HARDWARE Y SOFTWARE DEL SISTEMA DE ADMINISTRACION DEL LA CLAVE DE AUTENTICACION

Después de implementar los equipos para el centro de autenticación, se debe complementar otros equipos especiales para la administración de la clave de autenticación, los cuales lo enunciamos en la siguiente tabla:

**Tabla 4.17**

<b>PRODUCTO</b>	<b>PRECIO</b>
Computadores Sun Microsystems	\$ 2.500,00
Modems Cisco Systems	\$ 500,00
Batería de módems 3Com	\$ 120,00
Sistema de administración de Base de Datos de Oracle.	\$ 3.000,00
Sun Solaris de UNIX	\$ 2.500,00
Sistema operativo UNIX Sun Solaris.	\$ 2.500,00
Administrador Sun StorEdge Volume	\$ 1.000,00
Sistema de Administración de base de datos Oracle8 Enterprise,	\$ 3.000,00

## 4.5 IMPACTO ESTIMADO DEL SISTEMA DE AUTENTICACIÓN

El impacto estimado de la autenticación y el cómputo de la actividad para la autenticación se hace específicamente para el modelo de llamadas y los diversos periférico del switch. Además, la autenticación por sí mismo tiene subcomponentes que analizan individualmente el impacto de la autenticación. Las asunciones siguientes fueron utilizadas para el modelo de llamadas de autenticación:

- porcentaje de averías de la autenticación.
- actualización del SSD una vez
- el SSD se comparta entre los MSCs
- MSC y HLR co-localizados
- Las registraciones iniciales son el 30% de registraciones locales.

## CONCLUSIONES

Entre los beneficios de nuestro sistema de autenticación estarán especificados en la teoría básica de la autenticación, es decir que los mecanismos para generar, distribuir y administrar los parámetros de una central o switch junto con los mensajes de señalización IS 41C deberán ser apropiados para que el proceso de autenticación sea exitoso. A continuación presentamos las conclusiones de este proyecto:

- 1) Previene pérdidas de inversión para la operadora, es decir restringe el acceso no autorizado a la red a los terminales que están clonados.
- 2) Se incrementa las oportunidades de hacer roaming, es decir elimina la necesidad de implementar servicios al cliente en mercados plagados por fraude.



- 3) Da seguridad a los canales de voz de tal forma que sean proveídos solamente para suscriptores autorizados.
- 4) Reduce los costos de operación, es decir con un manual necesario que se le debe proveer al analista de fraude, éste podrá detectar la actividad de fraude.
- 5) Da satisfacción al suscriptor: Este es un beneficio de gran importancia ya que con ello atraemos más suscriptores al servicio celular de tal forma que no sean perjudicados al hacer las llamadas en sus celulares.
- 6) Además se incrementa la libertad de hacer roaming y virtualmente se elimina las cargas no autorizadas.
- 7) El sistema de autenticación elimina los tipos de fraude usando los diferentes métodos de autenticación como son el RF Fingerprinter, y otros más que permiten a la operadora intervenir a tiempo para localizar las llamadas fraudistas.
- 8) Permite dar flexibilidad al centro de autenticación para localizar las llamadas sin tener que contactar un centro de servicio al cliente para la validación y almacenamiento de llamadas de privilegios internacionales.
- 9) Ofrece la habilidad para compartir el SSD con el sistema servidor.

- 10) Tanto los procedimientos Global y Unique Challenge son soportados por el centro de autenticación.
- 11) Se puede iniciar manualmente un proceso Unique Challenge que pueda ser ejecutado debido a un fraude sospechoso en una estación móvil particular.
- 12) Se puede generar también un proceso de autenticación selectivo que puede ser iniciado en los tipos de accesos al sistema, incluyendo registración, originación, respuesta de un page.

## RECOMENDACIONES

En lo que a recomendaciones se refieren, citamos los siguientes puntos:

- 1) Desde el punto de vista del cliente para comparar autenticación vs. RF Fingerprinting, tenemos:

Esta claro a través del análisis anterior que RF Fingerprinting es la menos costosa de las opciones. La autenticación es mas cara de implementar y más significativa, requiere que el cliente haga alguna acción. Primer factor, cambiar su teléfono por uno nuevo y nuevamente aprender como hacer llamadas y tener acceso al nuevo sistema con sus propiedades y servicios. Segundo factor, encontrar el momento justo o la oportunidad cuando los clientes no necesiten de su teléfono por algunas horas o días para que lo envíen y retiren del centro de servicios para hacerle la actualización.

2) Desde el punto de vista de la empresa portadora:

Las portadoras analógicas se enfrentan a un gran debate, actualizar sus redes para que soporten autenticación o RF Fingerprinting por un lado, y por otro lado pueden perder clientes al querer pasar a tecnologías PCS que son inherentemente más seguras. Las portadoras analógicas enfrentan dos riesgos si su posición es estática frente a la prevención del fraude por clonación:

- Un incremento del problema de clonación
- Riesgo de perder clientes que prefieran usar tecnologías PCS para no ser presa del fraude en redes analógicas.

3) Por el análisis anterior, recomendamos que RF Fingerprinting sea implementado en redes analógicas que tienen una base embebida de teléfonos análogos viejos.

4) Un portador no debería decidir entre autenticación y RF Fingerprinting como opciones mutuamente exclusivas. En un análisis más a fondo los porcentajes de fraude en los mercados de portadores junto con los tipos de teléfono podrían conducir a un despliegue estratégico de las técnicas de prevención del fraude. RF

5) Fingerprinting debería ser implementado en áreas de alto fraude como ciudades metropolitanas. La autenticación debería ser implementada en áreas de fraude

moderado con un número pequeño de usuarios los cuales deberían cambiar sus celulares o por lo menos actualizarlos.

- 6) El análisis final para las empresas portadoras debería ser evaluar su actual situación y la situación a la cual se quieren proyectar, y así emplear selectivamente varias tecnologías de prevención de clonación, de modo que no afecte los clientes actuales ni los potenciales.

# APPENDICES

---

**APENDICE A**

**ESTANDARES**

**AUTENTICABLES**

**DE RED**

**Y MOVILES**

---

# **ESTANDAR IS41 Revision C**

## **INTRODUCCION.-**

Las especificaciones del IS-41 REVISION C contienen modificaciones e innovaciones significantes sobre la IS-41 revisión B. Hay que recalcar que en las innovaciones del Modelo propio de red de la revisión IS-41 C, se especifica la funcionalidad de las entidades y asocia interfaces definidas dentro de las especificaciones que comprometen lógicamente a la red celular.

La interface IS-41 C provee sucesos basados en el mecanismo para la comunicación con la plataforma del hardware, produciéndose así cambios en algunos parámetros y mensajes de las ultimas versiones.

La segunda generación del modelo de referencia de red IS-41 es especificado en IS-41 Revision C. Los siguientes cambios fueron hechos al modelo de referencia original:

---



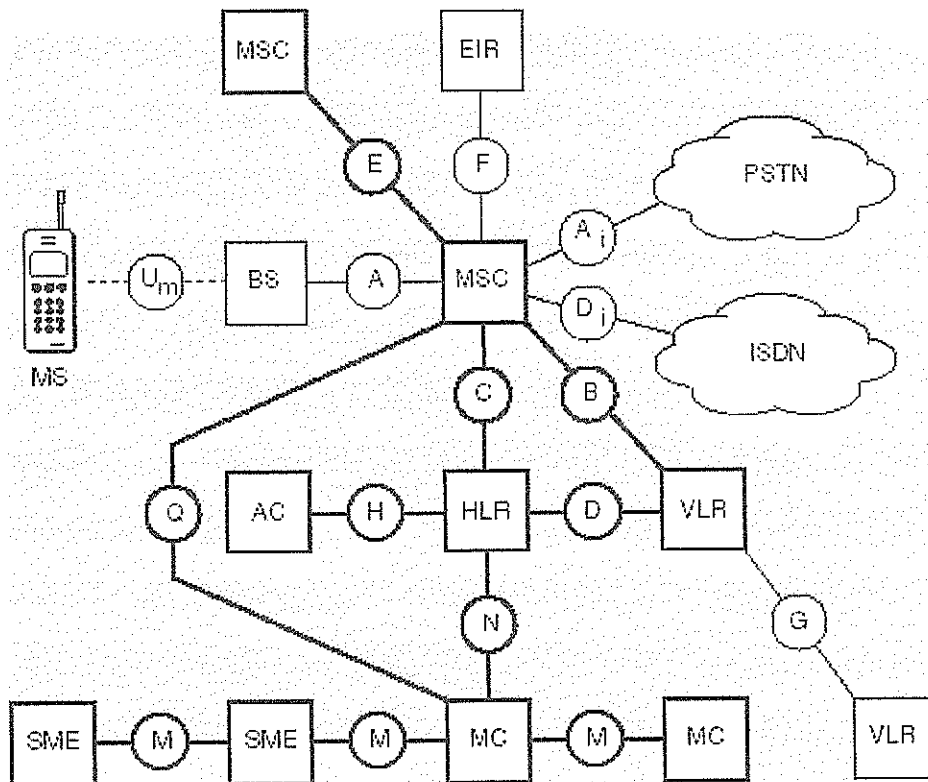
1. El nombre del CSS (Cellular Subscriber Station) fue cambiado a la de estación móvil.
2. La interface Sm fue removida.
3. Las entidades funcionales del Short Message Service (SMS) y sus interfaces fueron agregadas.

En la figura siguiente se presenta el modelo de referencia de segunda generación IS-41. El cambio más prominente del modelo previo es la adición de entidades funcionales soportando el SMS. El SMS es un grupo de servicios que soporta el almacenaje y transferencia de mensajes de texto corto (200 bytes o menos) a través de la red móvil. Las entidades funcionales del SMS fueron agregadas al modelo después de la etapa dos de la descripción del SMS justificando sus presencias. El cambio de nombre de CSS a MS no implica algún cambio de funcionalidad. La necesidad para mostrar una distinción entre esta entidad funcional y otra similar y entidades análogas especificadas en otras redes estandars no fue por mucho tiempo que una consideración importante. El cambio fue implementado para hacer de la terminología de la telefonía móvil algo más consistente con la industria común y corriente.

---

**FIGURA A.1**

**ESTRUCTURA DEL MODELO IS-41 C**



- AC — authentication center
- BS — base station
- EIR — equipment identity register
- HLR — home location register
- ISDN — integrated services digital network
- MC — message center
- MS — mobile station
- MSC — mobile switching center
- PSTN — public switched telephone network
- SME — short message entity
- VLR — visitor location register

Hay que recalcar que la interfaces en negrillas representan las interfaces que son estandarizadas en IS-41 C.

El Centro de Mensajes (MC) es una entidad funcional que almacena y encamina los mensajes cortos para el SMS. La función de almacenamiento y encaminamiento proporciona un método de encaminamiento de mensajes cortos a su lugar de destino o almacenamiento de aquellos mensajes si el destino no esta disponible para recibirlos. La función de almacenamiento y encaminamiento puede ser distinguida para los requerimientos de tiempo real de llamadas de voz. Los mensajes cortos pueden ser almacenados en una base de datos hasta que sea conveniente para ellos ser enviados a sus destinos específicos. El MC puede almacenar mensajes que son ya sea enviados desde una estación móvil o destinada a una estación móvil. Tras el almacenamiento y la entrega de mensajes cortos, el MC ejecuta funciones de señalización para soportar las otras funciones de entrega, tanto como localización del MS y el status queries y el mapeo de las direcciones de destino.

Los mensajes cortos pueden ser enviados al MC desde una entidad funcional que incluya la función para soportar originaciones de mensaje SMS. Inversamente, los mensajes cortos pueden ser recibidos por cualquier entidad funcional que incluye la función para soportar terminaciones de mensaje. Estas entidades funcionales son conocidas como entidades de mensaje corto o short message entities. (SMEs)

Los SMEs son entidades que pueden originar mensajes cortos, terminar mensajes cortos, o hacer ambas cosas. Básicamente, el SME es un término genérico para

---

cualquier entidad que pueda enviar o recibir mensajes cortos mediante el SMS IS 41. Un SME puede ser asociado con una entidad con una entidad funcional IS-41 (HLR, MC, o MSC) o con una entidad externa a IS-41. Una estación móvil también requiere funcionalidad SME para soportar la transmisión de mensajes cortos originados por el móvil y la recepción de mensajes cortos terminados en los móviles.

### **Puntos de referencia.-**

La siguiente tabla presenta los puntos de referencia de la interface específica en la red IS-41C.

**TABLA A.1**

Interface	Interface Functional entities	Where addressed (most current standard)
A interface	BS-MSC	IS-634 & IS-653
Ai interface	MSC-PSTN	IS-93
B interface	MSC-VLR	IS-41-C
C interface	MSC-HLR	IS-41-C
D interface	HLR-VLR	IS-41-C
Di interface	MSC-ISDN	IS-93
E interface	MSC-MSC	IS-41-C
F interface	MSC-EIR	Not standardized
G interface	VLR-VLR	Not standardized
H interface	HLR-AC	IS-41-C

M interface	SME-SME, SME-MC, MC-MC	IS-41-C
N interface	MC-HLR	IS-41-C
Q interface	MC-MSC	IS-41-C
Um interface	MS-BS	ANSI/TIA/EIA-553-AIS- 91, IS-95A, IS-136*

\*Hay que notar que las interfaces de radio hacen que exista., pero estas son las especificaciones más representativas de la tecnología soportada por IS-41C.

Las interfaces M, N, y Q fueron desarrolladas para soportar el MC y el SMEs. Estas interfaces representan la señalización y las comunicaciones de servicio portador requeridos para proveer las funciones SMS.

EL IS-41C y otros estándares relacionados han evolucionado para direccionar muchas de las interfaces que fueron incluidas, pero no aún estandarizadas, en la red original del modelo de referencia (IS-41-A y IS-41-B). La estandarización de la interface A es un requerimiento del nuevo sistema. Los estándares de la interface A soporta la interoperación de los sistemas de radio y de los MSCs desarrollados por fabricantes diferentes. Corriente hay 3 protocolos estandarizados por la TIA para el uso de una interface A: SS7- basado en la (TIA/EIA IS-634), frame relay basado (también en la TIA/EIA-634) y en ISDN-basado en la TIA/EIA IS-653).

Las interfaces Ai y Di son especificadas en la especificación de la TIA (TIA/EIA IS-93). El A y el D en estas interfaces permanecen en lo analógico y digital, respectivamente. El subíndice i permanece para la interface. Ellas son las interfaces solamente en la red del modelo de referencia del cual las designaciones de las letras (A y D) actualmente permanecen en palabras. Ellas representan las interfaces entre la red celular y la PSTn analógica e ISDN, respectivamente. Estas interfaces sin embargo son tratadas como una interface particular en IS-93, soportando tanto protocolos de interconexión de red análogo y digital. Esta interface especificada puede ser mapeada dentro de ya sea en la interface Ai o Di del modelo. LA razón es que la distinción entre el uso de protocolos de señalización de red diferente para la PSTN y la ISDN no existe en la forma de las redes que son desarrolladas hoy en día.

La interface H esta estandarizada en IS-41-C. Representa la interface entre el HLR y el AC soportando las funciones de autenticación. Esta interface fue originalmente estandarizada en la especificación de la TIA TSB 51, como un addendum al ya publicado IS-41-B. LA información en TSB 51 fue subsecuentemente redefinida, revisada e incorporada en IS-41-C.

## **Subsistemas**

La mensajería de IS41C usando los subsistemas siguientes:

1. Mobile Application Part (MAP)
  2. Home Location Register (HLR)
-

3. Visitor Location Register ( VLR)
4. Mobile Switching Center (MSC)
5. Authentication Center (AuC)

Entre el HLR y el MSC, se necesita los subsistemas 1, 2, 3, y 4 activos. El subsistema 5 se utiliza entre el HLR y la AuC.

## **OPERACIONES DE LOS MENSAJES DE AUTENTICACION.-**

Las operaciones de mensajes son agrupadas en bloques usados para construir secuencias de mensajes más complejas. Esta parte del modulo define la autenticación celular por roaming automático.

Los siguientes mensajes TCAP de IS-41 revisión C están asociados con la autenticación:

- AUTHENTICATION REQUEST (AUTHREQ)
  - AUTHENTICATION DIRECTIVE (AUTHDIR)
  - BASE STATION CHALLENGE (BSCHALL)
  - AUTHENTICATION STATUS REPORT <sup>1</sup> (ASREPORT)
-

- AUTHENTICATION FAILURE REPORT <sup>1</sup> (AFREPORT)
- SECURITY STATUS REPORT (TSB-51) (SSREPORT)

Estos mensajes logran 3 funciones básicas de autenticación. Estas funciones son:

1. Autenticación del MS
2. SSD Updating (el MS es instruido para calcular un nuevo valor de SSD)
3. Actualización del contador de historial de llamadas. ( MS indica cuando incrementar el Call History Counter)

### **AUTHENTICATON REQUEST**

Una Authentication Request (AUTHREQ) es un mensaje de autenticación iniciado por el MSC para autenticar a un MS. Si el SSD no esta compartido con el VLR, la AUTHREQ siempre ira al AC. Si el SSD se comparte con el VLR, entonces según el tipo del acceso del sistema se determinará si el VLR puede mantener el AUTHREQ o si debe ser enviado al AC.

- La autenticación por control de canal de radio ( MSC soporta global Challenge) que resulta en un AUTHREQ enviado por el MSC da lugar a:
  - Initial Registration (Registro Inicial)
  - Call Origination (Origen de llamada)
  - Page Response (Call Termination)



Nota: Si el VLR tiene SSD del MS, entonces el VLR procesara la autenticación y el AUTHREQ no será reenviado al AC.

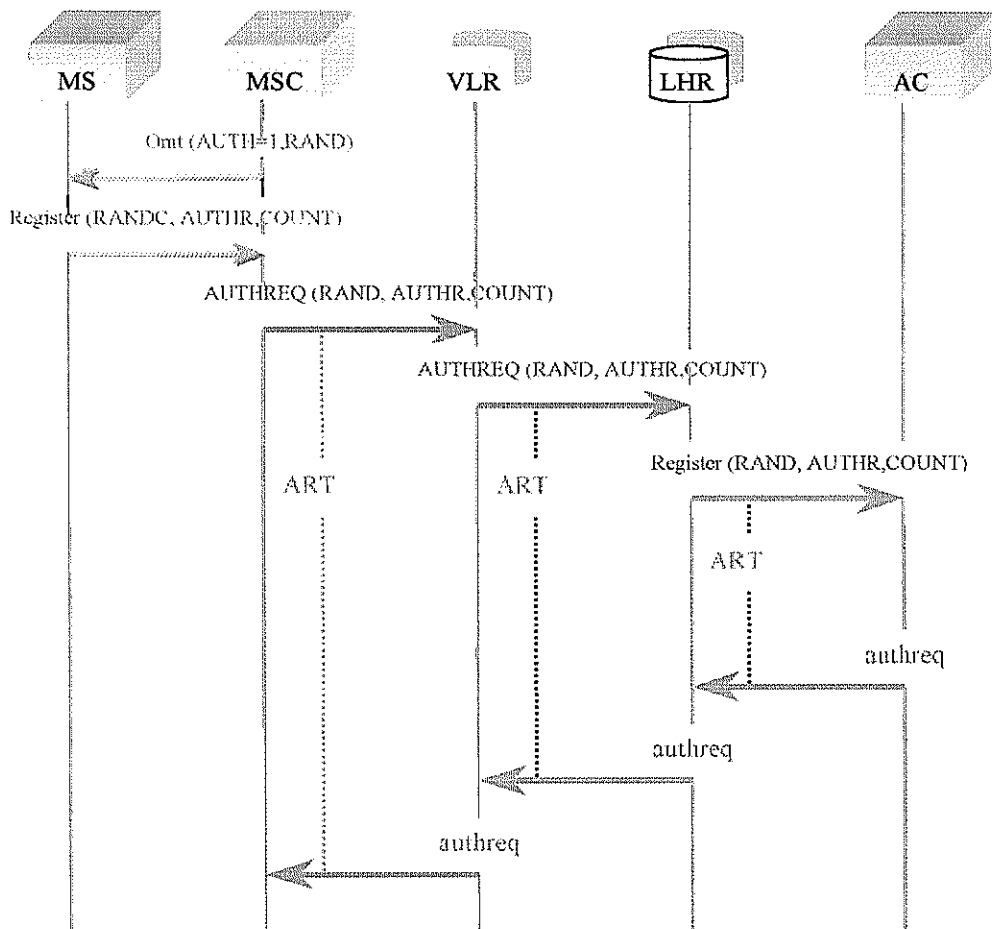
- La autenticación del canal de voz (MSC hace uso de Unique Challenge.) que resulta en una AUTHREQ enviada por el MSC dando lugar a:
  - El MSC no soporta recusación global en canal de radio.
  - Initial Registration (Registro Inicial)
  - Call Origination (Origen de llamada).
  - Page Response (Llamada en espera o conferencia de llamada)
- Flash Request (llamada en espera o conferencia)

Nota: Si el VLR tiene SSD del MS, entonces el VLR procesara la autenticación y hace una petición al MSC para que inicie un Unique Challenge. El AUTHREQ no se reenviara al AC.

---

FIGURA A.2

AUTHENTICATION REQUEST



## **AUTHENTICATION DIRECTIVE**

El Authentication Directive ( AUTHDIR) es un mensaje de autenticación usualmente iniciado por el AuC. Si el SSD esta compartido con el VLR, el VLR puede iniciar un AUTHDIR con una petición de recusación única para el MSC que enviara al MS.

El mensaje Authentication directive inicia cualquiera de Los siguientes escenarios de autenticación de mensaje:

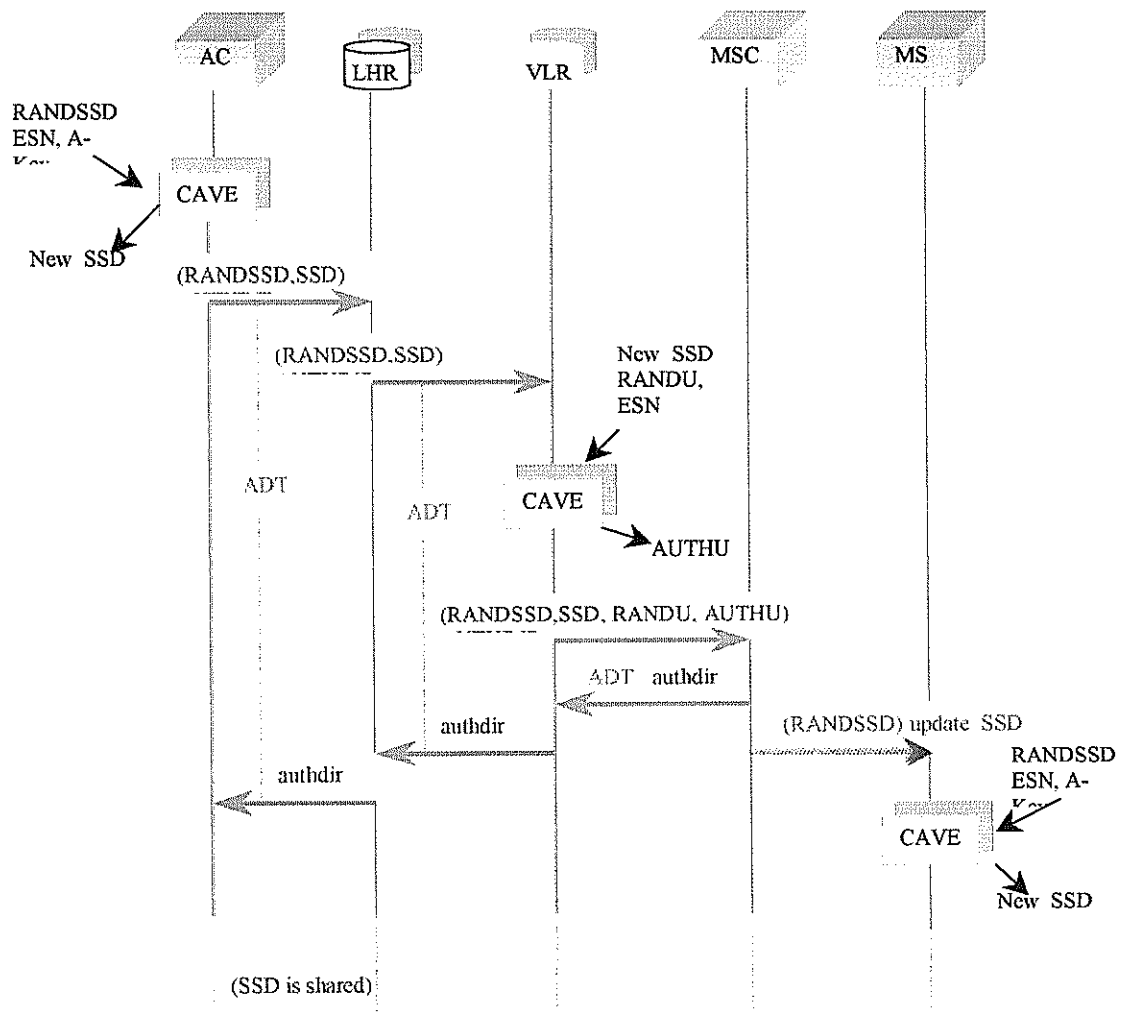
1. Actualización del SSD cuando el SSD esta compartido
2. Actualización del SSD cuando el SSD no esta compartido
3. VLR inicia una recusación única cuando el SSD esta compartido
4. AuC Inicia una recusación única cuando el SSD no esta compartido
5. Revocación de la comparación del SSD
6. Actualización del valor de parámetro Call History Count (COUNT)

En este ejemplo, AuC envía una AUTHDIR pidiendo al MS actualizar el SSD usado el RANDSSD como una entrada de valor aleatorio para el algoritmo CAVE. El SSD esta compartido en este ejemplo.

---

**FIGURA A.3**

AUTHENTICATION DIRECTIVE



## **BASE STATION CHALLENGE**

La Base Station Challenge (BSCHALL) es una secuencia de mensajes que permite al MS verificar el nuevo valor calculado del SSD

El MS usa este nuevo SSD, MIN, ESN y un numero aleatorio (RANDBS) como valor de entrada para el algoritmo CAVE. El MS envía la Base Station Challenge al MSC sobre la interface aérea de radio la cual contiene la entrada del numero aleatorio (RANDBS). El MSC pasa esta información al VLR en un mensaje Base Station Challenge (BSCHALL). El VLR usa esta copia del nuevo SSD, MIN, ESN y el numero aleatorio (RANDBS) que fue recibido del MS como una entrada para el algoritmo CAVE.

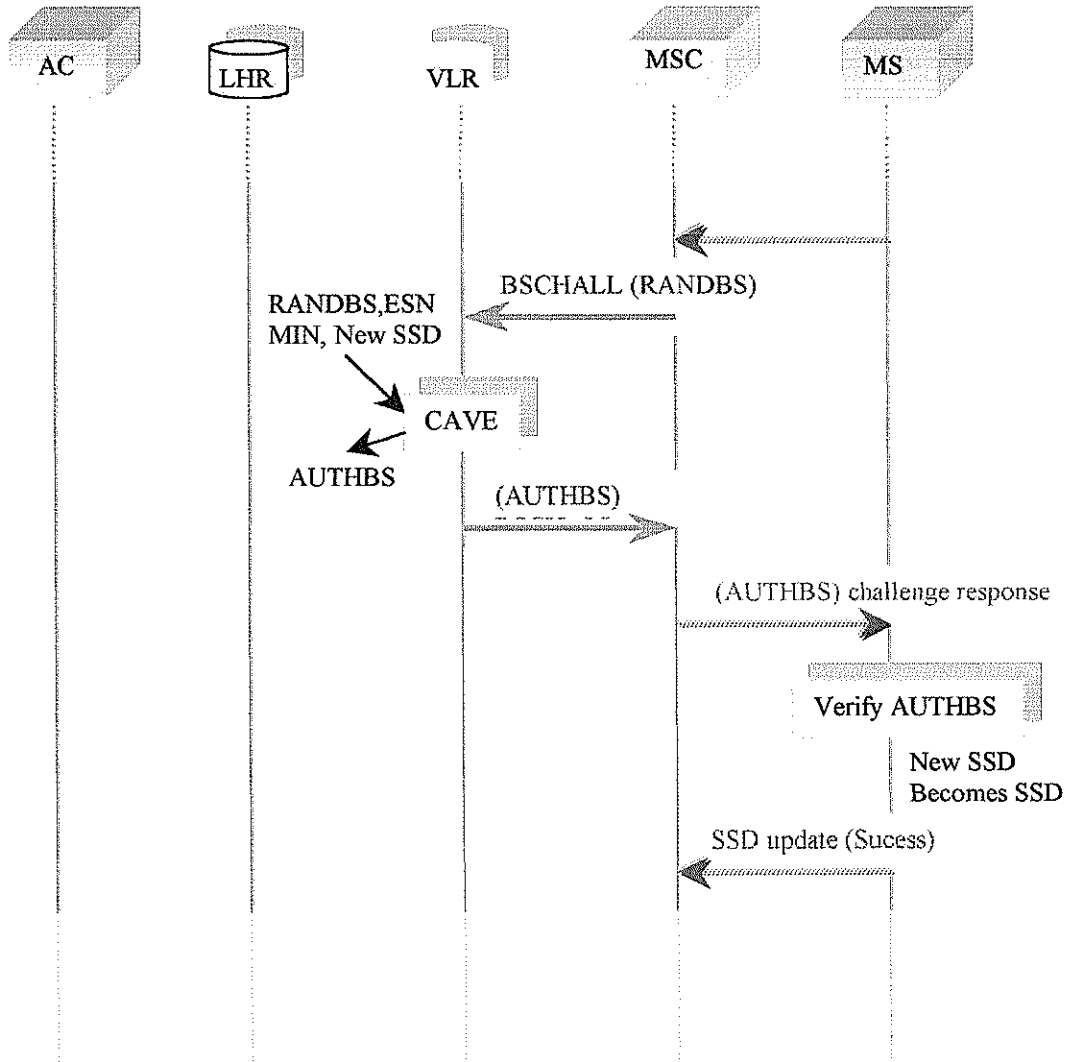
El VLR envía el numero resultante de la salida del CAVE al MSC en una respuesta BSCHALL. El MSC pasa el BSCHALL al MS sobre la interface aérea de radio.

Una vez que el MS recibe el BSCHALL desde el MSC, el MS compara el RANDBS que ha calculado con el RANDBS que ha recibido del MSC. Si Los valores coinciden entonces el MS reemplaza el antiguo SSD con el nuevo SSD. Después que el MS ha actualizado el SSD, este envía un mensaje de Successful SSD Update al MSC.

---

FIGURA A.4

BASE STATION CHALLENGE



## **AUTHENTICATION STATUS REPORT (ASREPORT)**

El mensaje Autenticación Status Report (reporte de estado de Autenticación, ASREPORT) es usado para reportar la seguridad de algún evento asociado al MSC que fue iniciado por AuC o VLR.

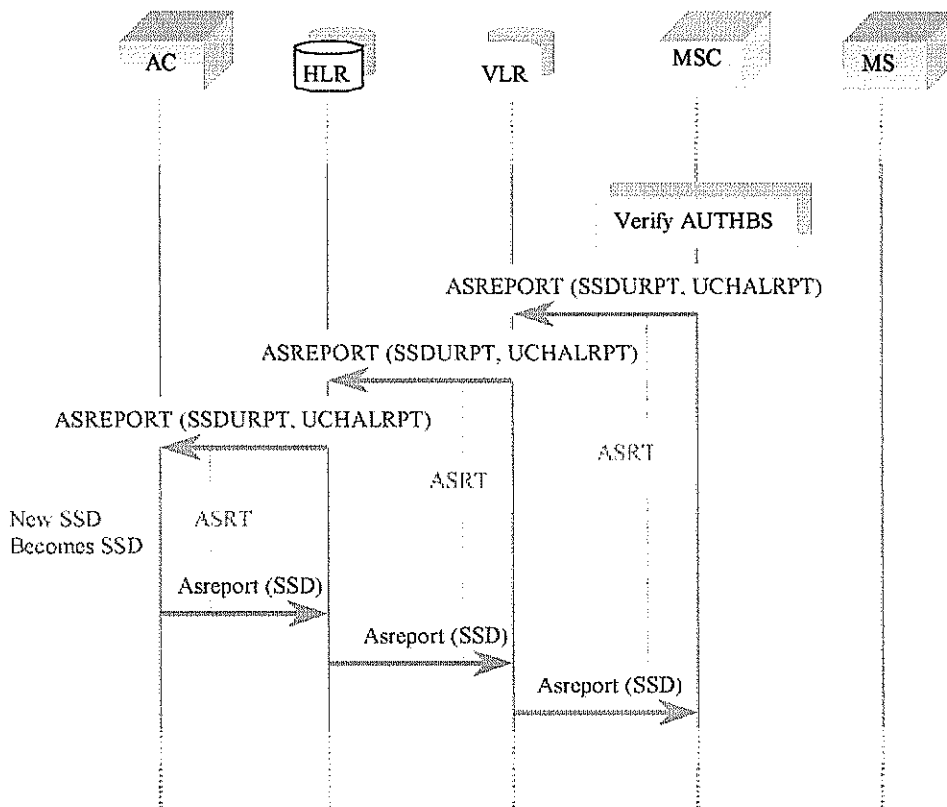
Después de que el MSC verifique el valor del AUTHU que recibió del MS, este enviaría un ASREPORT con una indicación de suceso o no suceso para la actualización del SSD y del Unique Challenge

Si el ASREPORT indica que se a completado la operación iniciada por el VLR, entonces el VLR envía de vuelta una respuesta *asreport* al MSC, en caso contrario el VLR reenviara el ASREPORT al AuC (vía HLR). El AuC retorna una respuesta *asreport* al MSC (vía HLR y VLR).

---

**FIGURA A.5**

**AUTHENTICATION STATUS REPORT (ASREPORT)**



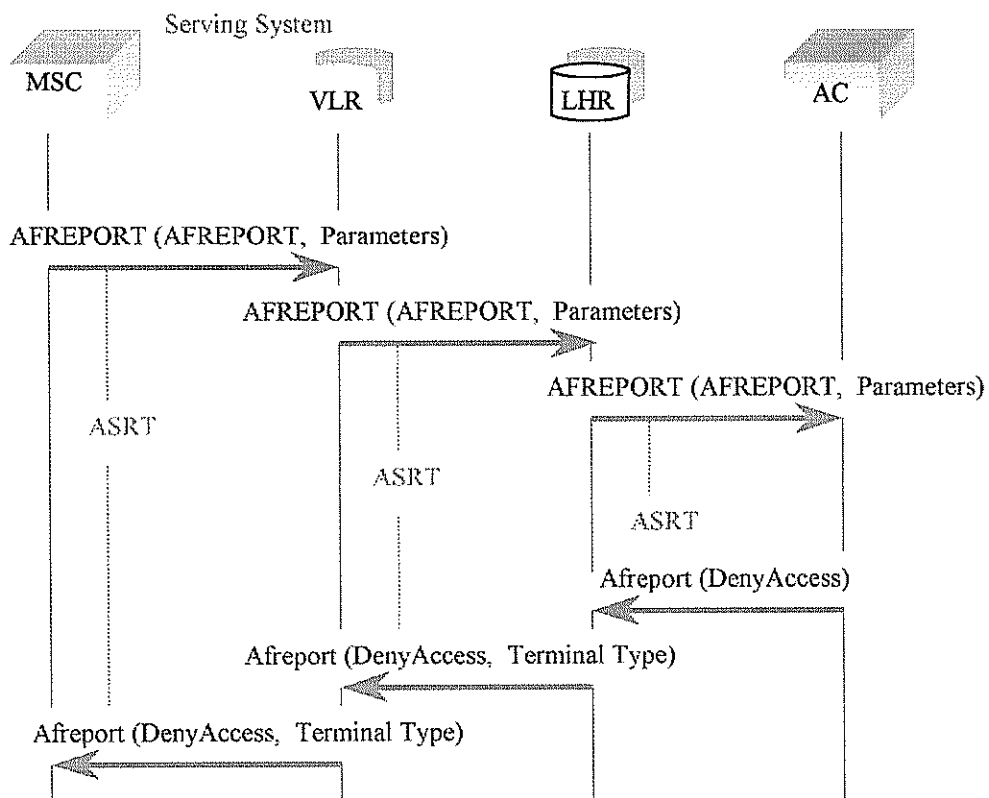


## AUTHENTICATION FAILURE REPORT (Reporte de falla de autenticación)

El Authentication Failure Report message ( AFREPORT) se usa para reportar la falla de un evento de seguridad asociado con un MSC el cual no es iniciado por el AC o VLR.

**FIGURA A.6**

### AUTHENTICATION FAILURE REPORT



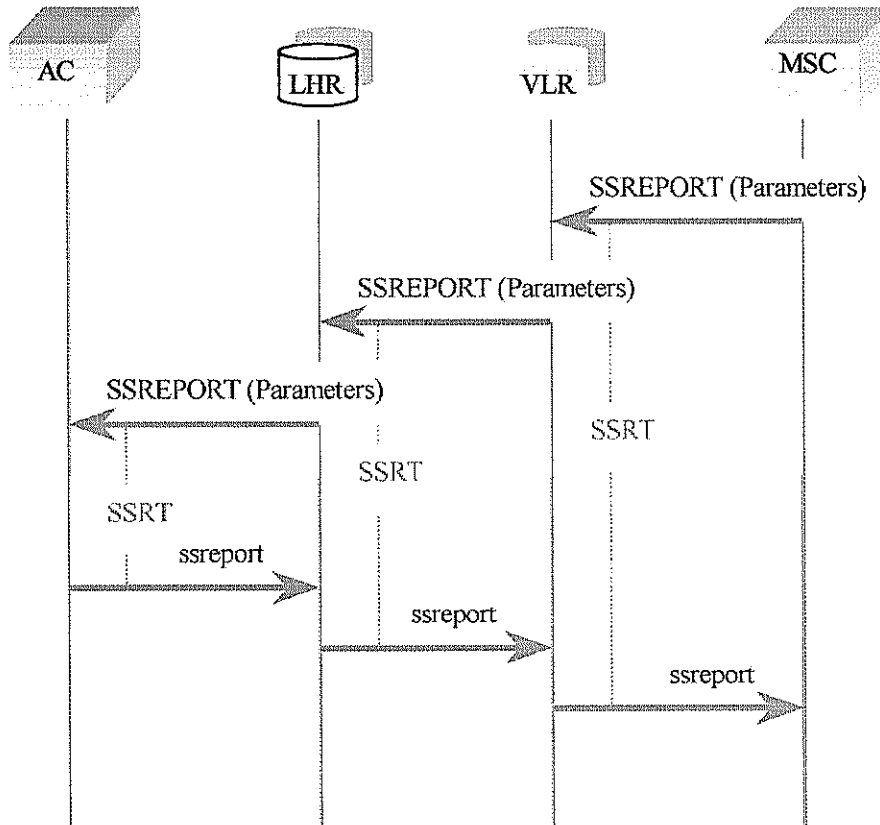
## SECURITY STATUS REPORT

El Security Status Report message ( SSREPORT ) fue definido por el Boletín de Sistemas de Telecomunicaciones #15 ( TSB-51) el cual reconoce las actualizaciones y modificaciones del IS-41.

Debido a cierta confusión creada por la implementación de solo este mensaje, el SSREPORT message fue reemplazado por dos mensajes en la nueva revisión IS-41C, el mensaje ASREPORT y el mensaje AFREPORT.

FIGURA A.7

## SECURITY STATUS REPORT



# **OPERACIONES DE LOS MENSAJES DE AUTENTIFICACION**

En este momento todas las operaciones de mensajes que se aplican al Centro de autenticación ya han sido discutidas. Ninguno de estos mensajes pueden proveer autenticación por sí solos. Tienen que ser usados juntos en un flujo de mensajes para completar la autenticación celular.

## **SECUENCIA DE MENSAJES DE AUTENTIFICACION**

Ahora que conocemos los mensajes básicos de operaciones de autenticación, lo siguiente es poner todos estos mensajes juntos para manejar los diferentes escenarios.

Todas las posibles secuencias de autenticación de mensajes no se cubren en este documento. Los siguientes flujos de mensajes han sido seleccionados para ser discutidos:

- Registro Inicial con autenticación sobre canal de radio
  - Originación con autenticación sobre canal de radio
  - Terminación con autenticación sobre canal de radio
  - Autenticación sobre canal de voz
  - VLR Initiated Unique Challenge
  - Actualización del SSD con SSD compartido.
-

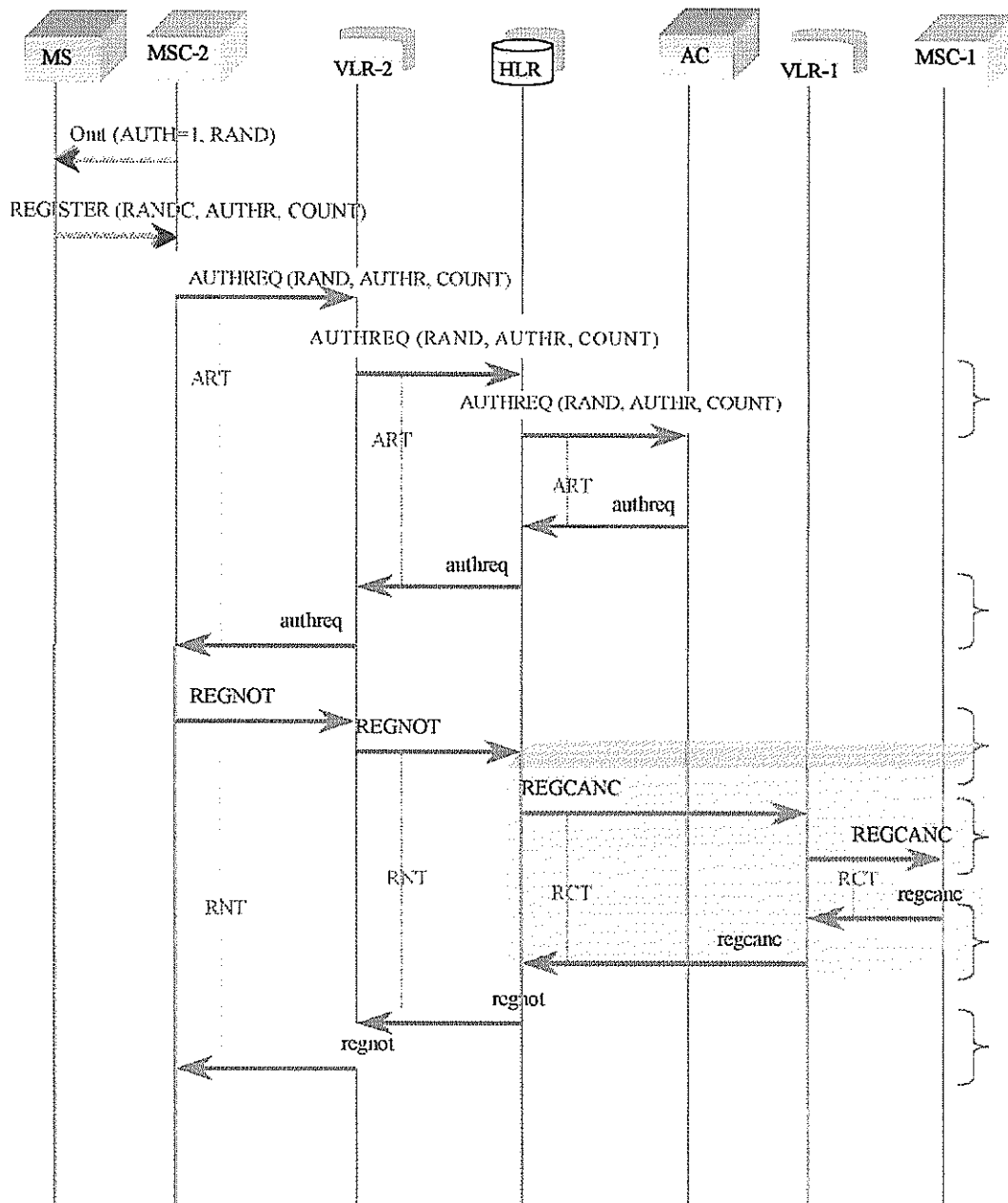
## **REGISTRACION INICIAL CON AUTENTICACION EN EL CANAL DE RADIO**

- a) El MS determina del Overhead Message Train (OMT) que un nuevo sistema servidor ha entrado y que es requerida una autenticación (AUTH=1). El número aleatorio (RAND) que es usado para la autenticación también puede ser obtenido por el MS en ese momento. El MS ejecuta el algoritmo CAVE usando el SD almacenado, el ESN, el MIN y el valor RAND para producir el Registration Authentication Result (AUTHR)
  - b) El MS se registra en el nuevo MSC-V, enviándole el MIN, ESN y el AUTHR, y el RANDC derivado del RAND usado para calcular el AUTHR.
  - c) El MSC-2 verifica el RANDC enviado por el MS y envía el apropiado valor de RAND en un AUTHREQ al nuevo VLR servidor VLR-2.
  - d) VLR-2 reenvía el AUTHREQ al HLR asociado con ese MIN, donde el HLR reenvía el AUTHREQ a su AC.
  - e) El AC verifica el MIN y el ESN entonces ejecuta el CAVE usando el SSD-A actualmente almacenado, el ESN, el MIN1 y el RAND para producir un registration Authentication Result (AUTHR). El AC verifica que el AUTHR recibido por el MS coincida con el calculado por él CAVE.
  - f) El AC envía un authreq al HLR. El authreq puede incluir el SSD y las directivas para manejar una recusación única, para actualizar el SSD del MS o para actualizar el contador del MS de acuerdo con la forma de administración local del AC/HLR.
-

- g) El HLR reenvía el AUTHREQ al VLR-2 el cual lo reenvía al MSC-2 siguiendo con una autenticación exitosa del MS, el MSC-2 envía un REGNOT a al VLR-2. El VLR-2 reenvía el REGNOT al el HLR
- h) Si el MS fue previamente registrado en otro sistema, el HLR envía un REGCANC al antiguo VLR-1. El VLR-1 reenvía el REGCANC al antiguo MSC-1. El MSC-1 regresa el regcac al VLR-1 y este al HLR. El HLR graba la nueva localización del MS en su memoria local y responde el regnot con un regnot que incluye la información requerida por el VLR-2. El VLR-2 reenvía el regnot al MSC-2
-

FIGURA A.8

INITIAL REGISTRATION WITH AUTHENTICATION OVER RADIO CHANNEL



## ORIGEN CON AUTENTIFICACION SOBRE CANAL DE RADIO

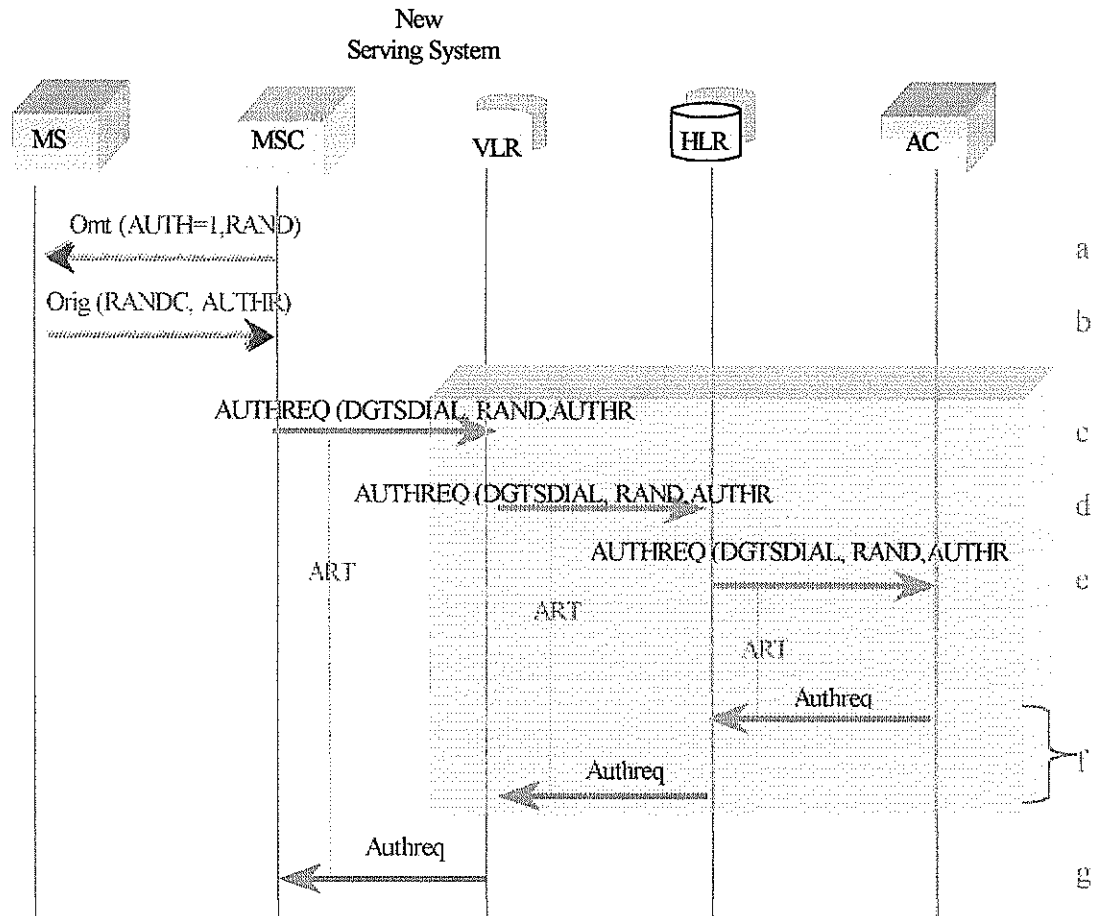
- a. El MS determina del Overhead Message Train (OMT) que una autenticación es requerida (AUTH=1). El número aleatorio usado para autenticar (RAND) puede también ser obtenido por el MS en este momento. Si no es así, el valor de cero es usado por el MS, como lo indica la autenticación TR-45. El MS ejecuta el CAVE usando los números digitados, el RAND, el ESN y el SSD almacenado, para producir el Origination Authentication Request.
  - b. EL MS envía un mensaje de originación al nuevo MSC-V, enviándole los números digitados, el MIN, el ESN, el Authentication Result (AUTHR) y el RANDC que es el RAND usado para calcular el AUTHR.
  - c. El MSC verifica el RANDC enviado por el MS y envía los números digitados al nuevo VLR con el valor apropiado de RAND en el AUTHREQ.
  - d. Si el SSD esta actualmente compartido con el VLR, el VLR realizara la validación del MS han e ira al paso h; caso contrario, el VLR reenviara el AUTHREQ al HLR asociado con el MIN.
  - e. El HLR reenviara el AUTHREQ al AC.
  - f. El AC verifica el MIN y el ESN reportados por el MS y entonces ejecuta el CAVE usando el SSD, el MIN y el ESN actualmente asociado con el MS a través del valor de RAND y los dígitos marcados provistos por el MSCV para producir el Origination Authentication Response (AUTHR). El AC verifica que el AUTHR recibido del MS coincide con el resultado del CAVE.
-

- g. El authreq incluiría el SSD y directivas para editar una recusación única (Unique Challenge), para actualizar el SSD del MS, o para actualizar el MS COUNT de acuerdo con las practicas administrativas del AC local. Alternativamente, el authreq incluiría Deny Access. El AC envía un authreq al HLR. El HLR reenvía el authreq al VLR.
  - h. El VLR regresa el authreq al MSC. Siguiendo una autenticación segura del MS, el MSC asigna el MS a un canal de voz analógico o a un canal de trafica digital o conserva la asignación actual.
-



FIGURA A.9

ORIGINATION WITH AUTHENTICATION  
OVER RADIO CHANNEL



Note: Voice/traffic channel shall be assigned by this time

## **TERMINACION CON AUTENTIFICACION SOBRE CANAL DE RADIO**

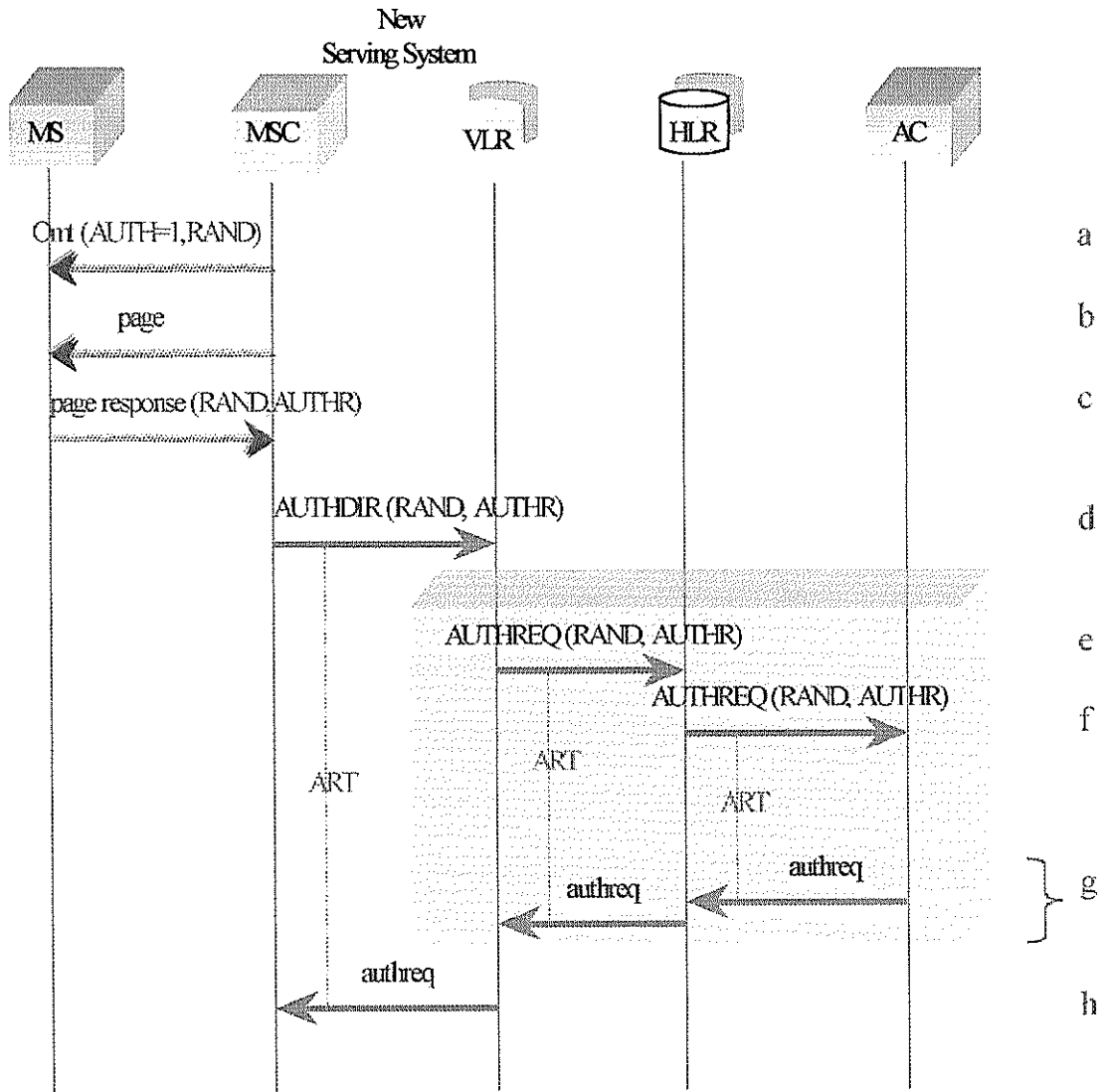
- a. El MS determina del Overhead Message Train (OMT) que una autenticación es requerida en los sistemas de acceso con AUTH=1. El número aleatorio usado para la autenticación (RAND) puede ser obtenido también por el MS en este momento; Si no es así el valor de cero es usado por el MS, como lo indica la autenticación por TR-45.
  - b. El MS reconoce un mensaje de rastreo con su MIN y ejecuta el CAVE usando el SSD que tiene almacenado, el ESN, el MIN y el valor RAND para producir el Termination Authentication Result (AUTHR)
  - c. El MS envía un mensaje de respuesta de rastreo al nuevo MSC-V entregándole el MIN, el ESN, el Authentication Result (AUTHR), y el RANDC que es el mismo del RAND usado para calcular el AUTHR.
  - d. El MSC verifica el RANDC enviado por el MS y envía el valor apropiado de RAND en un AUTHREQ al nuevo VLR.
  - e. Si el SSD es compartido con el VLR, el VLR realizaría la validación del MS e iría al paso i; caso contrario, el VLR reenviaría el AUTHREQ al HLR asociado con el MIN.
  - f. El HLR reenvía el AUTHREQ a su AC.
  - g. El AC verifica el MIN y el ESN enviados por el MS. Entonces el AC ejecuta el CAVE usando el SSD almacenado, el ESN, el MIN asociado al MS, y el RAND
-

entregado por el sistema servidor para producir un termination Authentication Response (AUTHR). El AC verifica que el AUTHR recibido por el MS coincida en los resultados del CAVE.

- h. El authreq incluiría directivas de edición de la recusación única, para actualizar el SSD del MS, o para actualizar el MS COUNT de acuerdo con las practicas administrativas del AC local. Alternativamente, el authreq incluiría un DenyAccess. El AC envía un authreq al HLR. El HLR reenvía el authreq al VLR.
  - i. El VLR retorna un authreq al MSC. Seguido de la autentificación exitosa del MS, el MSC asigna un canal de voz analógica, o un canal de trafica digital, o conserva la asignación existente.
-

**FIGURA A.10**

**TERMINATION WITH AUTHENTICATION  
OVER RADIO CHANNEL**



Note: Voice/traffic channel shall be assigned by this time

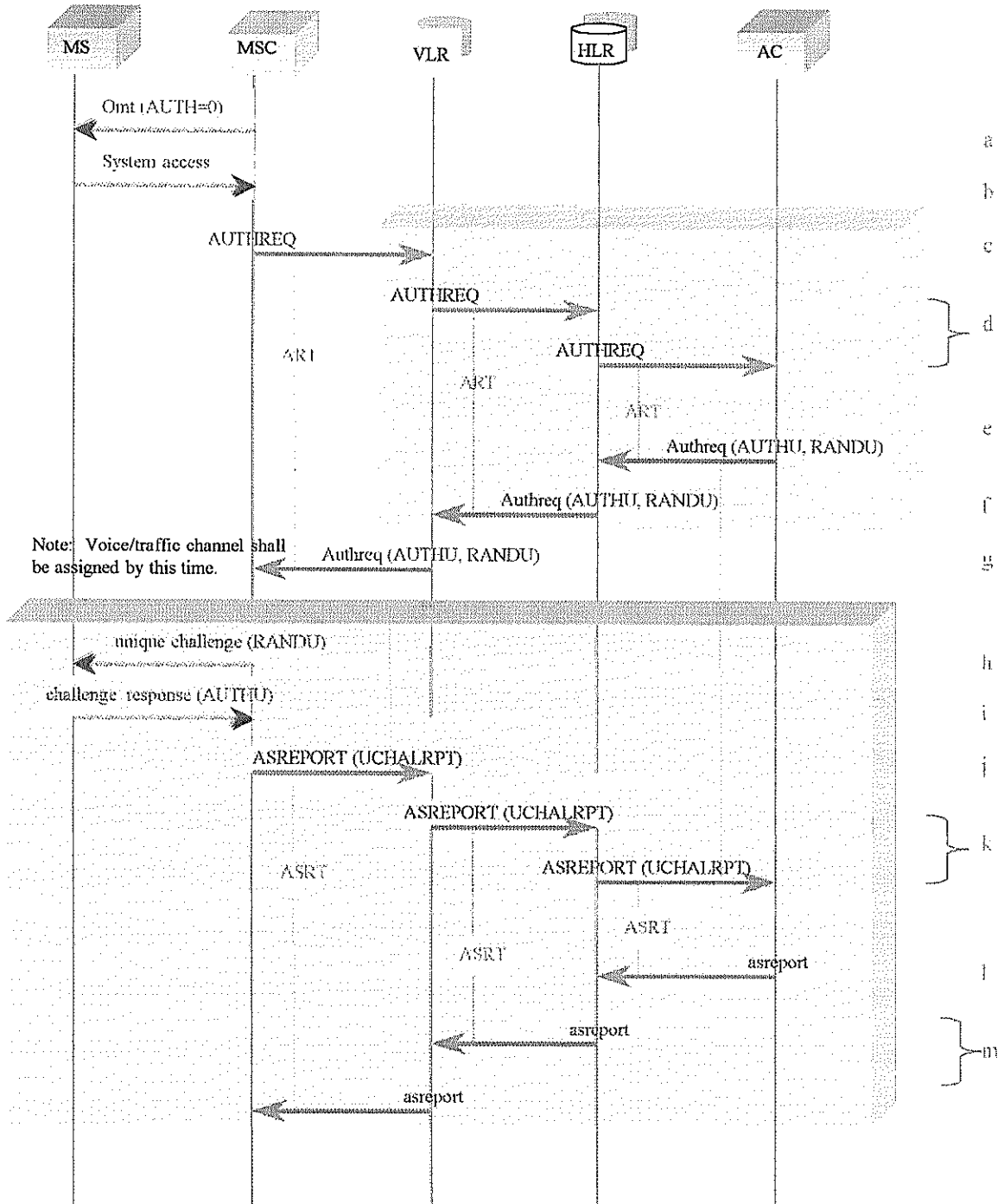
## AUTENTICACION SOBRE CANAL DE VOZ

- a. El MS determina por el Overhead Message Train (OMT) que una autenticación no es requerida sobre los sistemas de acceso ( AUTH=0)
  - b. El MS envía un Message system Access (registration , origination o page response) al MSC-V , enviándole solo el MIN y el ESN.
  - c. El MSC-V envía un AUTHREQ al VLR servidor con el System Access Type seteado como UNSPECIFIED.
  - d. El VLR reenvía el AUTHREQ al HLR asociado con el MIN. El HLR reenvía el AUTHREQ al AC.
  - e. El AC verifica el MIN y el ESN enviados por el MS. El AC escoge una variable aleatoria única (RANDU) y ejecuta el CAVE usando el SSD almacenado, el ESN y el MIN asociados con el MS , para producir un Unique authentication Response ( Authu) El AC envía un authreq al HLR incluyendo el RANDU y el resultado del AUTHU esperado.
  - f. El HLR reenvía el authreq al VLR servidor.
  - g. El VLR servidor ENVIA UN authreq al MSC-V, conteniendo los valores del AUTHU y el RANDU recibidos en el authreq del HLR. El MSC-V asigna el MS a un canal de voz analógico o a un canal de tráfico digital. Opcionalmente (específicamente si el system Access es un registration), el Unique Challenge Messages podría ser intercambiado sobre el canal de control, antes de la asignación del canal de voz o de tráfico, como lo describen los siguientes pasos.
-

- h. El MSC –V envía una orden de recusación única al MS usando el RANDU provisto por el authreq.
  - i. El MS ejecuta el CAVE usando el RANDU y el SSD almacenado , el ESN y el MIN para producir el Authentication Result ( AUTHU) el cual es enviado al MSC –V. El MSC-V compara los valores de AUTHU provistos en el authreq con los recibidos del MS.
  - j. El MSC-V envía un ASREPORT al VLR servidor indicando suceso o falla en la recusación única.
  - k. El VLR reenvía el ASREPORT al HLR. El HLR reenvía el ASREPORT a su AC.
  - l. El AC responde con un asreport que incluiría el SSD y las directivas para denegar el acceso o la actualización del SSD.
  - m. El HLR reenvía el asreport al VLR servidor. El VLR servidor envía un asreport al MSC-V.
-

FIGURA A.11

AUTHENTICATION OVER VOICE CHANNEL



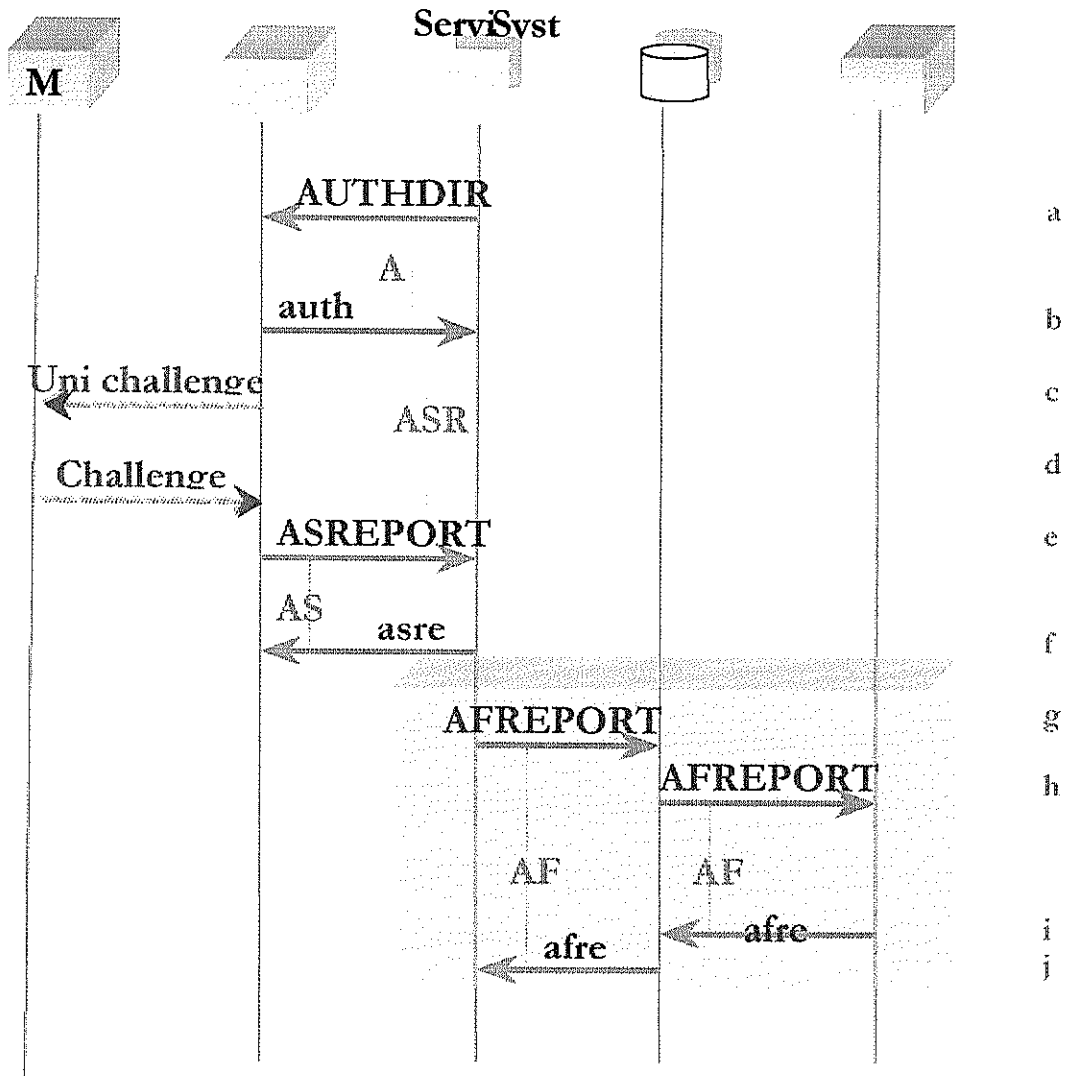
## **VLR INICIANDO UN UNIQUE CHALLENGE**

- a. El VLR servidor escoge una variable aleatoria única (RANDU) y ejecuta el CAVE usando el SSD almacenado, el ESN y el MIN asociado con el MS, para producir el Authentication Response para la recusación única ( AUTHU)
  - b. El authdir del MSC-V hacia el VLR sirve solo para informar al VLR que el MSC-V ha aceptado la directiva.
  - c. El MSC-V envía una orden de recusación única al MS usando el RANDU provisto por el AUTHDIR.
  - d. El MS ejecuta el CAVE usando el RANDU y el SSD almacenado, el ESN y el MIN para producir un Unique Challenge Response ( AUTHU) el cual es enviado al MSC -V,
  - e. El MSC-V compara el valor del AUTHU provisto por el AUTHDIR con el recibo por el MS. El MSC-V envía un ASREPORT al VLR indicando que la recusación única se ha completado.
  - f. El VLR servidor regresa un asreport al MSC-V
  - g. Si la operación falla, el VLR servidor envía un AFREPORT al HLR.
  - h. El HLR reenvía el AFREPORT al AC.
  - i. El AC envía un afreport al HLR, indicándole que la acción ha sido recibida del VLR.
  - j. El HLR reenvía el afreport al VLR.
-



FIGURA A.12

VLR INITIATED UNIQUE CHALLENGE



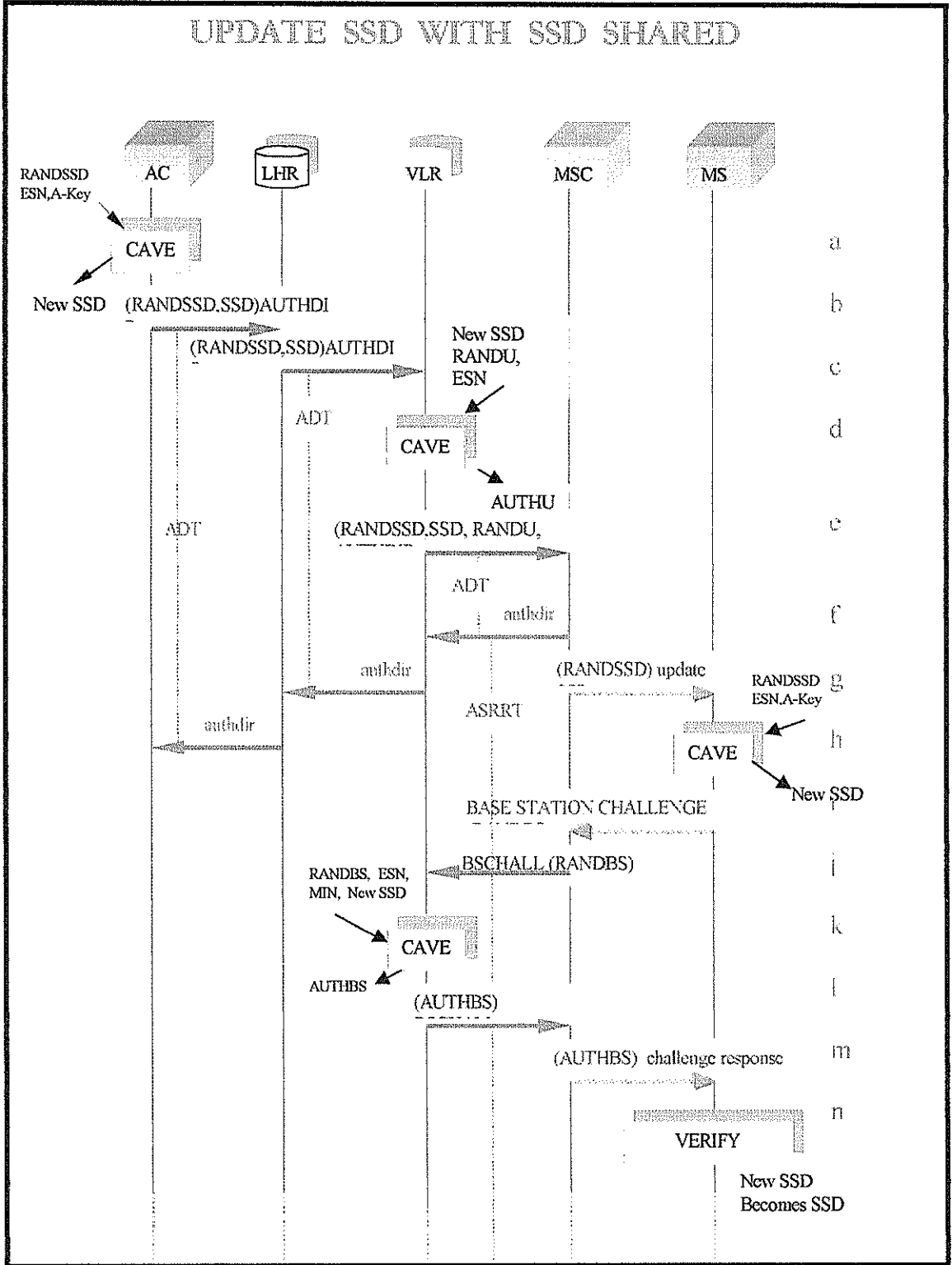
## **ACTUALIZACION DEL SSD CON EL SSD COMPARTIDO**

- a. El AC determina que el Shared Secret Data (SSD) debe ser actualizado. Esto puede ser por el resultado de un procedimiento administrativo en el AVC, expiración de un intervalo de tiempo de autenticación en el AC, o el reporte de violación de seguridad de un sistema ajeno.
  - b. Un AUTHDIR es enviado desde el AC al HLR asociado con el MS.
  - c. El HLR reenvía el AUTHDIR al VLR servidor actual.
  - d. El SSD pendiente seria usado para calcular el RANDU , el AUTHU y el AUTHB para la operación de actualización del SSD. El VLR escoge una variable aleatoria única ( RANDU) y ejecuta él CAVE usando el valor pendiente de SDD, el ESN, y el MIN asociado con el MS para producir una Unique Authentication Response. ( AUTHU).
  - e. El VLR reenvía el AUTHDIR al MSC incluyendo el RANDU y el resultado AUTHU esperado.
  - f. Un AUTHDIR vacio es enviado desde el MSC-V al VLR servidor. El authdir sirve solo para informar al VLR que el MSC-V ha aceptado la directiva. El VLR servidor reenvía el AUTHDIR al HLR. El HLR reenvía el authdir al AC.
  - g. El MSC-V envía una orden de actualización del SSD al MS usando el valor de RANDSSD provisto por el AC. El mensaje puede ser enviado por el canal de control o por el canal de voz o trafico.
  - h. El MS ejecuta él CAVE para producir un valor pendiente de SSD usando el valor RANDSSD provisto por el SSD Update order, el ESN y el A-key.
-

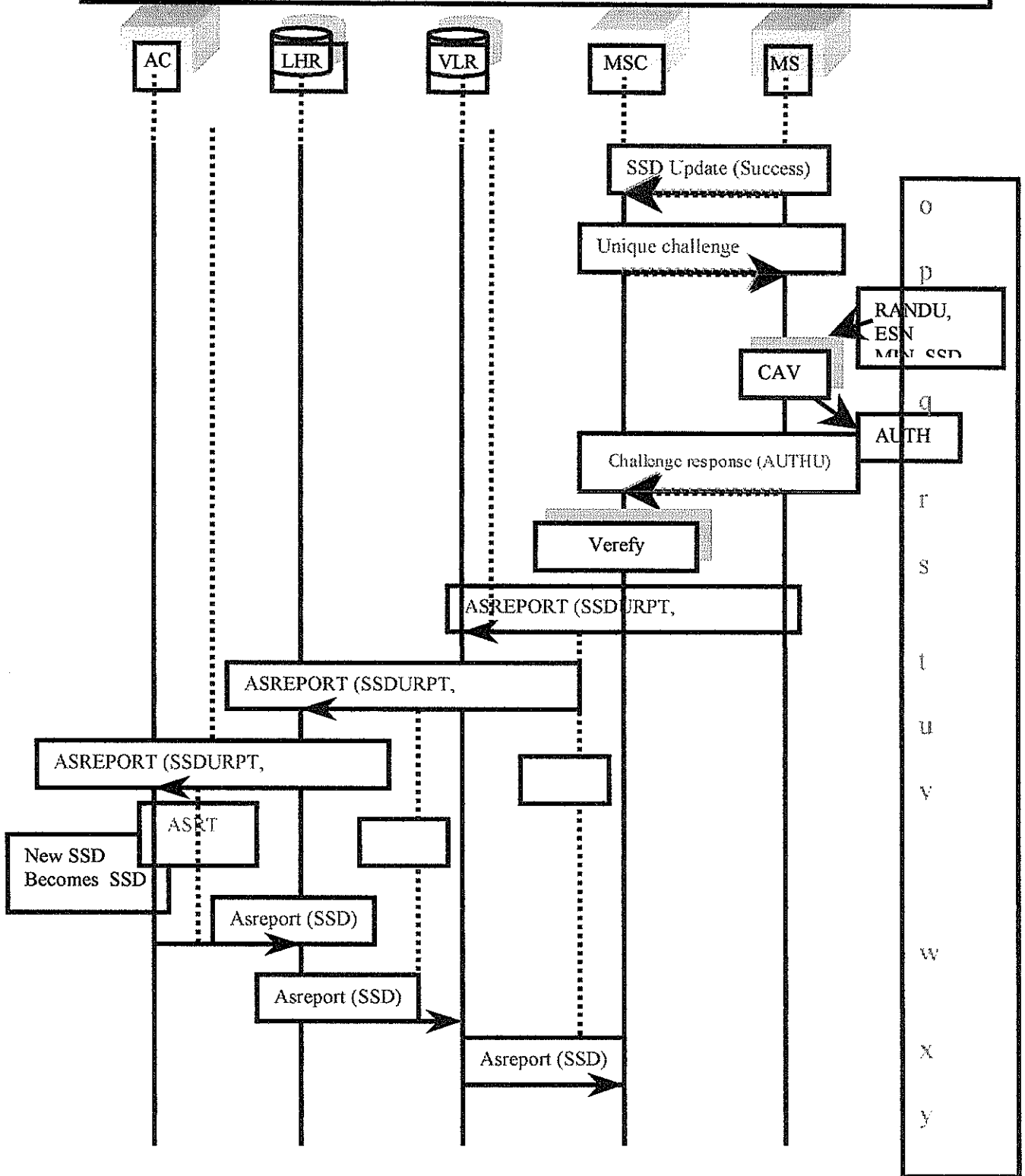
- i. El MS selecciona un número aleatorio (RANDBS ) y envía una orden de recusación de estación base al MSC-V incluyéndole el valor de RADS
  - j. El MS ejecuta el CAVE para producir un Authentication Result ( AUTHBS) usando el valor pendiente de SSD, el ESN, el MIN y el número aleatorio (RANDBS). El VLR también ejecuta el CAVE para producir un Authentication Result (AUTHBS) usando el valor pendiente del SSD, el ESN ,el MIN del MS y el número aleatorio (RANDBS) provisto por el MS.
  - k. El VLR provee su valor calculado de AUTHBS al MSC-V en un bschall.
  - l. El MSC-V pasa esta información a través del MS en un Base Station Challenge response Message.
  - m. Si el AUTHBS resultante provisto por el VLR coincide con el valor calculado por el MS, el MS almacena el valor del SSD pendiente para subsecuentes ejecuciones del CAVE.
  - n. Si el resultado de AUTHBS provisto por el VLR coincide con el valor calculado por el MS, el MS almacena el valor pendiente del SSD para su uso en ejecuciones subsecuentes de CAVE.
  - o. El MS envía un mensaje de confirmación de actualización de SSD al MSC-V
  - p. El MSC-V envía una orden de recusación única al MS usando el RANDU provisto en el AUTHDIR
  - q. El MS ejecuta el CAVE usando el RANDU y el SSD actualmente almacenado, el ESN, y el MIN para producir una Authentication Response para la recusación única. (AUTHU)
-

- r. El MS envía un AUTHU al MSC-V
  - s. El MSC-V envía un ASREPORT al VLR servidor indicando que la actualización del SSD se ha completado exitosamente.
  - t. El VLR servidor reenvía el ASREPORT al HLR y remueve el SSD pendiente.
  - u. El HLR reenvía el ASREPORT al AC.
  - v. El AC almacena el valor pendiente de SSD para su uso en ejecuciones subsecuentes de CAVE por el MS si la actualización de SSD ha sido exitosa
  - w. El AC envía un asreport indicando que servicio será provisto al MS. El AC incluye el nuevo SSD en el asreport para compartirlo con el VLR.
  - x. El HLR reenvía el asreport al VLR servidor. El VLR el SSD recibido
  - y. El VLR servidor reenvía el asreport al MSC servidor.
-

FIGURA A.13



UPDATE SSD WITH SSD SHARED (CONTINUED)



# ESTANDAR IS-136

## INTRODUCCIÓN

Es a menudo suponer que el estándar AMPS/D-AMPS (IS-136) para comunicaciones inalámbricas es un estándar regional el cual esta solamente implementado en Norte América. La realidad se presenta de otra manera. Primero se desarrollo en los Estados Unidos, el AMPS también ha ganado mucha atención a través del mundo.

Hoy en día su versión digital D-AMPS (IS-136) es encontrado aproximadamente en 90 países en todo el mundo, y cuenta cerca de 74 millones de suscriptores. Los tres estándares inalámbricos (D-AMPS, GSM, PDC) ampliamente implementados están basados en la misma tecnología TDMA. Este estándar es usado en sistemas PCS y esta estructurado en diferentes capas cada una con propósitos diferentes. Este concepto hace que sea más fácil comprender las interacciones entre la estación base y el celular a través de la interface aérea. Además este estándar especifica la adición de un canal de control digital DQPSK para la existencia del canal de control FSK usado en AMPS y en el

---

sistema celular en modo dual (IS-54B). También especifica un magnífico mejoramiento del codificador de voz digital, nuevas características celulares y otros atributos de protocolo que permiten una estupenda administración móvil y un mejor servicio celular. El protocolo IS 136 puede ser usado tanto en la banda celular de los 800 MHz y en la banda de los 1900 MHz de los PCS.

Este documento da una rápida visión del protocolo IS-136, con énfasis en la funcionalidad que no está presente en los protocolos previos celulares tanto como en AMPS y en IS-54B. En este documento, las descripciones serán hechas desde la perspectiva del móvil puesto que este es el enfoque del estándar.

## **NUEVOS SERVICIOS**

El estándar IS 136 introduce un número de nuevas características. Algunas de las más importantes se enuncian aquí:

- Compatibilidad entre la banda celular de los 800 MHz y la banda de los 1900 MHz en PCS.
  - Mejor calidad de voz: Esto produce una reducción del ruido en el canal de voz y evita que las llamadas sean infructuosas.
  - Mensajería corta en dos vías.
  - Llamadas de emergencia.
-



- Mejoramiento de la identificación de la parte llamada, y
- Servicios rebajados para sistemas privados y residenciales.

Los sistemas privados permiten que una organización contrate los servicios con el carrier celular para ofrecerle alternativas de planes tarifarios para suscriptores dentro de la organización. La gente que usa teléfonos móviles no registrados con la organización debería ser dado el servicio en una tasa regular.

Los sistemas residenciales permiten a los teléfonos móviles con IS-136 duplicarse como teléfonos alámbricos dentro del hogar. En efecto el hogar debería tener su propia estación base enganchada en la red telefónica pública.

## **OPERACIÓN EN MODO DUAL**

Los teléfonos PCS operan en la banda de los 800MHz y 1900 Mhz habilitando a los usuarios para recibir características de los sistemas antes mencionados y servicios para sistemas con IS 136 siempre y cuando los suscriptores hagan roaming. La habilidad en modo dual provee continuidad de servicio e interoperabilidad entre redes analógicas y digitales. Como resultado de esto un teléfono PCS puede tener acceso a todos los servicios inalámbricos sean usados en un sistema privado de infraestructura y para servir como un teléfono alámbrico digital en una casa.

---

## **EL CANAL DE CONTROL DIGITAL (DCCH)**

El Canal de Control Digital constituye el núcleo de la especificación del IS 136 y es el resurgimiento primario para tecnologías inalámbricas celulares TDMA. Se trata de un nuevo mecanismo de canal de control agregado al canal de control analógico (ACC), el canal de voz analógico (CVA) y el canal de tráfico digital (DTC) de la interface aérea TDMA. La tecnología del canal de control digital TDMA con plataforma IS 136 provee la infraestructura para PCS introduciendo nuevas funcionalidades y características importantes que hacen de los PCS un sistema muy poderoso. Entre las más importantes tenemos:

- **Identificación de la llamada:** Permite a los que llaman ser identificados antes de ser contestados.
  - **Autenticación:** Se incrementa la seguridad de los teléfonos y la resistencia a la clonación.
  - **Ambiente Jerárquico:** Provee soporte para operación de macroceldas y microceldas.
  - **Inteligente pre-exploración:** Permite un control más ajustado de la selección del sistema.
  - **Servicio de Mensajes Cortos:** se transfiere mensajes alfanuméricos hacia y desde el celular y teléfonos PCS.
-

- Sleep mode: es cuando el teléfono extiende su tiempo de espera e incrementa la vida de la batería.
- Roaming: Es capaz de hacer roaming entre frecuencias usando teléfonos en banda dual y provee soporte para roaming internacional.
- Indicador de mensajes en espera: Notifica a los usuarios que ellos tienen mensajes de correo de voz.
- Texto paging: Esta habilidad del estándar IS 136 permite a los operadores detectar mensajes de personas que llaman y enviarlos en texto paging a los teléfonos con PCS-IS 136.
- Privacidad de voz y datos para evitar fraude
- Identificaciones del sistema privado y residencial: Provee un servicio de oficina más simplificado y controlado y características de la estación base personal.
- Soporte de datos de Circuitos conmutados: Provee transmisión de datos altamente realizable para correo electrónico inalámbrico, fax y acceso a Internet.

## **El Ambiente del Canal de Control Digital**

Un canal de radio consiste de 2 frecuencias dentro de un espectro de RF que son separados por una distancia fijada. Estas dos frecuencias permiten a una celda y al

---

teléfono inalámbrico transmitir y recibir señales simultáneamente. La celda se comunica con el teléfono inalámbrico usando dos canales de radio diferentes: un canal de voz y un canal de control.

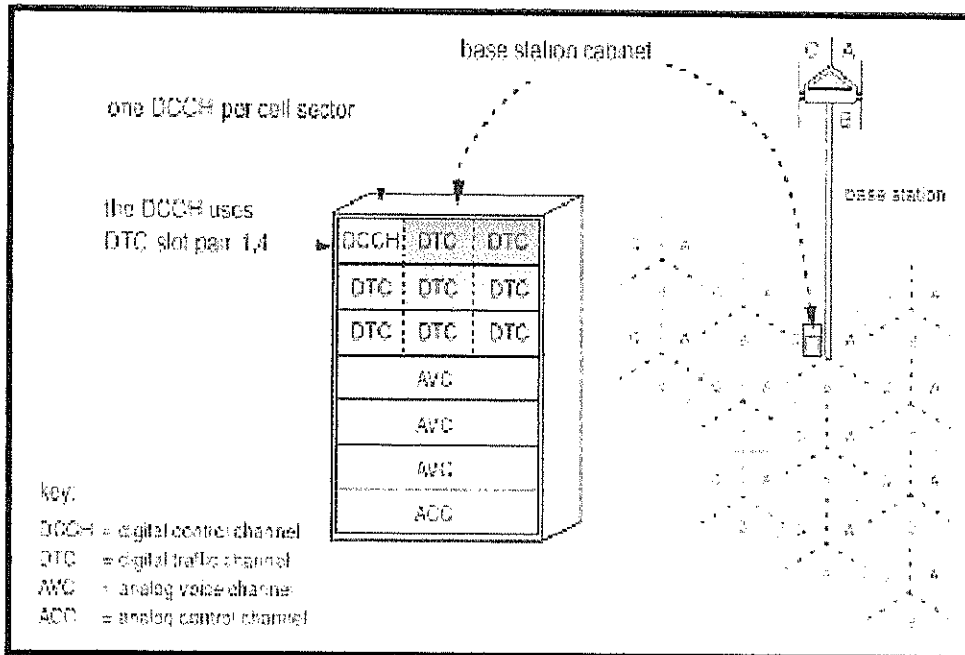
En sistemas TDMA cada canal de radio digital puede llevar 3 llamadas por multiplexación de tráfico de voz de tiempo en time slots. Un canal de voz puede ser introducido en el sistema TDMA por la reprogramación de aquellos canales de tráfico, denominados canales de Tráfico Digital, para llegar a ser el DCCH en una frecuencia que contenga los canales de tráfico digital existentes.

La siguiente figura se muestra el par del slot DTC (1,4) usado para un DCCH, y presenta cada celda dividida en sectores (A, B, C). Solamente un par slot es requerido para un DCCH en cada sector de celda sin tomar en cuenta el número de radios digitales en el sector.

---

**FIGURA A.14**

**ESTRUCTURA DE LOS SLOTS DEL CANAL DCCH**



**Principio de operación**

La información llevada en el canal de control digital DCCH fluye en dos direcciones en la interface aérea: desde el sistema hacia el teléfono (downlink) y desde el teléfono hacia el sistema (uplink). En la figura 2, la estación base representa el sistema.

Los teléfonos PCS y los que tienen capacidad de soportar IS 136 con el DCCH monitorean un canal de control digital en cada sector de un sistema inalámbrico que soporte servicios IS 136. Un teléfono PCS escaneará por este canal, de tal forma que se gane sincronización, y empiece a decodificar la información proporcionada en el canal

de control broadcast en el DCCH. El DCCH sirve como canal de control del teléfono hasta que el teléfono encuentre otra celda que sea más apropiada.

Los teléfonos PCS reciben los pages, envían originaciones, y se comunican con el sistema en el DCCH. Después de recibir un page o de ejecutar una llamada de originación, un canal de tráfico es luego designado para la llamada, y el teléfono puede hacer hand off de celda a celda como que si se moviera alrededor del sistema. Al completarse la llamada, el teléfono retorna al DCCH para esperar una próxima interacción.

## **LA INTERFACE AÉREA: EL PROTOCÓLO MULTICAPA**

El Canal de Control Digital consiste básicamente de 4 capas:

- La Capa Física (Capa 1) que es la que se encarga de administrar las tramas, slots, las rafagas y las supertramas.
  - La Capa de Red (Capa 2) que es la que maneja el empaquetamiento de los datos, corrección de error y transporte de mensajes.
  - La Capa de Procesamiento de Llamada (Capa 3), la cual crea y maneja mensajes enviados y recibidos a través del aire.
-

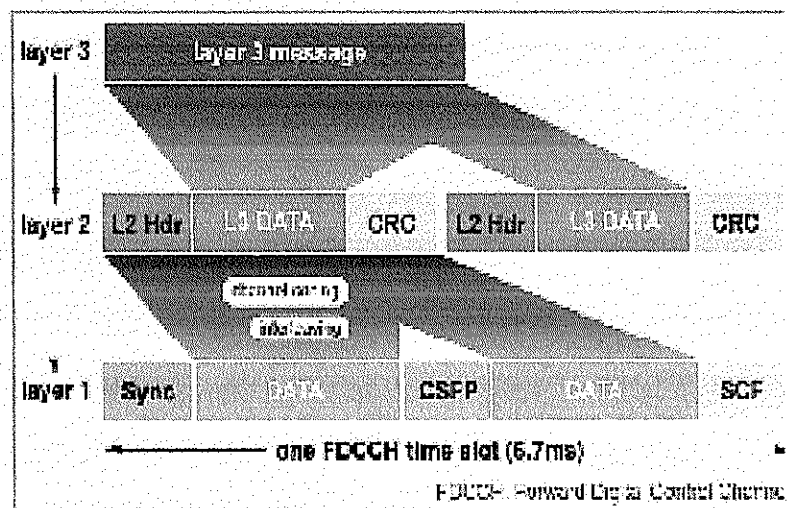
- Adicionalmente hay capas superiores de aplicación, las cuales representan el teleservicio corriente que esta siendo usado, tanto como voz y transacciones de mensajería, o servicios futuros como en programación aérea.

La figura 4 presenta como un mensaje de la capa 3 es mapeado en varios frames de la capa 2 y como un frame de tiempo de la capa 2 es mapeado dentro de un time slot. El time slot es por supuesto mapeado dentro de un canal DCCH. La figura presenta, como la información es pasada desde una capa a otra a través de la pila hasta que una ráfaga sea creada, lista para la transmisión. Al final de la recepción, la información es desmenuzada, de tal forma que el mensaje sea pasado a la aplicación.

## FIGURA A.15

### CAPAS DE LA INTERFACE IS 136

Figure 4: Layered 3-2-1 Mapping



El mensaje de la capa 3 presentada en la figura 4 puede ser una registraci3n uplink, un mensaje downlink PCS, una respuesta page, o un mensaje broadcast. La capa de mensaje (capa 3) es empaquetada en el frame de la capa 2 donde el encabezado y los campos de correcci3n de error son agregados. El paquete es luego codificado y los bits individuales para contrarrestar el error son introducidos en el medio de radio.

## **La Capa F3sica**

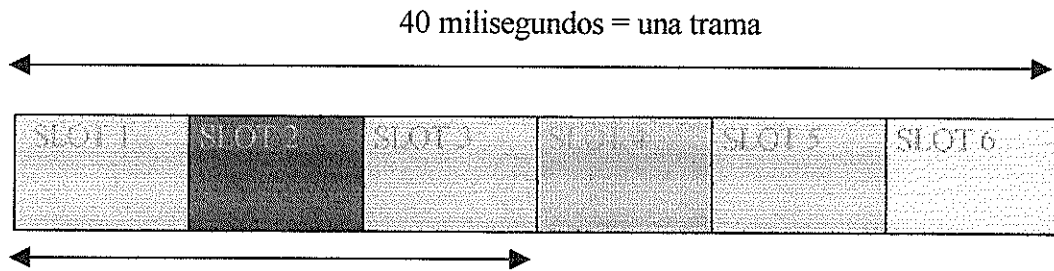
Es un canal de 48 kbps con modulaci3n DQPSK  $\pi / 4$ . Est3 dividido en tramas de 40 ms cada uno, y cada trama est3 dividida en 6 slots. Un canal de control digital de tasa completa usa cada tercer slot, mientras que un canal de control digital de tasa media usa el sexto slot. El dato es codificado convolucionadamente en una relaci3n de 2:1. Esto resulta en la capa 2 cerca de 125 bits por slots como datos siendo transmitidos en el canal delantero, es decir, desde la estaci3n base a la estaci3n m3vil. Adem3s para llevar los datos de la capa 2, la capa 1 lleva los bits del (SCF) Share Control Feedback los cuales son usados por el m3vil para la determinaci3n del estatus de su m3s reciente transmisi3n del canal reverso.

---



**FIGURA A.16**

**TRAMA DE SLOTS DE DATOS DEL IS 136**



20 ms en un bloque. Un bloque está formado por tres slots o tres llamadas.

### **La capa de Red**

Ejecuta cuatro funciones importantes:

- Monitoreo y control de accesos reversos incluyendo retransmisión requerida.
- Decodificación de los paquetes de la capa 2 y protección de los datos de la capa 2.
- Filtración de paquetes no destinados para el móvil, y
- Control de la baja potencia del móvil.

La capa de Red se versa sobre Supertramas. Una supertrama consiste de 16 tramas. Un Canal de tasa completa desde luego tendrá 32 slots por supertramas. Incluido con la información de la Capa 1 por cada slot esta la fase de la supertrama en uno de los siguientes tipos de mensajes: FBCCH, EBCCH, y el SPACH. Los mensajes, FBCCH y el EBCCH, son mensajes de difusión, es decir que no son direccionados a móviles individuales, pero contienen información requerida para todos los móviles. Los mensajes SPACH son direccionados y desde luego contienen información particular para móviles individuales, esto es cuando se realizan llamadas entrantes para intentos de originación de llamadas. Los mensajes SPACH son por lo general divididos por la capa 2 en una de las dos supertramas, una primaria y una secundaria, para formar una hipertrama. Hay pocas distinciones entre las supertramas. La excepción a esto es que todos los mensajes PCH transmitidos en la supertrama sean repetidos en la supertrama secundaria.

- PCH es usado para la notificación inicial de un móvil de un evento,
- SMSCH es usado para la transmisión de mensajes cortos,
- ARCH es usado para transportar respuestas al móvil después de que el móvil ha transmitido un mensaje.

Hay que recalcar que el Canal Paging lleva mensajes que inicialmente notifica a un móvil de un evento. Un mensaje del canal Paging será enviado en uno de los slots de la supertrama denominado el paging slot. Un algoritmo basado en Los números del teléfono móvil determine esta fase supertrama. Mientras los canales PCH enviados en la

---

supertrama primaria sean repetidos en la supertrama secundaria, una estación móvil necesita solamente leer la información del slot en su paging slot en cada una de las otras supertramas es decir cada 1,28 ms. Tan largo sea el tiempo en que el móvil se tarde en leer toda la información de difusión que necesite , este puede estar en baja potencia entre los paging slots.

### **La capa de mensaje**

Es especificada como un estado de máquina. El estado en que el móvil en el cual es encendido y está esperando para noticias entrantes es conocido estado “camping”. El móvil deja el estado camping para manejar un mensaje de entrada del PCH, para manejar un intento de originación de llamada, registrar o enviar un corto mensaje. Mientras en el estado camping, el móvil esta continuamente monitoreando Los niveles RSSI en las vecindades de Los canales de control. La información de estos canales vecinos es transmitida en el canal EBCCH(Canal de transmisión extendido- Extended Broadcast Channel). Si el móvil determina que un canal vecino es mejor que el canal que esta en estado camping., entonces se conmuta al nuevo canal.

---

# CANALES LÓGICOS

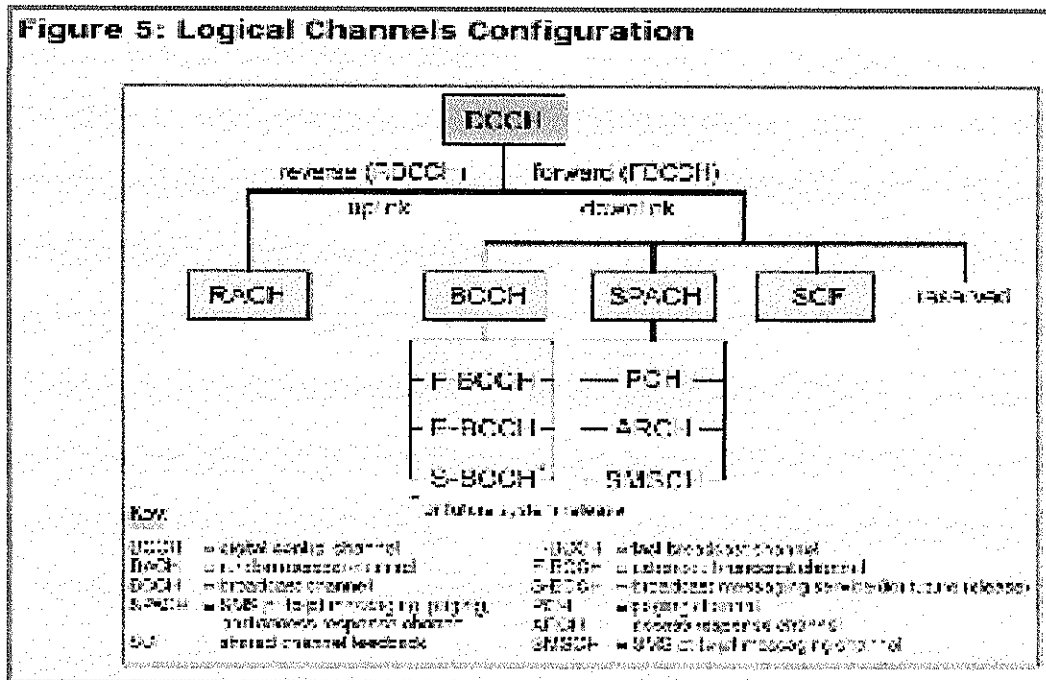
Los canales lógicos fueron desarrollados en la tecnología DCCH IS-136 para organizar los PCS y otra información digital que fluya a través de la interface aérea.

## Configuración de los canales lógicos

Los canales lógicos son mostrados gráficamente en la figura 5. La figura muestra como el canal delantero del DCCH (FDCCH) consiste de muchos canales lógicos llevando información desde el sistema hacia el teléfono. El canal reverso del DCCH (RDCCH), que lleva información desde el teléfono hacia el sistema, consiste de un canal lógico.

FIGURA A.17

### CONFIGURACION DE LOS CANLES IS 136



## **Principio de operación**

Los canales lógicos reparten y priorizan la información de señalización para uso funcional. El dato es luego mapeado en un DCCH, el cual es un canal físico. Los canales físicos son las porciones actuales del ancho de banda electromagnético consistiendo de frecuencias y divisiones de tiempo. El canal lógico de datos fluye en el DCCH en ambas direcciones: desde el sistema hacia el teléfono (downlink) y desde el teléfono hacia el sistema (uplink).

## **Funciones de los canales lógicos**

El canal de radio transmisión multiplexado (BCCH) presentado en la figura 5 está diseñado para llevar información acerca de la configuración del sistema y las normas que los teléfonos deben seguir en el acceso del sistema. Sus canales lógicos primarios son:

- El canal fast broadcast (F-BCCH), lleva información que el teléfono necesita inmediatamente, tanto como la identificación del sistema e información de registración.
  - El canal extendido broadcast (E-BCCH), llevando información que no está como tiempo crítico, tales como listas de celdas vecinas.
-

El sistema usa la mensajería SMS punto a punto multiplexada, paging, y el canal de respuesta de acceso (SPACH) presentada en la figura 5 para comunicarse con un teléfono específico. Sus canales lógicos son:

- El canal de servicio de mensajes cortos (SMSCH) llevando mensajería IS-136 y activación en el aire y programación (OAA/P)--- la información IS 136 es llevada en los canales lógicos en tanto los 800 MHz y 1900 MHz.
- El canal paging (PCH) llevando texto en pages desde el sistema al teléfono.
- El canal de respuesta de acceso (ARCH) proporcionando respuesta del sistema al teléfono que es prescindible e información de administración.

A continuación se describe los canales lógicos:

**Tabla A.2**

**CANALES LOGICOS DEL IS 136**

<b>Canal Lógico</b>	<b>Descripción</b>
BCCH (Broadcast Channel)	Este es un canal multiplexado downlink y comprimido de los canales: F-BCCH - the fast broadcast channel y del E-BCCH - the extended broadcast channel.
SPACH (SMS punto a punto)	Aquí se transmite mensajería, paging y el canal de respuesta de acceso. Este es un canal multiplexado downlink y comprimido

	de los canales: SMSCH - el canal de mensajería SMS, del PCH - el canal paging y del canal de respuesta de acceso ARCH.
RACH (Canal de Acceso Aleatorio)	Este es un canal particular uplink con todos los time slots usados para el acceso del sistema.
SCF(Shared Channel Feedback)	Los campos SCF en el downlink son usados para proporcionar un mecanismo colisión-prevencción para el uplink.

## **MODO SLEEP Y TIEMPO TEMPORAL (STANDBY)**

El IS 136 utiliza el canal de control digital para proporcionar un modo sleep durante el cual los teléfonos pueden apagarse en la mayoría de su circuitería hasta que ellos necesiten ser activados, en intervalos predeterminados, para recibir la mensajería del sistema. Esta característica incrementa la vida de la batería, mientras se incrementa el tiempo de standby de los teléfonos. El tiempo de standby es el tiempo de un teléfono inalámbrico en el cual esta libre; es decir el teléfono esta prendido, pero no hay llamadas que son hechas o recibidas.

### **Principio de operación**

Empecemos diciendo que un teléfono libre se encuentra suspendido en el DCCH. El teléfono chequea por el ingreso de llamadas cada pequeños milisegundos entonces reingresa al modo sleep. Esto difiere de un teléfono usando un canal de control analógico

(ACC), donde un teléfono libre debe monitorear el canal de control constantemente, desgastando la batería.

Los mensajes del sistema recibidos por el teléfono pueden ser pages o mensajes broadcast (por ejemplo, actualizar los cambios de celda o celdas vecinas) llevados en el downlink DCCH. El teléfono necesita decodificar la información de regreso solamente en intervalos de sus paging slots predeterminados o en los slots de retransmisión si la información de retransmisión cambia. En esta forma, el teléfono ha extendido períodos de tiempo en el cual puede descargar algo de su circuitería y estar libre entre próximos mensajes paging.

## **Consumpción y períodos Sleeps**

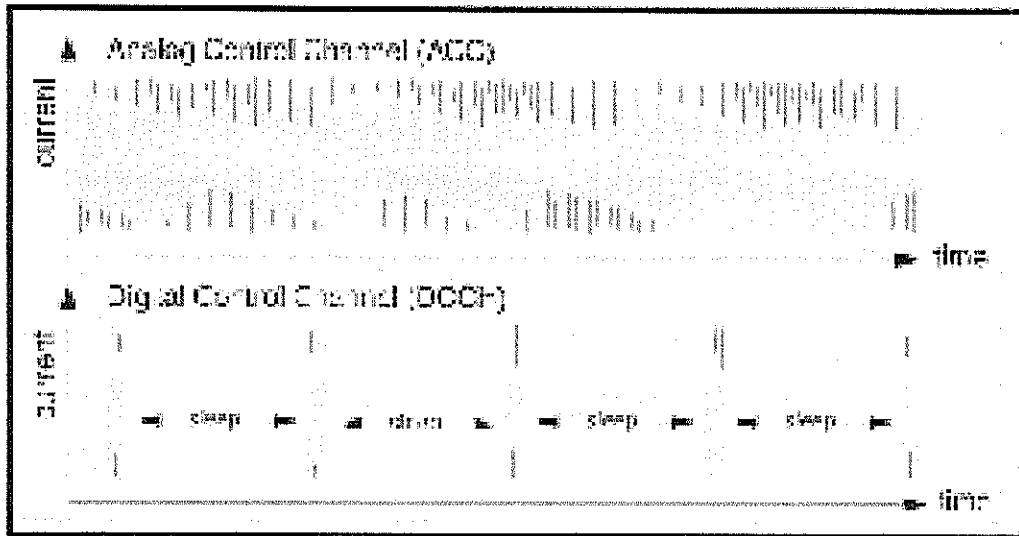
La figura A.18 muestra el canal de control analógico (ACC) versus la consumpción corriente de la batería en el DCCH e indica los periodos en modo sleep en el DCCH. El tiempo que apunta en el segmento DCCH del dibujo son representativos de los paging slots predeterminados.

---



## FIGURA A.18

### CANAL DE CONTROL ANALÓGICO (ACC) VERSUS LA CONSUMCIÓN CORRIENTE DE LA BATERÍA EN EL DCCH



## MENSAJERIA IS 136

La mensajería de IS 136 es una característica del servicio de mensajes cortos (SMS) que permite un teléfono inalámbrico para recibir pages numéricos y mensajes de texto corto. Esto deja que un dispositivo hacer el trabajo de tanto de pager y de teléfono. Los usuarios pueden recibir mensajes en las pantallas de sus teléfonos desde una variedad de fuentes: computadoras, teléfonos, e-mail, correo de voz, y texto dispatch.

El IS 136 usa el DCCH y canales de tráfico digital para repartir los mensajes alfanuméricos hacia y desde el teléfono inalámbrico. Los mensajes son enviados y recibidos mediante un centro de mensajes, el cual es un nodo en la red inteligente inalámbrica. Los mensajes contienen una variedad de atributos controlando sus entregas, almacenamiento y comportamiento del display.

## **Arquitectura del mensaje**

Cada mensaje originado en la red de IS-136 consiste de tres elementos básicos:

- Información de dirección, la cual le dice al sistema a cual teléfono el mensaje está para ser entregado.
- Texto alfanumérico, en el cual están los caracteres que construyen el mensaje de texto actual.
- Atributos de mensajes, los cuales le dicen al teléfono como manejar y mostrar el mensaje cuando es recibido.

## **Principio de operación**

La característica de la mensajería Is-136 usa un terminal paging dedicado. Cuando la red recibe un mensaje IS 136, localiza el teléfono en cuestión y entrega el mensaje. El teléfono notifica al usuario con un mensaje icon, un beep, o ambos. El mensaje luego puede ser mostrado y leído. Si los usuarios dejan una área de mensajería IS 136, la red

---

almacena cualquiera de los mensajes hasta que ellos regresen. La red repetidamente tratará de entregar un mensaje hasta que el teléfono sea capaz de recibirlo.

## **Generación del mensaje**

Las siguientes entidades pueden ser usadas para la generación de mensajes IS-136:

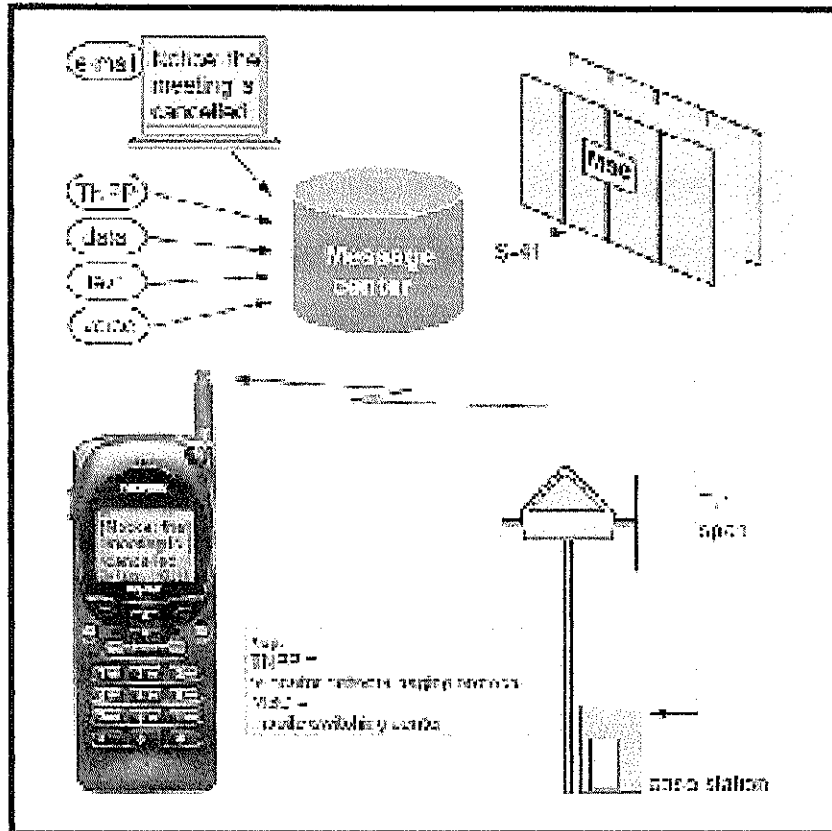
- Interconexión desde terminales paging existentes.
- Unidad voz-respuesta.
- servicio de envío vivo del texto del operador
- Marcación dial-up vía módem.
- Gateway con e-mail
- Fuente de información de datos
- Sistema de correo de voz.

La figura A.19 muestra la mensajería de teleservicio en la cual un mensaje es formulado en una PC y enviado al teléfono del mensaje recipiente. Las pantallas de los teléfonos difieren dependiendo del modelo y del fabricante.

---

## FIGURA A.19

### MENSAJERÍA DE TELESERVICIO CON IS-41



### Entrega de mensajes

La mensajería IS 136 está diseñada para operar en todas las situaciones de carácter inalámbrico:

- **Encendido:** Si el teléfono está encendido, el mensaje esta disponible inmediatamente solo como un page.
  - **Teléfono enganchado:** Si el teléfono está enganchado en una conversación de voz, la red entrega el mensaje al teléfono usando el mismo canal de tráfico digital siendo usado para la conversación.
  - **Teléfono apagado:** Si el teléfono está apagado, o el teléfono está fuera de una área de servicio, el centro de mensajes de la red almacena el mensaje para entregarlo más tarde. Tan pronto que el teléfono esté encendido, los mensajes son entregados. Esta forma de mensajes no son perdidos si un teléfono está apagado, si está fuera del área de servicio o si está en una área con una pobre recepción.
  - **Correo de voz:** Cuando una persona llama al correo de voz de un usuario, el sistema proporciona la opción para enviar un mensaje callback al teléfono o para enviar un mensaje alfanumérico usando el software Message Flash.
  - **Roaming:** si el usuario está haciendo roaming en una área que no soporta mensajería IS 136, el centro de mensajes, almacenará el mensaje y lo entregará cuando el teléfono reingrese a una área soportada con IS 136.
-

## **RELACIONES JERARQUICAS DE CELDAS**

Los sitios de celda han existido tradicionalmente como macroceldas en torres que cubren a varias millas en el diámetro. Las macroceldas son típicamente celdas públicas sirviendo a todos los usuarios de teléfonos inalámbricos. La tecnología TDMA del estándar IS 136 con DCCH habilita el uso de muchas celas más pequeñas llamadas microceldas. Las microceldas proporcionan servicios comercializados dentro de la cobertura de macroceldas existentes. Típicamente las microceldas ofrecen las características del servicio de oficio inalámbrico (WOS) para teléfonos específicos dentro de un edificio privado o un ambiente de campus.

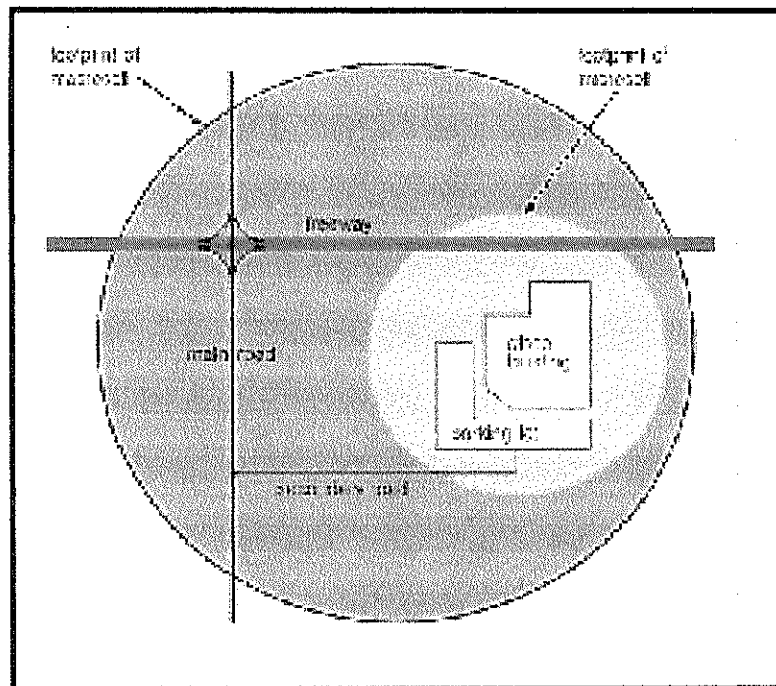
### **Cobertura de la celda jerárquica**

La cobertura combinada de tanto las macroceldas y microceldas es llamada cobertura de celda jerárquica, con las microceldas crean un segundo nivel de cobertura debajo del nivel existente. Mientras las macroceldas sean públicas y las microceldas sean usualmente privadas, ellas pueden cambiar los papeles. La figura 8 muestra un sistema de microcelda privado dentro de una macrocelda pública.

---

## FIGURA A.20

Sistema de microcelda privado dentro de una macrocelda pública con IS 136



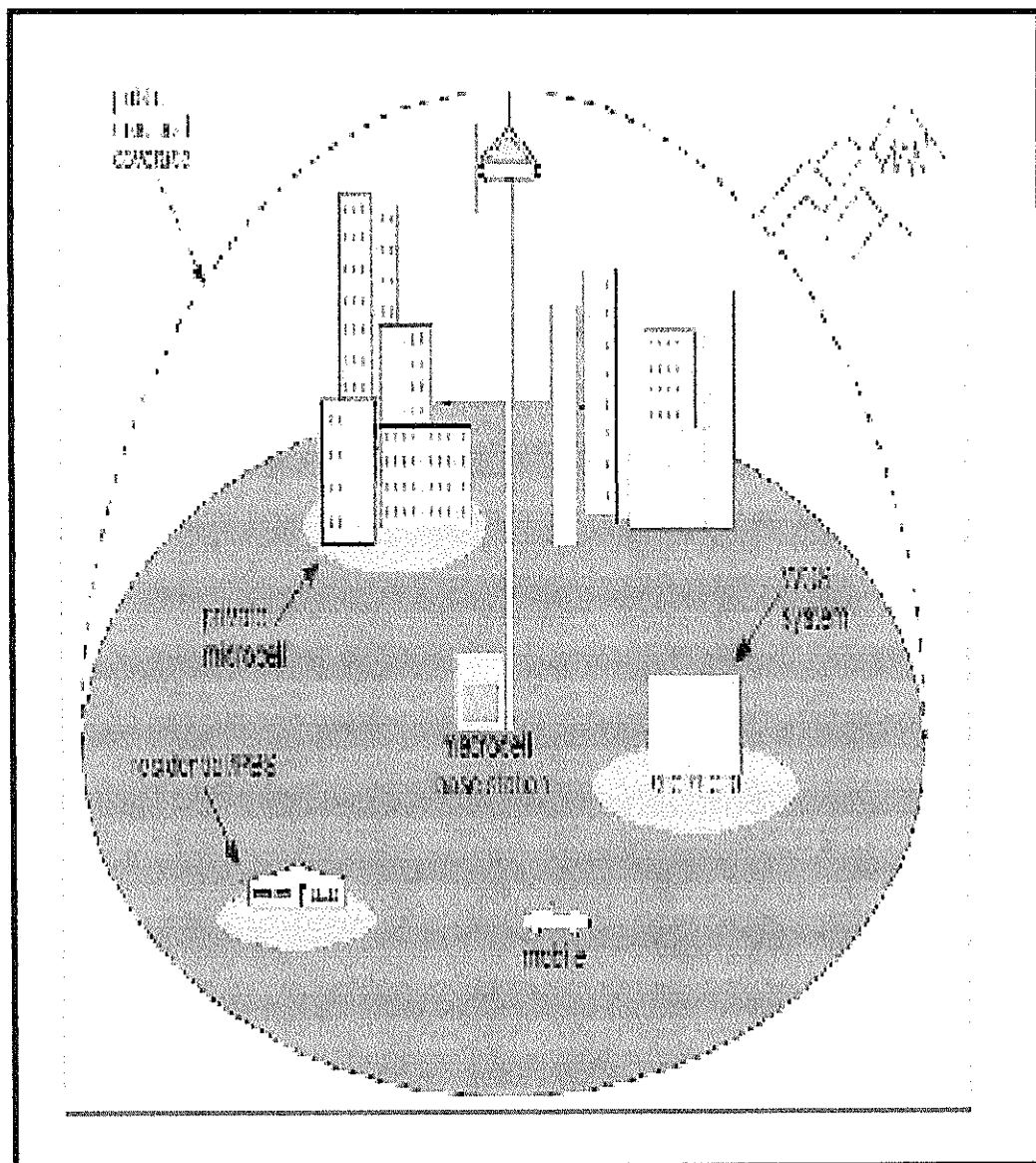
### Estructuras de celdas jerárquicas

En un ambiente IS 136, una área geográfica podría ser cubierta por una mezcla de macroceldas y microceldas tan bien como sistemas públicos y privados. Un teléfono IS 136 debe por supuesto acceder a la mayoría de los canales de control en el cual se pueda proporcionar el servicio, aun si la señal extraña de una celda vecina no es la señal más

alta siendo recibida por el teléfono, pero es de un nivel suficiente para proporcionar la calidad de servicio.

FIGURA A.21

ESTRUCTURAS DE CELDAS JERARQUICAS EN IS 136



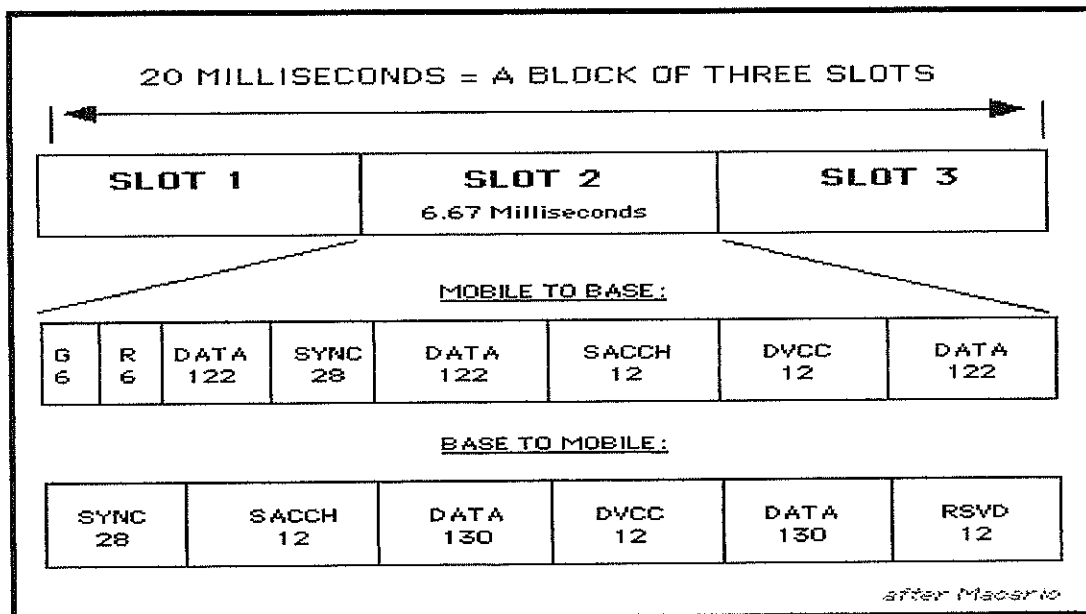


## CANAL DE TRAFICO DIGITAL

En la capa física, el canal de tráfico digital es muy similar al DCCH: en TDMA el canal es “esloteado” a 48 kbps en modulación DQPSK. El canal DTC fue introducido con IS-54B, pero ha sido magníficamente mejorado con un nuevo codificador de voz y con capacidades importantes de señalización. El canal de tráfico a 30 khz en TDMA permite tres conversaciones simultaneas. El IS-136 tiene también agragados nuevos mensajes de control mensajes previos expandidos en el DTC, proveyendo nuevos servicios y soportando extensión transparente de servicios celulares en la banda PCS.

FIGURA A.22

### DISTRIBUCIONES DE LOS CANALES IS 136



# ESTANDAR IS 91 REV. A

## INTRODUCCION

Esta sección trata muchos temas referentes a IS-91 A en sistemas AMPS, tales como:

- Descripción del Servicio de Mensajes Cortos (SMS) en AMPS.
- Requerimientos del SMS en AMPS.
- Configuraciones de hardware soportadas para el SMS en sistemas AMPS.
- Nuevas medidas operacionales para el servicio SMS en AMPS.

IS-91A proporciona un mecanismo para entregar los mensajes cortos limitados a una longitud máxima de 15 caracteres de los datos del portador. Los 15 caracteres de datos del portador contienen un máximo 14 caracteres de texto comprimido del ASCII y 1 carácter de control. Estos mensajes incluyen:

- paginación numérica
- mensajería de texto

El sistema entrega los mensajes a móviles registrados que estén libres y no tienen ninguna llamada de voz activa. El sistema entrega los mensajes en el canal D. El sistema usa hardware existente como ICP, ICRM o ICRM+, y TRUI/TRUII, basado en

---

el protocolo IS-91 A SMS extendido que usa el ACCH. El sistema también utiliza la paginación móvil activa y una forma de paginación zonal para los móviles con sistemas AMPS para utilizar móviles terminales del SMS terminado móvil en el MSC.

## **Requerimientos del IS 91 A en SMS**

El cuadro 6-1 describe el diseño de IS-91A amperios SMS en el nivel componente. Las interfaces se indican al lado de los componentes.

Los requerimientos específicos para implementar IS-91A SMS proporcionan el mecanismo para entregar los mensajes cortos limitados a un máximo de 15 caracteres de los datos del portador. Los datos del portador contienen del un máximo de 14 caracteres de texto comprimido en ASCII y 1 carácter de control. El carácter de control es el CM e ICP al TRU. Los datos del portador proporcionan funciones de terminación de móviles del fin SMS y utilizan los siguientes algoritmos de paginación: Paginación móvil activa, paginación zonal, y paginación de la difusión del ICP y de ICRM.

IS-91A soporta las siguientes plataformas:

- XPM+ (UP) basado en ICP
  - CAP basado en ICP
  - XPM+ (UP) basado en ICPO
  - CAP basado en ICPO
-

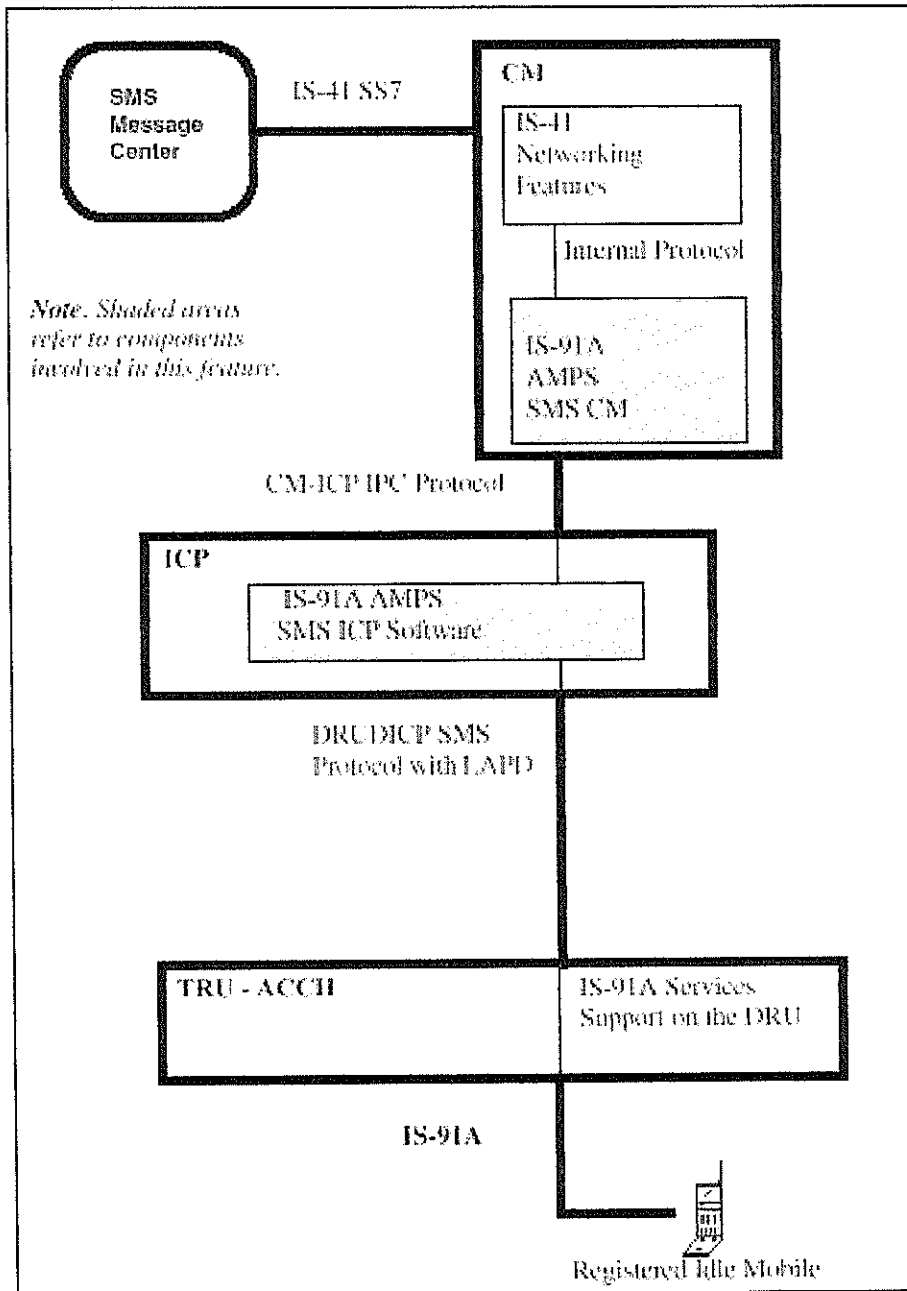
- ICRM e ICRM+.
- TRU I y TRU II

Se recomienda usar el software lógico de TRU para IS-91 A SMS. Esta característica soporta la interfaz de la conexión del aire definido por el protocolo ampliado IS-91A de Teleservicio de los servicios realizados del protocolo.

---

**FIGURA A.23**

**COMPONENTES DEL SMS EN IS 91 A**



## **Hardware soportado para IS-91 A en el SMS**

El IS-91 A soporta las Siguietes configuraciones de hardware:

- CM: Supernodo CM y SNSE
- ICP: UP basado en ICP y CAP basado en ICP
- ICRM: ICRM e ICRM+.
- Capacidades del Protocolo Extendido IS-91 A con TRU I y TRU II.

## **Radio cargas soportadas en IS 91 A en el SMS**

El IS-91 A en sistema de Servicios de Mensajes Cortos pueden soportar los siguientes radio cargas:

- La radio carga TRU1ATxx para radios TRU I
- La radio carga TRU2ATxx para radios TRU II

## **Nuevas medidas operacionales para IS-91 A en sistemas AMPS para el Servicio de Mensajes Cortos**

El ICPSMS (grupo de mensajes delantero OM del Servicio de Mensajes Cortos del ICP) no pierde de vista los mensajes y la recesión relacionados al servicio de mensajes cortos que ocurren en el ICP. Diez nuevos OMs se agregan a este grupo para el servicio de mensajes cortos del IS-91A. Seis de estos OMs estiman el tráfico

---

de IS-91A SMS. Cuatro OMs de repuesto están para el desarrollo futuro de SMS.

## **Entrega de mensajes**

El cuadro 6-2 resume el proceso de entregar un mensaje corto a un móvil libre concluido el canal del control. La parte sombreada muestra las funciones proporcionadas por esta característica. Los números van con los acontecimientos enumerados abajo.

Todos los mensajes intercambiados entre el CM-ICP y el ICP-TRU son mensajes internos. Estos nombres del mensaje se utilizan para los propósitos de la ilustración solamente.

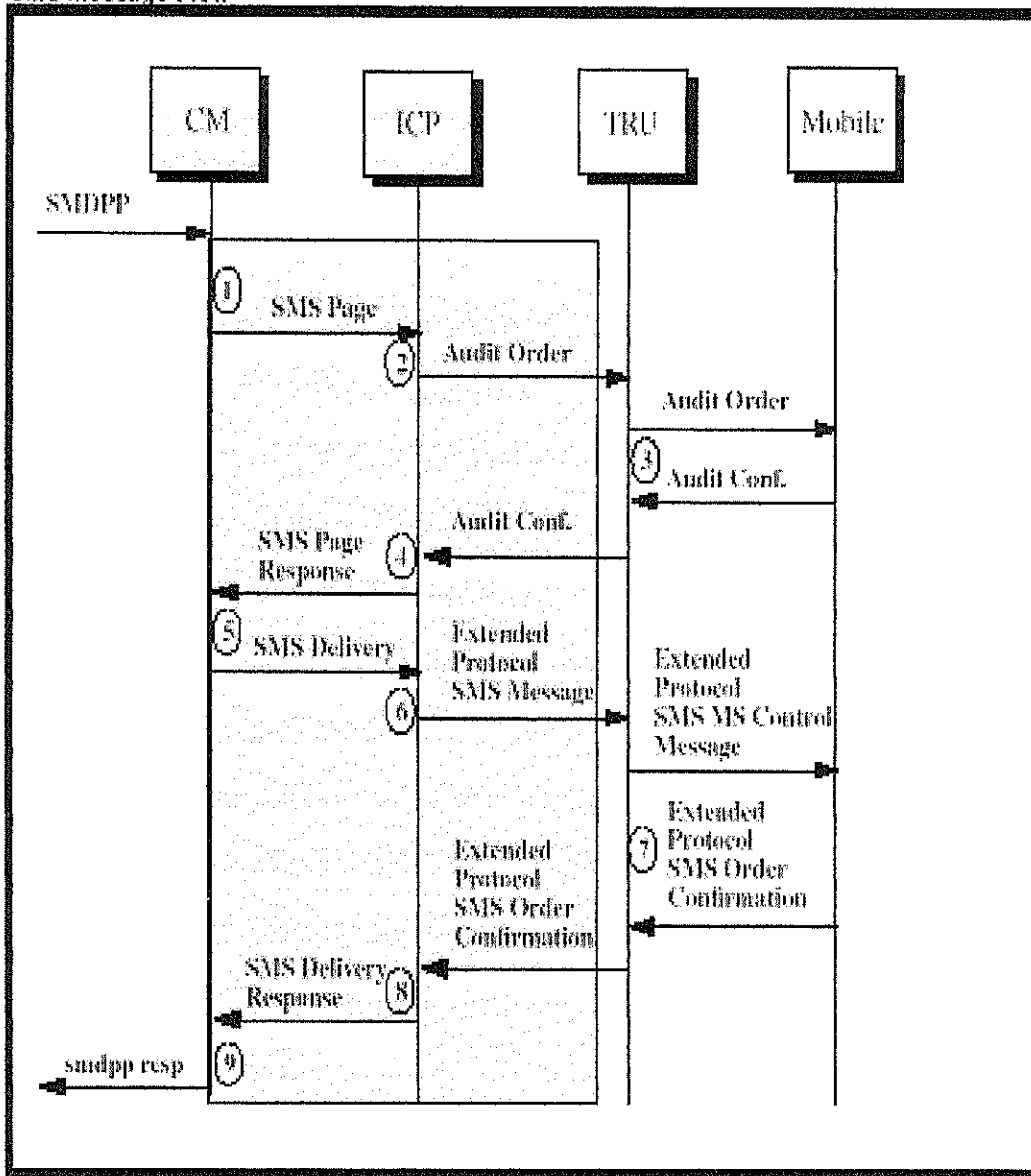
1. El CM recibe un mensaje de SMDPP de un centro del mensaje. El mensaje de SMDPP le dice al CM que entregue el protocolo los servicios realizados ampliados SMS de Teleservicio del en el sistema AMPS SMS al móvil indicado. El CM determina el estatus de llamada del móvil (es decir marcha lenta, no en una llamada de voz). Si el móvil no está en una llamada, el CM envía una paginación de SMS a la celda del ICP que es servido.
  2. Cuando el ICP recibe la paginación de SMS, el ICP formatea un Audit Order. El ICP envía el Audit Order a cada celda indicada en la paginación de SMS. El ICP envía el Audit Order a través de la paginación de la difusión del ICP o de ICRM. Si el ICP está en una condición de sobrecarga del ICP, el ICP desecha la paginación de SMS.
-

3. El TRU valida y procesa el mensaje del orden de la intervención del ICP. Cuando el TRU recibe el Audit Confirmation, el TRU transmite a la confirmación el ICP.
  4. Cuando el ICP recibe el confirmación de la intervención, el ICP formatea una respuesta de la paginación de SMS y la envía al CM.
  5. Después de que el CM reciba la respuesta de paginación del SMS, el CM pone al día la localización del móvil en el VLR. El CM formatea un mensaje de la salida del SMS que incluya los datos del portador del SMS. El CM envía el mensaje de la salida de SMS tratado por el ICP, a la celda, y a la partición donde el móvil es contestado.
  6. Cuando el ICP recibe el mensaje de la salida de SMS, el ICP formatea y envía un mensaje extendido del protocolo SMS al TRU. Si el ICP está en una condición de sobrecarga del ICP, el ICP desecha el mensaje de la salida de SMS.
  7. El TRU valida y procesa el mensaje extendido del protocolo SMS del ICP. Cuando el TRU recibe una confirmación extendida del orden del protocolo SMS, el TRU envía la confirmación de la orden al ICP.
  8. Cuando el ICP recibe la confirmación extendida del orden del protocolo SMS, el ICP formatea y envía una respuesta de la salida del SMS al CM.
  9. Cuando el CM recibe la respuesta de la salida de SMS, el CM formatea una respuesta del smdpp. Esta respuesta vuelve un éxito de la salida o un incidente de la salida con el IS-41C correcto SMS CauseCode.
-



FIGURA A.24

MENSAJERIA IS 91 A



# **ESTANDAR IS 54 REV. B**

## **INTRODUCCION**

La primera generación del sistema analógico AMPS no fue diseñada para soportar la demanda para usuarios en grandes ciudades. Los sistemas celulares que usan técnicas de modulación digital ofrecen grandes mejoras en la capacidad y en el funcionamiento del sistema. Para ello se diseñó el estándar americano celular IS 54 B que permite soportar más usuarios en un espectro de localización fijo. El estándar IS 54 Re. B es un sistema de acceso múltiple por división de tiempo TDMA el cual soporta tres usuarios de tasa completa o seis usuarios de tasa media en cada canal AMPS. Así pues el estándar ofrece seis veces más que la capacidad de AMPS. El estándar IS 54 B usa el mismo esquema de FDD a 45 MHz. Como en AMPS. La presencia de este estándar fue tal que se lo denominó SISTEMA MODO DUAL IS 54B/ AMPS.

---

El sistema mencionado fue diseñado para formar las mismas frecuencias, plan de rehusos de frecuencia, y estaciones base en AMPS, tal que las estaciones base y las unidades subscriptoras podrían ser equipadas con canales tanto en AMPS como en IS 54B dentro del mismo pedazo del equipo. Para soportar tanto AMPS e IS 54B, las operadoras celulares son capaces de proveer nuevos clientes con teléfonos IS 54B y pueden gradualmente reemplazar estaciones base AMPS con estaciones base IS 54B, canal por canal, todo esto a tiempo. Puesto que el estándar IS 54B mantiene compatibilidad con AMPS en un número de formas, así pues a este estándar se lo llama también D AMPS IS54B.

Corrientemente en áreas rurales donde la inmunidad de los sistemas celulares está en uso, solamente 666 de los 832 canales AMPS son activados.

En estos mercados los canales con IS 54B pueden ser instalados en el espectro extendido para soportar teléfonos con dicho estándar y los subscriptores hagan roaming en mercados metropolitanos. En mercados urbanos donde existe una alta densidad de tráfico celular es necesario cambiar a un ambiente IS 54B.

El paso de lo analógico a lo digital en la misma banda de radio fue un esfuerzo que valió la pena en el desarrollo del estándar IS 54B y para mantener esta compatibilidad con teléfonos AMPS, los canales de control delantero y reverso del estándar IS 54B usan exactamente las mismas técnicas de señalización como en AMPS. Así pues

---

mientras los canales de voz usan modulación DQPSK 4-ary  $\pi/4$  con una tasa de velocidad de 48.6 kbps, los canales de control delantero y reverso no son diferentes que en AMPS y usan el mismo esquema de señalización FSK a 10 kbps y los canales de control estandarizados.

Para asegurar una buena transmisión de AMPS a IS 54B, el sistema IS 54 es especificado para operar usando ambos estándares AMPS y IS 54B (modo dual) el cual hace roaming entre los dos posibles sistemas con un simple tono.

El sistema IS 54 usa la misma banda de frecuencia y el canal espaciado como AMPS y soportes múltiples de IS 54B usados en cada canal de AMPS. Los esquemas IS 54B usan TDM, tiene la flexibilidad de incorporar más usos dentro de un simple canal de radio con la menor velocidad de bits de códigos de comunicación que llegan ha ser validables. La siguiente tabla indica la interface de aire para IS 54B.

---

**TABLA A.3****ESPECIFICACIONES DE LA INTERFACE AEREA IS-54b**

<b>PARAMETRO</b>	<b>ESPECIFICACION DEL IS 54B</b>
Acceso múltiple	TDMA/FDD
Modulación	$\pi/4$ DQPSK
Ancho de Banda	30 kHz
Banda de frecuencia canal reverso	824 - 849 MHz.
Banda de frecuencia canal delantero	869 - 894 MHz.
Velocidad de datos canal delantero y reverso	48.6 kbps
Eficiencia del Spectrum	1.62 bps/Hz.
Ecuador	no especificado
Canal codificador	7 bit CRC y velocidad $\frac{1}{2}$ convulocional codificado de constante longitud 6
Salida	2 slots
Usos por canal	3 (full velocidad códigos de 7.95 kbps/uso) 6 (con media velocidad códigos de 3.975 kbps/uso)

**CANALES IS 54B-** Los canales de control IS 54B son idénticos a los canales de control analógicos AMPS. Además de los 42 canales primarios AMPS, IS 54B especifica 42 canales de control adicionales llamados canales de control secundarios. Entonces, IS 54B tiene el doble de canales de control que el AMPS así que el doble de canales de control del tráfico puede ser compaginado durante una marcación. Los

canales de control secundarios convenientemente seguidos de carrier son dedicados solamente para usos de IS 54B, mientras los tonos de AMPS no son monitoreados o los códigos de canales de control secundarios. Cuando se convierte un sistema AMPS a IS 54B/AMPS, un carrier puede decidir programar el MSC y enviar pages para IS 54B móviles sobre los canales de control solamente, mientras siga existiendo AMPS, el tráfico envía solamente en los canales de control de AMPS. Para cada uno de los sistemas IS 54B suscribe la unidad que debe ser programada automáticamente al monitor solamente hacia el control de canales secundarios cuando se opera en el modo IS 54B, tanto como el usuario IS 54B llegue a ser popular a tal punto que los canales de control sea requeridos, los pages del IS 54B eventualmente sería enviadas a ambos canales de control tanto primario como secundario. El canal de voz del IS 54B ocupa 30 kHz de ancho de banda en cada enlace delantero y reverso, y soportando un máximo de tres usuarios. Cada canal de voz soporta un esquema TDMA que provee 6 slots de tiempo. Para una taza completa de comunicación, los tres usuarios utilizan los 6 slots de tiempo en un igual modelo de espacio. Por ejemplo, el usuario 1 ocupa el slot de tiempo 1 y 4, el usuario 2 ocupa el slot de tiempo 2 y 5 y el usuario 3 ocupa el slot de tiempo 3 y 6. Para media velocidad de comunicación, cada usuario ocupa un tiempo de slot por trama.

En cada canal de voz del IS 54B, hay actualmente 4 canales de datos los cuales son proveídos simultáneamente. El canal más importante de datos tan lejos como el final del usuario este conveniente, es el Canal Digital de Tráfico (DTC), el cual lleva el

---

usuario la información (comunicación o usuario de datos) y los otros 3 canales llevan información supervisora dentro del sistema celular. El Reverso del Canal Digital de Tráfico (RDTC), lleva datos de voz desde el subscriptor a la estación base y el Delantero del Canal Digital de Tráfico (FDTC), lleva datos del usuario desde la estación base al subscriptor.

El canal de supervisión 3, incluye el código digital de la verificación del color de código (CDVCC), el canal de control bajo asociado, y el canal de control rápido asociado (FACCH). El CDVCC es un mensaje de 12 bits que se envía en cada slot de tiempo, y es similar al funcionamiento al usado en el SAT en AMPS. El CDVCC es un número de 8 bits que se encuentra en el rango de 1 y 255, el cual se encuentra protegido con 4 canales adicionales codificados en bits desde un corto código Hamming. La estación base transmite un valor CDVCC en el canal de voz delantero y cada subscriptor usa un canal TDMA que debe recibir, decodificar y retransmitir el mismo valor CDVCC a la estación base en el canal de voz de reversa. Si el CDVCC vibra, este no está completo apropiadamente, luego un slot de tiempo será abandonado para otro usuario y el transmisor del subscriptor será apagado automáticamente.

El SACCH es enviado en cada slot de tiempo, y provee un canal de señalización en paralelo con la comunicación digital. El SACCH lleva varios controles y supervisa mensajes en la unidad del subscriptor y la estación base, El SACCH provee mensajes

---

simples sobre muchos slots de tiempo consecutivos y es usado para cambios en los niveles de poder de comunicación.

El SACCH es también usado por la unidad móvil para reportar los resultados de las medidas de longitud de las estaciones bases vecinas de tal manera que la estación base debe implementarse un HANDOFF asistido (MAHO).

El FACCH es otro canal de señalización el cual es usado para enviar controles importantes o tráfico de datos especializado entre la estación base y el usuario móvil.

Los datos FACCH, cuando se transmiten toman el lugar del usuario de los datos de información dentro de un cuadro. El FACCH soporta la transmisión de un tono de frecuencia múltiple dual (DTMF) desde que se toca el tono de las teclas, las instrucciones llamadas se liberan, las instrucciones en flash se enlazan y el MAHO o subscriber del Status Request.

El FACCH también provee amplia flexibilidad permitiendo llevar a la mano tráfico interno a una red celular si el DTC está parado durante un slot de tiempo del TDMA como se discutió consecuentemente, los datos FACCH son tratados similarmente a la comunicación de datos en la forma en que son empaquetados e interllevados para calzar en un slot de tiempo.

---



De cualquier modo un no deseado dato de comunicación el cual protege solamente ciertos bits con canales codificados de slots de tiempo IS 54B. Los datos FACCH usados a  $\frac{1}{4}$  de la tasa del código de canal protegerán todos los bits que son transmitidos en un solo slots de tiempo.

La estructura de la trama para el tráfico de canales IS 54B como se muestra en la fig. Una trama de TDMA en el sistema IS 54B consiste de 6 slots de tiempo que soportan 3 tazas completas de tráfico d canales o 6 medias tazas de canales de tráfico.

La trama TDMA tiene como duración 40 ms. Desde el IS 54B se usa el FDD existen delanteros y reversos canales que operan simultáneamente en slots de tiempo, cada slot de tiempo es generado para llevar comunicación de datos intercalados desde 2 adyacentes tramas del codificador de comunicación. El IS 54B requiere que los datos desde dos adyacentes codificados de comunicación sean enviados a un particular slot de tiempo.

El codificador de comunicación IS 54B, produce 159 bits, la comunicación de datos codificada dura 29 ms en una trama pero el canal codificado trae codificada la trama de comunicación por arriba de los 260 bits por un mismo periodo de 20 ms.

Si las pages enviadas en vez de la comunicación de datos, luego una trama de comunicación de datos es reemplazada con un bloque de datos FACCH y los datos

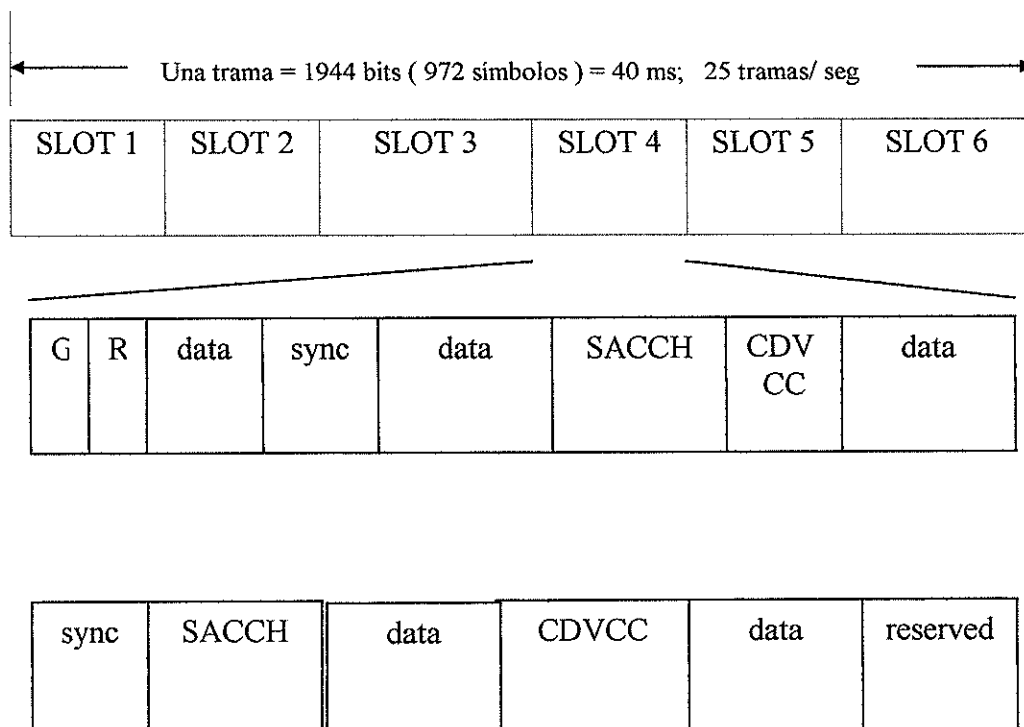
---

FACCH dentro de un slot de tiempo son actualmente hechos de datos FACCH desde dos adyacentes bloques de datos FACCH en el canal reverso de voz cada slot consiste de 2 arranques de 122 bits y un arranque de 16 bits desde dos tramas de comunicación intercaladas. Además 28 bits, 12 bits de datos SACCH, 12 bits de verificación de códigos digital con control de color de código (CDVCC) y 12 bits de guarda son enviados en un slot de tiempo de un canal reverso.

En el canal de voz delantero cada slot de tiempo consiste de 130 bits de arranque de datos desde 2 consecutivos intercalando las tramas de comunicación, 28 bits, 12 bits de datos SADS 12 bits de CDVCC y 12 bits de Reversa. Hay un total de 324 bits por slot de tiempo en el canal delantero y en reverso y cada slot de tiempo dura 6.667 ms.

**FIGURA A.25**

**TRAMA DE DATOS DEL ESTANDAR IS-54B**



El tiempo de slots en los canales reverso y delantero están tambaleando en el tiempo del slot 1 el la trama del canal delantero exactamente un tiempo de slots mas 44 símbolos (i.e. 206 símbolos = 412 bits) antes del comienzo del tiempo del slot de la trama del canal de reversa. Estos siguen cada móvil para el uso simple de transmisión y recepción, en lugar de un duplexor para una operación full duplex con los canales delantero y reversa. El IS 54B provee la habilidad de ajustar el tiempo tambaleando en el canal delantero y de reversa. El tiempo de slot al integrar incrementa a la mitad de un tiempo de slot. El sistema puede sincronizar nuevos subscriptores que son asignados un tiempo de slots.

**CÓDIGO DE COMUNICACIÓN.-** El Código de comunicación IS 54B es denominado (VSELP) Vector Sum Excited Linear Predictive Coder, esto corresponde a la celda de código Excited Predictive Coder (CELP) o Stochastically Excited Predictive (SELP). Estos códigos están basados en el libro de códigos los cuales determinan como se cuantifica la señal de excitación residual. El algoritmo VSELP usa un código de libro que tiene una estructura predefinida para cada numero de computo requerido. Para el código de libro que registra los procesos es significativamente reducido, el algoritmo VSELP puede desarrollarse para un consorcio de compañías y la implementación MOTOROLA puede hacerse por el estándar IS 54. El código VSELP tiene una velocidad de salida de bits de 795 bps y produce una trama cada 20 ms, en cada segundo 50 tramas cada una conteniendo 159 bits son producidas por el código para un uso particular.

---

**CANAL DE CÓDIGO.**- Los 159 bits los cuales son el código de trama están divididos en dos clases de acuerdo a un significado perceptual, hay 77 bits clase 1 y 82 bits clase 2, los bits clase 1 son los más significativos tienen un error protegido usando un código de velocidad  $\frac{1}{2}$  convolucional de longitud  $K = 6$ . Además el código convolucional del bit 12 más significativo de los bits de clase 1, son bloqueados por un código usando 7 bits CRC del código de error de detección, estos valores son los más importantes para los bits de códigos de comunicación, son detectados con un alto grado de probabilidad. Los bits clase 2 son perceptualmente más significativos, no tienen error de percepción después del código de canal, los 159 bits de cada código de comunicación son representados para 260 bits de códigos de canal y la velocidad de trama del bit ordinario del código de comunicación con el código de canal es de 3.0 Kbps.

El código de canal usado para el dato FACCH es diferente para el que es usado para el dato del código de comunicación. Un bloque FACCH de datos contiene 49 bits de datos por cada 20 ms de trama. Un código de palabra de 16 bits CRC es anexado para cada bloque de datos FACCH, proveyendo a cada código de palabra FACCH de 65 bits.

Los códigos de palabras de 65 bits están entonces pasando a una velocidad  $\frac{1}{4}$  convolucional por cada 20 ms de la trama. Un bloque de datos FACCH ocupan la

---

misma cantidad de ancho de banda como una simple trama del código de comunicación en el DTC puede ser reemplazada con los códigos de datos FACCH. Interviniendo el DTC y el dato FACCH es identificado en la interface IS 54B.

Los datos SACCH de palabra consisten de 6 bits durante cada 20 ms de trama de comunicación. Cada código de palabra de datos SACCH es pasado a una velocidad  $\frac{1}{2}$  convolucional contiene una longitud 5 que produce 12 códigos de bits durante cada 20 ms o 24 bits durante cada trama del IS 54B.

## **APENDICE B**

### **ALGORITMO DE AUTENTICACION CAVE**

---

# ALGORITMO DE AUTENTICACION CAVE

## Introducción

Este documento describe varias funciones criptográficas para uso en sistemas celulares que están bajo desarrollo. La primera función, denominada CAVE, ejecuta un algoritmo de autenticación por combinación número aleatorio (RAND) desafío del switch celular con información del equipo subscriptor. Si el resultado que es calculado por el subscriptor se iguala al resultado producido por el switch, entonces el subscriptor será considerado como auténtico.

El CAVE es también usado para generar un grupo de criptovariantes para el Algoritmo de Encriptación de Mensajes Celular (CMEA).

Una aplicación semejante del CAVE es la generación de 520 bits para las máscaras de privacidad de voz duplex.

La generación del SSD del subscriptor desde su clave de autenticación A-key también se produce con el algoritmo CAVE.

Los fabricantes son cuidadosos ya que ningún mecanismo debería ser proveído para mostrar en la estación móvil el A-key, SSDA, SSDB o otras criptovariantes asociadas con las funciones criptográficas descritas en este apéndice. La invocación del modo de prueba en la estación móvil no debe alterar los valores operacionales del A-key, SSD\_A, SSD\_B o otras criptovariantes.

---

## **Definiciones**

### **AAV**

Versión Algoritmo de Autenticación, una constante de 8 bits igual al hexadecimal 0xC7, usado en el algoritmo. Uso de diferentes valores para esta constante en una versión futura permitiría otras versiones o gustos del algoritmo básico CAVE.

### **A-key**

Es una clave criptográfica de 64 bits almacenada en la memoria semipermanente de la estación móvil y también reconocida por el HLR(Home Location Register) del switch móvil. Esta clave es ingresada una vez por teclado de la estación móvil cuando la estación móvil es primero puesta en servicio con un suscriptor particular, y usualmente permanecerá inalterada a menos que el operador determine que su valor ha sido comprometido. Esta clave es usada en la transacción para actualizar el SSD.

### **CAVE**

Algoritmo de Autenticación Celular y Encriptación de Voz.

### **Tabla CAVE**

Es una tabla de 256 posiciones ocupando 2 dígitos hexadecimales en cada posición.

### **CMEA**

Algoritmo celular para Encriptación de Mensajes.

---



## **CMEA-key**

Es una clave generada por 8 registros diferentes de 8 bits identificadores separadamente como  $k_0, k_1, \dots, k_7$ . Los datos en estos registros resultan de la acción del algoritmo CAVE y son usados para encriptar ciertos mensajes.

## **Iteración**

Es la ejecución del algoritmo Cave. Todas las aplicaciones del CAVE a través de este apéndice usa ya sea 8 o 4 rondas por iteración.

## **$k_0, k_1, \dots, k_7$**

Son los 8 registros de 8 bits en los cuales contienen a la clave CMEA-key.

## **LFSR**

Registro de desplazamiento de realimentación lineal (Linear Feedback Shift Register).

## **LFSR\_A**

Es el registro A, es un sinónimo para 31 a 24 bits del LFSR.

## **LFSR\_B**

Es el registro B, es un sinónimo para 23 a 16 bits del LFSR.

---

## **LFSR\_C**

Es el registro C, es un sinónimo para bits 15 a 8 del LFSR.

## **LFSR\_D**

Es el registro D, es un sinónimo para bits 7 a 0 del LFSR.

## **LFSR-Cycle**

Es un registro que consiste de las siguientes etapas:

1. Procesa el valor del bit A7 usando la formula  $A7 = B6 \text{ XOR } D2 \text{ XOR } D1 \text{ XOR } D0$ . Guarda temporalmente este valor sin el cambio del valor anterior del bit A7 en el registro A.
2. Ejecuta un desplazamiento de un bit hacia la derecha en los 4 registros A,B, C,D y descarta el bit D0 el cual ha sido desplazado hacia fuera.
3. Usa el valor del bit A7 previamente almacenado y procesado para el primero de estas tres etapas.

## **Offset1**

Es una cantidad de 8 bits que apunta a uno de los 256 valores de 4 bits en la tabla 0. Las operaciones aritméticas en el offset1 son ejecutadas en modulo 256.

## **Offset2**

Es una cantidad de 8 bits que apunta a uno de los 256 valores de 4 bits en la tabla 1. Las operaciones aritméticas en el offset2 son ejecutadas en modulo 256.

---

## **R00-R15**

Son 16 registros mezcladores 8 bits usados en el algoritmo CAVE. También se lo llama register[0 through 15]

## **SSD**

Share Secret Data. Consiste de dos cantidades, SSD\_A y SSD\_B. Un nuevo valor de las cantidades SSD pueden ser generados en la estación móvil cuando desee el operador mediante la transacción de mensaje para actualizar el SSD.

## **SSD\_A**

Es una cantidad binaria en la memoria semipermanente de la estación móvil y también conocida por el centro de conmutación MSC serving.

## **SSD\_A\_NEW**

Es la cantidad revisada de 64 bits mantenida separadamente del SSD\_A, esta cantidad es generada como un resultado del proceso de generación del SSD.

## **SSD\_B**

Es una cantidad binaria en la memoria semipermanente de la estación móvil y también conocida por el centro de conmutación MSC serving. Es usada en el procesamiento del CMEA y VPM.

---

## **SSD\_B\_NEW**

Es la cantidad revisada de 64 bits mantenida separadamente del SSD\_B, esta cantidad es generada como un resultado del proceso de generación del SSD.

### **Tabla 0**

Consiste en los 4 bits de menor orden que ocupan una de las 256 posiciones de la tabla usada por el algoritmo CAVE. Es procesada como  $\text{CaveTable}[\ ] \text{ AND } 0xF0$

## **VPM**

Voice Privacy Mask (Mascara para privacidad de voz). Este nombre describe 2 diferentes valores binarios de 260 bits. Uno es XORed con los bits en el Canal de Trafico digital Delantero y el otro es XORed con los bits en el Canal de Trafico Digital Reverso para proveer la tal denominada privacidad de voz. El VPM usado para la estación base a la transmisión de la estación móvil es el VPM Delantero; así misma para la estación móvil a la transmisión de la estación base es el VPM Reverso.

## **2. Proceso CAVE.**

El CAVE es un software compatible como función mezcladora no lineal cuyos componentes son: Un registro de desplazamiento para reglamentación lineal de 32 bits (LFSR), 16 registros mezcladores de 8 bits, y una tabla de búsqueda con 256 posibilidades. La tabla completa con estas 256 posibilidades se muestra en la figura 2.3. Los 4 bits de menor orden comprenden la tabla 0 y los 4 bits de mayor orden comprenden la tabla 1.

---

El arreglo pictórico de la tabla se muestra en la fig. 2.1. Ahí se muestra las 4 etapas (A, B, C, D) cada una con 8 bits del registro LFSR. El proceso CAVE usa repetidamente el LFSR y la atabla para aleatorizar los contenidos de los 16 registros mezcladores de 8 bits con la siguiente simbología: R00, R01,R02,....., R15. Además dos punteros offsets de la tabla de búsqueda aleatorizan la tabla de acceso. Finalmente 8 permutaciones ejecutadas son ingresadas en las tablas de búsqueda para arrastrar a los registros R00 a través de R15 después de cada ronda de procesamiento a través del algoritmo.

La operación del algoritmo consiste de tres etapas: un arranque inicial, una aleatorización repetida consistiendo de 4 u 8 rondas y el procesamiento de la salida. El arranque inicial consiste en el aislamiento de los LFSR, 16 registros R00,.....,R15 y de los punteros offsets con información que es específica para la aplicación . El proceso de aleatorización es común para todos los casos.

La aleatorización es una operación detallada que es descrita en las figuras 2.1, 2.2, 2.3. La salida procesante utiliza los contenidos finales aleatorizados de los registros R00 a través R15 en una función simple en la cual el resultado es enviado a la tarea subsiguiente.

El algoritmo CAVE puede ser aplicado en un número de diferentes casos . En cada caso hay diferentes requerimientos de inicialización, y diferentes salidas procesadas.

---

Figura A.26

Elementos del Algoritmo CAVE

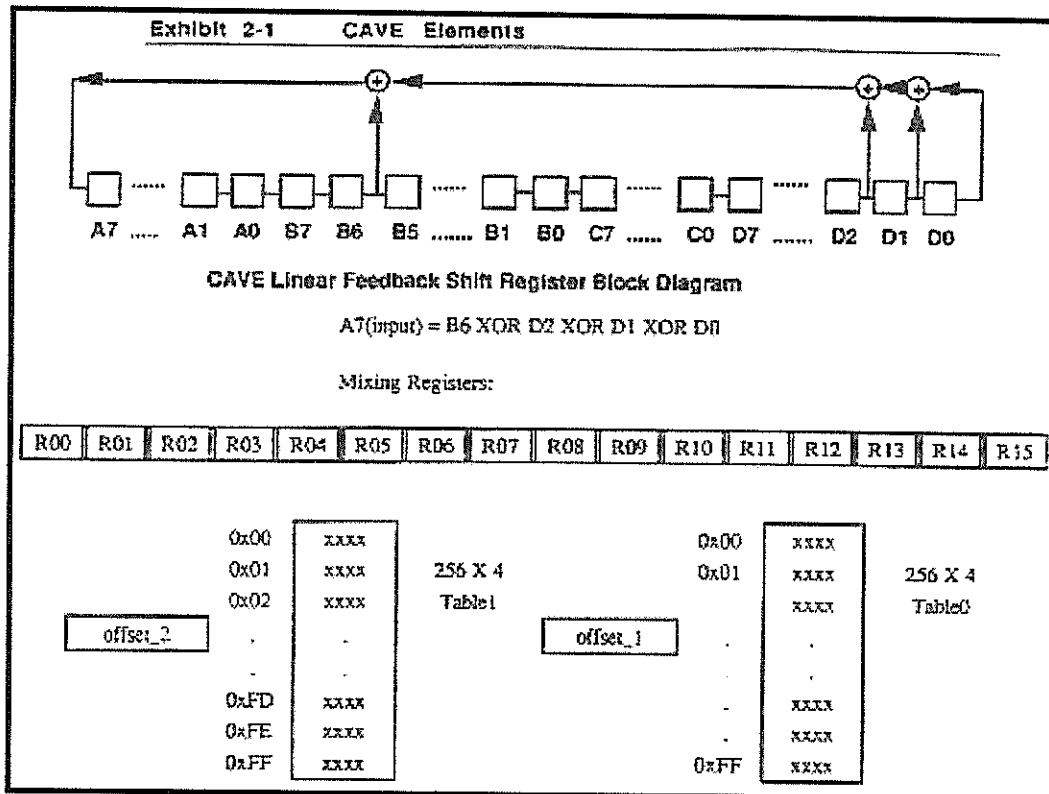


Figura A.27

Algoritmo CAVE

LOMASK = 0x0F;

HIMASK = 0xF0;

Inputs:

number\_of\_rounds: integer; /\* will be either 8 or 4 \*/

LFSR: 32 bit integer;

/\* LFSR\_A: 8 MSBs of LFSR;

\* LFSR D: 8 LSBs of LFSR: \*/

offset\_1, offset\_2: unsigned 8 bit integer;

register[0 through 15]: 8 bit integer; /\* R00 to R15 \*/

T[0 through 15] : 8 bit integer; /\* temporary registers \*/

CaveTable[0 through 255]: 8 bit integer;

Variables:

```
temp_reg0: 8 bit integer;
lowNibble: 8 bit integer;
hiNibble: 8 bit integer;
temp: 8 bit integer;
round_index: integer;
R_index: integer;
fail_count: integer;
```

Functions:

```
LFSR_cycle(); /* perform an LFSR cycle */
Rotate_right_registers(); /* rotate the mixing registers */
```

For round\_index = number\_of\_rounds-1 to 0

```
{
/* Save R0 for re-use later */
temp_reg0 = register [0];
For each register from R_index = 0 to 15
{
fail_count = 0;
while (TRUE)
{
offset_1 = offset_1+(LFSR_A XOR register[R_index]);
lowNibble = CaveTable[offset_1] AND LOMASK;
if (lowNibble is equal to register[R_index] AND LOMASK)
{
do LFSR_cycle;
fail_count = fail_count + 1;
if (fail_count is equal to 32)
{
LFSR_D = LFSR_D + 1; /* no carry to LFSR_C */
break while; /* with no carry to LFSR_C */
}
}
else
break while;
}

fail_count = 0;
```

```

while (TRUE)
{
  offset_2 = offset_2 + (LFSR_B XOR register[R_index]);
  hiNibble = CaveTable[offset_2] AND HIMASK;
  if (hiNibble is equal to register[R_index] AND HIMASK)
  {
    do LFSR_cycle;
    fail_count = fail_count + 1;
    if (fail_count is equal to 32)
    {
      LFSR_D = LFSR_D + 1; /* no carry to LFSR_C */
      break while;      /* with no carry to LFSR_C */
    }
  }
  else
    break while;
}

temp = (lowNibble OR hiNibble);
if (R_index is equal to 15)
  register[R_index]=temp_reg0 XOR temp;
else
  register[R_index] = register[R_index+1 ] XOR temp;
do LFSR cycle;
}
do Rotate_right_registers;

/* Shuffle the mixing registers */

For each register from R_index = 0 to 15
{
  temp = CaveTable[16*round_index + R_index] AND LOMASK;
  T[temp] = register[R_index];
}

For each register from R_index = 0 to 15
register[R_index] = T[R_index];

```

---



```
}
```

Function:

```
LFSR_cycle();
```

```
{
```

Variable:

```
temp: 1 bit binary;
```

```
temp = LFSR_B[6] XOR LFSR_D[2] XOR LFSR_D[1] XOR LFSR_D[0];
```

```
Shift right LFSR /* Discard LFSR_D[0] bit */
```

```
LFSR_A[7] = temp;
```

```
}
```

Function: /\* 128 bit cyclic shift right on R00 to R15 \*/

```
Rotate_right_registers();
```

```
{
```

Variable:

```
temp_reg: 8 bit binary;
```

```
temp_reg = register [15];
```

```
For each register from R_index = 15 to 1
```

```
{
```

```
Shift register[R_index] one place right; /* set MSB = 0 */
```

```
If (register[R_index-1] AND 0x1)
```

```
register[R_index] = register[R_index] OR 0x80;
```

```
}
```

```
Shift register[0] one place right; /* set MSB = 0 */
```

```
if (temp_reg AND 0x1)
```

```
register[0] = register[0] OR 0x80;
```

```
}
```

**Tabla A.4**  
**TABLA DEL ALGORITMO CAVE**

hi/lo	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	D9	23	5F	E6	CA	68	97	B0	7B	F2	0C	34	11	A5	8D	4E
1	0A	46	77	8D	10	9F	5E	62	F1	34	EC	A5	C9	B3	D8	2B
2	59	47	E3	D2	FF	AE	64	CA	15	8B	7D	38	21	BC	96	00
3	49	56	23	15	97	E4	CB	6F	F2	70	3C	88	BA	D1	0D	AE
4	E2	38	BA	44	9F	83	5D	1C	DE	AB	C7	65	F1	76	09	20
5	86	BD	0A	F1	3C	A7	29	93	CB	45	5F	E8	10	74	62	DE
6	B8	77	80	D1	12	26	AC	6D	E9	CF	F3	54	3A	0B	95	4E
7	B1	30	A4	96	F8	57	49	8E	05	1F	62	7C	C3	2B	DA	ED
8	BB	86	0D	7A	97	13	6C	4E	51	30	E5	F2	2F	D8	C4	A9
9	91	76	F0	17	43	38	29	84	A2	DB	EF	65	5E	CA	0D	BC
A	E7	FA	D8	81	6F	00	14	42	25	7C	5D	C9	9E	B6	33	AB
B	5A	6F	9B	D9	FE	71	44	C5	37	A2	88	2D	00	B6	13	EC
C	4E	96	A8	5A	B5	D7	C3	8D	3F	F2	EC	04	60	71	1B	29
D	04	79	E3	C7	1B	66	81	4A	25	9D	DC	5F	3E	B0	F8	A2
E	91	34	F6	5C	67	89	73	05	22	AA	CB	EE	BF	18	D0	4D
F	F5	36	AE	01	2F	94	C3	49	8B	BD	58	12	E0	77	6C	DA

**Tabla A.5**  
**Tabla CAVE en ASCII**

hi/low	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	d9	23	5f	e6	ca	68	97	b0	7b	f2	0c	34	11	a5	8d	4e
1	0a	46	77	8d	10	9f	5e	62	f1	34	ec	a5	c9	b3	d8	2b
2	59	47	e3	d2	ff	ae	64	ca	15	8b	7d	38	21	bc	96	00
3	49	56	23	15	97	e4	cb	6f	f2	70	3c	88	ba	d1	0d	ae
4	e2	38	ba	44	9f	83	5d	1c	de	ab	c7	65	f1	76	09	20
5	86	bd	0a	f1	3c	a7	29	93	cb	45	5f	e8	10	74	62	de
6	b8	77	80	d1	12	26	ac	6d	e9	cf	f3	54	3a	0b	95	4e
7	b1	30	a4	96	f8	57	49	8e	05	1f	62	7c	c3	2b	da	ed
8	bb	86	0d	7a	97	13	6c	4e	51	30	e5	f2	2f	d8	c4	a9
9	91	76	f0	17	43	38	29	84	a2	db	ef	65	5e	ca	0d	bc
A	e7	fa	d8	81	6f	00	14	42	25	7c	5d	c9	9e	b6	33	ab
B	5a	6f	9b	d9	fe	71	44	c5	37	a2	88	2d	00	b6	13	ec
C	4e	96	a8	5a	b5	d7	c3	8d	3f	f2	ec	04	60	71	1b	29
D	04	79	e3	c7	1b	66	81	4a	25	9d	dc	5f	3e	b0	f8	a2
E	91	34	f6	5c	67	89	73	05	22	aa	cb	ee	bf	18	d0	4d
F	f5	36	ae	01	2f	94	c3	49	8b	bd	58	12	e0	77	6c	da

### Verificación del A-key

El valor incumplido del A-key cuando la estación móvil es enviada desde la fabrica estará reseteada en binarios ceros. El valor del A-key es especificado por cada operador. Una estación móvil múltiple NAM requerirá de múltiples A-keys, tan bien como múltiples posiciones de las correspondientes criptovariables por claves A-key.

Cuando los dígitos de la clave A-key son ingresados desde el teclado, el numero de dígitos ingresados debe ser por lo menos de 6, y puede ser hasta máximo e

incluyendo a 26. El procedimiento entrante especificado por el fabricante de la estación móvil indicara inambiguamente el fin de la secuencia de los dígitos ingresados. En el caso de que el numero de dígitos ingresados por teclado sea menos de 26, los dígitos mas significativos serán puestos en cero, con el propósito de producir una cantidad de 26 dígitos llamada “valor entrante”.

El proceso de verificación chequea la precisión de los 26 dígitos decimales de valor entrante. Los primeros 20 dígitos son convertidos en una representación de 64 bits para servir como una entrada al CAVE, junto con el ESN de la estación móvil. El CAVE esta luego corriendo de la misma manera como en el modo de autenticación y su respuesta comparada de 18 bits al equivalente binario de los últimos 6 dígitos ingresados. Una participación del A-key causara que el patrón de 64 bits llegar a ser escrito a la memoria semipermanente de la estación móvil. Además el SSD\_A y el SSD\_B serán puestos en cero. En el caso de no haber dicha participación, un resultado erróneo es mostrado al subscriptor por medio de indicaciones especificadas por el fabricante de la estación móvil, y ningún dato interno es actualizado.

El primer dígito decimal del valor entrante es considerado a ser el mas significativo de los 20 dígitos decimales, seguidos en sucesión por el anterior. El vigésimo primer dígito es el mas significativo de los dígitos chequeados, seguido en sucesión por los 5 bits que permanecen. Un proceso de conversión de decimal a binario convierte tanto la secuencia de dígitos en sus equivalentes en base dos. Por ejemplo, los 26 dígitos:

1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0, 1 3 1 1 3 6

tiene una equivalente hexadecimal de

---

AB54A98CEB1F0AD2,20040

El CAVE será inicializado y corrido como sigue. Primero, los 32 bits mas significativos de los 64 bits ingresados serán cargados en el LFSR. Si este patrón de 32 bits llena el LFSR con todos los ceros entonces el LFSR será cargado con el ESN. Así pues el numero de 64 bits ingresados será puesto en R00 hasta R07. El vigésimo cuarto bit menos significativo será repetido en R09, R10 y R11. El Algoritmo de Versión Autenticación (hexadecimal C7) ocupara en el registro R08, y el ESN será cargado en R12 hasta R15. El CAVE se ejecutara para 8 rondas como se describió en la sección 2. Por otro lado el AUTHR es obtenido del valor final de los registros del CAVE (R00,R01,.....,R15). Los dos bits más significativos del AUTHR son iguales a los dos bits menos significativos de la operación R00 XOR R13. Los 8 próximos bits del AUTHR son iguales a R01 XOR R14. Finalmente, los bits menos significativos del AUTHR son iguales a R02 XOR R15.

El dieciochoavo bit de respuesta será comparado al equivalente binario de los 6 últimos dígitos ingresados. Una ejecución de este tipo se almacenara en la memoria semipermanente. Si no hay una ejecución puede iniciarse una acción correctiva.

### Figura A.28

Pseudo-codigo para verificación del A-key

```
In case of A-key verification
{
  if (32 MSBs of A-key are not equal to 0)
    LFSR = 32 MSBs of A-key;
  else
    LFSR = ESN;
  register[0 through 7] = A-key;
  register[8] = AAV;
  register[9 through 11] = 24 LSBs of A-key;
```

```

register[12 through 15] = ESN;
number_of_rounds = 8;
offset_1 = offset_2 = 128;
do CAVE;
Answer[2] = (register[0] XOR register[13]) AND 0x3;
Answer[1] = register[1] XOR register[14];
Answer[0] = register[2] XOR register[15];
if (Answer is equal to A-key check_sum)
    A-key is verified;
else
    A-key is not verified;
}

```

### **Generación y Actualización del SSD.**

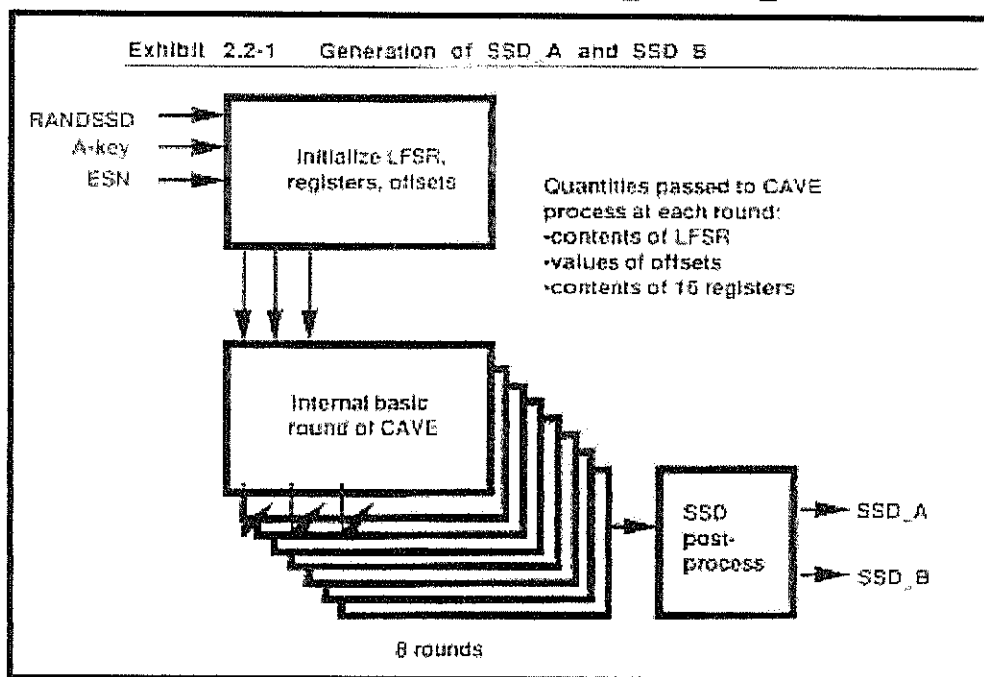
En esta sección se adiciona los detalles para habilitar la implementaron en el subscriptor y en el equipo base. La figura 2.2-1 muestra el proceso gráficamente. La figura 2.2-2 indica las operaciones en Pseudo-código.

Las variables de entrada para este procedimiento son: RANDSSD (56 bits), Algoritmo de Versión Autenticación (8 bits), ESN (32 bits), y el A-key (64 bits). El CAVE será inicializado como sigue. Primero el LFSR será cargado con los 32 bits menos significativos del A-key. Si el patrón de bit resultante llena al LFSR con todos ceros, entonces el LFSR será cargado con los 32 bits menos significativos del RANDSSD para prevenir un resultado trivial nulo.

Los registros R00 hacia R07 serán inicializados con el A-key, el registro R08 será el Algoritmo de Autenticacion Version (11000111). R09, R10 y R11 serán los bits más significativos del RANDSSD, y el ESN será cargado en R12 hasta R15. Offset1 y Offset2 inicialmente serán puestos a 128.

El CAVE estará corriendo por 8 rondas como se describió previamente en la sección 2. Cuando esto se complete , los registros R00 hacia R07 llegaran a producir el SSD\_A\_NEW y los registros R08 hacia el R15 llegaran a dar el valor de SSD\_B\_NEW.

**FIGURA A.29**  
**GENERACION DEL SSD\_A Y SSD\_B**



**Figura A.30**  
**Pseudo –código para actualizar el SSD**

```
In case of SSD Update
{
  number_of_rounds = 8;
  LFSR = 32 LSBs of RANDSSD;
  LFSR = LFSR XOR 32 MSBs of A-key XOR 32 LSBs of A-key;
  if (LFSR is equal to 0)
    LFSR = 32 LSBs of RANDSSD;
  register[0 through 7] = A-key;
```

```

register[8] = AAV;
register[9 through 11] = 24 MSBs of RANDSSD;
register[12 through 15] = ESN;
offset_1 = offset_2 = 128;
do CAVE;
SSD_A_NEW = register[0 through 7];
SSD_B_NEW = register[8 through 15];
}

```

### **Calculo del AUTHR y AUTHU.**

Durante algunos de los procedimientos de autenticación, el dato secreto consiste del SSD\_A. Los registros R12 hasta el R15 son inicializados con el ESN. El CAVE es corrido para 8 rondas. El resultado del AUTHR que es el bit 18, es enviado en palabra C donde el MSB del AUTHR esta próximo al campo RANDC y el LSB del AUTHR es próximo al campo de paridad. La instalación completa para los cálculos del AUTHR es presentada en la tabla.

La figura 2.3-2 muestra el proceso en forma gráfica mientras el Pseudocódigo para el proceso esta dado en la figura 2.3-3. Una explicación mas detallada del caso dependiente de procedimientos de instalación inicial se sigue. El AUTHU es la respuesta en el caso de un Unico Desafío (Unique Challenge). Fuera de la diferencia en la inicialización de la variable indicada en la figura 2.3-1, el tratamiento del AUTHU es idéntico al del AUTHR, y ya sea que la variable sea referida como AUTHU/AUTHR.

La instalación de los registros R09, R10, y R11 es el caso dependiente. Para registros, terminaciones de llamadas y los casos de respuesta del Unique Challenge, los registros antes mencionados son inicialmente cargados con el MIN1. Para originar llamadas de la estación móvil, un sub ajuste de los dígitos marcados es cargado en el registro R09 hasta el R11. El estándar IS-54 declara que los últimos 6 dígitos



marcados transmitidos por la estación móvil son para ser usados. Cada dígito marcado esta representado por un código de 4 bits non-zero. El MIN1 es usado para llenar inicialmente el registro R09, R10, R11 y luego los últimos dígitos marcados por el subscriptor son usados para reemplazar todo o parte de este valor inicial. Si los 6 dígitos son marcados, el primer dígito de los 6 que fueron marcados es usado como el mas significativo de los 4 bits de R09. El segundo dígito es el menos significativo de los 4 bits del registro R09. El tercer dígito es el bit más significativo de R10. El cuarto dígito es el menos significativo de los 4 bits de R10. El quinto dígito es el bit mas significativo de los 4 bits de R11. El sexto dígito es el bit menos significativo de los 4 bits de R11. Si menos de 6 dígitos son ingresados entonces el menos significativo de los 4 bits de R11 son el ultimo dígito marcado, el penúltimo dígito marcado llegar a ser el mas significativo de los 4 bits de R11, y así sucesivamente hasta el primer de los dígitos marcados.

La instalación inicial del LFSR es también un caso dependiente. Para registrar, terminar y originar llamadas de la estación móvil, el LFSR será inicialmente instalado con los 32 bits del RAND. Para el caso de respuesta Unique Challenge, los 24 bits más significantes del LFSR serán cargados con los 8 bits menos significantes del LFSR que serán cargados con los 8 bits menos significantes del MIN2. Para todos los casos, la carga inicial del LFSR será luego procesada mediante la operación XOR con los 32 bits mas significantes del SSD\_A, luego este resultado se le hará otro XOR con los 32 bits menos significantes del SSD\_A, entonces se recarga el resultado en el LFSR. Si el patrón bit resultante llena el LFSR con todos los ceros, entonces el LFSR será restaurado a su carga inicial previo a la operación SSD\_A XOR para prevenir un resultado trivial nulo.

Para todos los casos, el resultado de autenticación de 18 bits AUTHR/AUTHU es obtenido del valor final de los registros del CAVE R00, R01, R02, R13, R14, R15. Los dos bits mas significantes del AUTHR/AUTHU son iguales

---

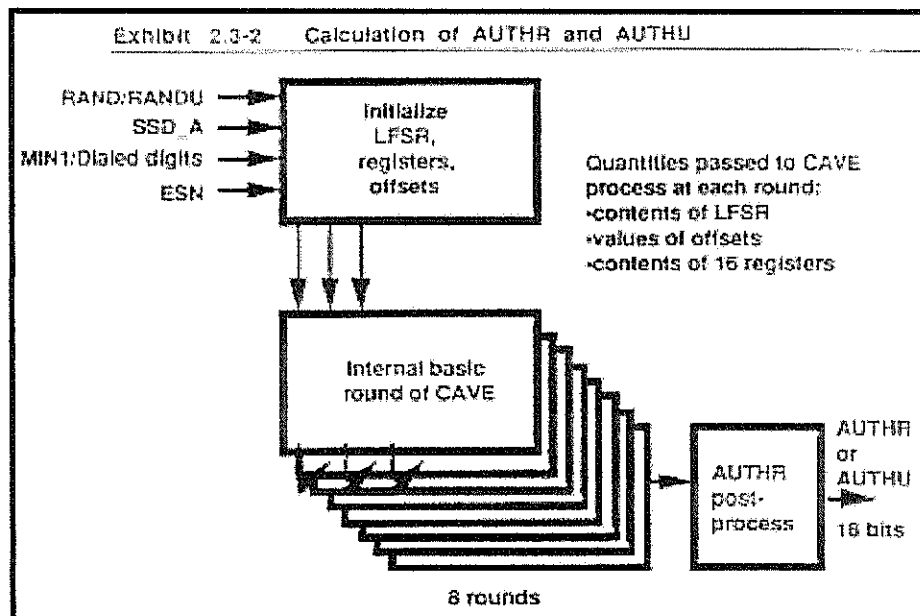
a los dos bits menos significantes de R00 XOR R13. Los próximos 8 bits del AUTHR/AUTHU son iguales a R01 XOR R14. Finalmente, los bits menos significantes del AUTHR/AUTHU son iguales a R02 XOR R15.

**FIGURA A.31**  
**CARGA INICIAL DEL CAVE PARA CALCULOS DEL**  
**AUTHR/AUTHU**

**Exhibit 2.3-1 CAVE Initial Loading for AUTHR/AUTHU Calculations**

CAVE Item	CASE			
	MS Registration	Unique Challenge-Response	MS Origination	MS Termination
LFSR	RAND	RANDU (24 bits) MIN2 (8 bits)	RAND	RAND
Reg [0-7]	SSD_A	SSD_A	SSD_A	SSD_A
Reg [8]	AAV	AAV	AAV	AAV
Reg [9-11]	MIN1	MIN1	Subset of Dialed Digits	MIN1
Reg [12-15]	ESN	ESN	ESN	ESN

**FIGURA A.32**  
**CÁLCULO DEL AUTHR Y AUTHU**



**FIGURA A.33**  
**PSEUDO-CODIGO PARA CALCULO DEL AUTHR**

Variables:

```
AUTHR: 18 bit binary value; /* same for AUTHU */
AUTHR[2]: 2 MSBs of AUTHR;
AUTHR[1]: next 8 MSBs of AUTHR;
```

In case of AUTHR/AUTHU calculation

```
{
number_of_rounds = 8;
if (case is MS reg. or MS origination or MS termination)
    LFSR = RAND XOR 32 MSBs of SSD_A XOR 32 LSBs of SSD_A;
    if (LFSR is equal to 0)
        LFSR = RAND;
if (case is unique challenge-response)
    LFSR = (RANDU<<8 OR 8 LSBs of MIN2)
        XOR 32 MSBs of SSD_A XOR 32 LSBs of SSD_A;
/* RANDU<<8 indicates left shift 8 places */
    if (LFSR is equal to 0)
        LFSR = (RANDU<<8 OR 8 LSBs of MIN2);
register[0 through 7] = SSD_A;
register[8] = AAV;
register[9 through 11] = MIN1;
If (case is MS origination)
    replace a nibble of register[9 through 11] with each of the
    last 1 to 6 dialed digits such that the low nibble of R11
    contains the last dialed digit;
register[12 through 15] = ESN;
offset_1 = offset_2 = 128;
do CAVE;
AUTHR[2] = (register[0] XOR register[13]) AND 0x03;
AUTHR[1] = register[1] XOR register[14];
AUTHR[0] = register[2] XOR register[15]; /* same for AUTHU */
}
```

### **Generación de la clave CMEA key y del VPM .**

El proceso para la generación de la clave CMEA y de la Mascara de privacidad de voz (VPM) generalmente será mas eficiente cuando sean concatenados como se describe mas adelante. Las criptovariables de autenticación a ser usadas son aquellas del proceso ultimo del global Challenge, y no aquellas de algún proceso Unique Challenge.

Si el bit AUTH en el bloque de mensajes es cero, el móvil ignorara los bits MEM y VPM y los bits MEM son el Mensaje de Designación del Canal de Trafico Inicial, el Mensaje de Designación del canal de Voz Inicial y el Mensaje de Status. La estación móvil no aplicara la Mascara de Encipción de Mensaje o la Mascara de Privacidad de Voz.

### **Generación de la clave CMEA key.**

Los 8 bytes de la clave de sesión CMEA son derivados por la corrida del algoritmo CAVE a través de una iteración de 8 rondas y luego las dos siguientes iteraciones de 4 rondas son la autenticación. Esto es presentado en la parte superior de las figuras 2.3-2 y 2.3-3,. La inicialización de post-autenticación y los requerimientos para la salida procesante son los siguientes:

- Primero, el LFSR será reinicializado a la suma or exclusiva de sus contenidos de post-autenticacion y tantas hojas del SSD\_B. Si el resultado del bit patrón llena el LFSR con todos los ceros, entonces el LFSR será cargado con el RAND.
  - Segundo, los registros R00 hasta el R07 serán inicializados con SSD\_B en vez del SSD\_A.
-

- Tercero, Los registros R09, R10 y R11 deberían ser cargados como la descripción del AUTHR.
- Cuarto, los registros R12 hacia el R15 podrían ser cargados con el ESN.
- Quinto, los punteros de tabla offset empezaran este proceso en sus valores de autenticación final, mas bien que empezar a resetear a un estado predeterminado.
- Sexto, el LFSR es cargado antes de la segunda y tercera iteración de post-autenticacion con un “revolvedor RAND” comprendido de los contenidos de R00, R01, R14 y R15. Si el resultado bit patrón llena el LFSR con todos los ceros, entonces el LFSR será cargado con RAND.

Los bytes dibujados de las iteraciones 2 y 3 son marcados así:

- k0 = register[4] XOR register[8]; (iteration 2)
- k1 = register[5] XOR register[9]; (iteration 2)
- k2 = register[6] XOR register[10]; (iteration 2)
- k3 = register[7] XOR register[11]; (iteration 2)
- k4 = register[4] XOR register[8]; (iteration 3)
- k5 = register[5] XOR register[9]; (iteration 3)
- k6 = register[6] XOR register[10]; (iteration 3)
- k7 = register[7] XOR register[11]; (iteration 3)

### **Generación de la Mascara de Privacidad de Voz.**

La generación del VPM es una continuación de la clave de generación CMEA y podría ser ejecutada en el mismo momento bajo las mismas condiciones como la clave CMEA. El algoritmo CAVE es corrido en 11 iteración, aparte de aquellas

---

iteraciones que son producidas por los bytes CMEA. Cada iteración consiste de 4 rondas. Los registros del CAVE R00 hasta el R15 no son reseteados entre iteraciones, pero el LFSR es recargado entre iteraciones con el “rollover RAND” como se describió en la sección. Los asignamientos del bit mascara son los siguientes; los MS transmisión/BS recepción son los primeros 260 bits generados por este proceso iniciando en la iteración 4 y concluyendo durante la iteración 9. Los bits MS recepción/BS transmisión son los bits de permanencia generados durante la iteración 9 y terminando con el bit final de la iteración 14. Para cada caso, el bit más significativo será el bit de mas alto orden de la primera suma XOR, seguido en orden por los bits de permanencia de esa suma. El próximo bit de mas alto será el bit alto de la segunda suma, etc. El bit menos significativo del caso MS transmisión/BS recepción será el bit 4 de (R04 XOR R10) durante la iteración 9. El siguiente bit, el bit 3 de esa palabra, será el bit más significativo de la mascara para el caso de MS recepción/BS transmisión.

Los bits codificados Clase 1  $cc0[i]$  y  $cc1[i]$  representan los bits de información 0 hacia el 177 en el siguiente orden:

$cc0[0]; cc1[0]; cc0[1]; cc1[1]; \dots; cc0[88]; cc1[88]$ .

Los bits de Clase 2  $CL2 [i]$  representa información de los bits 178 hacia el 259 en el siguiente orden:

$CL2[0]; CL2[1]; \dots; CL2[81]$ .

El transmisor MS hará la operación XOR con la información del bit 0 de sus tramas con el bit más significativo (bit 7) de  $R02 \text{ XOR } R08$  de la iteración 4. El bit 1 se le hará la operación XOR con el bit 6, etc., hasta que la información del bit 259 se le

haga Xor con el bit 4 de (R04 XOR R10) de la iteración 9. El receptor BS ejecutara la misma operación en el bit recuperado para decriptar el trafico.

En una manera similar, el transmisor BS hará operación XOR con la información del bit 0 de sus tramas con el bit 3 de la iteración 9 (R04 XOR R10),el bit 1 se le hará la operación XOR con el bit 2 de la iteración 9, (R04 XOR R10) etc., hasta que la información del bit 259 se le haga Xor con el bit 0 de (R06 XOR R12) de la iteración 14. El receptor MS ejecutara la misma operación en el bit recuperado para decriptar el trafico.

EL VPM no esta para ser cambiado durante una llamada. Si el VPM no esta disponible en el momento de una designación del canal de trafico inicial sobre el ingreso de la tarea de Conversación, (típicamente debido al calculo de retardo en su generación) entonces un VPM lleno de ceros esta para ser usado hasta que el VPM operacional haya sido completamente generado.

#### FIGURA A.34

##### PSEUDO CODIGO PARA CLAVE CMEA Y GENERACION DEL VPM.

Outputs:

```
cmeakey[0 through 7]: 8 bit binary key values; /* k0 - k7 */
VPM[0 through 64]: 8 bit binary values (520 bits total)
/* first 260 bits of VPM are Reverse Mask
* second 260 bits generated are Forward Mask */
```

In case CMEA key & VPM generation

```
{
/* Iteration 1: first pass through CAVE */
number_of_rounds = 8;
LFSR = post_auth_LFSR;
LFSR = LFSR XOR 32 MSBs of SSD_B XOR 32 LSBs of SSD_B;
if (LFSR is equal to 0)
    LFSR = RAND;
```

```

register[0 through 7] = SSD_B;
register[8] = AAV;
register[9 through 11] = MIN1;
if (case is MS origination)
    replace a nibble of register[9 through 11] with each of the
    last 1 to 6 dialed digits such that the low nibble of R11
    contains the last dialed digit;
register[12 through 15] = ESN;
offset_1 = post_auth_offset_1; /* restore offsets to their */
offset_2 = post_auth_offset_2; /* post authentication values */
do CAVE;

/* Iteration 2: generation of first CMEA key parameters */
number_of_rounds = 4;
do roll_LFSR;
do CAVE;
cmeakey[0] = register[4] XOR register[8];
cmeakey[1] = register[5] XOR register[9];
cmeakey[2] = register[6] XOR register[10];
cmeakey[3] = register[7] XOR register[11];

/* Iteration 3: generation of next CMEA key parameters */
number_of_rounds = 4;
do roll_LFSR;
do CAVE;
cmeakey[4] = register[4] XOR register[8];
cmeakey[5] = register[5] XOR register[9];
cmeakey[6] = register[6] XOR register[10];
cmeakey[7] = register[7] XOR register[11];

/* Iteration 4 - 13: generation of VPM */
vpm_ptr = 0;
For 10 repetitions
{
    do roll_LFSR;
    number_of_rounds = 4;
    do CAVE;
    For r_ptr = 0 to 5

```

---



```

    {
    VPM[vpm_ptr] = register[r_ptr+2] XOR register[r_ptr+8];
    vpm_ptr = vpm_ptr + 1;
    }
}

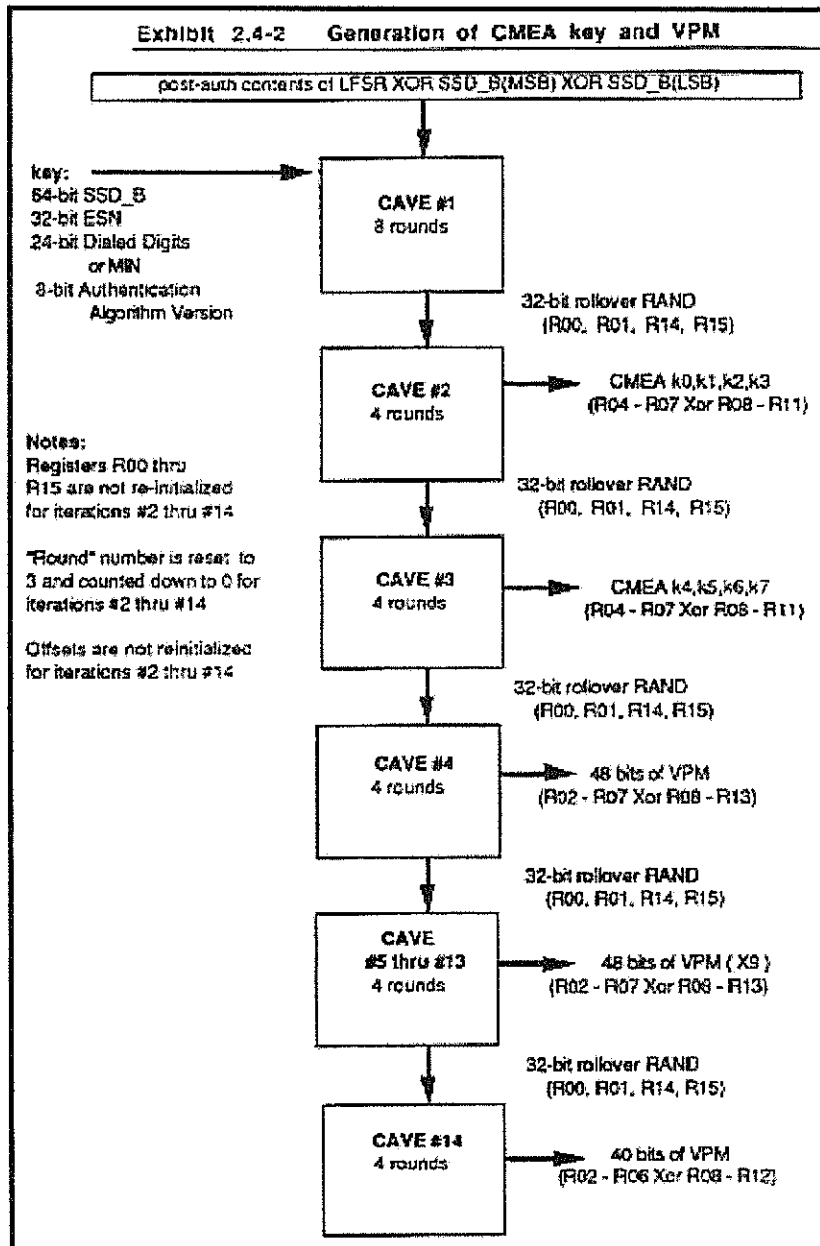
/* Iteration 14: generation of last VPM bits */
do roll_LFSR;
number_of_rounds = 4;
do CAVE;
For r_ptr = 0 to 4
    {
    VPM[vpm_ptr] = register[r_ptr+2] XOR register[r_ptr+8];
    vpm_ptr = vpm_ptr + 1;
    }
}

Function:
roll_LFSR;
{
LFSR_A = register[0];
LFSR_B = register[1];
LFSR_C = register[14];
LFSR_D = register[15];
if (LFSR is equal to 0)
LFSR = RAND;
}

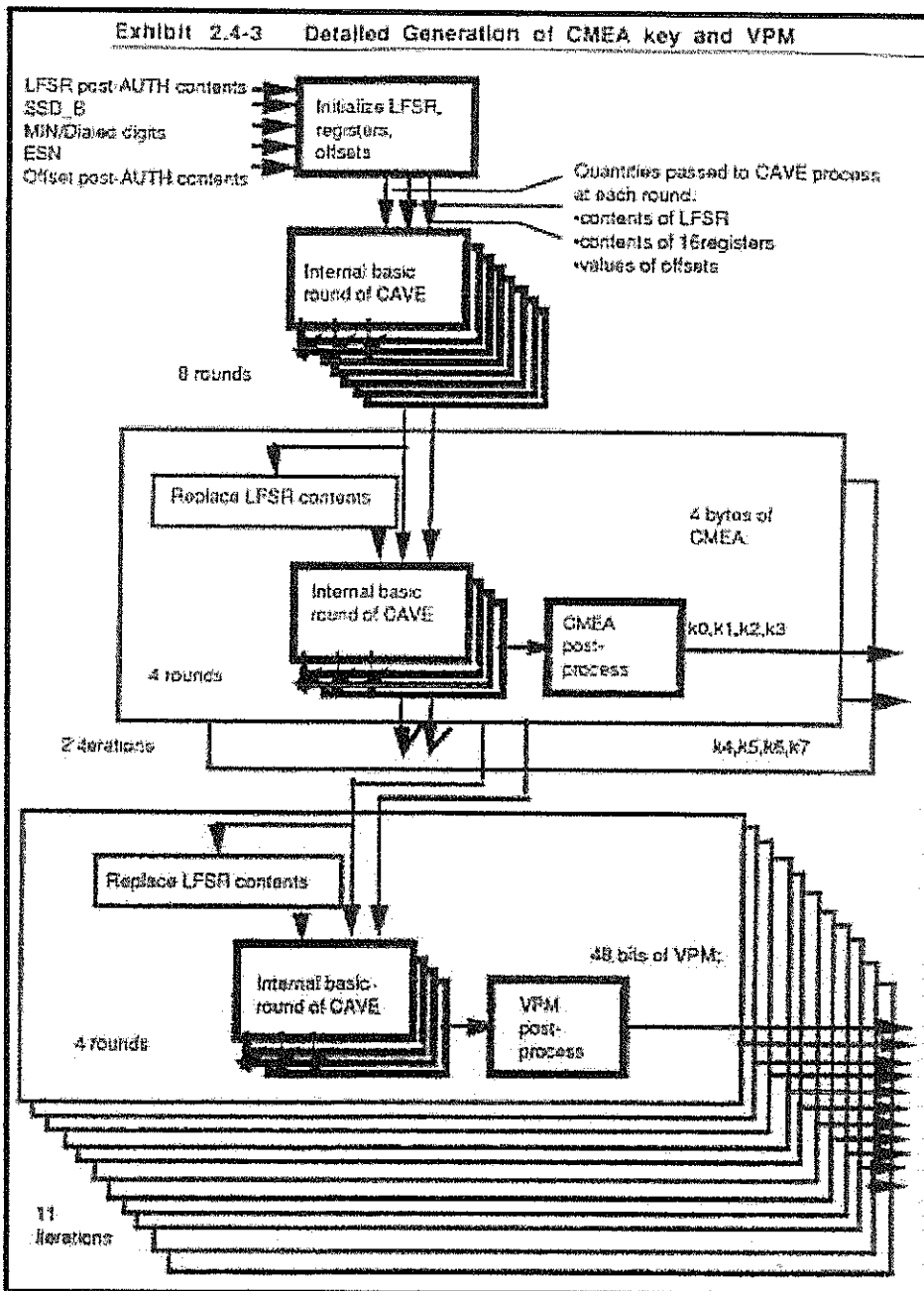
```

---

**FIGURA A.35**  
**GENERACION DE LA CLAVE CMEA Y DE LA MASCARA DE**  
**PRIVACIDAD DE VOZ.**



**FIGURA B. 11**  
**GENERACION DETALLADA DE LA CLAVE CMEA Y DE LA**  
**MASCARA DE PRIVACIDAD DE VOZ.(VPM)**



**APENDICE C**

**ALGORITMO DE ENCRIPCIÓN**

**DE MENSAJES**

**CMEA**

---

# ALGORITMO DE ENCRIPCIÓN DE MENSAJES

## CMEA

### 1. Proceso de Encriptación de Mensajes CMEA

Este proceso usa la clave de sesión CMEA de 8 bytes para producir mensajes descifrados mediante un algoritmo único CMEA. Este proceso de generación de la clave CMEA es descrito en el Apéndice B sección 2.4. Una descripción de los mensajes que son descifrados está incluido en esta sección. Se observa que el CMEA está generado después de cada origen o respuesta de un page (móvil terminal).

#### 2.1 Algoritmo CMEA.

Este algoritmo encripta y desencripta mensajes que son de longitud  $8*n$  bits, donde  $n$  es el número de mensajes bytes. El mensaje es primero almacenado en un buffer  $n$ -byte llamado `msg_buf[ ]`, tanto que cada byte sea asignado a un valor "`msg_buf[ ]`". El `msg_buf[ ]` será encriptado por medio de tres operaciones antes de que este listo para la transmisión. La desencriptación será ejecutada en la misma manera como la encriptación.

La función `tbox()` es frecuentemente usada. Esta definida así:

---

$$tbox(z) = C(((C(((C(((C((z \text{ XOR } k_0) + k_1) + z) \text{ XOR } k_2) + k_3) \\ + z) \text{ XOR } k_4) + k_5) + z) \text{ XOR } k_6) + k_7) + z$$

donde

- “+” denota el modulo de adición 256,
- “XOR” es la función XOR,
- “z” es la función argumento,
- $k_0, \dots, k_7$  ya esta definido en apéndice B,

y  $C()$  es la salida de la tabla buscadora. (Ver figura 2-3 del apéndice B)

La siguiente figura es el pseudo código para un procedimiento algorítmico para  $tbox()$ . Note que todas las adiciones ejecutadas en las variables “temp” y “z” son modulo 256.

### **Figura A.37**

#### **Pseudo-código para t-box.**

Input:

z: unsigned integer range 0 to 255;

Variables:

temp: unsigned 8 bit integer;

k\_index: integer;

```

tbox (z);
{
k_index = 0;
temp = z;
For 4 repetitions
{
temp = temp XOR cmeakey[k_index];
temp = temp + cmeakey[k_index + 1]; /*mod 256 addition*/
temp = z + CaveTable [temp];          /*mod 256 addition*/
k_index = k index + 2;
}
return (temp);
}

```

El algoritmo CMEA es el proceso de encriptación de mensajes usado tanto para la encriptación y desencriptación de un mensaje. Cada mensaje para el cual el algoritmo CMEA es aplicado debe ser un múltiplo de 8 bits en longitud. El Algoritmo CMEA puede ser dividido en tres distintas manipulaciones. Ver figura 3.1-2.

### **FIGURA A.38**

#### **PSEUDO-CODIGO DEL ALGORITMO CMEA.**

Inputs:

```

byte_count: integer; /* number of bytes in the message */
msg_buf[0 to byte_count-1]: octet by octet representation of
                                message;

```

Variables:

```
msg_index: integer;
k: unsigned integer range 0 to 255;
z: unsigned integer range 0 to 255;
```

/\* First Manipulation: \*/

```
z = 0;
```

```
For msg_index 0 to byte_count-1
```

```
{
  k = tbox(z XOR msg_index);
  msg_buf[msg_index] = msg_buf[msg_index]+k; /*mod 256 addition*/
  z = z + msg_buf[msg_index];                /*mod 256 addition*/
}
```

/\* Second Manipulation: \*/

```
half = byte_count/2;
```

```
For msg_index = 0 to half; /*[? By hand a "-1" at "half" ?]*/
```

```
{
  msg_buf[msg_index] = msg_buf[msg_index] XOR
    (msg_buf[byte_count-1-msg_index] OR 0x1);
}
```

/\* Third Manipulation: \*/

```
z = 0;
```

```
For msg_index = 0 to byte_count-1
```

```
{
  k = tbox(z XOR msg_index);
  z = z + msg_buf[msg_index];
  msg_buf[msg_index] = msg_buf[msg_index] - k;
}
```

---



```
}          /* this subtraction is mod256 */  
          /* without borrow */
```

## **2.2 Descripción de Mensajes.**

Lo siguiente es una descripción de los 8 mensajes que son descifrados. Por cada mensaje, los campos descifrados son designados. Los mensajes son agrupados por designación del canal.

### **2.2.1 Canal de voz Delantero.**

#### **2.2.1.1 Alert With Info**

El mensaje Alert With Info es encriptado. La palabra 1 del Mensaje de Control de la estación móvil contiene el orden y los campos calificadores de orden que identifican este mensaje como ALERT WITH INFO. Ningún campo en la Palabra 1 es encriptado. Ningún campo en la palabra 2 – Primera palabra Alert With Info es encriptado.

Las palabras subsiguientes contienen una representación de carácter. Cada carácter transmitido es representado en la forma IA5 en un campo de 8 bits. Cada palabra contiene mas de 3 caracteres. Los 24 bits que comprenden los 3 caracteres en

---

cada palabra FVC son tratados por el CMEA como un mensaje simple. Ninguno de los campos adicionales son encriptados.

#### **2.2.1.2 Flash With Info.**

El mensaje Flash With Info es encriptado. . La palabra 1 del Mensaje de Control de la estación móvil contiene el orden y el campo calificador de orden que identifican este mensaje como FLASH WITH INFO. Ningún campo en la Palabra 1 es encriptado. Ningún campo en la palabra 2 – Palabra Flash With Info es encriptado.

Las palabras subsiguientes contienen una representación de carácter. Cada carácter transmitido es representado en la forma IA5 en un campo de 8 bits. Cada palabra contiene mas de 3 caracteres. Los 24 bits que comprenden los 3 caracteres en cada palabra FVC son tratados por el CMEA como un mensaje simple. Ninguno de los campos adicionales son encriptados.

### **2.2.2 Canal de voz Reverso**

#### **2.2.2.1 Mensaje de Dirección de la Llamada**

Los 32 bits en Palabra D que es la Primera palabra del Mensaje de Dirección de la Llamada la cual comprende los dígitos del 1 al 8, son encriptados. Estos 32

---

dígitos son tratados por el CMEA como un mensaje simple. Ninguno de los campos en la Palabra D son encriptados.

Los 32 bits en cada Palabra E, F, y G del mensaje de dirección de la llamada que comprende los dígitos marcados, son encriptados. Estos 32 bits son tratados por el CMEA como un nuevo mensaje particular. Ningunos de los campos adicionales en estas palabras son encriptados.

### **2.2.3 Canal de Trafico Digital Delantero.**

#### **2.2.3.1 Alert With Info**

El mensaje FACCH contiene a n caracteres cada uno representados como 8 bits en el formato IA5. Estos son encifrados primero para la codificación convolucional. El CRC es computado en los 48 bits resultantes. Para el primer slot de un mensaje multi/slot \*continuación Flag = 0\* todos los campos excepto el Tipo de Mensaje ( 40 bits en total ) son encriptados por CMEA. Para los subsiguientes slots de un mensaje multi slot (continuación Flag = 1 ) todos los campos son encriptados ( 48 bits en total ) por el CMEA.

#### **3.2.3.2 Flash With Info**

El mensaje FACCH contiene a n caracteres cada uno representados como 8 bits en el formato IA5. Estos son encifrados primero para la codificación

---

convolucional. El CRC es computado en los 48 bits resultantes. Para el primer slot de un mensaje multi/slot \*continuación Flag = 0\* todos los campos excepto el Tipo de Mensaje ( 40 bits en total ) son encriptados por CMEA. Para los subsiguientes slots de un mensaje multi slot ( continuación Flag = 1 ) todos los campos son encriptados ( 48 bits en total ) por el CMEA.

## **2.2.4 Canal de Trafico Digital Reverso**

### **2.2.4.1 Flash With Info**

El mensaje FACCH contiene 63 caracteres cada uno representados como 8 bits en el formato IA5. Estos son encifrados primero para la codificación convolucional. El CRC es computado en los 48 bits resultantes. Para el primer slot de un mensaje multi/slot \*continuación Flag = 0\* todos los campos excepto el Tipo de Mensaje (40 bits en total) son encriptados por CMEA. Para los subsiguientes slots de un mensaje multi slot (continuación Flag = 1 ) todos los campos son encriptados ( 48 bits en total ) por el CMEA.

### **2.2.3.2 Envío de la ráfaga DTMF**

El mensaje FACCH contiene 64 dígitos cada uno representados como 4 bits. Estos son encifrados previo a la codificación convolucional. El CRC es computado en los 48 bits resultantes. Para el primer slot de un mensaje multi/slot \*continuación

---

Flag = 0\* todos los campos excepto el Tipo de Mensaje ( 40 bits en total ) son encriptados por CMEA. Para los subsiguientes slots de un mensaje multi slot ( continuación Flag = 1 ) todos los campos son encriptados ( 48 bits en total ) por el CMEA.

### 2.2.3.3 Envío continuo del DTMF

El mensaje FACCH contiene un dígito representado como 4 bits. El mensaje es encifrado previo a la codificación convolucional. El CRC es computado en los 48 bits resultantes. Todos los campos excepto el Tipo de Mensaje ( 40 bits en total ) son encriptados por el CMEA.

### 3. Vectores de prueba.

Estos dos casos de prueba utilizan la siguiente entrada de datos fijada {expresado en forma decimal}

RANDSSD	=	4D	18EE	AA05	895C
Authentication	=				C7
Algorithm Version					
MIN1	=		79		2971
MIN2	=				28D

---

```
ESN                                     D75A 96EC
msg_buf[0]                             = B6, 2D, A2, 44, FE, 9B
...
msg_buf[5]
```

Los siguientes dígitos, A/key y de chequeo serán ingresados en forma decimal

```
14 1421 3562 3730 9504 8808 6500
```

La conversión del A/key, el chequeo de dígito entrante en forma hexadecimal producirá

```
A-key, check bits = C442 F56B E9E1 7158, 1 51E4
```

La entrada de arriba, cuando se combino con el RANDSSD, se generara

```
SSD_A = CC38 1294 9F4D CD0D
```

```
SSD_B = 3105 0234 580E 63B4
```

### **3.1 Vector [Terminación MS)**

```
If RAND = 34A2 B0SF:
```

```
AUTHR = 3 66F6
```

---

CMEA key  $k_0, \dots, k_7 = A0\ 7B\ 1C\ D1\ 02\ 75\ 69\ 14$

CMEA output =  $E5\ 6B\ 5F\ 01\ 65\ C6$

VPM =  $18\ 93\ 94\ 82\ 4A\ 1A\ 2F\ 99\ A5\ 39\ F9\ 5B\ 4D\ 22\ D5\ 7C$   
 $EE\ 32\ AC\ 21\ 6B\ 26\ 0D\ 36\ A7\ C9\ 63\ 88\ 57\ 8C\ B9\ 57$   
 $E2\ D6\ CA\ 1D\ 77\ B6\ 1F\ D5\ C7\ 1A\ 73\ A4\ 17\ B2\ 12\ 1E$   
 $95\ 34\ 70\ E3\ 9B\ CA\ 3F\ D0\ 50\ BE\ 4F\ D6\ 47\ 80\ CC\ B8$   
 $DF$

### 3.2 Vector 2 (MS Termination)

If RAND =  $5375\ DF99$ :

AUTHR =  $0\ 255A$

CMEA key  $k_0, \dots, k_7 = F0\ 06\ A8\ 5A\ 05\ CD\ B3\ 2A$

CMEA output =  $2B\ AD\ 16\ A9\ 8F\ 32$

VPM =  $20\ 38\ 01\ 6B\ 89\ 3C\ F8\ A0\ 28\ 48\ 98\ 75\ AB\ 18\ 65\ 5A$   
 $49\ 6E\ 0B\ BB\ D2\ CB\ A8\ 28\ 46\ E6\ D5\ B4\ 12\ B3\ 8C\ 9E$   
 $76\ 6C\ 9E\ D4\ 98\ C8\ A1\ 4A\ D2\ DC\ 94\ B0\ F6\ D4\ 3E\ E0$   
 $D1\ 6C\ 7E\ 9E\ AC\ 6B\ CA\ 43\ 02\ C9\ 23\ 63\ 6F\ 61\ 68\ E8$   
 $8F$

## BIBLIOGRAFÍA

1. ANDERSON, S., Dropping the bomb on fraud, Cellular Business, June 1997, pag. 76.
  2. COMPAQ, Managing Fraud in Wireless Communications Networks(Compaq's solution for Fraud Managment), March 1999 Pags. 5 a 32.
  3. BUCKLEY, W., Stop, thief! , Wall Street Journal, 11 Sep 97.
  4. Cellular One launches advanced technology to combat fraud for digital customers, Cox New Service, 29 Jan. 97.
  5. Corsair Communications, "Phoneprint's Benefits", <<http://corsair.com/phoneprint.html>, 05 Oct. 97.
  6. Corsair Communications, "What is RF Fingerprinting", <<http://corsair.com/fingerprint.html>, 01 Nov. 97.
  7. Corsair Communications, "Focus on Architecture" <<http://corsair.com/architecture.html>, 10 Oct. 97.
  8. Corsair Communications, "Roaming", <<http://corsair.com/roaming.html>, 12 Oct. 97.
  9. CTIA Authentication Implementation Guide, 1997.
  10. FCC rule 22.919 - "All cellular phones manufactured after, 01 Jan. 95 must be authentication capable".
  11. MEYERS, J. A.M. report risk assessment, study probes security of rival wireless technology platforms, wireless Network Editor, 1997, pag 11.
  12. MULLINS, R., Trying to hang up on cellular phone frud, Business Journal - Milwaukee, 01 Jun. 97. Pags.: 13-19.
-



13. NORTH AMERICAN CELLULAR NETWORK, "Authentication",  
<http://www.nacn.com>, 15 Oct. 97.
  14. SIEDSMA, A., Cellular phone companies unitfight fraud, San Diego Business Journal, 26 Nov. 96, Pags: 1- 48.
  15. TELECOMMUNICATION INDUSTRY ASSOCIATION, The IS-54 authentication protocol has been adopted for Is-95, Is-91, and Is-136 systems. April 1992.
  16. SYNACOM, CloneSafe Validator,  
<http://www.synacom.com/map.php3?id=products/home.php3>
  17. SYNACOM, CloneSafe SAMS,  
<http://www.synacom.com/map.php3?id=products/home.php3>.
  18. JEPSON, R., Cellular Authentication and Voice Privacy, Nortel Wireless Networks, 07 Jul. 95, pags: 5, 9, 10, 11, 12, 17, 18, 19, 20, 21.
  19. TR 45.3, Appendix A to IS-54 Rev. B,  
<http://www.replay.com/mirror/cave/>.
  20. RANDALL A. SNYDER AND MICHAEL D. GALLAGHER, Mobile Telecommunications Networking with IS-41, McGraw-Hill, March 1997.
  21. COMMUNICATIONS INFORMATION SERVICES, "Why is RF Fingerprinting the best anti fraud technology?", CIS, Florida, 1997-1998.
  22. KIMBERLY A. STEWART, Cellular Telephone Fraud, EE 4984 Telecommunications Networks, 052 Jan. 95, Pags: 1, 2, 3.
-

23. ISOTEL Corporation, TDMA Technology for Cellular and PCS wireless Communications,  
<http://www.isotel.com/is136.htm>, 2-Feb-99.
  24. "An Introduction to Telecommunications Fraud", Nortel Fraud Solutions, 1999, pag 1. <http://www.fraud-solutions.com/fraudprimer/>
  25. "Additional fraud types in mobile networks", Nortel Fraud Solutions, 1999 pags: 1-2.  
<http://www.fraud-solutions.com/fraudprimer/tmobile.html>
  26. "The Case for Action", Nortel Fraud Solutions, 1999, pags: 1-2.  
<http://www.fraud-solutions.com/fraudprimer/action.html>
  27. International Engineering Consortium, Personal Communication Services, 27 Jun 99, pags 1-12.
-