UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA

DEFINICIÓN DEL PERFIL ELECTRICO DE TARJETAS SIM PARA REDES GSM

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

FRANCISCO JAVIER SILVA ORELLANA

PROMOCIÓN
1997-I

LIMA, PERU
2008

DEFINICIÓN DEL PERFIL ELECTRICO DE TARJETAS SIM PARA REDES GSM

Agradecimiento

A mis hijos Nicolás y Joaquín.
A mi esposa Rocío
A mis padres Angélica y Francisco.
A mis hermanas Milagros, Mercedes y María.

SUMARIO

La tarjeta SIM o módulo de identificación del subscriptor, es un dispositivo crítico dentro de la arquitectura de las redes de telefonía móvil de tecnología GSM, no solo porque permite el acceso a los servicios ofrecidos por el operador debido a que almacena la identidad del usuario, los algoritmos de autenticación que garantizan dicha identidad y los algoritmos de cifrado que garantizan la confidencialidad de las comunicaciones, sino porque además sobre esta se pueden montar servicios de valor agregado que permiten al usuario disponer de una cantidad creciente de nuevos servicios y al operador de nuevas fuentes de ingreso.

Por tales motivos la puesta en operación de nuevos perfiles eléctricos de tarjetas SIM es una actividad crítica para cualquier operador de telefonía móvil de tecnología GSM.

El presente informe analiza los conceptos básicos relacionados con las tarjetas SIM como son su arquitectura, estructura de archivos y los archivos más importantes que componen el perfil eléctrico de una tarjeta SIM y su contenido, de acuerdo a la especificación ETSI GSM 11.11.

El objetivo general del presente informe es presentar una visión general de la tecnología de tarjetas SIM muy utilizado en el ámbito de las redes móviles de tecnología GSM y que se basa en las definiciones establecidas en la norma GSM 11.11 (Anexo B). Por otro lado, el objetivo específico del mismo es servir como base para la definición del perfil eléctrico básico de tarjetas SIM en redes GSM.

ÍNDICE

INTRODUCCIÓN

La importancia de las tarjetas SIM en el acceso a los servicios ofrecidos por los operadores GSM obliga a realizar una adecuada definición de los parámetros del perfil eléctrico de las mismas.

El presente informe hace un análisis de los principales parámetros del perfil eléctrico en base a la GSM11.11.

En el capítulo I se realizará una breve descripción de la metodología a utilizar así como del alcance del presente informe. En el capitulo II, dentro del marco teórico se describirá la arquitectura y componentes del Sistema Global de Comunicaciones Móviles (GSM). En tanto que en el capítulo III se analizará con mayor detalle la arquitectura de las tarjetas SIM, la estructura de archivos que la componen y finalmente se analizará el contenido de los principales archivos que componen el perfil eléctrico de una tarjeta SIM.

CAPITULO I

EL PROBLEMA

1.1 Título

Definición del Perfil Eléctrico de Tarjetas SIM para Redes GSM.

1.2 Formulación del Problema

Para que los usuarios puedan tener acceso a los servicios ofrecidos por los operadores de telefonía móvil que utilizan tecnología GSM es necesario contar además de un terminal adecuado un dispositivo que preste las siguientes funciones:

- Autenticación.
- Acceso a distintos servicos.
- Almacenamiento de información personal.
- Plataforma de servicios de valor agregado.

Tal dispositivo es la tarjeta SIM (Subscriber Identity Module – Módulo de Identificación del Usuario). La tarjeta SIM está basada en la tecnología de tarjetas inteligentes (smartcard) y su principal función al momento de ser introducida fue el de autenticación, es decir un dispositivo que asegure que sólo el usuario que contrata el servicio puede disfrutar de los servicios ofrecidos por el operador.

El presente informe de hace un análisis de los principales parámetros que componen el perfil eléctrico de una tarjeta SIM.

1.3 Hipótesis

El perfil eléctrico propuesto permitirá a los operadores móviles facilitar el acceso a los distintos servicios ofrecidos.

1.4 Objetivos

Los objetivos del informe son los siguientes:

- Analizar los parámetros más importantes del perfil eléctrico de tarjetas SIM en base a las normativas vigentes.

- Proveer un perfil eléctrico básico que permita ofrecer distintos servicios.

1.5 Alcances y Limitaciones

El presente informe pretende ofrecer un documento base que sirva para definir el perfil eléctrico básico que facilite el acceso a los servicios ofrecidos por operadores de telefonía móvil de tecnología GSM.

1.6 Metodología

La Metodología usada en este proyecto de investigación esta basada en las siguientes actividades:

- Revisión de documentación respecto a los sistemas celulares.
- Estudio de estándares y protocolos relacionados al tema.
- Ordenamiento y Sumarización de la información.
- Observaciones y Conclusiones.

CAPITULO II

MARCO TEORICO

2.1 El Sistema Global para las Comunicaciones Móviles (GSM)

El presente capitulo tiene como objetivo describir el marco teórico que permite comprender el funcionamiento de una red celular de telefonía móvil que implementa el Sistema Global para las Comunicaciones Móviles más conocido como GSM.

Las comunicaciones móviles celulares representan un punto importante en el proceso de evolución de las Telecomunicaciones, puesto que permiten emprender nuevas actividades principalmente debido a su movilidad, ya que donde exista cobertura y se tengan recursos disponibles en la red del operador, un abonado siempre será ubicado y podrá utilizar todos los servicios a los cuales se ha suscrito. A partir de un concepto básico, los sistemas inalámbricos han evolucionado hacia sistemas de uso masivos y complejos, compuestos por entidades muy diferentes utilizando a su vez distintos tipos de transmisión inalámbrica de datos.

Aunque existen muchos tipos de sistemas, actualmente sólo se utilizan tres técnicas de acceso al medio básicos, los cuales son:

El sistema de acceso múltiple por división de frecuencia (FDMA - Frequency Division Multiple Access) transmite un circuito de voz por frecuencia. La información se transporta en formato analógico.

El sistema de acceso múltiple por división de tiempo (TDMA - Time Division Multiple Access) es un formato digital que "codifica" la señal analógica. El canal asignado se divide en varios intervalos de tiempo. Cada intervalo de tiempo puede transportar un circuito de voz. Dependiendo del ancho de banda y del tipo de sistema, 3 o más circuitos de voz pueden reemplazar un circuito de voz analógico.

El sistema de acceso múltiple por división de código (CDMA - Code Division Multiple Access) es una tecnología digital de espectro extendido. CDMA asigna uno de 4,4 billones de códigos disponibles a cada circuito de voz digital. La unidad receptora decodifica sólo la señal que se le envió. Esto permite enviar varias conversaciones utilizando una misma portadora.

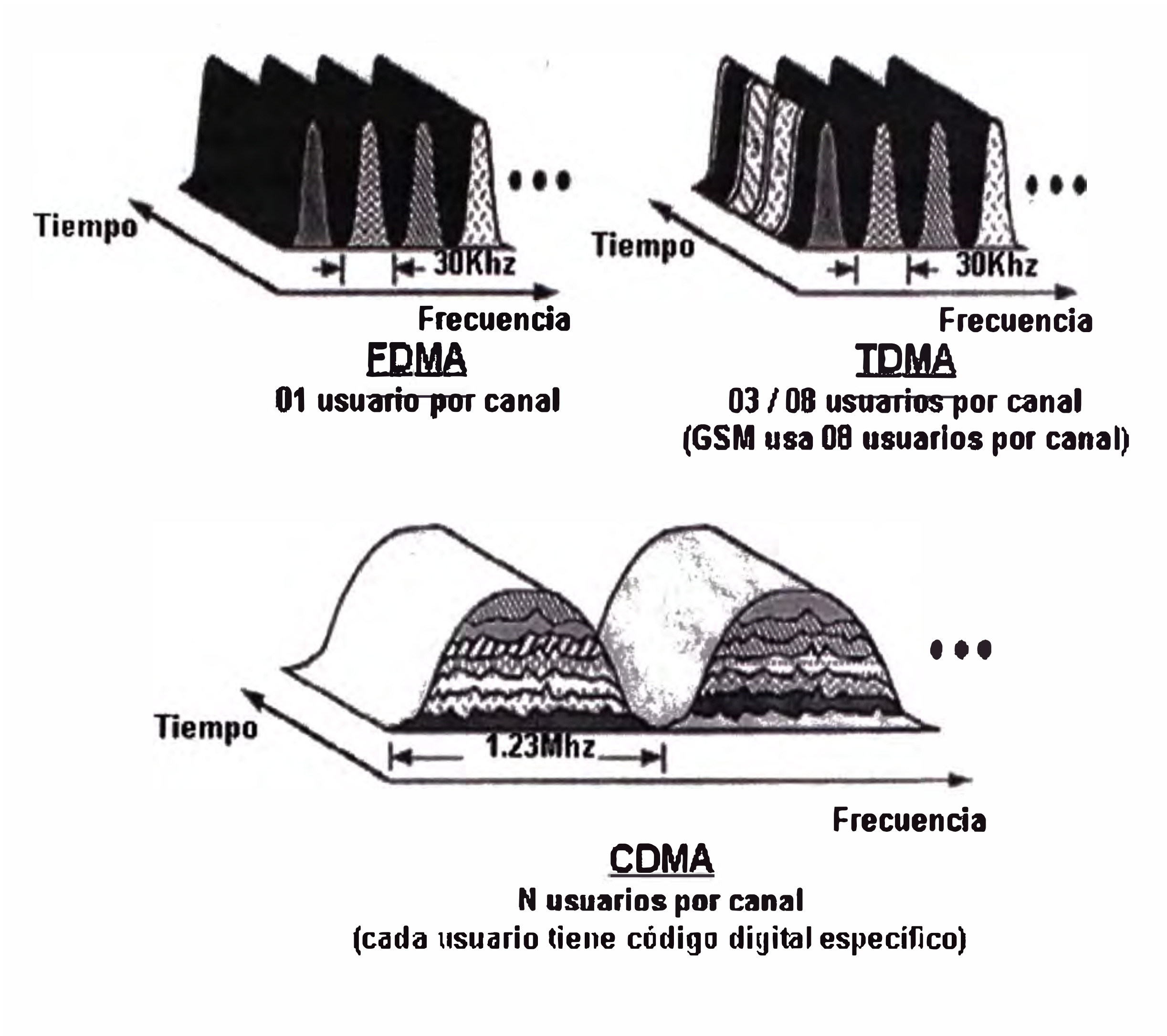


Figura 2.1 Sistemas de Modulación

El sistema digital que se desarrolló en Europa y que predomina actualmente en todo el mundo es el sistema global de comunicaciones móviles (GSM - Global System for Mobile Communications). El GSM fue uno de los primeros sistemas digitales seguido a la era analógica. Surgió principalmente para resolver los problemas de los sistemas analógicos, que eran la capacidad, disponibilidad de frecuencias, sistemas no seguros, etc., debido a ello, se creó en 1982 en la CEPT (Conference Européenne des Postes et Telecommunications) un grupo de trabajo denominado GSM (Groupe Spéciale Mobile), con el fin de preparar un estándar europeo de red móvil ó PLMN (Public Land Mobile Network) para todos los países pertenecientes a la CEPT. Una de las primeras decisiones adoptadas fue la de reservar una banda de frecuencia común que permitiera el roaming internacional. La banda elegida consta de dos sub-bandas de 25MHz de ancho de banda, cada una: 890-915 MHz y 935-960 MHz.

El nombre del grupo acabo designando la norma, la cual hoy día se conoce como red PLMN-GSM, ó abreviadamente GSM. En el año 1989 la responsabilidad de normalización recae en el ETSI (European Telecommunications Standards Institute), reestructurándose los grupos de trabajo, que adquieren otra denominación. Entonces se reinterpreta el significado del acrónimo GSM pasando a designar el término Sistema Global para las Comunicaciones Móviles (en inglés Global System for Mobile Communications). Este sistema utiliza el acceso múltiple por división de tiempo (TDMA) como tecnología de acceso al medio. Los canales GSM tienen 200 kHz de ancho de banda y soportan hasta ocho usuarios por canal. Este sistema fue diseñado para operar en Europa inicialmente en la banda de 900 MHz. Posteriormente y debido al crecimiento del número de abonados se designó la banda de 1800 MHz.

En la región americana (América del Norte, Centro y Sur) existen variantes GSM que operan en las bandas de 1900 MHz y 850 MHz (inicialmente los operadores GSM en Brasil operaban únicamente en la banda de 1800MHZ).

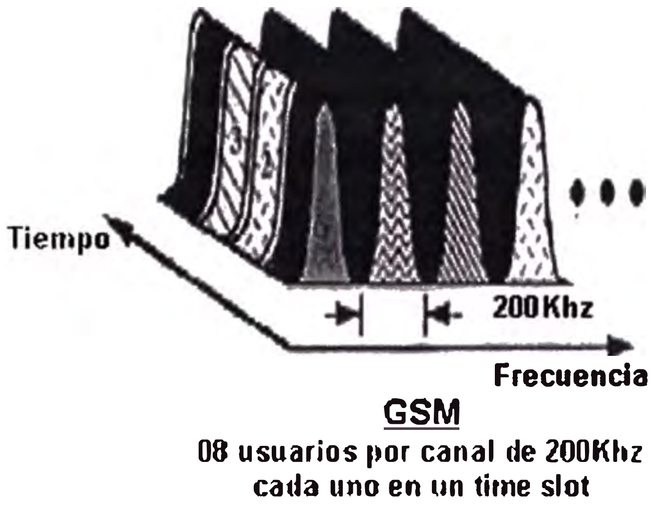


Figura 2.2 Sistemas GSM

Una forma de mejorar la capacidad del GSM y al mismo tiempo, aumentar los servicios es introducir la tecnología de conmutación de paquetes. Para tal fin se desarrolló el Servicio General de Paquetes de Radio (GPRS - General Packet Radio Service). El GPRS utiliza esencialmente, la misma interfase aire que el GSM convencional, pero incluye una nueva capa de control de acceso al medio (MAC - Médium Access Control) y una nueva capa de control de enlace de radio (RLC - Radio Link Control) permitiendo que la transmisión de la información se pueda realizar a distintas velocidades dependiendo del tipo de codificación. Asimismo para obtener mayores velocidades se desarrolló sobre la red GPRS técnicas de modulación 8PSK, es así como aparecen las Tasas de Datos mejoradas para la evolución del GSM (EDGE - Enhanced Data rates for GSM of Evolution) también conocido como GPRS mejorado (EGPRS - Enhanced GPRS).

2.2 Arquitectura de la Red GSM

A partir de este capitulo hacia delante, nos concentraremos específicamente a desarrollar la arquitectura de los núcleos de red GSM/MAP utilizado en las redes GSM/GPRS/EDGE.

2.2.1 Subsistemas

Puede definirse un subsistema como una entidad constituida por uno ó más equipos físicos encargados de ejecutar una tarea específica. La unión de todas estas tareas asegura el funcionamiento de la red. En la red GSM se distinguen los siguientes subsistemas:

- Subsistema de Estaciones Base, BSS (Base Station Subsystem)
- Subsistema de Conmutación y Gestión, SMSS (Switching and Maintenance Subsystem)
- Subsistema de Operación y Mantenimiento, OMSS (Operation and Maintenance Subsystem)

Cada subsistema está formado por una o varias entidades funcionales que se intercomunican a través de diferentes interfases mediante protocolos de señalización específicos. Las interfaces se designan por letras. Fuera de lo que es estrictamente la red, está el conjunto de unidades móviles MS que al no tener relación mutua no forman un subsistema, pero sí tienen una entidad común. La relación entre este conjunto y la red se realiza a través de la "interfase aire" (air interface) llamado también interfase radio, que se designa abreviadamente por la "interfase Um".

El BSS se relaciona con el SMSS a través de la denominada "interfase A". En la siguiente figura se muestra una estructura general del subsistema GSM (se representan los subsistemas en cajas rectangulares):

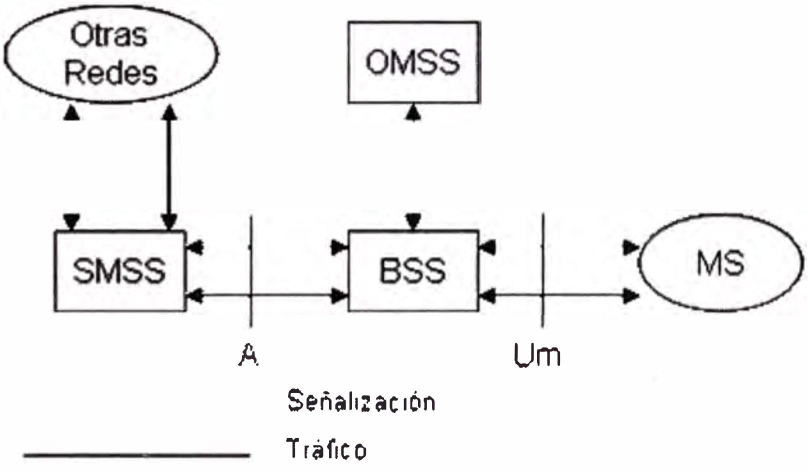


Figura 2.3 Subsistemas en GSM

a) Subsistema de Estación Base

El subsistema de estación base comprende las funciones de capa física, según el modelo OSI, para interconexión con las MS a través de la interfase Um. Para ello hace uso de un conjunto de canales lógicos. Los canales lógicos son estructuras de datos y protocolos que realizan funciones de intercambio de información para:

- Seguimiento/Localización de las MS y aviso a las mismas
- Establecimiento de las llamadas
- Mantenimiento de las comunicaciones establecidas
- Supervisión y control de la calidad
- Facilidades operativas

En el BSS se identifican dos unidades funcionales:

- Controlador de estación base, BSC (Base Station Controller)
- Estación base, BTS (Base Transceiver Station)

Donde la interfase entre el BSC y la BTS se denomina “A-bis”.

b) Subsistema de Conmutación y Gestión

El subsistema de conmutación y gestión tiene a su cargo todas las funciones requeridas para manejar los protocolos de señalización necesarios para el establecimiento, mantenimiento y liberación de las llamadas, con la componente específica de la movilidad.

Las funciones básicas del SMSS son:

- Localización y registro con autenticación de los abonados
- Enrutamiento de las llamadas
- Administración de los recursos de radio durante la llamada
- Administración de la movilidad
- Intercambio de señalización entre entidades funcionales de la red GSM con redes externas.

El subsistema de conmutación y gestión está constituido por las siguientes unidades funcionales:

- Centro de Conmutación Móvil, MSC (Mobile Switching Center)
- Registro de Ubicación Local, HLR (Home Location Register)
- Registro de Ubicación Visitante, VLR (Visitor Location Register)

c) Subsistema de Operación y Mantenimiento

El subsistema de operación y mantenimiento tiene a su cargo las funciones de gestión de red, características de las redes de telecomunicaciones y los aspectos relativos a la seguridad del acceso a la red y de las comunicaciones para los usuarios y los equipos.

La primera aplicación se realiza mediante el centro de operaciones y mantenimiento (Operations and Maintenance Center). Para la segunda hay dos unidades funcionales:

- Centro de Autenticación, AuC (Authentication Center)
- Registro de Identidad de Abonados, EIR (Equipment Identity Register)

2.2.2 Arquitectura Funcional de la Red GSM

La arquitectura funcional de una red GSM esta compuesto por diferentes entidades funcionales, pertenecientes a los subsistemas descritos anteriormente, con las interfaces e interconexiones lógicas que las separan. En la siguiente figura se representa la arquitectura denominada también modelo de referencia de GSM.

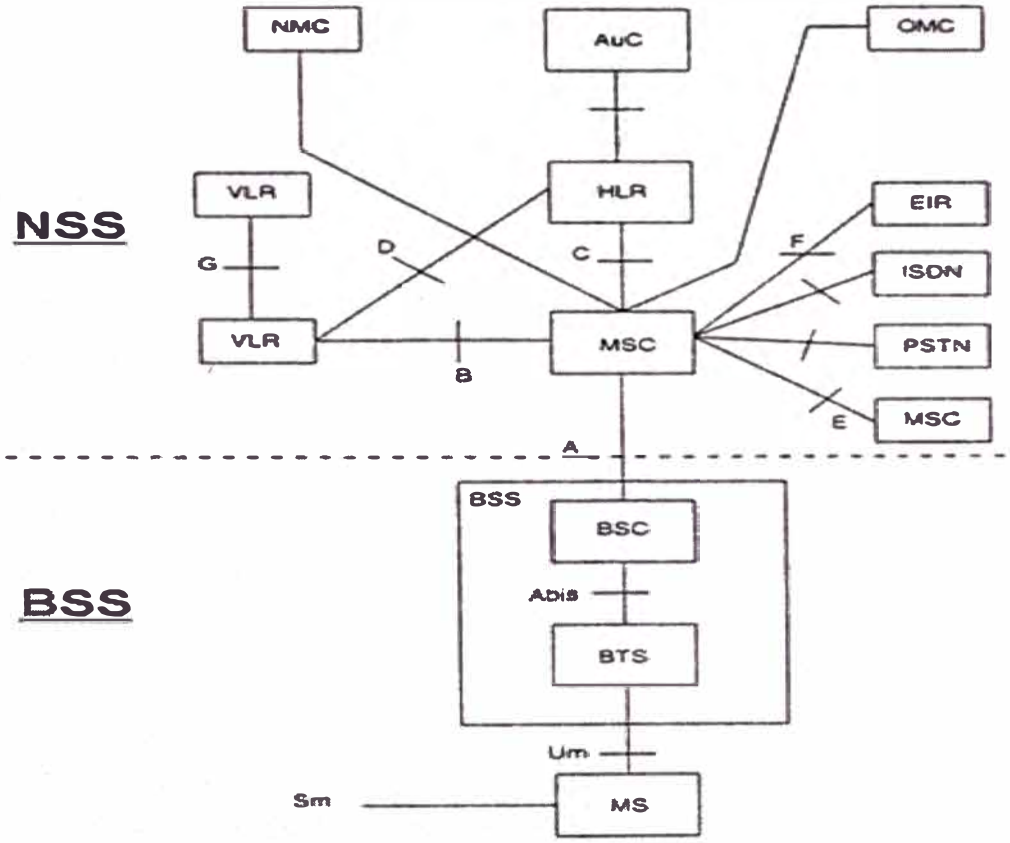


Figura 2.4 Arquitectura Funcional de una Red GSM

Una unidad funcional puede corresponder a un equipo físico concreto ó alternativamente, un mismo equipo físico puede comprender dos unidades funcionales, en cuyo caso la interfase entre ellas es interna al equipo.

A continuación se describen las diferentes unidades funcionales.

a) Estación Móvil

La estación móvil, MS (Mobile Station), es el equipo físico utilizado por el usuario GSM para acceder a los servicios proporcionados por la red a través de la interfase Um. Se ha especificado esta interfase de forma que las tecnologías de MS y de red GSM puedan evolucionar por separado, sin tener alguna restricción entre ellos.

Como equipo, la MS proporciona la plataforma física para el acceso, pero es "anónima" y no puede funcionar con la red hasta que sea "personalizada" mediante la inserción de una "tarjeta inteligente" (smart card) denominada módulo de identidad de abonado, SIM (Subscriber Identity Module) donde figura, entre numerosas informaciones, la identidad del abonado, IMSI (International Mobile Subscriber Identity) que equivale a la "línea virtual" que conecta al usuario con la red.

En GSM se considera por separado al usuario y a los terminales, lo que acrecienta la movilidad personal. Por ejemplo, un usuario que viaja fuera de su lugar de residencia no necesita llevarse el terminal. Puede alquilar uno en lugar de destino y personalizarlo con su tarjeta SIM. En cuanto se inserta la tarjeta en cualquier MS homologada, ésta queda preparada para efectuar / recibir llamadas y acceder a los servicios inscritos.

La MS desempeña las siguientes funciones básicas:

- Proporcionar una interfase de comunicaciones entre los usuarios y la red vía radio.
- Realizar la transmisión / recepción de las informaciones de usuario y de señalización a través de la interfase radio.
- Efectuar la inicialización de la conexión con la red.
- Realizar la sintonización de frecuencias y seguimiento automático de las estaciones base en cuya zona de cobertura se encuentre.
- Efectuar funciones de procesamiento de la voz: conversión analógico / digital y viceversa.
- Realizar la adaptación de interfases y velocidades para las señales de datos.

b) Subsistema de Estaciones Base

El BSS comprende el conjunto de equipos utilizados para proporcionar cobertura radioeléctrica en el área celular. Se divide en dos partes: las estaciones transceptoras de base BTS y los controladores de esas estaciones, BSC.

Las BTS están constituidas por los equipos transmisores – receptores de radio (transceptores), los elementos de conexión al sistema radiante (combinadores, multiacopladores, cables coaxiales), las antenas y las instalaciones accesorias (torres soporte, pararrayos, tomas de tierra, etc.).

Debido al elevado número de BTS de una red y a que éstas funcionan en lugares donde no hay mantenimiento "in situ", los equipos de BTS deben ser sencillos, fiables, duraderos y de costo moderado. Por ello, la mayoría de las funciones de control se realizan en el BSC. El BSC se encarga de la gestión de varias BTS en lo relativo a los recursos de radio: asignación, utilización y liberación de las frecuencias, traspasos, funcionamiento con saltos de frecuencia, etc. También puede realizar ciertas funciones de conmutación. Las interfaces del BSC con las BTS y con la red, son la A-bis y la A, respectivamente. El BSS desempeña las siguientes funciones:

- Transmisión / recepción radioeléctrica a través de la interfase Um.
- Localización de las MS para su registro inicial ó actualización.
- Establecimiento, supervisión y conclusión de las llamadas.
- Traspaso entre BTS controladas por el mismo BSS.
- Procesado de voz y adaptación de velocidad.
- Control de equipos y funciones de re-configuración.
- Control de mantenimiento rutinario.

En la siguiente figura se representa esquemáticamente un BSS formado por un BSC y dos BTS, cada una de las cuales tiene varios transceptores radio TRX con ciertas funciones de control. Se han indicado también las interfaces A-bis y A.

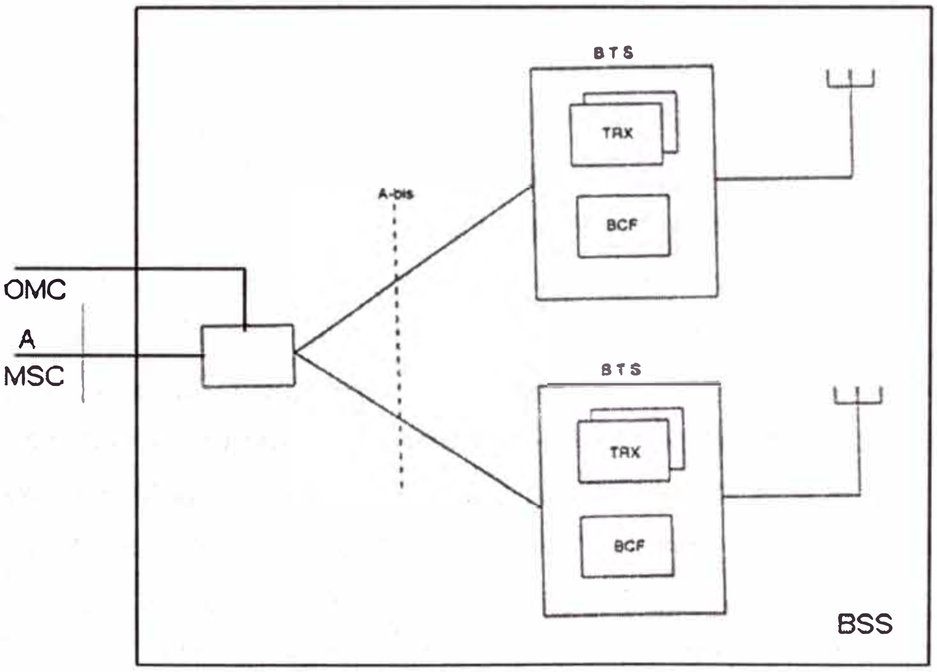


Figura 2.5 Sistema de Estaciones Base

c) Componentes del Subsistema de Conmutación

En la siguiente figura podemos ver los componentes principales del subsistema de conmutación. Esta muestra los flujos de información entre los diferentes elementos: con línea continua la transmisión de voz ó datos y con línea discontinua la señalización. En está gráfica no se ha representado ninguna conexión con redes externas.

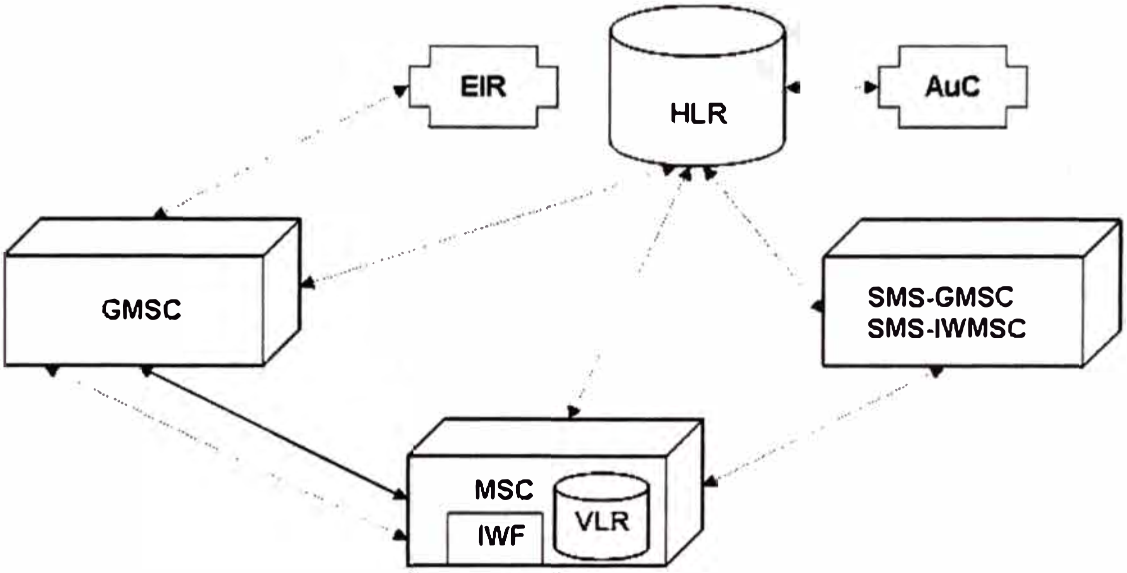


Figura 2.6 Subsistema de Conmutación

- **MSC/VLR**

  Ambos son imprescindibles para la existencia de la red GSM. Aunque funcionalmente son diferentes, se les suele tratar conjuntamente ya que están íntimamente relacionados. El MSC (Mobile Switching Center) es el nodo que contiene las funciones de conmutación y señalización básicas, es decir, su principal misión consiste en la gestión completa (establecimiento, encaminamiento, control y finalización) de las llamadas desde y hacia usuarios GSM.

  El VLR (Visitor Location Register) es una base de datos en la que se guarda información temporal de cada cliente que se encuentra en el área de influencia de los MSC a los que está asociado (las especificaciones GSM permiten que un VLR esté asociado a un único MSC ó a varios). El VLR intercambia información frecuentemente con el HLR. Para el VLR, todos los clientes bajo su área de influencia son visitantes. El tipo de información que guarda de cada uno de ellos es variada: desde datos de identificación del usuario como el IMSI o el TMSI, datos que permiten el encaminamiento de llamadas como el MSRN, servicios aprovisionados, datos relativos a la seguridad como la autenticación, etc.

  Suponiendo que el VLR y el MSC estuvieran físicamente localizados en nodos diferentes, el intercambio de señalización entre ambos para cada llamada sería muy elevado, debido a ello, normalmente se fabrica en un solo nodo MSC / VLR las dos entidades funcionales, los cuales interaccionan usando protocolos propietarios, que normalmente son una variante del protocolo MAP. Otra funcionalidad del MSC, es la realización de traspasos entre dos BSC que estén conectado a él ó a otro MSC. Para ello, el MSC tiene una parte exclusivamente dedicada a este propósito, que se denomina aplicación de control de traspasos, HOCA (HandOver Control Application). El MSC también proporciona el control de la autenticación y de la actualización de posición de los móviles, la prestación de servicios suplementarios y la tarifación de las llamadas.

El MSC constituye la interfase entre el sistema radio y la red fija. Por tanto, una de las fronteras del MSC es siempre el subsistema BSS, en forma de uno ó varios BSC, dependiendo el número de los mismos, de la tecnología y estrategia elegidas por el operador. El resto de las fronteras pueden ser otros nodos internos ó externos a la red GSM. La cobertura de un MSC puede ser muy diversa y se denomina área del MSC. Un área de MSC puede estar formada por una o varias áreas de localización LA (Location Area).

- **HLR**

El HLR es una base de datos inteligente en la que se guarda información estática relativa al servicio de todos los clientes de la red GSM y también información dinámica relativa a los mismos, como el VLR en el que se encuentran. Para dar de alta a un nuevo usuario en la red, es necesario introducir un registro con sus datos en el HLR.

Conceptualmente, existe un único HLR por red GSM. Sin embargo, en la práctica, puede estar distribuido dependiendo de la cantidad de clientes de la red, de la capacidad de los nodos ó bien por razones de seguridad. Otra opción es disponer de HLR redundantes (Mated Pair) como medida de precaución. Entre los datos que guarda el HLR, se encuentran el MSC y VLR que están sirviendo al abonado, los servicios contratados por el usuario y datos adicionales como el número C en el caso de desvío de llamada y la autenticación.

Los nodos con los que el HLR se comunica directamente a través de los enlaces de señalización son los VLR (por ejemplo, para actualizar la posición del móvil), el AuC para hacer la autenticación, y el GMSC, por el cual se intercambian números de encaminamiento MSRN, necesarios para dirigir la llamada al MSC apropiado.

En la siguiente figura se muestran todas las interfaces del HLR y el tipo de información que intercambia con cada una de ellas.

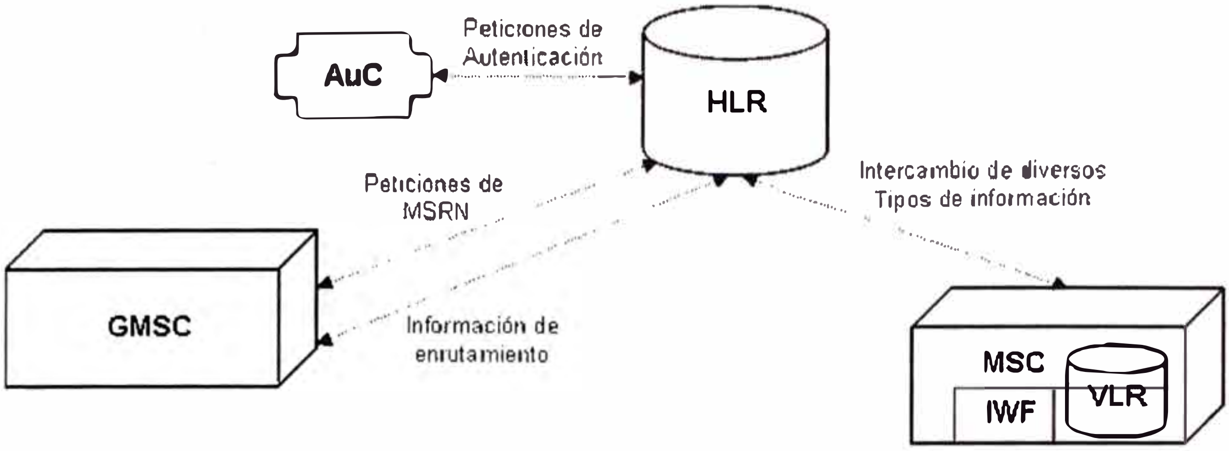

AuC
Peticiones de Autenticación
HLR
Peticiones de MSRN
Intercambio de diversos Tipos de información
GMSC
Información de enrutamiento
MSC
IWF
VLR

Figura 2.7 Flujo de Información al HLR

- **GMSC**

El GMSC (Gateway Mobile Switching Center) es un nodo que permite interrogar al HLR para obtener información de encaminamiento para una llamada dirigida a un móvil. Por tanto, entre sus funciones está la de ser el nexo de unión de la red GSM con otras redes externas.

Quizás el nombre no es muy adecuado, ya que hace pensar en que debe tener VLR ó subsistema BSS asociado, cuando no es necesario, pues estas funciones pueden ser realizadas por un nodo dedicado exclusivamente a la conmutación. En consecuencia, es imprescindible que pueda interrogar al HLR.

Cuando a la red GSM llega una llamada (desde el exterior ó generada en la propia red) hacia un móvil cuya localización no se conoce, dicha llamada se encamina hacia un GMSC, que será el encargado de interrogar al HLR para obtener de él la información de encaminamiento necesaria y luego enviar la llamada hacia el MSC correcto.

El número de GMSC que puede haber en una red GSM puede ser variable, lo más común, es que todos los MSC sean GMSC. De esta manera podrán interrogar al HLR para saber cómo encaminar una llamada que les llega desde un móvil que se encuentra en su área de influencia, sin necesidad de dirigirla a otro nodo para que obtenga esta información. Por esta razón, muchas veces existe ambigüedad entre los términos MSC y GMSC.

En la siguiente figura se esquematiza el proceso de obtención de información de enrutamiento:

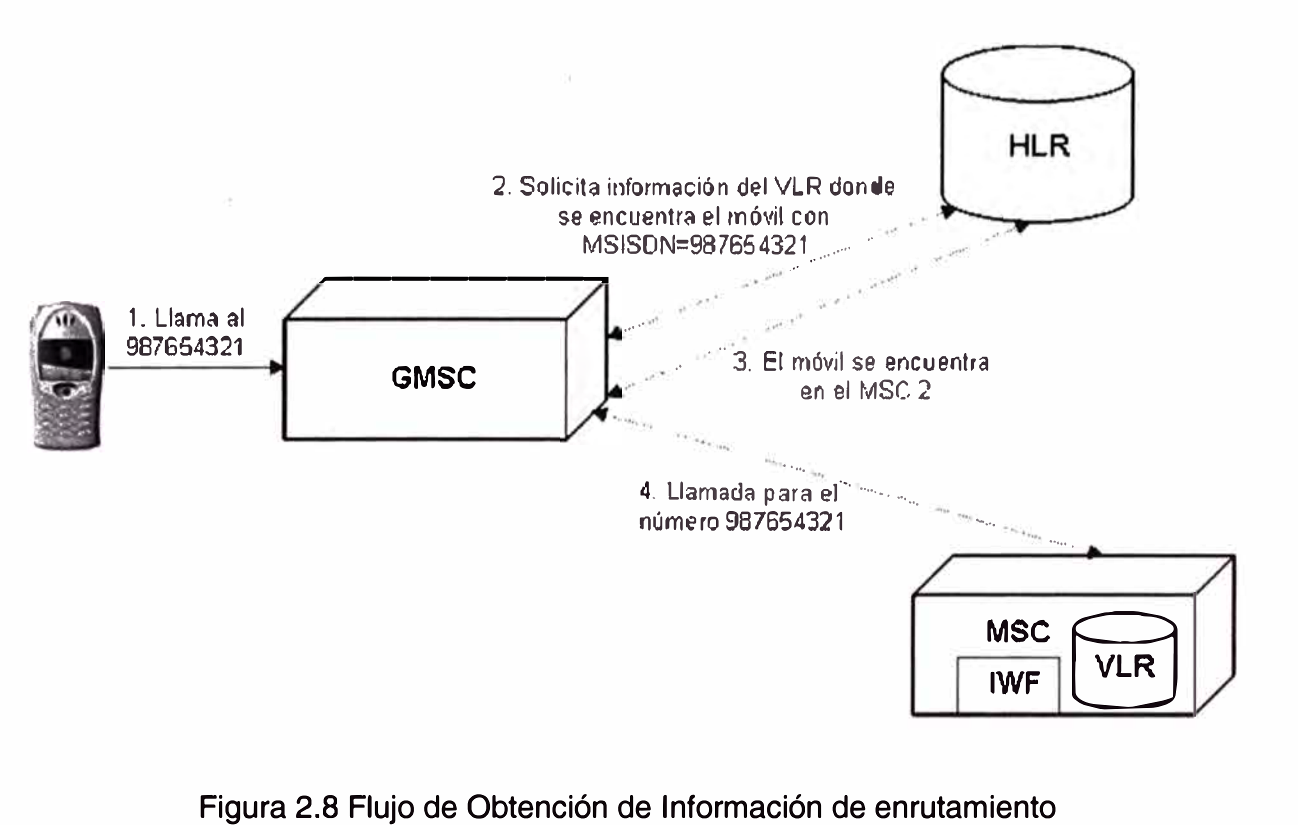

HLR
2. Solicita información del VLR donde se encuentra el móvil con MSISDN=987654321
1. Llama al 987654321
GMSC
3. El móvil se encuentra en el MSC 2
4. Llamada para el número 987654321
MSC
IWF
VLR

Figura 2.8 Flujo de Obtención de Información de enrutamiento

- **AuC**

El centro de autenticación de la red GSM, AuC (Authentication Center), es una base de datos que se podría considerar conceptualmente como parte del HLR. Sin embargo, en la práctica, puede encontrarse tanto como un nodo aislado como integrado con el HLR. Las especificaciones GSM tratan de separar el concepto de AuC del de HLR, lo que va encaminado a dar más importancia a la seguridad, tema clave en redes móviles, en las que la interfase radio constituye un gran riesgo.

Cuando se da de alta a un nuevo cliente en la red, se le proporciona junto a su IMSI una clave de autenticación Ki. La pareja IMSI-Ki, quedará almacenada en la SIM por un lado y en el AuC por otro. El AuC producirá un número aleatorio RAND que junto con el Ki, se harán pasar por dos algoritmos diferentes, A3 y A8, para obtener la respuesta firmada SRES (Signed Response) y la clave de cifrado Kc. Así, el AuC obtiene las llamadas tripletas de autenticación (RAND, SRES, Kc) que enviará al HLR en el caso que este requiera.

Es importante señalar que la clave Ki nunca se transmite a través de la red. La siguiente figura muestra el contenido del AuC y el proceso de petición de las tripletas por parte del HLR.

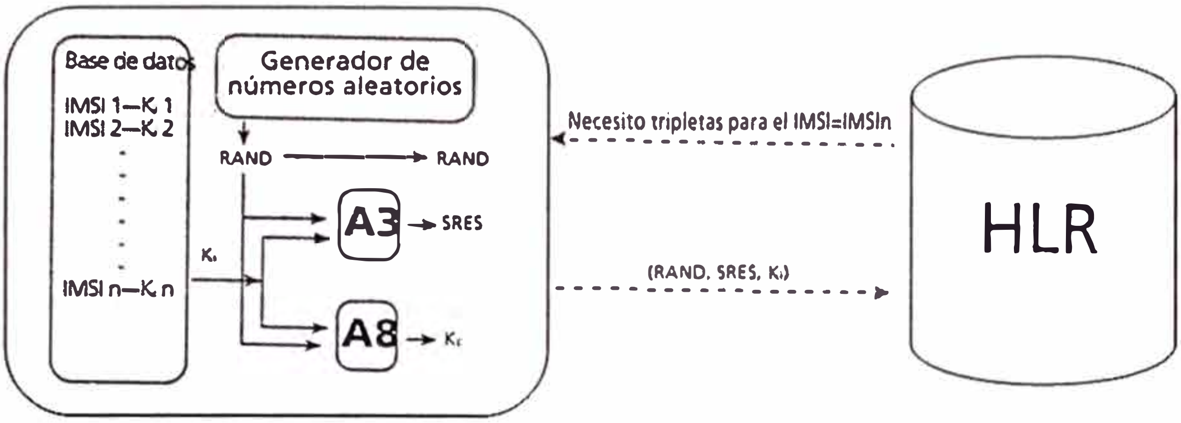


Figura 2.9 Flujo de Autenticación

- **EIR**

El EIR (Equipment Identity Register) es el registro de identificación de equipos terminales. Su función consiste en evitar que se utilicen equipos móviles que no están autorizados en la red, por ejemplo, porque han sido robados ó porque pueden producir perturbaciones a la misma.

Para la comprobación se utiliza el IMEI ó identificación internacional del equipo móvil. El EIR es básicamente una base de datos que clasifica los IMEI en tres listas:

- Blanca: no tiene ninguna restricción.
- Negra: se les impide el acceso a la red.
- Gris: degradan la calidad de la red, pero no lo bastante como para impedir que sean utilizados.

El EIR va conectado directamente sólo a los MSC y GMSC. Su implementación física consiste en una base de datos con un software de comunicaciones para establecer el diálogo con el MSC y/o GMSC. Puede encontrarse como nodo aislado, pero también integrado con otros nodos GSM, como el HLR y el AuC.

- **IWF**

El IWF (InterWorking Function) es una entidad funcional asociada al MSC. Proporciona los medios necesarios para interactuar la red GSM con las redes externas fijas (PSTN, ISDN y redes de paquetes PDN).

Sus funciones dependerán de los servicios y del tipo de red fija a la que se conecte. Puede que en algunas ocasiones, no aporte ninguna funcionalidad en el caso que ambas redes son compatibles.

- **VMS**

  Es el nodo que da soporte al servicio de buzón de voz, VMS (Voice Mail System). El VMS lleva asociado en algunos casos un centro de mensajes cortos, el cuál es utilizado para avisar a los usuarios cuando tienen mensajes en sus casillas de voz. En general, el SMSC encargado de esta actividad es el mismo que el que proporciona los servicios MOSMS y MTSMS.

- **SMSC - Centro de Mensajes Cortos**

  El SMSC es un nodo interno ó externo a la red GSM, que debe ser capaz de enviar, almacenar y recibir mensajes cortos (SM – short message) hacia y desde los móviles. También debe ser capaz de intercambiar mensajes de confirmación de la recepción ó envío de los SM con la red GSM. No necesariamente, cuando el SMSC reciba un mensaje para un determinado móvil, éste será enviado inmediatamente, pues es posible que el móvil se encuentre apagado. En ese caso, deberá esperar a que esté encendido para enviárselo.

  Si esto sucede, la red notificará al SMSC para que tenga constancia e intente volver a enviárselo más tarde. Para ello, el SMSC suele disponer de una tabla de reintentos, en la que se especifican los intervalos de tiempo entre los que el SMSC debe intentar de nuevo el envío. Un SMSC puede estar conectado a uno ó varios MSC.

- **SMS-GMSC**

  Es el nodo que realiza las funciones de gateway para el servicio de entrega de mensajes de texto SMS (MT-SMS), es decir, sólo interviene cuando hay un SM dirigido a un móvil. Físicamente, puede ser un MSC cualquiera.

  Cuando el SMS-GMSC recibe un SM desde el SMSC, comprueba que todos los parámetros son correctos e interroga al HLR para que le envíe la información de encaminamiento que necesita para entregar el SM. Con esta información, el SMS-GMSC envía el SM al MSC correspondiente, quien finalmente intentará entregar el mensaje al móvil.

  El SMS-GMSC informará al HLR del resultado de la entrega, tanto si ha sido satisfactoria ó no. En este último caso, deberá indicar la causa por la que no se ha podido entregar el mensaje al HLR, así éste informará al SMSC para que utilice la tabla de reintentos.

- **SMS-IWMSC**

  Es el nodo que realiza las tareas de enrutamiento en el escenario de MOSMS, es decir, sólo interviene cuando hay un SM originado por un móvil.

  Cuando un móvil genera un SM, el MSC recibe dicho SM desde el móvil y pide a su VLR asociado información para poder continuar la operación de entrega del SM. Cuando recibe la confirmación por parte del VLR de que todo es correcto, entonces entrega el SM al SMS-IWMSC.

  El SMS-IWMSC recibe el SM y establece una comunicación con el SMSC correspondiente para entregárselo. Una vez que el SMSC recibe el SM, responderá al SMS-IWMSC indicándole el estado final del mensaje, es decir, si es satisfactorio ó si se ha producido algún error. El SMS-IWMSC deberá remitir esta información al MSC donde está el móvil que ha originado el SM.

  En el caso de que pase el intervalo de tiempo estipulado por el operador, sin que el SMS-IWMSC reciba respuesta del SMSC, éste informará al MSC de que ha habido algún error, ya que no ha recibido confirmación del SMSC.

  El SMS-IWMSC tiene otra función, que consiste en avisar al SMSC de que un móvil para el que tiene guardado un SM, ya está disponible para recibir el mensaje. Cuando el móvil entra en actividad, el HLR es notificado y avisa al SMS-IWMSC para que le comunique al SMSC que ya puede enviar el SM al móvil. El HLR avisa al SMS-IWMSC sólo cuando sabe que dicho móvil tiene mensajes cortos por entregar. Esto lo sabe a través de unos indicadores de espera de mensajes, MWI (Message Waiting Indication), entre los que están las direcciones de los SMSC que tienen mensajes hacia ese móvil.

2.2.3 Interfases de la Red GSM

Para el sistema de comunicaciones GSM definen las siguientes interfases:

- Um
- Abis
- A
- B
- C
- D
- E

- F
- G
- H

La siguiente figura representa todas las interfaces de una red GSM:

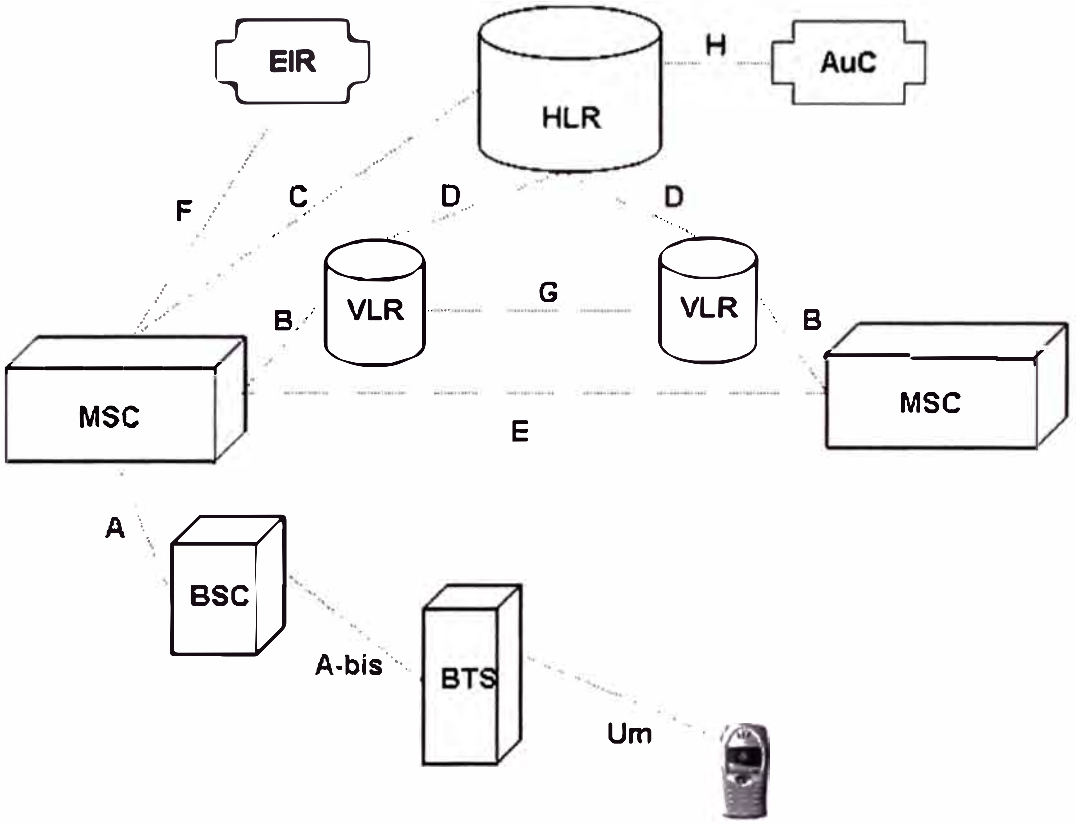


Figura 2.10 Interfases de la Red GSM

a) Interfase A (MSC-BSC)

Esta interfase se utiliza para intercambiar información sobre la gestión del subsistema BSS de las llamadas y de la movilidad de los móviles. Por ejemplo, a través de esta interfase se negocian los circuitos a utilizar entre el BSS y el MSC.

b) Interfase A-bis (BSC-BTS)

Es la interfase entre la estación base y el BSC. Permite el control del equipo de radio. No existe norma específica para esta interfase. Cada fabricante establece su propia normativa (no estandarizado).

c) Interfase B (VLR y MSC asociados)

El VLR es la base de datos que contiene toda la información que permite dar el servicio a los clientes que se encuentran en el área de influencia de sus MSC asociados. Por tanto, cuando un MSC necesite cualquier información sobre un móvil acudirá a su VLR y de la misma manera, le informará debidamente cuando tenga que hacerlo, por ejemplo, al recibir por parte de un móvil una petición de actualización de posición.

En algunos casos, cuando el móvil requiera un servicio especial ó cambiar los datos suscritos con el operador, el MSC informará al HLR (siempre vía el VLR). Debido a que en esta interfase se intercambian muchos mensajes de señalización, se recomendó que esta interfase no sea externa. Ésta es la razón por la que prácticamente todos los fabricantes tienen nodos MSC / VLR integrados.

d) Interfase C (HLR-GMSC)

Es la interfase utilizada por los GMSC cuando necesitan interrogar al HLR para obtener el número de roaming - MSRN del móvil llamado y poder así enrutar la llamada hacia el MSC destino. No debe confundirse con la interfase D, ya que el GMSC no tiene porqué tener VLR, puede ser perfectamente un nodo que sólo haga un enrutamiento de las llamadas.

e) Interfase D (HLR-VLR)

Es la interfase existente entre el HLR y el VLR. Principalmente sirve para intercambiar información entre ambas bases de datos, relativas a la posición del móvil y a la gestión del servicio contratado por el cliente.

Por ejemplo, cuando un móvil entra en el área de influencia de un VLR, éste envía una notificación al HLR. El HLR también se encarga de avisar al VLR anterior de que cancele el registro de posición del móvil, pues éste ya se encuentra en otro VLR.

También se utiliza esta interfase para intercambiar información cuando el móvil requiere un servicio especial, cuando el cliente desea cambiar datos suscritos, cuando deben cambiarse datos de la misma por motivos administrativos, para el intercambio de tripletas de autenticación, etc.

f) Interfase E (MSC-MSC)

Esta interfase la utilizan los MSC para intercambiar la información necesaria para iniciar y realizar una transferencia a otro MSC, con objeto de que la comunicación continúe cuando el móvil cambia de área de influencia de un MSC a otro.

g) Interfase F (MSC-EIR)

Se utiliza cuando el MSC quiere comprobar el IMEI de un equipo.

h) Interfase G (VLR-VLR)

Se utiliza en el caso de que un móvil inicie la petición de actualización en un nuevo VLR.

i) Interfase H (HLR-AuC)

Es la interfase utilizada por el HLR para solicitar tripletas al AuC, cuando no dispone de ellas. El protocolo utilizado para la transferencia de estos datos, no es estándar. Muchas veces se encuentran nodos HLR / AuC integrados.

j) Interfase Um (BSS-Móvil)

Es la interfase radio, que se encuentra entre el móvil y el BSS.

2.2.4 Numeración en la Red GSM

A continuación se describen los diferentes números y direcciones que son utilizados en una red GSM.

a) Identificación de usuarios móviles: IMSI, TMSI, LMSI

El IMSI (International Mobile Subscriber Identity) es la identidad internacional del usuario móvil y por tanto es único para cada abonado en todo el mundo. Para asegurar la privacidad del IMSI y evitar que esté viajando continuamente en la interfase radio, el VLR asigna un número temporal TMSI (Temporary Mobile Subscriber Identity) a cada uno de sus visitantes.

De forma opcional y para acelerar la búsqueda de los datos de un cliente en el VLR se define el LMSI (Local Mobile Station Identity). El LMSI es asignado por el VLR en el procedimiento de actualización de posición y es enviado al HLR junto con el IMSI. Aunque el HLR no lo utiliza, en caso de que disponga de él, lo envía siempre junto al IMSI en todos los mensajes referentes a dicho móvil hacia el VLR para facilitarle la búsqueda dentro de su base de datos.

- **IMSI**

  La estructura del IMSI es la que se muestra en la siguiente figura:

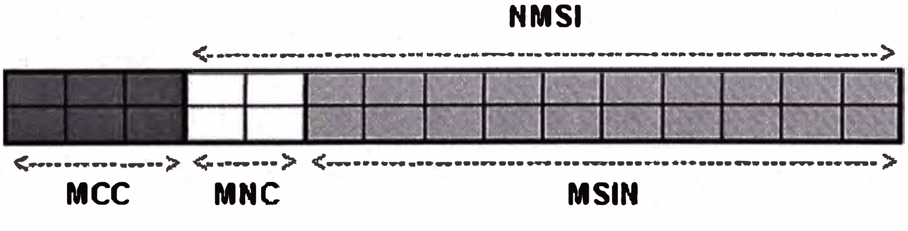


Figura 2.11 Estructura del IMSI

Todos los caracteres deben ser numéricos y en ningún caso se excede los 15 dígitos de longitud.

Tal como se observa en la figura 2.11, el IMSI está formado por tres partes:

- MCC (Mobile Country Code), que consta de tres dígitos e identifica unívocamente el país donde está domiciliado el cliente móvil. Para Perú el MCC es el 716.
- MNC (Mobile Network Code), que tiene dos dígitos e identifica dentro de un país, la red GSM a la que pertenece el usuario. La asignación de los MNC dentro de un país la realiza la administración de ese país. Si en un mismo país hay más de una red GSM, a cada una se le asignará un MNC único. Para Perú se tienen los siguientes casos:

Claro	MNC=10
Movistar	MNC=06

- MSIN (Mobile Subscriber Identification Number), identifica al abonado en dentro de su red GSM. Así como el MCC y el MNC están completamente prefijados por administraciones y organismos, el MSIN no lo está y lo asigna cada operador. Es una práctica recomendable en aquellas redes en las que exista más de un HLR físico, que los primeros dos dígitos del MSIN hagan referencia al HLR en el que está dado de alta el IMSI para facilitar la administración de los mismos.

Adicionalmente se define el NMSI (National Mobile Subscriber Identity) como el conjunto del MNC y el MSIN. Con la estructura definida, bastará que un nodo determinado analice el conjunto MCC+MNC para saber a qué red GSM pertenece el móvil.

- **TMSI**

Es un número de identificación temporal que sólo tiene significado dentro del VLR en el que se encuentra registrado el suscriptor y en su zona de influencia. Con respecto a la estructura de este número de identificación no hay regulación establecida, sino que deberán ser el operador y el suministrador de los equipos de red los que lleguen a un acuerdo sobre el mismo.

La longitud del TMSI es de 4 octetos (1 octeto = 8 bits), que se pueden expresar en forma hexadecimal. Para asegurarnos de que al producirse un reinicio en un VLR, no se duplican sus TMSI, una parte de los mismos debe incluir información que señale de alguna forma que se ha producido un reinicio. La red deberá evitar mandar TMSI que sean 31 bits a "1", puesto que esto significaría que no hay TMSI disponible en ese momento.

- **LMSI**

  Puesto que es número interno del VLR, lo único que hay regulado sobre él es que debe tener una longitud de 4 octetos. Este es un número que asigna el VLR al móvil en el proceso de actualización de posición, con objeto de acelerar el proceso de búsqueda en dicho VLR.

b) **Plan de Numeración Móvil**

Cada operador realizará el plan de numeración para las redes móviles de su país. En principio, cualquier usuario de PSTN ó de ISDN deberá poder comunicarse con un móvil, por lo que los números de teléfono de los móviles deberán cumplir el plan de numeración de ISDN de cada país. Es importante que pueda cambiarse el IMSI sin necesidad de cambiar el número ISDN y viceversa. A cada usuario móvil se le podrá asignar uno o varios números ISDN.

- **MSISDN**

  Es el número ISDN internacional de la estación móvil, MSISDN (Mobile Station International ISDN Number), identifica de forma única al abonado móvil dentro del plan de numeración de la red telefónica pública. Su estructura es la que se muestra en la siguiente figura:

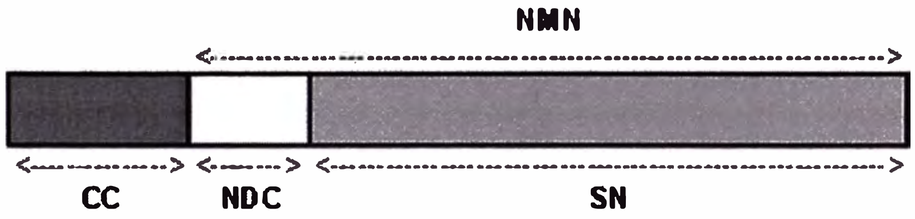


Figura 2.12 Estructura del MSISDN

Tiene tres partes principales:

- CC (Country Code), es el código del país al cual pertenece el móvil. Para el caso del Perú, el CC es 51.
- NDC (National Destination Code), es el código administrado por cada organismo nacional que identifica las áreas geográficas a las cuales pertenecen los suscriptores. En el caso del Perú, el Ministerio de Transportes y Comunicaciones (MTC) define el Plan Técnico Fundamental de Numeración, en el cual se establecen los NDC para cada uno de los departamentos del Perú.
- SN (Subscriber Number), son los dígitos que identifican al usuario.

Adicionalmente se define, el NMN (National Mobile Number), como NDC+SN. La longitud global del MSISDN dependerá de cómo esté definido el plan de numeración de cada operador. El MSISDN debe ser un número tal que pueda ser utilizado como una dirección global de enrutamiento para dirigir mensajes al HLR de la estación móvil. Está información la proporcionan el CC y el NDC. Si se necesitase información adicional, por ejemplo, para saber a qué HLR pertenece dentro de una red GSM que lo tuviera distribuido, ésta deberá estar incluida en los primeros dígitos del SN.

- **MSRN**

  Es el número de "roaming", el MSRN (Mobile Station Roaming Number) sirve para que el GMSC pueda encaminar una llamada terminada en móvil al MSC correcto. El proceso es el siguiente: cuando una llamada llega al GMSC, éste interroga al HLR para saber donde está el móvil llamado y le pasa como parámetro el MSISDN de dicho móvil. El HLR busca en su base de datos el VLR en que se encuentra el móvil en cuestión y le pide que le envíe un MSRN para dicho móvil. Una vez que el VLR le ha enviado el MSRN al HLR, éste se lo remite al GMSC.

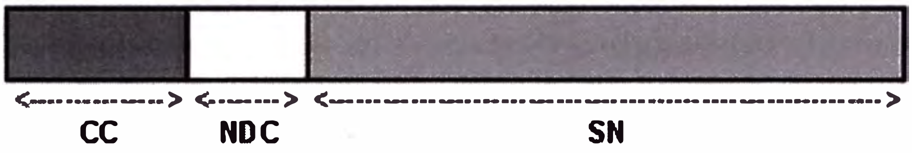


Figura 2.13 Estructura del MSRN

El MSRN tiene la misma estructura que el MSISDN, sólo que ahora el SN en vez de hacer referencia a un usuario, la hace a un MSC, es decir:

- El CC debe ser el del país en que se encuentre el VLR que proporciona el MSRN.
- El NDC de la red GSM a la que pertenece el VLR.
- Un SN con la estructura acorde a esa área de numeración.

Debe evitarse utilizar el MSRN como número de marcación, reservando cuidadosamente para ellos un rango de numeración. Debe hacerse notar que en determinados casos un MSISDN y un MSRN podrían ser idénticos. Para evitar errores, por ejemplo, que el GMSC encaminase basándose en un MSISDN erróneo que ha marcado un cliente y que es igual a un MSRN, deben utilizarse indicadores de encaminamiento en los nodos de conmutación.

2.2.5 Base de Datos Móviles

En una red GSM, es imprescindible la existencia de bases de datos que guarden los parámetros de cada móvil que hacen posible la gestión de la movilidad, de las llamadas, de la tarifación y de la seguridad, entre otras funciones.

Deben distinguirse dos tipos de bases de datos: por un lado tenemos la SIM, que reside en la parte del móvil y por otro, el resto de las bases de datos del sistema que se encuentran en la red. Dentro de estas últimas, las principales son el VLR y el HLR, que deben mantener la consistencia de los datos entre sí. Pero además existen otras, como el AuC y el EIR, que también guardan algunos parámetros del cliente y están enfocadas a funciones más específicas, como son las relacionadas con la seguridad de los usuarios y de la red.

a) SIM – Subscriber Identity Module

La SIM (Modulo de Identidad de Usuario) es más que una base de datos, puede ser considerada como una computadora que se encuentra integrada en una tarjeta. La información se estructura en archivos y es posible establecer una comunicación con la SIM mediante comandos estandarizados.

Las SIM además de almacenar datos del usuario (agenda, mensajes de texto SMS, etc.), almacena los algoritmos de autenticación y de obtención de Kc que permite el cifrado de los datos en la interfase aire.

La SIM adicionalmente sirve para almacenar pequeños programas ("applets") los cuales se comunican con los terminales móviles mediante comandos estandarizados (aplicaciones SIM Toolkit), lo cual abre un nuevo rango de posibilidades al ofrecer nuevos servicios desde la propia SIM. Adicionalmente es posible en la actualidad ofrecer servicios interactivos mediante la aplicación de navegadores integrados en la tarjeta SIM ("SIM Browsing").

b) VLR – HLR

Dentro de los datos que se guardan aquí, podemos distinguir aquellos que son permanentes como el número de teléfono (MSISDN) y que sólo los puede cambiar el operador de la red y otros que van variando como puede ser el parámetro del HLR que indica el VLR en que se encuentra un móvil.

El HLR contiene todos los datos permanentes de todos los clientes de su red GSM. También contiene datos temporales que se necesiten para el correcto funcionamiento de la red (por ejemplo el MSC y el VLR en que se encuentra el móvil en cada momento). Sin embargo, no contiene ningún tipo de información de usuarios que estén visitando su red GSM, pero que pertenezcan a otra.

El VLR contiene todos los datos de usuarios necesarios para la correcta gestión de las llamadas y otros procesos. Sólo contiene información de aquellos usuarios que se encuentran bajo su área de influencia, aunque sean clientes de otras redes GSM, que se encuentran de visita en la suya.

2.3 Servicio General de Paquetes de Radio (GPRS)

El servicio general de paquetes de radio más conocido como GPRS es una evolución de GSM y su característica principal es que permite a los usuarios móviles la comunicación basada en paquetes de datos. En modo de conmutación de paquetes no se reserva un canal de comunicaciones físicamente durante el tiempo que dura la transferencia de datos sino que los paquetes se envían a través de unos recursos compartidos por todos los usuarios (mayor eficiencia con respecto a una comunicación por circuitos). Además permite asignar calidades de servicio (QoS) diferenciadas a los distintos usuarios móviles.

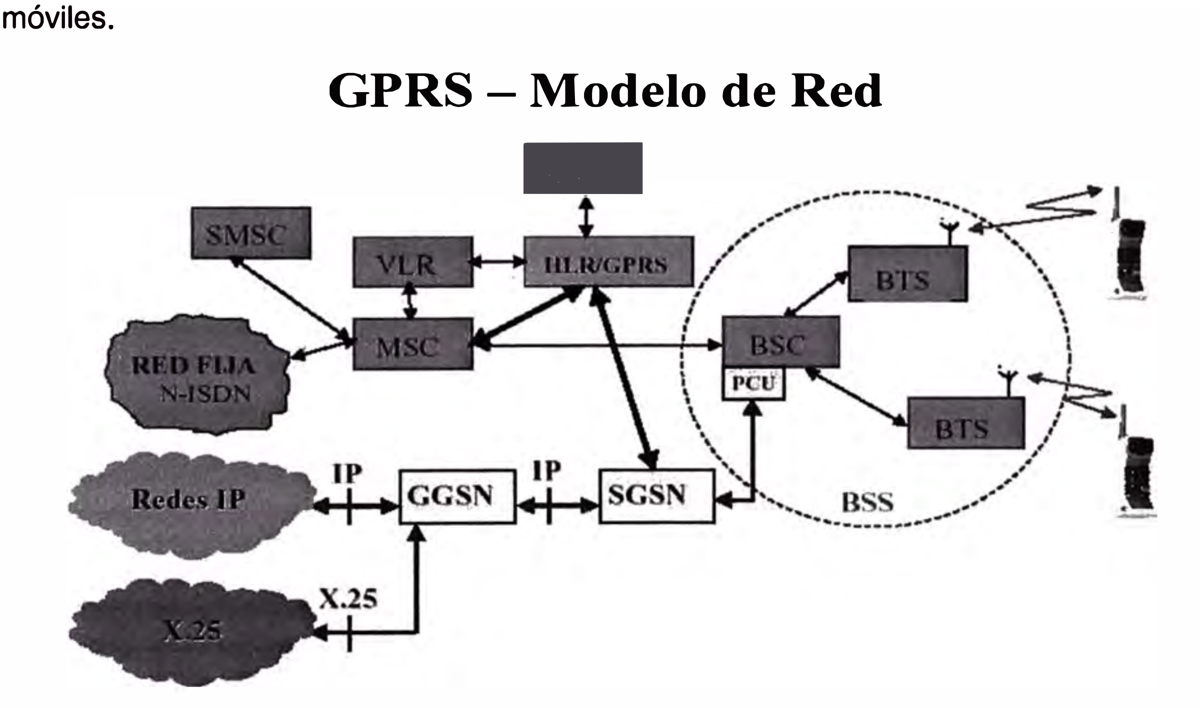


Figura 2.14 Arquitectura de una Red GPRS

El GPRS permite transmitir y recibir datos por conmutación de paquetes tanto sobre la interfaz radio, como en la infraestructura de red, sin utilizar recursos de conmutación de circuitos. La conmutación de paquetes es una tecnología idónea para las aplicaciones de datos y permite por ejemplo que varios usuarios puedan compartir un mismo canal GPRS. De hecho la arquitectura de red está basada en el protocolo TCP/IP que es el que se usa en las redes de datos.

Las tasas de transferencia de datos (throughput) dependen tanto del esquema de codificación que se utilice como del número de intervalos de tiempo que el terminal soporte (multislots). Para GPRS se definen cuatro esquemas de codificación (CS – Coding Schemes) los cuales son:

- CS-1 – Ofrece una tasa variable entre 8 kbps a 64 kbps.
- CS-2 – Ofrece una tasa variable entre 12 kbps a 96 kbps.
- CS-3 – Ofrece una tasa variable entre 14.4 kbps a 96+ kbps.
- CS-4 – Ofrece una tasa variable entre 20 kbps a 115+ kbps.

Todos estos dependen de las capacidades de la estación móvil (MS) y el número de timeslots aceptados (multislots). Las tasas de transmisión altas son más sensibles para la calidad del enlace de radio (C/I):

- CS-1 es mandatario para el BSS y es también usado para la señalización.
- CS-1, CS-2, CS-3 y CS-4 son mandatarios para la estación móvil.
- CS-4 no tiene corrección de error hacia delante ("Forward Error Correction") lo cual posibilita alcanzar mayores velocidades.

Tradicionalmente, la transmisión de datos inalámbrica en redes GSM se ha venido realizando utilizando un canal dedicado GSM a una velocidad máxima de 9.6 kbps (14.4 Kbps en algunos casos). Aunque también muchos operadores han implementado el HSCSD (High Speed Circuit Switched Data) que alcanzan velocidades hasta los 28 kbps (utilizando más de un canal dedicado a la vez). Pero con GPRS, la velocidad de transmisión de datos puede llegar a un máximo de 115 kbps por comunicación y en promedio a unos 40 kbps. El GPRS es una red superpuesta a GSM que comparte con ella la red de acceso. Sin embargo, con el GPRS se introducen dos nuevos nodos: Gateway GPRS Support Node (GGSN) y el Serving GPRS Support Node (SGSN). El GGSN actúa como una interfase hacia las redes de paquetes de datos externas mientras que el SGSN es responsable de la entrega de paquetes al usuario móvil en su área de servicio.

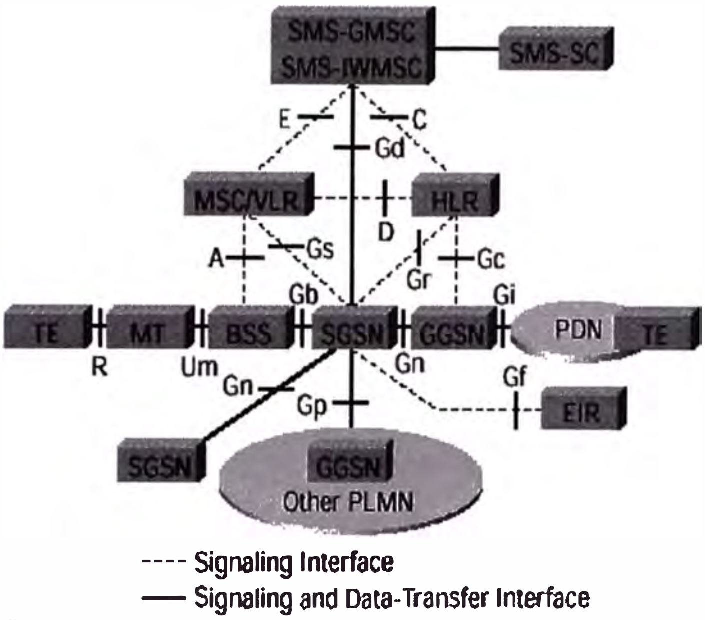
En cuanto a los tipos de servicios soportados mediante GPRS se encuentran los siguientes:

- Servicios basados en el envío de mensajes cortos.
- Servicios generales de Internet y conexiones a Intranets.
- Aplicaciones WAP.
- Servicios específicos de GPRS.

- Servicios basados en la localización.
- Servicios de Video en Demanda (VideoStreaming).
- Comunicaciones de Voz (PTT – Push To Talk).

2.3.1 Arquitectura de la Red GPRS

La red GSM clásica no ofrece funcionalidades adecuadas para el encaminamiento de datos de conmutación de paquetes. Por esta razón, la estructura convencional GSM ha sido extendida con la introducción de una nueva clase de entidades lógicas de red denominadas Nodos de Soporte para GPRS (GSN - GPRS Support Node).



Source: ETSI

Figura 2.15 Arquitectura de la Red GPRS

Los nodos GSN gestionan la interconexión con otras redes y desarrollan múltiples funciones: gestión de la movilidad, roaming y reencaminamiento geográfico, control de la conexión virtual, transmisión de los paquetes. El Serving GPRS Support Node (SGSN), que está conectado a la red de acceso y se encuentra al mismo nivel jerárquico que las centrales de conmutación (MSC/VLR), es el nodo que da servicio al terminal móvil GPRS, conservando la información de posición y ejecutando funciones relativas a la seguridad de la comunicación y al control del acceso. El Gateway GPRS Support Nade (GGSN) es visto, desde el exterior, como la puerta de acceso a la red GPRS y funciona como una unidad de interworking hacia las redes externas de conmutación de paquetes. Dentro de la red, el GGSN está conectado a los nodos SGSN a través de una red de transporte basada en el protocolo IP.

La base de datos HLR debe ser actualizada con las nuevas funciones para almacenar los datos relativos a los perfiles de los usuarios GPRS y a la información de encaminamiento. Finalmente, los centros de mensajes cortos (SMSC) están conectados al SGSN para permitir la transmisión de mensajes cortos también a través de los canales de radio GPRS. El área de cobertura, es decir, la parte del territorio sobre la que se garantiza el servicio, está organizada en zonas de localización que permiten a la red conocer la posición del terminal móvil durante sus movimientos. Dichas zonas, definidas análogamente a las Áreas de Localización (LA – Location Area) utilizadas por la red de conmutación de circuitos, se denominan Areas de Enrutamiento (RA - Routing Área) y determinan áreas de superficie inferior respecto a las de las LA.

Con el objetivo de satisfacer las necesidades de los diversos segmentos de mercado se definieron tres tipos de terminales distintos:

- **Terminal de clase A**: el terminal puede estar simultáneamente conectado tanto a la red GSM, para poder utilizar los servicios basados en conmutación de circuitos, como a la red GPRS, para poder transmitir y recibir datos de paquetes. En otras palabras, este tipo de terminales permite un uso simultáneo de tráfico de paquetes y de circuitos.
- **Terminal de clase B**: el terminal puede estar simultáneamente registrado sobre las dos redes, de circuito y de paquetes, pero no puede enviar y recibir tráfico a la vez en ambos modos. Comúnmente los terminales GSM/GPRS son de esta clase.
- **Terminal de clase C**: el terminal sólo puede estar registrado en la red a modalidad de paquetes ó en la de circuitos, por lo que sólo puede soportar tráfico relativo al tipo de servicio para el que está registrado.

2.3.2 Encaminamiento y Señalización

La infraestructura de red para la realización del servicio GPRS se basa en la tecnología IP. La utilización de esta tecnología para transmisiones desde/hacia usuarios móviles, exige soluciones particulares de encaminamiento, para permitir la entrega de los paquetes IP enviados. De hecho, la versión de IP utilizada en la norma GPRS no prevé ningún mecanismo para la gestión de la movilidad. Por ello, en el estándar GPRS ha sido introducido un método de encaminamiento específico que a continuación es ilustrado brevemente.

En la transmisión de los paquetes de información dentro de la red GPRS, el terminal móvil está caracterizado por una dirección IP que se le asigna permanente o dinámicamente, en el momento del establecimiento de la sesión. Los paquetes, provenientes de las redes externas son enviados al GGSN a la que el terminal pertenece.

El GGSN posee las informaciones de encaminamiento necesarias para enviar el paquete (utilizando el método de tunnelling) al nodo SGSN, que da servicio al área geográfica donde se encuentra actualmente localizado el móvil. El SGSN, a su vez, realiza una conexión lógica con el terminal, a través de la cual tiene lugar la entrega del paquete.

En el caso de una transmisión originada por un terminal móvil, el SGSN encapsula los paquetes entrantes y los transfiere a su GGSN, donde son transmitidos a las redes de datos de destino. Todos los datos relativos a los usuarios GPRS, necesarios en el nodo SGSN para realizar el encaminamiento y la transferencia de los datos, se encuentran almacenados en el registro GPRS, que conceptualmente forma parte del nodo HLR del sistema GSM. El registro GPRS contiene las informaciones de encaminamiento y la correspondencia entre la identificación del usuario (IMSI - Intemational Mobile Subscriber Identity) y la dirección IP asignada, y entre esta última y el GGSN correspondiente.

2.3.3 Tasas de Datos Mejoradas para la evolución de GSM (EDGE)

Para mejorar las velocidades de transferencia de datos alcanzadas en las redes GPRS surge la evolución del GPRS más conocido por su acrónimo en inglés EDGE. Esta tecnología implementa nueve esquemas de modulación y codificación algunos de los cuales están basados en 8PSK (8 Phase Shift Keying). Los siguientes son los esquemas de modulación y codificación definidos para EDGE:

- MCS1
- MCS2
- MCS3
- MCS4
- MCS5
- MCS6
- MCS7
- MCS8
- MCS9

De estos los cuatro primeros son básicamente similares a los implementados para GPRS, en los cuales se utiliza la modulación GMSK. En tanto que los cinco niveles superiores están basados en 8PSK. La utilización de 8PSK produce una palabra de 3 bits por cada cambio en la fase de la portadora. De esta forma se triplica el ancho de banda disponible que brinda el GSM. Los esquemas que se utilizan para transmitir información en EDGE dependen de la calidad de la señal definida por la relación entre el nivel de señal de la portadora entre el nivel de interferencia (C/I). El máximo teórico para las tasas de transferencias de datos en EDGE es de 384 Kbps, en tanto que en promedio se puede alcanzar hasta 200 Kbps de bajada (downlink).

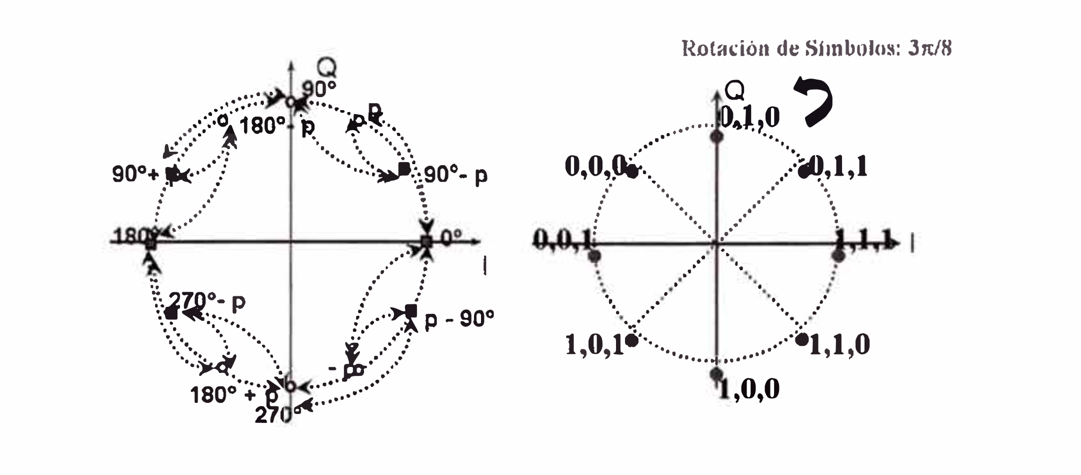


Figura 2.16 Modulación 8PSK y GMSK

Debido a que se trata de una mejora tecnológica en la red de acceso, la implementación de EDGE en las redes GSM/GPRS se lleva a cabo principalmente en las estaciones base (BTS), en las cuales es necesario cambiar o actualizar los radios (TRX) para que soporten EDGE. Asimismo es necesario realizar cambios en los controladores de estaciones base (BSC) para actualizar las unidades de control de paquetes (PCU) para que soporten EDGE. Asimismo es necesario actualizar el software del subsistema BSS. La siguiente figura muestra de manera sencilla los cambios a realizar en una Red GSM para implementar EDGE:

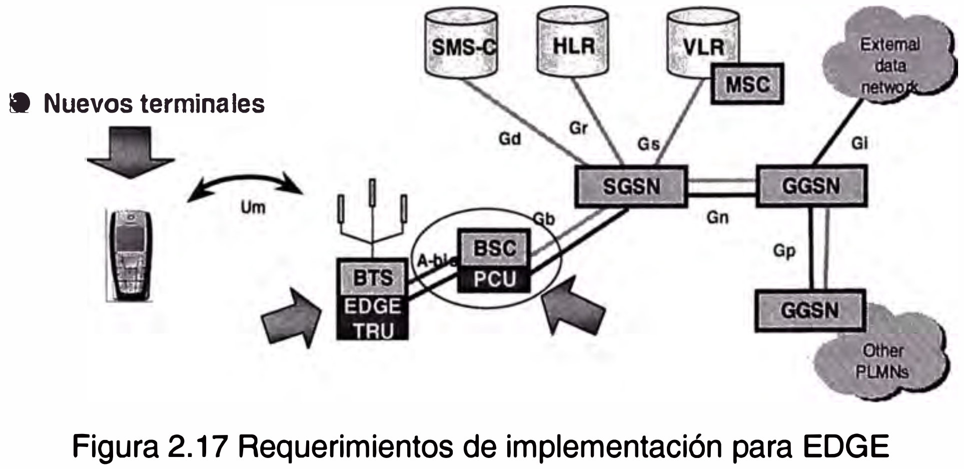


Figura 2.17 Requerimientos de implementación para EDGE

2.3.4 Comparación entre GPRS y EDGE

Las siguientes tablas permiten comparar las tasas de datos alcanzados al utilizar GPRS y EDGE a nivel de aplicación. Estas tablas incluyen datos prácticos medidos bajo buenas condiciones de red.

Scheme	Maximum net payload (bytes)	Maximum net RLC/MAC data rate (kbps)	Nominal data rate (kbps)	Application data rate (kbps)
CS-1	20	8	9.05	7.7
CS-2	30	12	13.4	11.5
CS-3	36	14.4	15.6	13.8
CS-4	50	20	21.4	19.2

Tabla 2.1. Tasas de datos obtenidos con GPRS

Como se puede apreciar en la tabla 2.1, la tasa máxima que se puede alcanzar utilizando el CS 2 es de 11.5 Kbps por intervalo de tiempo. Debido a que los terminales GPRS con mayor capacidad pueden utilizar hasta cuatro intervalos de tiempo en bajada (downlink), la máxima tasa real alcanzable es de alrededor de 42 Kbps a nivel de aplicación.

Scheme	Modulation	Raw Data within one Radio Block (bits)	Maximum net payload (bytes)	Maximum net RLC/MAC data rate (kbps)	Application data rate (kbps)
MCS-9	8PSK	2x592	2x74	59.2	56.8
MCS-8		2x544	2x68	54.4	52.2
MCS-7		2x448	2x56	44.8	43.0
MCS-6		592 544+48	74 68	29.6 27.2	28.4 26.1
MCS-5		448	56	22.4	21.5
MCS-4	GMSK	352	44	17.6	16.9
MCS-3		296 272+24	37 34	14.8 13.6	14.2 13.0
MCS-2		224	28	11.2	10.7
MCS-1		176	22	8.8	8.4

Tabla 2.2. Tasas de datos obtenidos con EDGE

Como se puede apreciar en la tabla 2.2, la tasa máxima que se puede alcanzar utilizando el MCS 9 es de 56.8 Kbps por intervalo de tiempo. Debido a que los terminales EDGE con mayor capacidad pueden utilizar hasta cuatro intervalos de tiempo en bajada (downlink), la máxima tasa real alcanzable es de alrededor de 220 Kbps a nivel de aplicación.

CAPITULO III

DESCRIPCIÓN DE LA SOLUCIÓN

El presente capitulo tiene como objetivo describir específicamente la tarjeta SIM, su tecnología, sus principales funciones (generación de claves de autenticación y cifrado). Su arquitectura, su estructura de archivos, los archivos más importantes, así como las características de los mismos y los valores recomendados para los mismos.

3.1 El Módulo de Identificación del Suscriptor (tarjeta SIM).

Los módulos de identificación del suscriptor o tarjetas SIM están diseñados para su uso en conjunto con los terminales móviles para proveer acceso a los servicios ofrecidos por los operadores de telefonía móvil de tecnología GSM de manera personal y segura, por medio de la autenticación y el cifrado de datos en la interfase aire. Actualmente es posible que los terminales operen en las siguientes bandas de frecuencia: 850 MHz, 1900 MHz, 900 MHz y 1800 MHz. En nuestro país los operadores de telefonía móvil que utilizan tecnología GSM tienen licencia en las bandas de 850 MHz y 1900 MHz.

La tarjeta SIM al ser considerada como una computadora integrada a una tarjeta, está equipada con una memoria de almacenamiento la cual es utilizada para distintas funciones, por ejemplo para almacenamiento de parámetros de Red y de aplicaciones.

El contenido básico de una tarjeta SIM en la actualidad incluye:

- Identificación de la tarjeta. Está dado por el código ICCID.
- Datos de usuario. Como son la agenda telefónica (ADN), almacenamiento de mensajes de texto SMS, etc.
- Algoritmos y llaves de autenticación de usuarios propios del sistema GSM.
- Aplicaciones SIM Toolkit (STK) y aplicaciones interactivas por medio del uso de un micro navegador integrado (“SIM Browsing”). Para ofrecer servicios a los usuarios.
- Mecanismos de certificación por medio de llaves DES, 3DES y RSA para el uso de aplicaciones seguras como por ejemplo banca móvil.

3.2 Normativa ETSI GSM.

Las normas que definen el funcionamiento de las tarjetas SIM fueron definidas por el instituto europeo de estándares de telecomunicaciones (ETSI -European Telecommunications Standards Institute), y son las que se muestran como referencias en la bibliografía.

La siguiente lista resume las normas necesarias que definen la comunicación coherente entre la tarjeta SIM y el equipo Terminal, el usuario y la red:

• SIM <=> MÓVIL	**GSM 11.11.**
• SIM <=> USUARIO (VAS via STK)	**GSM 11.14**
• SIM <=> RED (OTA)	**GSM 03.48 / GSM 03.40**

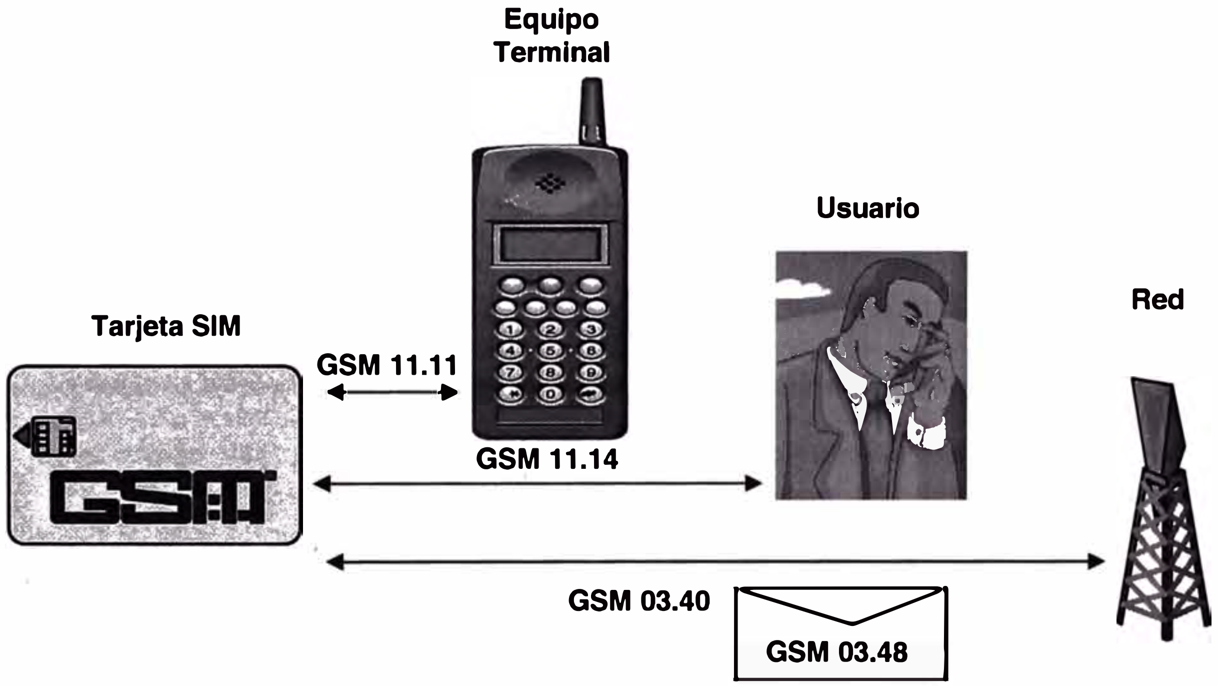


Figura 3.1. Normas GSM que permiten la comunicación coherente con la SIM

Debido al continuo desarrollo de la tecnología y los servicios ofrecidos, las normas experimentan una evolución. Las primeras normas GSM fueron emitidas antes del lanzamiento comercial (GSM Fase 1), posteriormente aparece GSM Fase 2 en el año 1995, que ya incluye la norma GSM 11.11. Luego hace su aparición la fase 2+ que en el año 1196 incluye dentro de la normativa la activación por aire (OTA) y posteriormente surge la normativa que estandariza la aplicaciones de valor agregado de las tarjetas SIM (STK – SIMToolkit) en el año 1997. La siguiente figura resume esta evolución de las normas GSM desde el punto de vista de las tarjetas SIM:

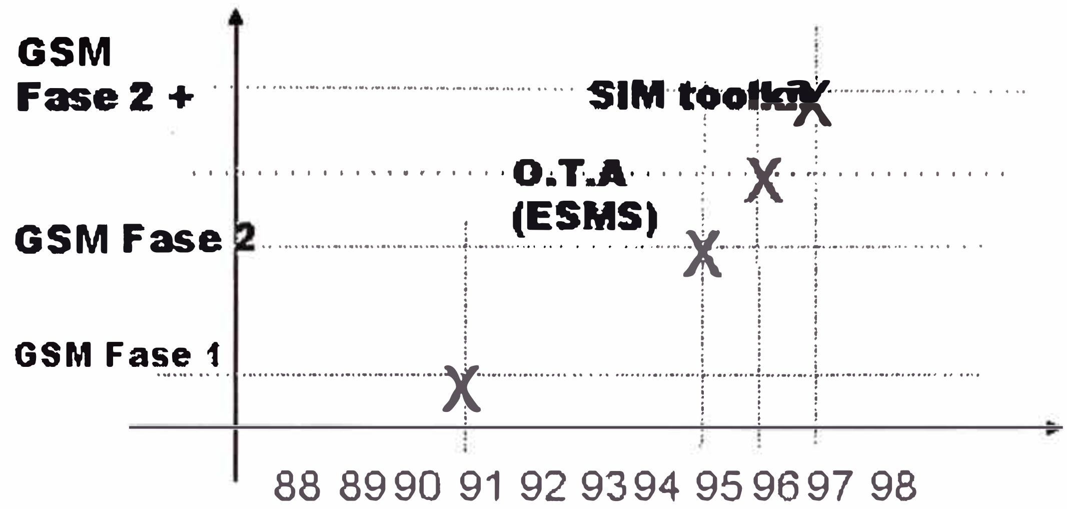


Figura 3.2. Evolución de las Normas GSM

Debido a lo extenso de las normas definidas por el ETSI para el GSM, el presente trabajo se centra principalmente en la especificación ETSI GSM 11.11.

Es necesario tener en cuenta que las normas ETSI fueron emitidas cuando solo se tenía redes y equipos de segunda generación (2G). Con la aparición de la tercera generación (3G) aparecen las normas 3GPP que en pocas palabras surge de la unión de los grupos de estandarización 2G y 3G. Es así que la norma ETSI GSM 11.11 para 3GPP cambia de identificación a 3GPP 51.011.

3.3 Funciones de las tarjetas SIM

3.3.1 Características funcionales

Las características funcionales deberán ser las mismas que las descritas en las normas ETSI y 3GPP listadas en la bibliografía.

3.3.2 Estructura Lógica e Interfase Tarjeta SIM/Terminal (SIM/ME)

La estructura lógica y la interfase SIM/ME debe considerar los siguientes puntos como referencia:

Norma GSM 11.11 en relación a lo siguiente:

- Características físicas de las tarjetas SIM, señales eléctricas y protocolos de transmisión.
- El modelo lógico a ser utilizado para la estructura de las tarjetas SIM.
- Elementos relacionados con la seguridad.
- Funciones de Interfase.
- Comandos.

- El contenido de los archivos requeridos para las aplicaciones GSM.
- El protocolo de aplicación.

Normas GSM 11.14, GSM 03.19, y GSM 03.48, en relación a:

- Comandos y procedimientos relacionados a las aplicaciones SIM Toolkit (STK).
- Los protocolos de comunicación par alas distintas aplicaciones.
- La interfase necesaria para garantizar la interoperabilidad entre la tarjeta SIM y los terminales.
- Los mecanismos y llaves que permitan la actualización del contenido de los archivos y aplicaciones en forma remota (OTA).

Norma GSM 11.17, en relación a:

- Pruebas de compatibilidad entre la tarjeta SIM y el terminal.

3.4 Especificaciones de las tarjetas SIM

3.4.1 Características Físicas

La norma ETSI GSM 11.11 define el formato "Plug-In" para las tarjetas SIM. Las dimensiones de dicho formato son las siguientes:

- 25 mm de largo.
- 15 mm de ancho.
- 0.76 mm de espesor.

Este formato debe ser realizado tomando como base el formato de las tarjetas ID-1 en el cual es posible la extracción física de la tarjeta "Plug-IN" por parte del usuario final. Esto generalmente se observa cuando el usuario adquiere una tarjeta nueva y tiene que extraer la tarjeta SIM para insertarlo en el equipo móvil y poder hacer uso por primera vez del servicio. Las dimensiones del formato ID-1 son:

- 85.6 mm de largo.
- 53.98 mm de alto.
- 0.76 mm de espesor.

Como referencia práctica el formato ID-1 es utilizado comúnmente para las tarjetas de crédito y/o débito. La siguiente figura define la ubicación del formato Plug-In dentro del formato ID-1:

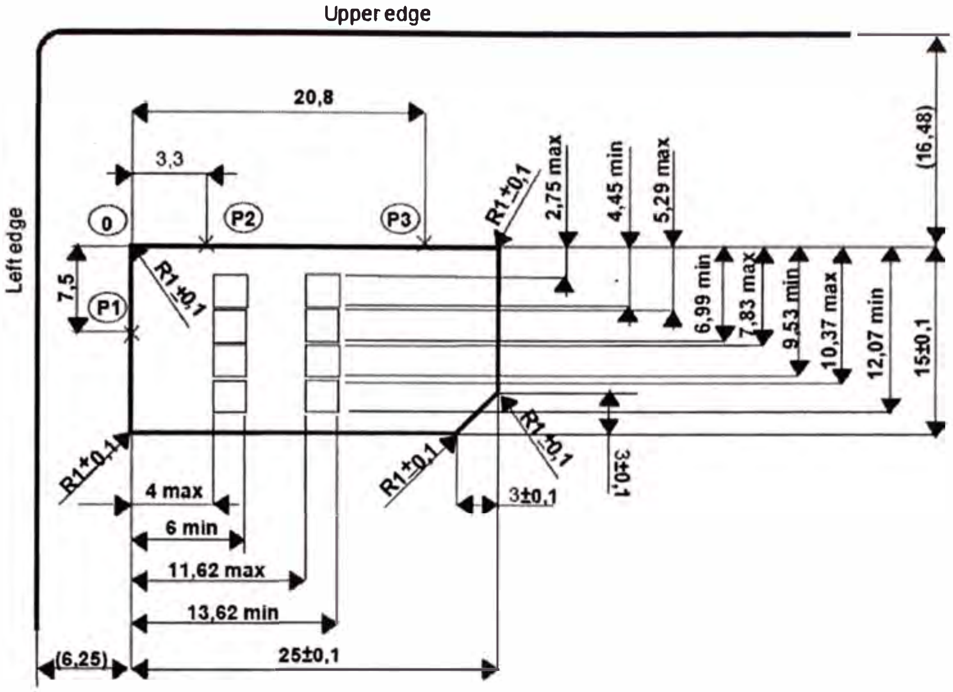


Figura 3.3. Dimensiones y ubicación del formato Plug-In

3.4.2 Características de los contactos

El número, posición y dimensiones de los contactos del formato ID-1 deben estar en conformidad a lo establecido por las normas ISO 7816-2 y GSM 11.11. Las funciones de los contactos deben ser conforme a lo definido por la norma GSM 11.11.

La siguiente figura muestra la disposición de los contactos definidos para una tarjeta SIM:

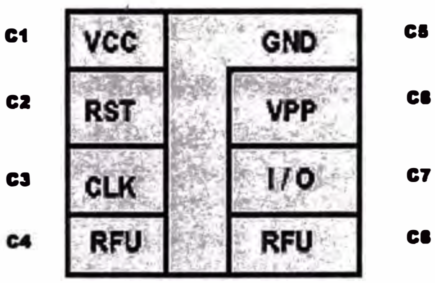


Figura 3.4. Contactos para una tarjeta SIM

La norma especifica que los contactos C4 y C8 no son utilizados y por lo tanto podrían no ser implementados. En la actualidad se tienen algunos modelos de tarjetas SIM que no tienen implementados dichos contactos.

3.4.3 Materiales

Los materiales utilizados para conformar la base plástica y los contactos deben estar de acuerdo a las normas indicadas. La materiales que conforman la base plástica deben poseer características que permitan la impresión láser además de permitir la personalización de la misma (imágenes, datos de la SIM, datos del operador, etc.). El material preferido para la base plástica de las tarjetas SIM es el cloruro de polivinilo (PVC) de alta temperatura.

3.5 Características Eléctricas de las tarjetas SIM

3.5.1 Fuente de Alimentación

Las tarjetas SIM deben cumplir con lo establecido por la norma GSM 11.11 en lo que respecta a las características eléctricas de las mismas, en especial los siguientes puntos:

- Voltaje de alimentación híbrido entre 3 y 5 voltios ± 10%. Con el objetivo de garantizar la compatibilidad con equipos terminales que operan con 3 V y 5V respectivamente (Tarjetas Tipo 1).
- Corriente de alimentación con un consume eléctrico no mayor a 200 µA, con una señal de reloj de 1 MHz a una temperatura de 25 °C, en modo “idle”.
- Señal de reloj entre 1 y 5 MHz.

3.5.2 Características del Microprocesador

Durante la fase de acuerdo comercial los fabricantes deberán entregar al operador documentación específica relacionada a las características funcionales del chip, utilizando el formato descrito en la tabla 3.1.

Cualquier cambio que se realice al chip por parte del fabricante deberá ser comunicado al operador en forma inmediata utilizando el formato antes descrito. El operador evaluará y aprobará dichos cambios.

Chip Type	Chip Maker	Memory capacity			Power supply	Operating Frequency	Cryptographic functions *			CPU (bit)	Additional Functions
		ROM (KB)	RAM (Bytes)	EEPROM			RSA (bit)	DES (bit)	3DES (bit)		

Tabla 3.1 – Especificaciones del microprocesador

3.5.3 Características de la EEPROM

(Electrically Erasable Programmable Read Only Memory)

La EEPROM deberá mantener las siguientes características:

- Actualmente la EEPROM no deberá tener una capacidad menor a 128 Kbytes. La capacidad de la EEPROM es considerada totalmente libre y por tanto disponible para fines de personalización.

- Duración: Como mínimo deberá soportar 20000 ciclos de lectura/escritura.
- Tiempo de retención de datos: La retención de datos en la memoria no deberá ser menor a 5 años.

3.6 Arquitectura de las tarjetas SIM

La arquitectura de una tarjeta SIM se organiza alrededor de un microprocesador con tres tipos de memoria:

- ROM (Memoria de Solo Lectura), que contiene el sistema operativo de la tarjeta, la máquina virtual Java y sus componentes de seguridad, algunas aplicaciones como por ejemplo micro navegadores (SIM Browsing). Los datos y las aplicaciones que residen en la ROM permanecen en esta aun cuando no hay una fuente alimentación conectada a la tarjeta.
- EEPROM (ROM que se puede borrar y programar eléctricamente), contiene cada uno de los campos definidos por la norma así como datos relativos a aplicaciones específicas. La información almacenada en la EEPROM permanece aun cuando no hay fuente de alimentación conectada a la tarjeta. La diferencia con la ROM es que la EEPROM es a la vez de lectura y escritura.
- RAM (Memoria de Acceso Aleatorio) contiene daros relativos a aplicaciones especificas cuando estas están ejecutándose. La información almacenada en la RAM se pierde cuando la SIM es desconectada de la fuente de alimentación. La ventaja de la RAM radica que en esta el ciclo de escritura es mucho más rápido que en la EEPROM.

La siguiente figura muestra la arquitectura de una tarjeta SIM tomando como referencia la memoria disponible para el usuario

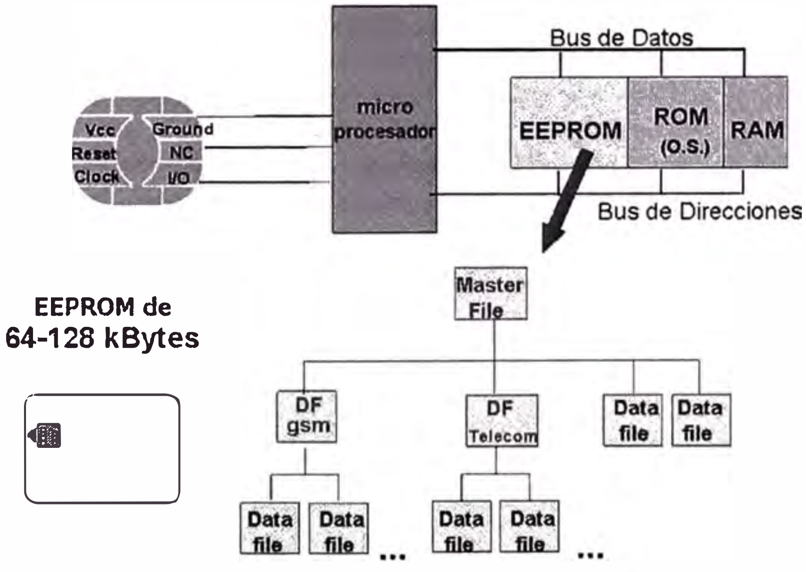


Figura 3.5. Arquitectura de una tarjeta SIM (I).

Por otro lado la siguiente figura muestra la misma arquitectura tomando como referencia el Sistema Operativo:

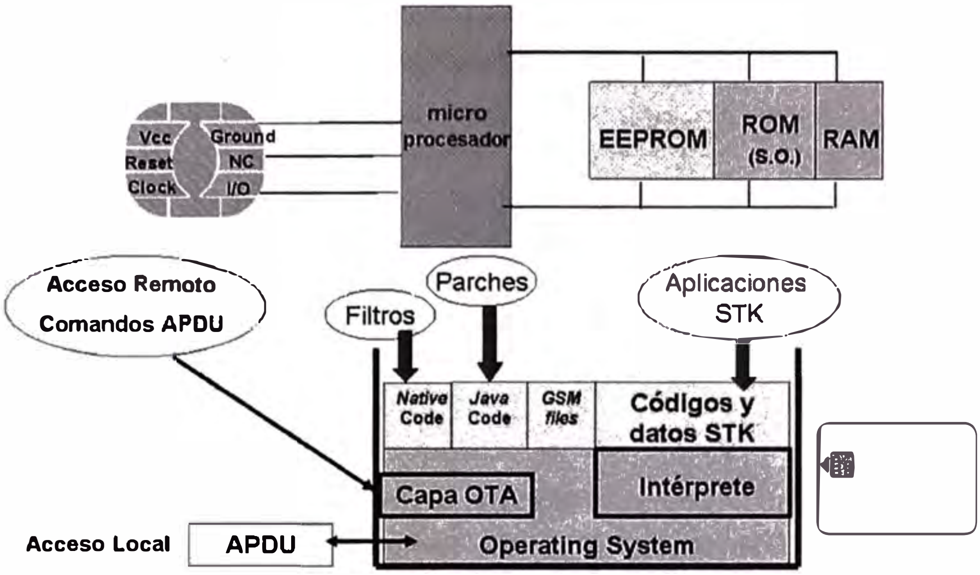


Figura 3.6. Arquitectura de una tarjeta SIM (II).

Como se puede apreciar en ambas figuras, en la memoria EEPROM (E^2PROM) se almacenan las aplicaciones (Java, Nativas, STK, etc.) además del perfil eléctrico.

3.7 Sistema de Archivos de las tarjetas SIM

3.7.1 Tipos de Archivos

Los archivos del sistema operativo de las tarjetas se dividen en tres tipos:

- Archivo Maestro (Master File – MF).
- Archivos Dedicados (Dedicated Files – DF)
- Archivos Elementales (Elementary Files – EF).

El Archivo Maestro (MF) es un archivo dedicado que es la raíz de la estructura de archivos. Este puede contener archivos dedicados (otros directorios) y archivos elementales (archivos de datos). La identificación (ID) del MF para las tarjetas SIM siempre es 3F00.

Los Archivos Dedicados (DF) son subdirectorios en la jerarquía de archivos. Estos pueden contener archivos elementales y otros archivos dedicados (subdirectorios). El tamaño de un DF está basado en el número y el tamaño de los archivos (encabezados y datos) que están o pueden ser almacenados en este. El tamaño de un DF existente no puede ser alterado.

Archivos Elementales (EF), son utilizados para almacenar datos de programas como nombres y fechas.

La siguiente figura muestra la organización típica de la estructura de archivos de una tarjeta SIM:

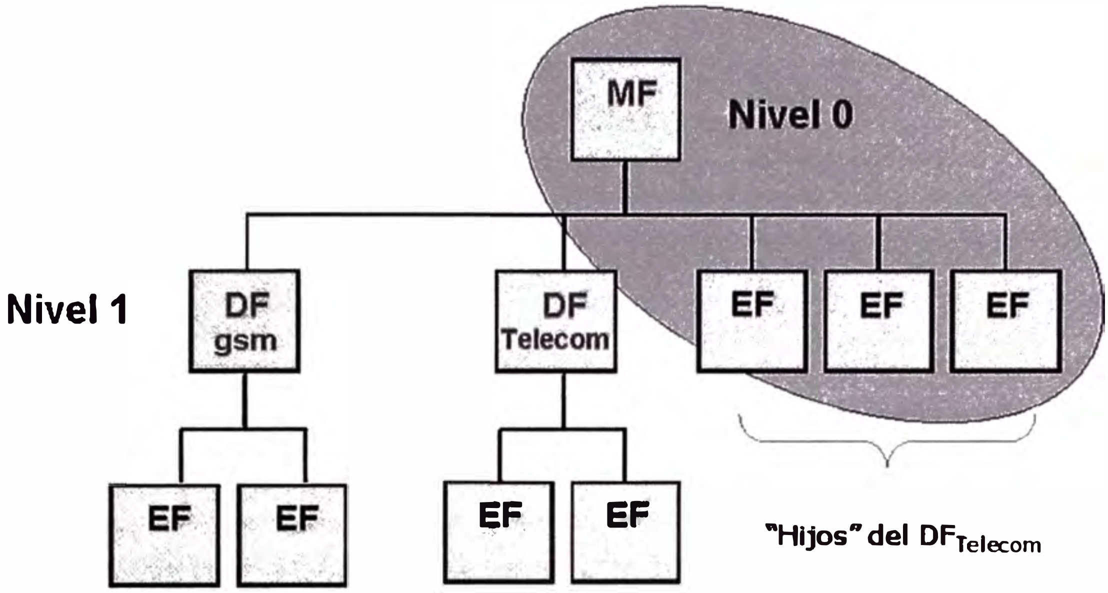


Figura 3.7 Estructura de archivos de una tarjeta SIM

Es necesario tener en cuenta que por motivos prácticos los archivos elementales que se ubican dentro de un archivo dedicado se denominan “hijos” del directorio “padre” en el que se ubican.

3.7.2 Identificación de Archivos

La norma especifica que para la identificación de archivos se utilizan dos bytes. Asimismo se establecen las siguientes reglas para la identificación de archivos:

- **Nivel 0**
  - Identificación del archivo maestro (MF): **3F00**
  - Archivos elementales dentro del MF: **2FXX**
- **Nivel 1**
  - Archivos dedicados dentro del MF: **7FXX**
  - Archivos elementales dentro de estos DF: **6FXX**
- **Nivel 2**
  - Archivos dedicados dentro de los DF: **5FXX**
  - Archivos elementales dentro de estos DF: **4FXX**

3.7.3 Estructura de Archivos Elementales

Las tarjetas SIM utilizan los siguientes tipos de archivos:

- Archivos Transparentes ("Binarios").
- Archivos orientados a Registros:
    - Lineales con registros de Longitud Fija.
    - Cíclicos.

Los archivos Transparentes contienen una secuencia de octetos. Se denominan transparentes porque permiten almacenar datos sin un formato específico, es decir estos archivos no tienen una estructura interna definida. Los archivos transparentes son útiles para almacenar objetos como llaves e imágenes. Como ejemplo tenemos el archivo elemental EF_{ICCID} con identificación 2FE2 que es "hijo" del MF.

Figura 3.8. EF transparente

Los archivos Lineales contienen subdivisiones llamadas registros que son de longitud fija. Cada registro en un archivo es identificado por un número. Los números de registro se utilizan para leer desde y escribir hacia un registro específico. Cada archivo lineal de longitud fija puede contener hasta 255 registros. Cada registro contiene una misma cantidad de octetos que puede ser entre 1 y 255 (longitud del registro). Este tipo de archivos tienen un puntero de registro que apunta al registro actualmente seleccionado. Como ejemplo de este tipo de archivo se tiene al archivo elemental EF_{ADN} con identificación 6F3A y ubicado dentro del $DF_{TELECOM}$. Este archivo contiene lo que comúnmente se conoce como agenda telefónica de la SIM.

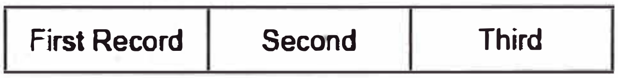


Figura 3.9. EF lineal de longitud fija

Los archivos Cíclicos pueden ser vistos como un anillo de registros, con todos sus registros de igual longitud. Cada nueva operación de escritura modifica el siguiente registro físico en el anillo. Si el círculo de registros está lleno, el nuevo registro sobrescribe el más antiguo en el archivo. El puntero de registro apunta hacia el registro escrito más reciente, que viene a ser el siguiente primer registro en el archivo. Los archivos cíclicos son especialmente útiles para almacenar por ejemplo datos de "las últimas 10 operaciones". Cada EF cíclico puede contener un máximo de 255 registros y la longitud de cada uno de estos puede ser entre 1 y 255 octetos. Como ejemplo de este tipo de archivos se tiene el archivo elemental EF_{LND} con identificación 6F44 ubicado dentro del $DF_{TELECOM}$. Este archivo almacena comúnmente la lista correspondiente a las 10 últimas llamadas efectuadas por el teléfono móvil.

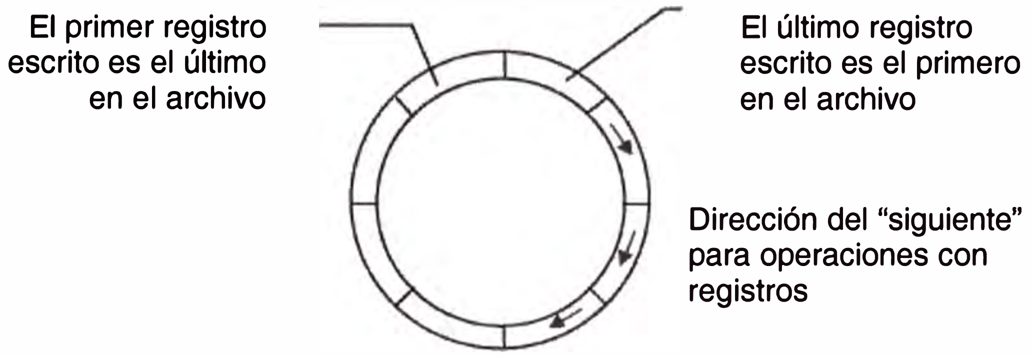

El primer registro escrito es el último en el archivo
El último registro escrito es el primero en el archivo
Dirección del "siguiente" para operaciones con registros

Figura 3.10. EF cíclico.

3.7.4 Arquitectura de Archivos

Los archivos en la tarjeta SIM están organizados en una arquitectura jerárquica. El directorio raíz (MF, ID 3F00) contiene por lo menos dos directorios: un directorio que contiene información relativa a los servicios de telecomunicaciones ofrecidos por el operador ($DF_{TELECOM}$, ID 7F20) y un directorio que contiene datos específicos de GSM (DF_{GSM}, ID 7F10).

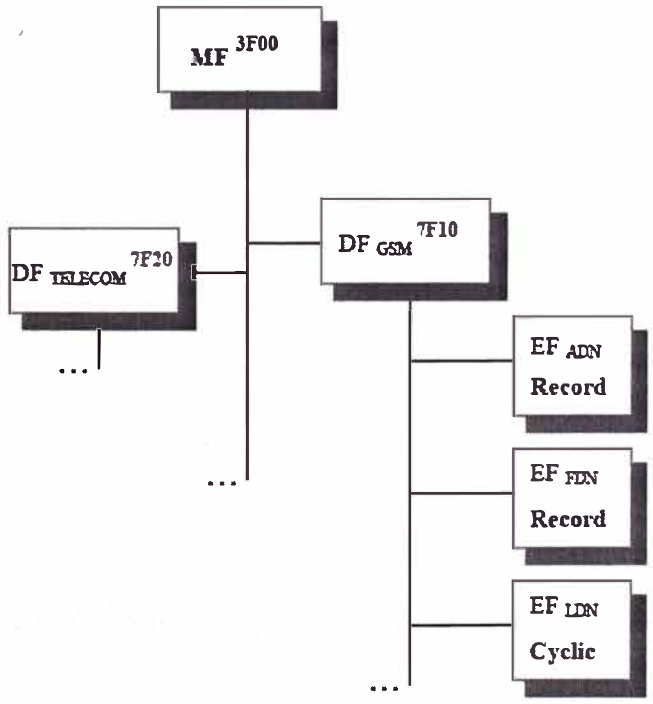
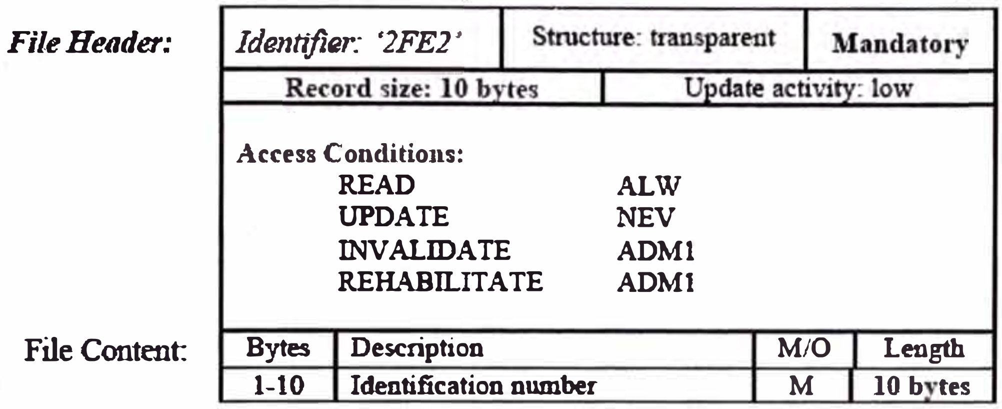


Figura 3.11. Arquitectura del Sistema de Archivos

3.7.5 Formato de Archivos

Cada archivo está conformado por un encabezado (2 octetos). El encabezado define la identidad del archivo, su estructura, su tamaño y las condiciones de acceso. El primer octeto del identificador define el tipo de archivo (MF, DF, EF) y el segundo octeto identifica el archivo en el directorio. El identificador del archivo es único para prevenir cualquier confusión.



File Header:

Identifier: '2FE2'	Structure: transparent	Mandatory
Record size: 10 bytes	Update activity: low	

Access Conditions:

READ	ALW
UPDATE	NEV
INVALIDATE	ADM1
REHABILITATE	ADM1

File Content:

Bytes	Description	M/O	Length
1-10	Identification number	M	10 bytes

Figura 3.12. Formato de un archivo

Para cada archivo las condiciones de acceso definen el nivel de acceso asociado a las acciones que pueden ejecutarse sobre el mismo (lectura, actualización, etc.). Existen cinco (05) niveles de acceso:

- ALLW (always): La acción puede ejecutarse aun cuando no se ha ingresado ninguna contraseña.
- CHV1: La acción puede ser ejecutada si el código CHV1 está deshabilitado o ha sido presentado correctamente a la tarjeta.
- CHV2: La acción puede ser ejecutada si el código CHV2 ha sido presentado correctamente a la tarjeta.
- ADM (administrativa): La acción puede ser ejecutada sólo por la entidad administrativa ADM.
- NEV (never): La acción no puede ser ejecutada nunca en la interfase SIM/ME.

El MF y los DF solo un encabezado mientras que los EF contienen además del encabezado un contenido.

Cuando el EF es transparente, el tamaño de su contenido es indicado en el encabezado. Para los archivos lineales de longitud fija y los archivos cíclicos, el tamaño del contenido es un conjunto de registros de igual longitud (el número de registros y su longitud están indicados en el encabezado).

3.8 Claves Secretas de la tarjeta SIM

Las claves secretas de las tarjetas SIM se dividen en dos clases. Las claves de Verificación del Propietario de la Tarjetas (CHV – Card Holder Verification) y Administrativas (ADM). Típicamente los códigos CHV son mantenidos por el usuario para asegurar el acceso a al información de la tarjeta SIM. Cada código CHV tiene su correspondiente código de desbloqueo (PUK – PIN Unblock Code) para el caso en el que ingrese incorrectamente el código CHV cierta cantidad de veces. Los códigos administrativos (ADM) son definidos y mantenidos por el operador Móvil y son utilizados para limitar le acceso a información sensible de las tarjetas SIM. Tanto los códigos CHV como los códigos ADM pueden ser definidos como fijos o variables.

Para los códigos CHV generalmente se tiene:

- CHV1 o PIN1. Tiene una longitud de cuatro (04) dígitos y puede ser utilizado como clave que permite el encendido del teléfono y protección de la información personal contenida en ésta como por ejemplo números de la agenda, mensajes de texto SMS almacenados, llamadas realizadas, etc. Para facilidad de uso de los servicios algunos operadores definen un código por defecto como por ejemplo 1111 además de desactivarlo. Al ser un código administrado por el usuario, éste tiene la opción de activar y cambiar dicho código cuando lo estime conveniente.
- CHV2 o PIN2. Este código permite el restringir las llamadas a una lista de prefijos definida en el archivo elemental EF_{FDN}. Por lo general es una clave aleatoria de cuatro (04) dígitos de longitud. Al ser un código administrado por el usuario, éste tiene la opción de cambiarlo cuando lo estime conveniente.
- PUK1 y PUK2. Son los códigos de desbloqueo de las llaves CHV1 y CHV2 respectivamente. Sucede que si el usuario introduce un código CHV en forma errónea una cierta cantidad de veces, éste se bloquea. El usuario tiene la opción de desbloquear el CHV bloqueado utilizando el código PUK respectivo. Sin embargo existe un límite máximo de intentos de ingresar las claves PUK por lo que se debe tener cuidado ya que alcanzado el límite de intentos la tarjeta SIM quedará inutilizable definitivamente. Los códigos PUK son números aleatorios de ocho (08) dígitos de longitud.
- Códigos ADM. Son códigos definidos y administrados por el operador. El operador tiene la posibilidad de definir un algoritmo de generación de dichos códigos, el cual por razones obvias deberá mantenerse en forma secreta. Estos códigos son propietarios, es decir que cada fabricante establece su propia norma con respecto al uso de los mismos.

3.9 Procedimientos relacionados con la Seguridad GSM

3.9.1 Procedimientos de Autenticación y Generación de llaves de Cifrado

El procedimiento de autenticación en GSM funciona de la siguiente manera: La Red genera y envía un número aleatorio (RAND) hacia el teléfono. El Terminal (ME) pasa dicho número (RAND) hacia la SIM en el comando RUN GSM ALGORITHM. LA SIM retorna los valores SRES y Kc hacia el ME. El ME envía SRES hacia la Red. La Red compara el SRES recibido con el SRES calculado. El resultado de la comparación define la autenticidad del usuario.

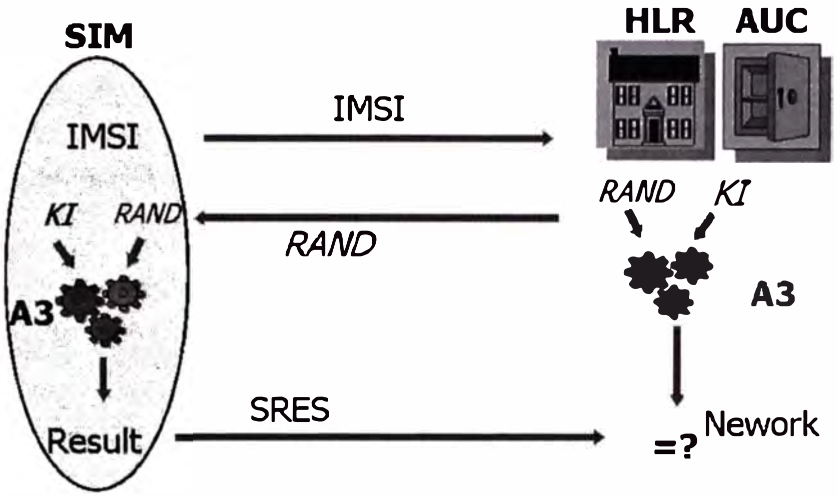


Figura 3.13. Procedimiento de Autenticación.

La llave Kc generada es utilizada por el ME para cualquier comunicación cifrada con la Red hasta la siguiente invocación del mecanismo de autenticación. El algoritmo A5 es el encargado de cifrar los datos en la interfaz aire. La versión en uso actualmente es A5/1 ya que la versión A5/2 fue retirada del mercado por recomendación de la GSMA.

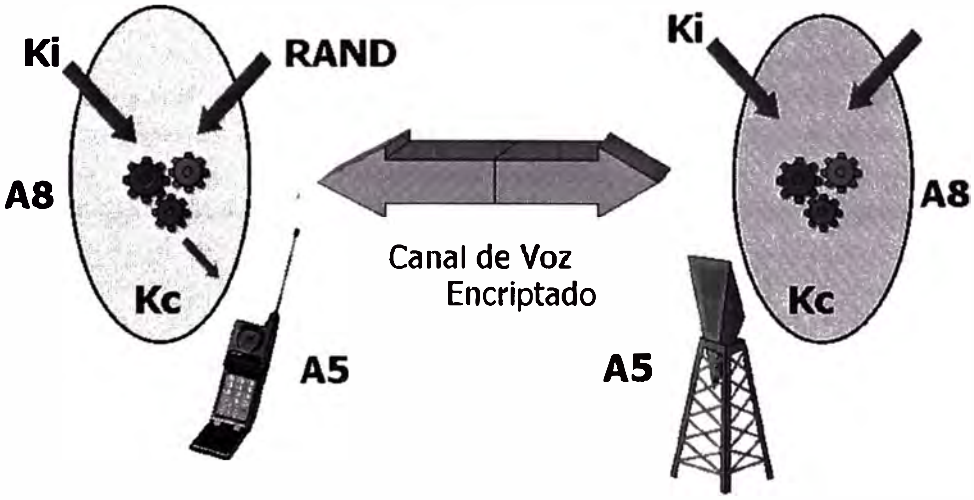


Figura 3.14. Cifrado de comunicaciones en GSM.

3.9.2 Algoritmos y procesos

Los siguientes son los algoritmos soportados por la SIM:

- A3. Sirve para autenticar el teléfono a la Red.
- A8. Sirve para generar la llave de cifrado.

Generalmente ambos algoritmos (A3 y A8) son implementados en conjunto, lo que se denomina COMP128. Al respecto se debe tener cuidado de elegir un algoritmo que sea por lo menos COMP128-2 o superior. Es necesario aclarar que la elección de la versión de dicho algoritmo depende de la versión implementada en la Red.

Las variables de entrada del algoritmo COMP128 son: la llave Ki (128 bits) internamente almacenada en la SIM y la variable RAND (128 bits) recibida de la interfase ME/SIM y generada por la Red (AuC). La variable de salida del COMP128 es SRES (32 bits)/Kc (64 bits).

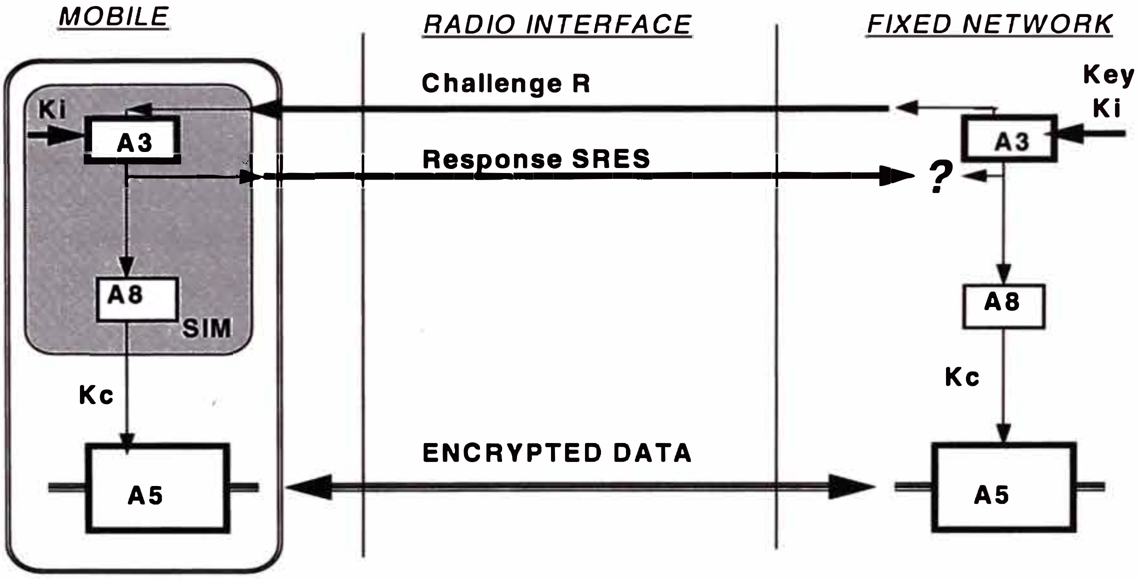


Figura 3.7. Flujo de Autenticación y Encriptación

La autenticación es positiva sí y sólo sí el resultado enviado por el móvil hacia la red coincide con el valor calculado en el AuC.

3.10 Juego de Comandos para la comunicación SIM/ME

La norma ETSI GSM 11.11 define una serie de comandos que permiten entre otros la administración de archivos, la administración de la seguridad y mecanismos de administración específicos. El conjunto de comandos definidos por la norma son:

- Mecanismos de Administración específicos:
    - Invalidate
    - Rehabilitate

- Administración de Archivos:
    - Select
    - Status
    - Get Response
    - Sleep (ME fase 1)
    - Read Binary
    - Update Binary
    - Read Record
    - Update Record (Enhanced)
    - Seek
    - Increase
    - Create File
    - Extend
- Administración de la Seguridad:
    - Verify CHV/ADM
    - Change CHV/ADM
    - Disable CHV/ADM
    - Enable CHV/ADM
    - Unblock CHV/ADM
    - Run GSM Algorithm (Autenticación)
    - Lock

3.11 Contenido de los Archivos Elementales (EF) del Perfil Eléctrico Básico

A continuación de analizará el contenido de los principales archivos elementales del perfil eléctrico de las tarjetas SIM. Los valores presentados en el presente informe son sólo referenciales y sirven como base para la elaboración de un perfil eléctrico básico.

3.11.1 Archivos Elementales (EFs) al nivel del Archivo Maestro (MF)

La norma GSM 11.11 define solo dos (02) EF a este nivel, de los cuales el más importante es el archivo elemental EF_{ICCID}.

EF_{ICCID}. Este archivo elemental almacena el número de serie de la tarjeta SIM o Identificador Internacional de la tarjeta de Circuitos (ICCID – Internacional Circuit Card ID). Este archivo permite identificar a la tarjeta SIM de forma no ambigua para propósitos administrativos. El identificador de este archivo elemental es: ‘2FE2’.

El contenido de este archivo deberá estar de acuerdo a lo especificado por la norma E.118. El ICCID puede tener la siguiente estructura:

8	9	CC	CC	MNC	MNC	a	b	c	d	E	f	g	h	i	J	k	l	CHK	F
N1	N2	N3	N4	N5	N6	N7	N8	N9	N10	N11	N12	N13	N14	N15	N16	N17	N18	N19	N20

Tabla 3.2 – Estructura del ICCD.

Donde:

89	Valor por defecto para operadores GSM
CC	Country Code: 51 (Perú)
MNC	Mobile Network Code: 06 (MoviStar) 10 (Claro)
abcdefghijkl	Definido por el operador (puede ser utilizado para definir HLR, fabricante de SIM, identificación del usuario).
CHK	Check Digit (calculado con el algoritmo de Luhn)
F	Valor de Relleno

Tabla 3.3 – Descripción de los componentes del ICCD.

Algunos fabricantes de tarjetas SIM implementan en este nivel archivos elementales que contienen los códigos CHV1 y CHV2. Es necesario tener en cuenta que el acceso al contenido de estos archivos está restringido y protegido por llaves administrativas.

3.11.2 Archivos Elementales (EFs) al nivel de aplicación GSM (DFGSM)

Los archivos elementales (EF) en este nivel contienen información relacionada a la red. Los siguientes EFs son los más importantes:

EF$_{LP}$ (Idioma Preferido). Tiene como identificador ‘6F05’. Este archivo define el idioma preferido por el usuario en orden de prioridad. El operador define uno o más idiomas para este archivo. Por ejemplo se tienen los siguientes códigos:

04	Español
01	Inglés
03	Francés
08	Portugués

Se espera que el terminal tome la lista definida en el presente EF para establecer el idioma en el que presentará las opciones del menú hacia el usuario final.

$\mathbf{EF}_{\mathbf{IMSI}}$ (Identidad Internacional de Usuario Móvil). Su identificador es '6F07'. El IMSI es una identificación única para cada usuario móvil en todas las redes GSM. El IMSI tiene la siguiente estructura:

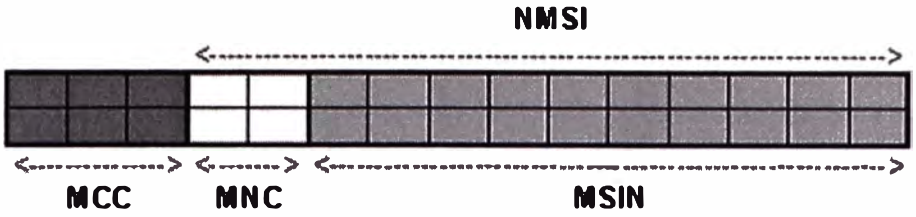


Figura 3.8. Estructura del IMSI

Para el Perú se tiene:

MCC 716

MNC 06 (Movistar) 10 (Claro)

MSIN Administrado por cada operador. Los primeros dígitos del MSIN se generalmente se utilizan para definir el HLR en el cual se encuentran almacenados los datos del suscriptor.

$\mathbf{EF}_{\mathbf{Kc}}$ (Llave de Cifrado Kc). Identificador '6F20'. Contiene la llave de cifrado Kc además del número de secuencia de la llave de cifrado n. El contenido de este archivo tiene una longitud de 9 octetos. Los 8 primeros corresponden a la llave de cifrado Kc. El octeto número 9 corresponde al valor de n, el cual se codifica de la siguiente forma:

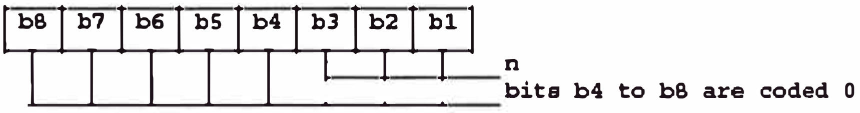


Figura 3.9. Codificación del valor n

La norma GSM 04.08 define el valor de n = '07' como "llave no disponible", por lo tanto el valor inicial de este octeto deberá ser '07' y no 'FF'

En consecuencia se recomienda que el valor inicial de este archivo sea:

FF FF FF FF FF FF FF FF 07

$\mathbf{EF}_{\mathbf{PLMNSel}}$ (Selector de PLMN). Tiene como identificador '6F30'. Utilizado para casos de "roaming". En este archivo elemental (EF) se define la lista de redes preferidas y su prioridad con las que el operador local tiene acuerdos de "roaming". Contiene por lo menos 8 registros. Los registros se codifican de acuerdo a la norma GSM 04.08. Por ejemplo el código de un operador representado por MCC=246 y MNC=81, se codifica como '42' 'F6' '18'.

EF_{SST} (Tabla de Servicios SIM). Su identificador es '6F38'. Este archivo define los servicios que están activados. Si un servicio no está activo entonces el equipo terminal (ME) no deberá seleccionar dicho servicio.

Los servicios definidos para este EF son:

Service n°1 : CHV1 disable function
Service n°2 : Abbreviated Dialling Numbers (ADN)
Service n°3 : Fixed Dialling Numbers (FDN)
Service n°4 : Short Message Storage (SMS)
Service n°5 : Advice of Charge (AoC)
Service n°6 : Capability Configuration Parameters (CCP)
Service n°7 : PLMN selector
Service n°8 : RFU
Service n°9 : MSISDN
Service n°10: Extension1
Service n°11: Extension2
Service n°12: SMS Parameters
Service n°13: Last Number Dialled (LND)
Service n°14: Cell Broadcast Message Identifier
Service n°15: Group Identifier Level 1
Service n°16: Group Identifier Level 2
Service n°17: Service Provider Name
Service n°18: Service Dialling Numbers (SDN)
Service n°19: Extension3
Service n°20: RFU
Service n°21: VGCS Group Identifier List (EF_{VGCS} and EF_{VGCSS})
Service n°22: VBS Group Identifier List (EF_{VBS} and EF_{VBSS})
Service n°23: enhanced Multi-Level Precedence and Pre-emption Service
Service n°24: Automatic Answer for eMLPP
Service n°25: Data download via SMS-CB
Service n°26: Data download via SMS-PP
Service n°27: Menu selection
Service n°28: Call control
Service n°29: Proactive SIM
Service n°30: Cell Broadcast Message Identifier Ranges
Service n°31: Barred Dialling Numbers (BDN)
Service n°32: Extension4
Service n°33: De-personalization Control Keys
Service n°34: Co-operative Network List
Service n°35: Short Message Status Reports
Service n°36: Network's indication of alerting in the MS
Service n°37: Mobile Originated Short Message control by SIM
Service n°38: GPRS
Service n°39: Image (IMG)
Service n°40: SoLSA (Support of Local Service Area)
Service n°41: USSD string data object supported in Call Control
Service n°42: RUN AT COMMAND command
Service n 43: PLMN Selector List with Access Technology
Service n 44: OPLMN Selector List with Access Technology

Service n 45 HPLMN Access Technology
Service n 46: CPBCCH Information
Service n 47: Investigation Scan
Service n°48: Extended Capability Configuration Parameters
Service n°49: MExE

EF$_{SPN}$ (Nombre del Proveedor de Servicios). Identificador ‘6F46’. Este archivo contiene el nombre del operador y los requerimientos apropiados para que el ME lo muestre. La longitud máxima del nombre del operador es de 16 octetos. El nombre del operador se codifica en 7 bits de acuerdo con la norma GSM 03.38.

EF$_{KcGPRS}$ (Llave de Cifrado para GPRS). Identificador ‘6F52’. Contiene la llave de cifrado KcGPRS además del número de secuencia de la llave de cifrado para GPRS n. El contenido de este archivo tiene una longitud de 9 octetos. Los 8 primeros corresponden a la llave de cifrado KcGPRS. El octeto número 9 corresponde al valor de n, el cual se codifica de la siguiente forma:

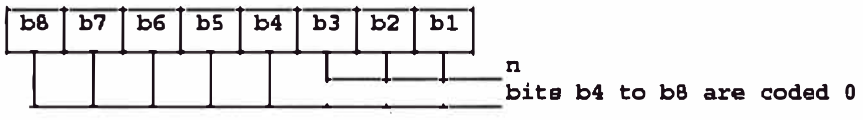


Figura 3.10. Codificación del valor n

La norma GSM 04.08 define el valor de n = ‘07’ como “llave no disponible”, por lo tanto el valor inicial de este octeto deberá ser ‘07’ y no ‘FF’
En consecuencia se recomienda que el valor inicial de este archivo sea:

FF FF FF FF FF FF FF FF 07

EF$_{LOCIGPRS}$ (Información de Localización de GPRS). Identificador ‘6F53’. Contiene la siguiente información de localización de GPRS:

- P-TMSI o Packet Temporary Mobile Subscriber Identity.
- P-TMSI signatura value.
- Routing Area Information.
- Routing Area Update Status.

El contenido del EF$_{LOCIGPRS}$ se codifica de acuerdo a la norma GSM 04.08.

EF$_{SUME}$ (SetUp Menu Elements). Contiene el título del menú de aplicaciones STK. Se codifica de acuerdo con la norma GSM 11.14.

EF$_{ACC}$ (Clase de Control de Acceso). Identificador ‘6F78’. Contiene la clase de control de acceso definida por la norma GSM 02.11, la cual define 15 clases, de las cuales las 10 primeras corresponden a las clases de acceso para usuarios normales (del 0 al 9) y las 5 restantes corresponden a las clases de acceso prioritario (del 11 al 15). Por lo general el valor del ACC es tomado como el último dígito del IMSI.

EF$_{Phase}$ (Identificación de Fase). Identificador ‘6FAE’. Contiene información concerniente a la fase de la tarjeta SIM. Se codifica de la siguiente forma:

'00': Fase 1

'02': Fase 2

'03': Fase 2+

Para las tarjetas SIM utilizadas en la actualidad el valor debe ser ‘03’ ya que permite el uso de aplicaciones STK.

3.11.3 Contenido de los archivos al nivel Telecom (DFTELECOM)

El archivo de directorio DF$_{TELECOM}$ contiene información relacionada a servicios.

EF$_{ADN}$ (Números de Marcación Abreviada). Identificador ‘6F3A’. También conocido como la agenda de la SIM. Se utiliza para almacenar números y nombres asociados a estos. Comúnmente tiene una cantidad máxima de 250 registros (aun cuando el máximo podría ser 255). Usualmente se define una longitud de 16 caracteres para el identificador alfanumérico. La longitud de cada registro es de 30 octetos.

EF$_{FDN}$ (Números de Marcación Fija). Identificador ‘6F3B’. Se utiliza para almacenar prefijos de números permitidos cuando se activa la marcación fija con la clave CHV2. La cantidad de registros depende del operador. Usualmente se define una longitud de 16 caracteres para el identificador alfanumérico. La longitud de cada registro es de 30 octetos.

EF$_{SMS}$ (Servicio de Mensajes Cortos). Identificador ‘6F3C’. Se utiliza para almacenar los mensajes de texto (definidos por la norma GSM 03.40). La cantidad de registros de este EF es determinada por el operador. Algunos terminales no utilizan este EF para almacenar los SMS ya que utilizan su propia memoria.

EF$_{SMSP}$ (Parámetros del Servicio de Mensajes Cortos). Identificador ‘6F42’. En este EF se almacena principalmente el número del centro de servicios SMS hacia el cual se envían los mensajes de texto para que luego sean encaminados hacia el destino.

EF$_{SMSS}$ (Estatus del Servicio SMS). Identificador ‘6F43’. En este EF se almacena información relacionada al estatus del servicio SMS. Tiene dos octetos de los cuales el segundo contiene información en caso al memoria de mensajes de texto SMS haya sido excedida (memoria llena).

EF$_{LND}$ (Últimos Números Marcados). Identificador ‘6F44’. Este EF contiene la lista de números marcados pro el usuario. Es un archivo cíclico.

EF$_{SDN}$ (Números de Marcación de Servicios). Identificador ‘6F49’. Almacena los números de servicios propios del operador (Atención al cliente, buzón de voz, etc.) y los números de servicios regulados (como por ejemplo Bomberos, Defensa Civil, Policía, etc.). Usualmente no son más de 16 números de servicio con una longitud de 16 caracteres para el nombre asociado a cada uno de estos. La longitud de cada registro es de 30 octetos.

CONCLUSIONES

La lista de archivos elementales y su contenido sugerido representa la base fundamental para la elaboración de un perfil eléctrico básico para tarjetas SIM.
Desde el punto de vista del operador la especificación adecuada del perfil eléctrico permite la interoperabilidad con los equipos terminales para que los usuarios puedan utilizar los servicios ofrecidos, no solo el servicio tradicional de comunicación de voz por circuitos sino que además permite el uso de servicios de valor agregado como mensajes de texto SMS y aplicaciones STK. Asimismo como parte de la definición del perfil eléctrico se establecen parámetros como el nombre del operador que se mostrará en las pantallas de los teléfonos de los suscriptores como elemento diferenciador.

Desde el punto de vista del usuario la tarjeta SIM permite tener control de la información personal como son los números almacenados en al agenda (ADN), almacenar los mensajes de texto SMS asi como el acceso a esta información al habilitar el código CHV1 el cual es requerido al momento del encendido.

Finalmente es necesario considerar que al momento de definir la estructura y el contenido de los archivos del sistema de archivos de las tarjetas SIM se define también el tamaño de la memoria que ocupan los mismos lo que permitirá conocer cuánto espacio queda disponible para ser utilizado por aplicaciones interactivas del tipo STK.

ANEXO A

GLOSARIO DE TERMINOS

GLOSARIO DE TERMINOS

3GPP: Third Generation Partnership Project – Proyecto de Alianza para la Tercera Generación, creado para facilitar el desarrollo de especificaciones técnicas abiertas aceptadas para los servicios 3G, al que pertenecen varios organismos de estandarización regionales.

A: Interfaz estándar entre la BSC y el MSC, en las redes GSM.

A-bis: Interfaz entre las BTS y el BSC asociado, en las redes GSM. No está estandarizado por lo que cada fabricante establece su propia norma.

Algoritmo A3: Es un algoritmo que se utiliza en el sistema de telefonía móvil GSM para la autenticación de usuarios.

Algoritmo A5: Es un algoritmo que se utiliza en el sistema de telefonía móvil GSM para la encriptación de la información asociada a las comunicaciones de los usuarios móviles en la interfase aire.

Algoritmo A8: Es un algoritmo que se utiliza en el sistema de telefonía móvil GSM para la generación de las claves de cifrado para la autenticación y encriptación.

AMPS: Advanced Mobile Phone System – Sistema de Telefonía Móvil Avanzada. Estándar móvil analógico desarrollado por los laboratorios Bell en la década de los años 70.

Ancho de Banda: Bandwidth – Capacidad de información de un recurso de comunicaciones, que suele medirse en bits por segundo en caso se utilice un sistema digital.

APN: Access Point Name – Nombre de punto de acceso.

AUC: Authentication Center. Centro de Autenticación.

BS: Base Station – Estación Base.

BSC: Base Station Controller - Controlador de Estación Base.

CDMA: Code Division Multiple Access – El Acceso Múltiple por División de Códigos, es la técnica de acceso múltiple empleada por las interfases de aire CDMAONE (IS-95), CDMA2000 y WCDMA (3G).

Celda: Unidad geográfica de un sistema de comunicación celular. La cobertura del servicio de un área determinada se basa en una red de células entrelazadas, cada una de las cuales tiene en el centro una estación base de radio (transmisor/receptor).

Cifrado: Proceso de transformación de la información, mediante un código y un algoritmo matemático, que la hace ininteligible para todo el que no conozca la clave de la comunicación.

Código PIN: Personal Identification Number – Código de identificación, de cuatro cifras, que tiene cada usuario para acceder a los servicios de su terminal móvil y que se le pide al activarlo. Generalmente los operadores optan por deshabilitar su uso para facilidad de sus usuarios.

Conmutación de circuitos: La base de la gestión de las llamadas telefónicas, en la que se establece una conexión de circuito entre la persona que llama y la que recibe la llamada. Esta conexión se mantiene abierta durante toda la llamada, aun cuando no se esté transmitiendo ninguna información (voz, datos, vídeo). Su alternativa es la conmutación de paquetes.

Conmutación de paquetes: Técnica de transmisión de red central con la que se divide la información en paquetes de datos que se encaminan de forma independiente a través de la red a los largo de distintas rutas, hasta su destino final. En este caso el espectro de radio sólo se utiliza cuando realmente se están transmitiendo datos. Su alternativa es la conmutación de circuitos. GPRS es una tecnología basada en paquetes diseñada para redes móviles digitales.

EDGE (Enhanced Data rates for Global Evolution) – Tasa de Datos Mejorada para la Evolución Mundial. Es una técnica mejorada de modulación de radio para GSM que implementa nuevos esquemas de codificación y modulación basados en 8PSK además de GMSK.

ETSI: European Telecommunications Standards Institute – Instituto Europeo de Estándares de Telecomunicaciones. Su finalidad consiste en establecer estándares que permitan al mercado internacional de las telecomunicaciones funcionar como uno solo. Miembro del 3GPP.

FDMA: Frequency Division Multiple Access – Acceso Múltiple por División de Frecuencia. Técnica para compartir el espectro radioeléctrico, según la cual a cada uno de los usuarios se le adjudica un parte (frecuencia), distinta de la que se asigna a otros.

GGSN: Gateway GPRS Support Node – Nodo de Soporte GPRS de Gateway.

GPRS: General Packet Radio Service – Servicio General de Paquetes por Radio. Mejora de la red GSM que introduce la transmisión de paquetes de datos. Utiliza muy eficazmente el espectro de radio disponible y los usuarios reciben un acceso con un ancho de banda mayor que con una conexión por circuitos. También se puede aplicar a las redes TDMA (ANSI-136).

GSM: Global System for Mobile Communications – Sistema Internacional para Comunicaciones Móviles. Definido inicialmente como un estándar europeo para una red telefónica celular digital que soporte el roaming entre países. GSM es ahora el principal estándar móvil digital en el mundo. Emplea una interfaz aire TDMA.

GTP: GPRS Tunnelling Protocol – Protocolo de Túnel de GPRS.

HLR: Home Location Register – Registro Local de abonados.

HSCSD: High Speed Circuit Switched Data – Especificación de la Fase 2+ de GSM, homologada por la ETSI. Se trata de un servicio multislot de transmisión de datos a alta velocidad mediante conmutación de circuitos. El HSCSD, junto con el esquema de codificación mejorado de 14.4 kbps, permite velocidades de transmisión de datos hasta 57.6 kbps, combinando varios slots de 9.6 kbps ó 14.4 kbps.

IMEI: Internacional Mobile station Equipment Identity – Identidad internacional de equipo móvil.

IMSI: Internacional Mobile Subscriber Identity – Identidad internacional de abonado móvil.

IP: Internet Protocol.

Itinerancia: Roaming – Posibilidad de que un usuario de teléfono móvil ó inalámbrico viaje de red en red, con absoluta continuidad de comunicación.

LA: Location Area – Área de Localización.

LAN: Local Area Network – Red de área local.

MAP: Mobile Application Part – Parte de aplicación móvil.

MMS: Multimedia Messaging Service – Servicio de Mensajes Multimedia. Permite transmitir imágenes en movimiento, gráficos y sonidos, junto con el texto de los mensajes.

MS: Mobile Station – Estación móvil.

MSC: Mobile Switching Center – Central de Conmutación Móviles.

MSISDN: Mobile Station Integrated Service Digital Number – Número ISDN de estación móvil.

PCS: Personal Communications Service – Término genérico para referirse al servicio de comunicaciones personales móviles del mercado masivo, independiente de la tecnología empleada para prestarlo.

PDN: Packet Data Network – Red pública de datos por paquetes.

PDP: Packet Data Protocol – Protocolo de datos por paquetes.

PLMN: Public Land Mobile Network – Red Pública de Comunicaciones Móviles Terrestres.

QoS: Quality of Service – Calidad de Servicio.

Roaming: La itinerancia es una funcionalidad de las redes móviles que permites utilizar los servicios incluso cuando el terminal se encuentra en otra red, distinta a la que se ha suscrito.

SGSN: Serving GPRS Support Node – Nodo servidor de GPRS.

SIM: Subscriber Identity Module – Pequeño circuito impreso colocado en un soporte de plástico que se coloca en el teléfono GSM para que éste pueda ser conectado a la red móvil. La tarjeta SIM desempeña dos funciones primarias en la red GSM: la de control de acceso a la red y la de personalización del servicio. Contiene la información sobre el usuario, la clave de seguridad y la memoria para almacenar números de teléfono.

STK: SIM Application Toolkit: Posibilidad de ejecutar aplicaciones cargadas en las tarjetas SIM.

SMS: Short Message Service – Servicio disponible en las comunicaciones móviles digitales que permite el envío y la recepción de mensajes de etxto a través del centro de mensajes del operador celular.

SS7: Signalling System Number 7 – Sistema de Señalización No. 7.

SSN: Subsystem Number – Número de subsistema.

TCP/IP: Protocolo de datos que se usa en Internet. El primero (TCP) se encarga de dividir en paquetes la información de origen, para luego recomponerla en el destino, mientras que el segundo (IP) se responsabiliza de encaminarla, mediante routers, adecuadamente a través de la red.

TDMA (Time Division Multiple Access): El Acceso Múltiple por División de Tiempo es una técnica digital empleada por las actuales interfases de aire GSM, TDMA y PDC, que asigna períodos temporales distintos (timeslots) a cada una de las comunicaciones.

TMSI: Temporary Mobile Subscriber Identity – Identidad temporal de abonado móvil.

UIT: Unión Internacional de Telecomunicaciones. Órgano de las Naciones Unidas responsable de la coordinación de las actividades internacionales relacionadas con las telecomunicaciones, especialmente en las áreas de definición de estándares, asignación de radio y legislación. Recientemente se ha reestructurado en tres sectores: el de normalización de telecomunicaciones (ITU-T), establecido para gestionar todas las actividades de normalización del antiguo CCITT, el de comunicaciones vía radio (ITU-R), y el sector de desarrollo, que gestiona la asistencia a países en vías de desarrollo en materia de telecomunicaciones.

UMTS: Universal Mobile Telecommunications System – El Sistema Universal de Telecomunicaciones Móviles es el sistema para prestar servicios de tercera generación, que esta dentro del IMT-2000, desarrollado bajo los auspicios del ETSI y dentro del 3GPP.

VLR: Visitor Location Register – Registro de Localización de Visitantes.

WAP: Wireless Application Protocol – El Protocolo de Aplicaciones Inalámbricas es el estándar internacional abierto para el acceso a servicios en línea (Internet) desde terminales móviles de pantalla reducida, empleando cualquier tecnología de acceso de radio.

ANEXO B

NORMA ETSI GSM 11.11

ETSI TS 100 977 V8.3.0 (2000-08)

Technical Specification

Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11 version 8.3.0 Release 1999)

GSM®

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

ETSI

Reference

RTS/SMG-091111Q8R1

Keywords

Digital cellular telecommunications system,
Global System for Mobile communications (GSM)

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at http://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by the Special Mobile Group (SMG).

The present document defines the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) within the digital cellular telecommunications system.

The contents of the present document may be subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of the present document it will then be re-submitted for formal approval procedures by ETSI with an identifying change of release date and an increase in version number as follows:

Version 8.x.y

where:

8 GSM Phase 2+ Release 1999.

x the second digit is incremented for changes of substance, i.e. technical enhancements, corrections, updates, etc..

y the third digit is incremented when editorial only changes have been incorporated in the specification.

1 Scope

The present document defines the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) for use during the network operation phase of GSM as well as those aspects of the internal organization of the SIM which are related to the network operation phase. This is to ensure interoperability between a SIM and an ME independently of the respective manufacturers and operators. The concept of a split of the Mobile Station (MS) into these elements as well as the distinction between the GSM network operation phase, which is also called GSM operations, and the administrative management phase are described in the GSM 02.17 [6].

The present document defines:

the requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;

the model which shall be used as a basis for the design of the logical structure of the SIM;

the security features;

the interface functions;

the commands;

the contents of the files required for the GSM application;

the application protocol.

Unless otherwise stated, references to GSM also apply to DCS 1800 and PCS 1900.

The present document does not specify any aspects related to the administrative management phase. Any internal technical reallocation of either the SIM or the ME are only specified where these reflect over the interface. It does not specify any of the security algorithms which may be used.

The present document defines the SIM/ME interface for GSM Phase 2. While all attempts have been made to maintain phase compatibility, any issues that specifically relate to Phase 1 should be referenced from within the relevant Phase 1 specification.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1999 document, references to GSM documents are for Release 1999 versions (version 8.x.y).

[1] GSM 01.02: "Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network (PLMN)".

[2] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[3] GSM 02.07: "Digital cellular telecommunications system (Phase 2+); Mobile Stations (MS) features".

[4] GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security aspects".

[5] GSM 02.11: "Digital cellular telecommunications system (Phase 2+); Service accessibility".

[6] GSM 02.17: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM) Functional characteristics".

[7] GSM 02.24: "Digital cellular telecommunications system (Phase 2+); Description of Charge Advice Information (CAI)".

[8] GSM 02.30: "Digital cellular telecommunications system (Phase 2+); Man-Machine Interface (MMI) of the Mobile Station (MS)".

[9] GSM 02.86: "Digital cellular telecommunications system (Phase 2+); Advice of charge (AoC) Supplementary Services - Stage 1".

[10] GSM 03.03: "Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification".

[11] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[12] GSM 03.38: "Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information".

[13] GSM 03.40: "Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[14] GSM 03.41: "Digital cellular telecommunications system (Phase 2+); Technical realization of Short Message Service Cell Broadcast (SMSCB)".

[15] GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[16] GSM 04.11: "Digital cellular telecommunications system (Phase 2+); Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[17] GSM 09.91: "Digital cellular telecommunications system (Phase 2+); Interworking aspects of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface between Phase 1 and Phase 2".

[18] CCITT Recommendation E.118: "The international telecommunication charge card".

[19] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[20] CCITT Recommendation T.50: "International Alphabet No. 5". (ISO 646: 1983, "Information processing - ISO 7-bits coded characters set for information interchange".)

[21] ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".

[22] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".

[23] ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

[24] ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[25] ISO/IEC 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".

[26] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[27] GSM 11.14: "Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[28] GSM 11.12: "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[29] GSM 02.22: "Digital cellular telecommunications system (Phase 2+); Personalization of GSM Mobile Equipment (ME) Mobile functionality specification".

[30] ISO 639 (1988): "Code for the representation of names of languages".

[31] ISO/IEC 10646-1 (1993): "Information technology - Universal Multiple-Octet Coded Character Set (UCS) - Part 1: Architecture and Basic Multilingual Plane".

[32] GSM 03.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[33] GSM 03.73: "Digital cellular telecommunications system (Phase 2+); Support of Localised Service Area (SoLSA); Service description; Stage 2".

[34] GSM 11.19: "Digital cellular telecommunications system (Phase 2+); Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station".

[35] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

[36] TIA/EIA-136-005: "Introduction, Identification, and Semi-Permanent Memory, November 1998".

[37] TIA/EIA-136-123-A: "Digital Control Channel Layer 3, November 1998".

[38] TIA/EIA-136-140-A: "Analogue Control Channel, November 1998".

[39] TIA/EIA-136-510-A: "Authentication, Encryption of Signaling Information/User Data and Privacy, November 1998".

[40] ANSI TIA/EIA-41: "Cellular Radio Telecommunications Intersystem Operations".

[41] EIA/TIA-553: "Mobile Station-Land Station Compatibility Specification".

[42] GSM 02.67: "Digital cellular telecommunications system (Phase 2+); Enhanced Multi Level Pre-emption and Priority (eMLPP) Services - Stage 1".

[43] TR45 AHAG "Common Cryptographic Algorithms, Revision C," October 27, 1998.

[44] ETS 300.812: "Terrestrial Trunk Radio; Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[45] GSM 03.22: " Digital cellular telecommunications system (Phase 2+); Functions related to Mobile Station (MS) in idle mode and group receive mode".

[46] GSM 05.05: "Digital cellular telecommunications system (Phase 2+); Radio transmission and reception".

[47] TS 24.008: "Mobile Radio Interface Layer 3 specification, Core Network Protocols".

[48] GSM 04.18: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification, Radio Resource Control Protocol".

[49] GSM 04.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station (MS) - Base Station System (BSS) interface; Radio Link Control/ Medium Access Control (RLC/MAC) protocol".

[50] TS 23.057: "Mobile Station Application Execution Environment (MExE);Functional description; Stage 2".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply. For further information and definitions refer to GSM 01.02 [1].

access conditions: set of security attributes associated with a file.

application: application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols).

application protocol: set of procedures required by the application.

card session: link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card.

current directory: latest MF or DF selected.

current EF: latest EF selected.

data field: obsolete term for Elementary File.

Dedicated File (DF): file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs).

directory: general term for MF and DF.

Elementary File (EF): file containing access conditions and data and no other files.

file: directory or an organized set of bytes or records in the SIM.

file identifier: 2 bytes which address a file in the SIM.

GSM, DCS 1800 or PCS 1900 application: set of security mechanisms, files, data and protocols required by GSM, DCS 1800 or PCS 1900.

GSM session: that part of the card session dedicated to the GSM operation.

IC card SIM: obsolete term for ID-1 SIM.

ID-1 SIM: SIM having the format of an ID-1 card (see ISO 7816-1 [24]).

Master File (MF): unique mandatory file containing access conditions and optionally DFs and/or EFs.

normal GSM operation: relating to general, CHV related, GSM security related and subscription related procedures.

padding: one or more bits appended to a message in order to cause the message to contain the required number of bits or bytes.

plug-in SIM: Second format of SIM (specified in clause 4).

proactive SIM: SIM which is capable of issuing commands to the ME. Part of SIM Application Toolkit (see clause 11).

record: string of bytes within an EF handled as a single entity (see clause 6).

record number: number which identifies a record within an EF.

record pointer: pointer which addresses one record in an EF.

root directory: obsolete term for Master File.

SIM application toolkit procedures: defined in GSM 11.14 [27].

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, in addition to those listed in GSM 01.04 [2]:

A3	Algorithm 3, authentication algorithm; used for authenticating the subscriber
A38	A single algorithm performing the functions of A3 and A8
A5	Algorithm 5, cipher algorithm; used for enciphering/deciphering data
A8	Algorithm 8, cipher key generator; used to generate K_c
ACM	Accumulated Call Meter
ADM	Access condition to an EF which is under the control of the authority which creates this file
ADN	Abbreviated Dialling Number
AHAG	Ad-Hoc Authentication Group
A-Key	Authentication Key
ALW	ALWays
AMPS	Analogue Mobile Phone System
ANSI	American National Standards Institute
AoC	Advice of Charge
APDU	Application Protocol Data Unit
ATR	Answer To Reset
BCCH	Broadcast Control CHannel
BCD	Binary Coded Decimal
BDN	Barred Dialling Number
BTS	Base Transmitter Station
CB	Cell Broadcast
CBMI	Cell Broadcast Message Identifier
CCITT	The International Telegraph and Telephone Consultative Committee (now also known as the ITU Telecommunications Standardization sector)
CCP	Capability/Configuration Parameter
CHV	Card Holder Verification information; access condition used by the SIM for the verification of the identity of the user
CLA	CLAss
CNL	Co-operative Network List
CPBCCH	COMPACT Packet BCCH
CTS	Cordless Telephony System
DCK	De-personalization Control Keys
DCS	Digital Cellular System
DF	Dedicated File (abbreviation formerly used for Data Field)
DTMF	Dual Tone Multiple Frequency
ECC	Emergency Call Code
EF	Elementary File
EIA	Electronics Industries Alliance (North America)
eMLPP	enhanced Multi-Level Precedence and Pre-emption Service
ETSI	European Telecommunications Standards Institute
etu	elementary time unit
FDN	Fixed Dialling Number
GSM	Global System for Mobile communications
HPLMN	Home PLMN
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ID	IDentifier
IEC	International Electrotechnical Commission
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
Kc	Cryptographic key; used by the cipher A5
Ki	Subscriber authentication key; the cryptographic key used by the authentication algorithm, A3, and cipher key generator, A8
LAI	Location Area Information; information indicating a cell or a set of cells
lgth	The (specific) length of a data unit
LND	Last Number Dialled

LSA	Localised Service Area
LSA ID	Localised Service Area Identity
LSB	Least Significant Bit
MCC	Mobile Country Code
ME	Mobile Equipment
MF	Master File
MMI	Man Machine Interface
MNC	Mobile Network Code
MS	Mobile Station
MSB	Most Significant Bit
MSISDN	Mobile Station international ISDN number
NAM	Numeric Assignment Module
NET	NETwork
NEV	NEVer
NPI	Numbering Plan Identifier
OFM	Operational Feature Monitor
OPLMN	Operator Controlled PLMN (Selector List)
OTA	Over The Air
PDC	Personal Digital Communications
PIN/PIN2	Personal Identification Number / Personal Identification Number 2 (obsolete terms for CHV1 and CHV2, respectively)
PLMN	Public Land Mobile Network
PPS	Protocol and Parameter Select (response to the ATR)
PUK/PUK2	PIN Unblocking Key / PIN2 Unblocking Key (obsolete terms for UNBLOCK CHV1 and UNBLOCK CHV2, respectively)
RAND	A RANDom challenge issued by the network
RFU	Reserved for Future Use
SDN	Service Dialling Number
SID	System IDentity
SIM	Subscriber Identity Module
SMS	Short Message Service
SoLSA	Support of Localised Service Area
SRES	Signed RESponse calculated by a SIM
SSC	Supplementary Service Control string
SW1/SW2	Status Word 1 / Status Word 2
TETRA	TErrestrial Trunk RAdio
TIA	Telecommunications Industries Association (North America)
TMSI	Temporary Mobile Subscriber Identity
TON	Type Of Number
TP	Transfer layer Protocol
TPDU	Transfer Protocol Data Unit
TS	Technical Specification
UNBLOCK CHV1/2	value to unblock CHV1/CHV2
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service
VPLMN	Visited PLMN

3.3 Symbols

For the purposes of the present document, the following symbols apply:

Vcc	Supply voltage
Vpp	Programming voltage
'0' to '9' and 'A' to 'F'	the sixteen hexadecimal digits

4 Physical characteristics

Two physical types of SIM are specified. These are the "ID-1 SIM" and the "Plug-in SIM".

The physical characteristics of both types of SIM shall be in accordance with ISO 7816-1,2 [24, 25] unless otherwise specified. The following additional requirements shall be applied to ensure proper operation in the GSM environment.

4.1 Format and layout

The information on the exterior of either SIM should include at least the individual account identifier and the check digit of the IC Card Identification (see clause 10, EF_{ICCID}).

4.1.1 ID-1 SIM

Format and layout of the ID-1 SIM shall be in accordance with ISO 7816-1,2 [24, 25].

The card shall have a polarization mark (see GSM 02.07 [3]) which indicates how the user should insert the card into the ME.

The ME shall accept embossed ID-1 cards. The embossing shall be in accordance with ISO/IEC 7811 [22, 23]. The contacts of the ID-1 SIM shall be located on the front (embossed face, see ISO/IEC 7810 [21]) of the card.

NOTE: Card warpage and tolerances are now specified for embossed cards in ISO/IEC 7810 [21].

4.1.2 Plug-in SIM

The Plug-in SIM has a width of 25 mm, a height of 15 mm, a thickness the same as an ID-1 SIM and a feature for orientation. See figure A.1 in normative annex A for details of the dimensions of the card and the dimensions and location of the contacts.

Annexes A.1 and A.2 of ISO 7816-1 [24] do not apply to the Plug-in SIM.

Annex A of ISO 7816-2 [25] applies with the location of the reference points adapted to the smaller size. The three reference points P1, P2 and P3 measure 7,5 mm, 3,3 mm and 20,8 mm, respectively, from 0. The values in table A.1 of ISO 7816-2 [25] are replaced by the corresponding values of figure A.1.

4.2 Temperature range for card operation

The temperature range for full operational use shall be between -25°C and +70°C with occasional peaks of up to +85°C. "Occasional" means not more than 4 hours each time and not over 100 times during the life time of the card.

4.3 Contacts

4.3.1 Provision of contacts

ME: Contacting elements in the ME in positions C4 and C8 are optional, and are not used in the GSM application. They shall present a high impedance to the SIM card in the GSM application. If it is determined that the SIM is a multi-application ICC, then these contacts may be used. Contact C6 need not be provided for Plug-in SIMs.

SIM: Contacts C4 and C8 need not be provided by the SIM, but if they are provided, then they shall not be connected internally in the SIM if the SIM only contains the GSM application. Contact C6 shall not be bonded in the SIM for any function other than supplying Vpp.

4.3.2 Activation and deactivation

The ME shall connect, activate and deactivate the SIM in accordance with the Operating Procedures specified in ISO/IEC 7816-3 [26].

For any voltage level, monitored during the activation sequence, or during the deactivation sequence following soft power-down, the order of the contact activation/deactivation shall be respected.

NOTE 1: Soft Power switching is defined in GSM 02.07 [3].

NOTE 2: It is recommended that whenever possible the deactivation sequence defined in ISO/IEC 7816-3 [26] should be followed by the ME on all occasions when the ME is powered down.

If the SIM clock is already stopped and is not restarted, the ME is allowed to deactivate all the contacts in any order, provided that all signals reach low level before Vcc leaves high level. If the SIM clock is already stopped and is restarted before the deactivation sequence, then the deactivation sequence specified in ISO/IEC 7816-3 [26] subclause 5.4 shall be followed.

When Vpp is connected to Vcc, as allowed by GSM (see clause 5), then Vpp will be activated and deactivated with Vcc, at the time of the Vcc activation/deactivation, as given in the sequences of ISO/IEC 7816-3 [26] subclauses 5.2 and 5.4.

Vcc is powered when it has a value between 4,5 V and 5,5 V.

4.3.3 Inactive contacts

The voltages on contacts C1, C2, C3, C6 and C7 of the ME shall be between 0 and ± 0,4 volts referenced to ground (C5) when the ME is switched off with the power source connected to the ME. The measurement equipment shall have a resistance of 50 kohms when measuring the voltage on C2, C3, C6 and C7. The resistance shall be 10 kohms when measuring the voltage on C1.

4.3.4 Contact pressure

The contact pressure shall be large enough to ensure reliable and continuous contact (e.g. to overcome oxidisation and to prevent interruption caused by vibration). The radius of any curvature of the contacting elements shall be greater than or equal to 0,8 mm over the contact area.

Under no circumstances may a contact force be greater than 0,5 N per contact.

Care shall be taken to avoid undue point pressure to the area of the SIM opposite to the contact area. Otherwise this may damage the components within the SIM.

4.4 Precedence

See GSM 02.17 [6] for precedence.

4.5 Static Protection

Considering that the SIM is a CMOS device, the ME manufacturer shall take adequate precautions (in addition to the protection diodes inherent in the SIM) to safeguard the ME, SIM and SIM/ME interface from static discharges at all times, and particularly during SIM insertion into the ME.

5 Electronic signals and transmission protocols

Electronic signals and transmission protocols shall be in accordance with ISO/IEC 7816-3 [26] unless specified otherwise. The following additional requirements shall be applied to ensure proper operation in the GSM environment.

The choice of the transmission protocol(s), to be used to communicate between the SIM and the ME, shall at least include that specified and denoted by T=0 in ISO/IEC 7816-3 [26].

The values given in the tables hereafter are derived from ISO/IEC 7816-3 [26], subclause 4.3 with the following considerations:

- V_{OH} and V_{OL} always refer to the device (ME or SIM) which is driving the interface. V_{IH} and V_{IL} always refer to the device (ME or SIM) which is operating as a receiver on the interface.
- this convention is different to the one used in ISO/IEC 7816-3 [26], which specifically defines an ICC for which its current conventions apply. The following clauses define the specific core requirements for the SIM, which provide also the basis for Type Approval. For each state (V_{OH}, V_{IH}, V_{IL} and V_{OL}) a positive current is defined as flowing out of the entity (ME or SIM) in that state.

5.1 Supply voltage Vcc (contact C1)

The SIM shall be operated within the following limits.

Table 1: Electrical characteristics of Vcc under normal operating conditions

Symbol	Minimum	Maximum	Unit
Vcc	4,5	5,5	V
Icc		10	mA

The current consumption of the SIM shall not exceed the value given in table 1 during any state (including activation and deactivation as defined in subclause 4.3.2).

When the SIM is in idle state (see below) the current consumption of the card shall not exceed 200 µA at 1 MHz and 25°C. If clock stop mode is allowed, then the current consumption shall also not exceed 200 µA while the clock is stopped.

The ME shall source the maximum current requirements defined above. It shall also be able to counteract spikes in the current consumption of the card up to a maximum charge of 40 nAs with no more than 400 ns duration and an amplitude of at most 200 mA, ensuring that the supply voltage stays in the specified range.

NOTE: A possible solution would be to place a capacitor (e.g. 100 nF, ceramic) as close as possible to the contacting elements.

5.2 Reset (RST) (contact C2)

The ME shall operate the SIM within the following limits.

Table 2: Electrical characteristics of RST under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{OH}	I_{OHmax} = +20 µA	Vcc-0,7	Vcc (note)
V_{OL}	I_{OLmax} = -200 µA	0V (note)	0,6 V
t_R t_F	C_{out} = C_{in} = 30 pF		400 µs
NOTE: To allow for overshoot the voltage on RST shall remain between -0,3 V and Vcc+0,3 V during dynamic operation.			

5.3 Programming voltage Vpp (contact C6)

SIMs shall not require any programming voltage on Vpp. The ME need not provide contact C6. If the ME provides contact C6, then, in the case of the ID-1 SIM the same voltage shall be supplied on Vpp as on Vcc, while in the case of Plug-in SIMs the ME need not provide any voltage on C6. Contact C6 may be connected to Vcc in any ME but shall not be connected to ground.

5.4 Clock CLK (contact C3)

The SIM shall support 1 MHz to 5 MHz. The clock shall be supplied by the ME. No "internal clock" SIMs shall be used.

If a frequency of 13/4 MHz is needed by the SIM to run the authentication procedure in the allotted time (see GSM 03.20 [11]), or to process an ENVELOPE command used for SIM Data Download, bit 2 of byte 1 in the file characteristics shall be set to 1. Otherwise a minimum frequency of 13/8 MHz may be used.

The duty cycle shall be between 40 % and 60 % of the period during stable operation.

The ME shall operate the SIM within the following limits:

Table 3: Electrical characteristics of CLK under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{OH}	I_{OHmax} = +20 µA	0,7xVcc	Vcc (note)
V_{OL}	I_{OLmax} = -200 µA	0 V (note)	0,5 V
t_R t_F	C_{out} = C_{in} = 30 pF		9 % of period with a maximum of 0,5 µs
NOTE: To allow for overshoot the voltage on CLK shall remain between -0,3 V and Vcc+0,3 V during dynamic operation.			

5.5 I/O (contact C7)

Table 4 defines the electrical characteristics of the I/O (contact C7). The values given in the table have the effect of defining the values of the pull-up resistor in the ME and the impedances of the drivers and receivers in the ME and SIM.

Table 4: Electrical characteristics of I/O under normal operating conditions

Symbol	Conditions	Minimum	Maximum
V_{IH}	I_{IHmax} = ± 20 µA (note 2)	0,7xVcc	Vcc+0,3 V
V_{IL}	I_{ILmax} = +1 mA	-0,3 V	0,8 V
V_{OH} (note 1)	I_{OHmax} = + 20µA	3,8 V	Vcc (note 3)
V_{OL}	I_{OLmax} = -1 mA	0 V (note 3)	0,4 V
t_R t_F	C_{out} = C_{in} = 30 pF		1 µs
NOTE 1: It is assumed that a pull-up resistor is used in the interface device (recommended value: 20 kohms).			
NOTE 2: During static conditions (idle state) only the positive value can apply. Under dynamic operating conditions (transmission) short term voltage spikes on the I/O line may cause a current reversal.			
NOTE 3: To allow for overshoot the voltage on I/O shall remain between -0,3 V and Vcc+0,3 V during dynamic operation.			

5.6 States

There are two states for the SIM while the power supply is on:

- the SIM is in operating state when it executes a command. This state also includes transmission from and to the ME;
- the SIM is in idle state at any other time. It shall retain all pertinent data during this state.

The SIM may support a clock stop mode. The clock shall only be switched off subject to the conditions specified in the file characteristics (see clause 9).

Clock stop mode. An ME of Phase 2 or later shall wait at least 1 860 clock cycles after having received the last character, including the guard time (2 etu), of the response before it switches off the clock (if it is allowed to do so). It shall wait at least 744 clock cycles before it sends the first command after having started the clock.

To achieve phase compatibility, the following procedure shall be adhered to:

- a SIM of Phase 2 or later shall always send the status information "normal ending of the command" after the successful interpretation of the command SLEEP received from a Phase 1 ME. An ME of Phase 2 or later shall not send a SLEEP command;
- a Phase 1 ME shall wait at least 744 clock cycles after having received the compulsory acknowledgement SW1 SW2 of the SLEEP command before it switches off the clock (if it is allowed to do so). It shall wait at least 744 clock cycles before it sends the first command after having started the clock.

5.7 Baudrate

The initial baudrate (during ATR) shall be: (clock frequency)/372. Subsequent baudrate shall be: (clock frequency)/372 unless the PPS procedure has been successfully performed. In that case the negotiated baudrate shall be applied according to subclause 5.8.2.

5.8 Answer To Reset (ATR)

The ATR is information presented by the SIM to the ME at the beginning of the card session and gives operational requirements.

5.8.1 Structure and contents

The following table gives an explanation of the characters specified in ISO/IEC 7816-3 [26] and the requirements for their use in GSM. The answer to reset consists of at most 33 characters. The ME shall be able to receive interface characters for transmission protocols other than T=0, historical characters and a check byte, even if only T=0 is used by the ME.

Table 5: ATR

Character	Contents	sent by the card	a) evaluation by the ME b) reaction by the ME
1. Initial character TS	coding convention for all subsequent characters (direct or inverse convention)	always	a) always b) using appropriate convention
2. Format character T0	subsequent interface characters, number of historical characters	always	a) always b) identifying the subsequent characters accordingly
3. Interface character (global) TA1	parameters to calculate the work etu	optional	a) always if present b) if TA1 is not '11' or '01', PPS procedure shall be used (see subclause 5.8.2)
4. Interface character (global) TB1	parameters to calculate the programming voltage and current	optional	a) always if present b) if PI1 is not 0, then reject the SIM (in accordance with subclause 5.10)
5. Interface character (global) TC1	parameters to calculate the extra guardtime requested by the card; no extra guardtime is used to send characters from the card to the ME	optional	a) always if present b) if TC1 is neither 0 nor 255, then reject the SIM (in accordance with subclause 5.10); see the note after the table
6. Interface character TD1	protocol type; indicator for the presence of interface characters, specifying rules to be used for transmissions with the given protocol type	always, if T=15 indicated in TDi (i>1)	a) always if present b) identifying the subsequent characters accordingly
7. Interface character (specific) TA2	not used for protocol T=0	optional	a) optional b) ――
8. Interface character (global) TB2	parameter to calculate the programming voltage	never	the allowed value of TB1 above defines that an external programming voltage is not applicable
9. Interface character (specific) TC2	parameters to calculate the work waiting time	optional	a) always if present b) using the work waiting time accordingly
10. Interface character TDi (i>1)	protocol type; indicator for the presence of interface characters, specifying rules to be used for transmissions with the given protocol type	optional	a) always if present b) identifying the subsequent characters accordingly

(continued)

Table 5 (concluded): ATR

Character	Contents	sent by the card	a) evaluation by the ME b) reaction by the ME
11. Interface character TAi, TBi, TCi (i>2)	characters which contain interface characters for other transmission protocols. If TD(i-1) indicates T=15, TAi is interpreted as global interface character	Always if TD(i-1) indicates T=15. Optional otherwise.	a) always b) If T=15 is indicated in TD(i-1), TAi indicates: XI clock stop indicator (b8 to b7) UI class indicator (b6 to b1)
12. Historical characters T1,...,TK	contents not specified in ISO/IEC	optional	a) optional b) ——
13. Check character TCK	check byte (exclusive -ORing)	not sent if only T=0 is indicated in the ATR. If T=0 and T=15 are present and in all other cases, TCK shall be sent	a) optional b) ——
NOTE:	According to ISO/IEC 7816-3:1997 [26], N=255 indicates that the minimum delay is 12 etu for the asynchronous half-duplex character transmission protocol. If '01' is indicated in TA1, PPS should be supported by the SIM to allow backward compatibility with existing MEs. For the interpretation of '01', see ISO/IEC 7816-3 [26].		

5.8.2 PPS procedure

Specifically related to this Technical Specification the PPS procedure according to ISO/IEC 7816-3 [26], clause 7, is applied, only if TA1 is not equal to '11' or '01', as follows:

a) for MEs only supporting default speed (F=372, D=1)

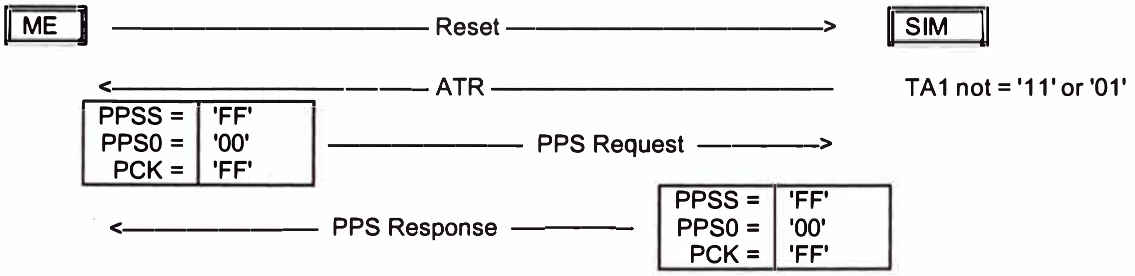


Figure 1: PPS procedure

PPS Request and PPS Response consist of the three (3) characters PPSS, PPSO and PCK of which PPSS is sent first.

After this procedure the protocol T=0 and the parameters F=372, D=1 and N=0 shall be used.

b) for MEs only supporting enhanced speed (F=512, D=8)

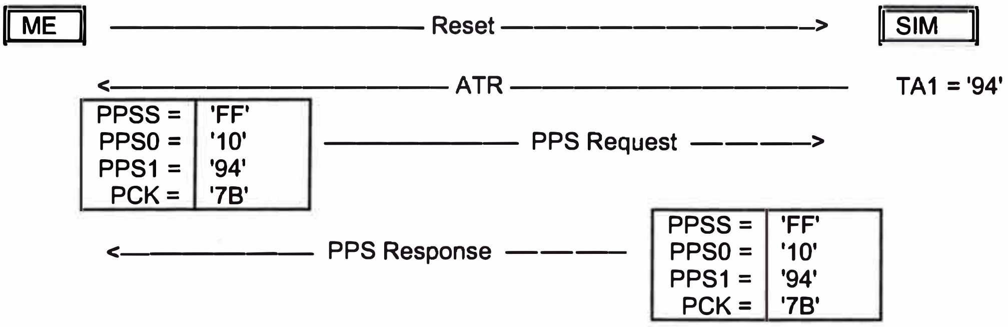


Figure 2: PPS procedure requesting enhanced speed values (F=512, D=8, see clause 5.8.3)

PPS Request and PPS Response consist of the four (4) characters PPSS, PPSO, PPS1 and PCK, of which PPSS is sent first.

After this procedure, the protocol T=0 and the parameters F=512, D=8 and N=0 shall be used.

5.8.3 Speed enhancement

If speed enhancement is implemented, the ME and the SIM shall at least support F=512 and D=8 in addition to F=372 and D=1. However, other values may also be supported. If the ME requests PPS using values other than those above then the PPS procedure shall be initiated accordingly.

The SIM shall support the default value (F=372 and D=1). If the speed enhancement is supported by the SIM it is mandatory that F=512 and D=8 is supported. However, the value in TA1 may even indicate a faster speed (F=512 and D=16). The SIM may also support other values between the default value (F=372 and D=1) and the values indicated in TA1. The SIM shall offer the negotiable mode, to ensure backwards compatibility with existing MEs. In the negotiable mode the SIM will use default values even if other parameters are offered in the ATR if the PPS procedure is not initiated.

The ME shall support the default value (F=372 and D=1). If the speed enhancement is supported in the ME it is mandatory to support F=512 and D=8. The ME may additionally support other values.

If the SIM does not answer the PPS request within the initial waiting time the ME shall reset the SIM. After two failed PPS attempts using F=512 and D=8 or values indicated in TA1, (no PPS response from the SIM) the ME shall initiate PPS procedure using default values. If this also fails (no PPS response from the SIM) the ME may proceed using default values without requesting PPS.

If the SIM does not support the values requested by the ME, the SIM shall respond to the PPS request indicating the use of default values.

5.9 Bit/character duration and sampling time

The bit/character duration and sampling time specified in ISO/IEC 7816-3 [26], subclause 6.3.2 are valid for all communications.

5.10 Error handling

Following receipt of an ATR, which is not in accordance with this specification, e.g. because of forbidden ATR characters or too few bytes being transmitted, the ME shall perform a Reset. The ME shall not reject the SIM until at least three consecutive wrong ATRs are received.

During the transmission of the ATR and the protocol type selection, the error detection and character repetition procedure specified in ISO/IEC 7816-3 [26], subclause 6.3.3, is optional for the ME. For the subsequent transmission on the basis of T=0 this procedure is mandatory for the ME.

For the SIM the error detection and character repetition procedure is mandatory for all communications.

6 Logical Model

This clause describes the logical structure for a SIM, the code associated with it, and the structure of files used.

6.1 General description

Figure 3 shows the general structural relationships which may exist between files. The files are organized in a hierarchical structure and are of one of three types as defined below. These files may be either administrative or application specific. The operating system handles the access to the data stored in different files.

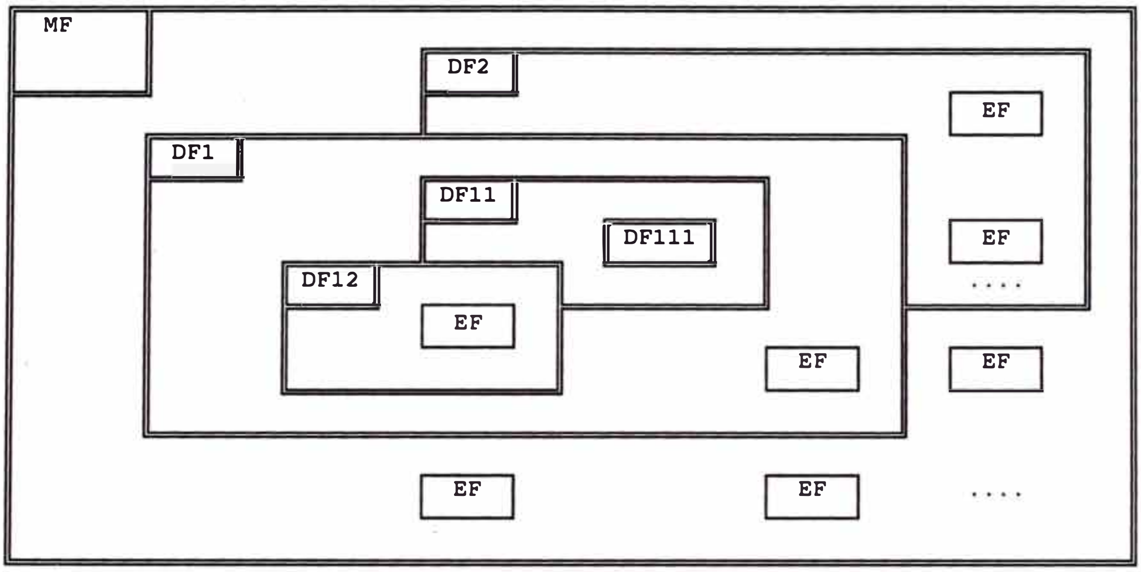


Figure 3: Organization of memory

Files are composed of a header, which is internally managed by the SIM, and optionally a body part. The information of the header is related to the structure and attributes of the file and may be obtained by using the commands GET RESPONSE or STATUS. This information is fixed during the adminisrative phase. The body part contains the data of the file.

6.2 File identifier

A file ID is used to address or identify each specific file. The file ID consists of two bytes and shall be coded in hexadecimal notation. They are specified in clause 10.

The first byte identifies the type of file, and for GSM is:

- '3F': Master File;
- '7F': 1st level Dedicated File;
- '5F': 2nd level Dedicated File;
- '2F': Elementary File under the Master File;

  '6F': Elementary File under a 1st level Dedicated File;
- '4F': Elementary File under 2nd level Dedicated File.

File IDs shall be subject to the following conditions:

- the file ID shall be assigned at the time of creation of the file concerned;
- no two files under the same parent shall have the same ID;
- a child and any parent, either immediate or remote in the hierarchy, e.g. grandparent, shall never have the same file ID.

In this way each file is uniquely identified.

6.3 Dedicated files

A Dedicated File (DF) is a functional grouping of files consisting of itself and all those files which contain this DF in their parental hierarchy (that is to say it consists of the DF and its complete "subtree"). A DF "consists" only of a header part.

Four 1st level DFs are defined in this specification:

- DF$_{GSM}$ which contains the applications for both GSM and/or DCS 1800;
- DF$_{IS41}$ which contains the applications for IS-41 as specified by ANSI T1P1;
- DF$_{TELECOM}$ which contains telecom service features;
- DF$_{FP\text{-}CTS}$ which contains the applications for the CTS fixed part (see GSM 11.19 [34]).

All four files are immediate children of the Master File (MF) and may coexist on a multi-application card.

2nd level DFs are defined in this specification under DF$_{GSM}$.

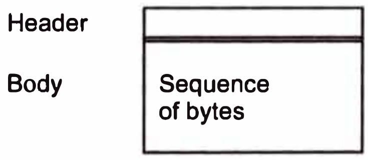
All 2nd level DFs are immediate children of the DF$_{GSM}$ and may coexist on a multi-application card.

6.4 Elementary files

An Elementary File (EF) is composed of a header and a body part. The following three structures of an EF are used by GSM.

6.4.1 Transparent EF

An EF with a transparent structure consists of a sequence of bytes. When reading or updating, the sequence of bytes to be acted upon is referenced by a relative address (offset), which indicates the start position (in bytes), and the number of bytes to be read or updated. The first byte of a transparent EF has the relative address '00 00'. The total data length of the body of the EF is indicated in the header of the EF.



NOTE: This structure was previously referred to as "binary" in GSM.

Figure 4: Structure of a transparent EF

6.4.2 Linear fixed EF

An EF with linear fixed structure consists of a sequence of records all having the same (fixed) length. The first record is record number 1. The length of a record as well as this value multiplied by the number of records are indicated in the header of the EF.

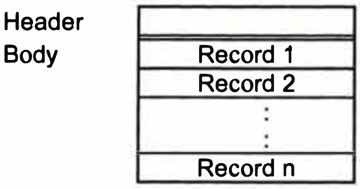


Figure 5: Structure of a linear fixed file

There are several methods to access records within an EF of this type:

absolutely using the record number;

- when the record pointer is not set it shall be possible to perform an action on the first or the last record by using the NEXT or PREVIOUS mode;
- when the record pointer is set it shall be possible to perform an action on this record, the next record (unless the record pointer is set to the last record) or the previous record (unless the record pointer is set to the first record);

by identifying a record using pattern seek starting:

forwards from the beginning of the file;

forwards from the record following the one at which the record pointer is set (unless the record pointer is set to the last record);

- backwards from the end of the file;

backwards from the record preceding the one at which the record pointer is set (unless the record pointer is set to the first record).

If an action following selection of a record is aborted, then the record pointer shall remain set at the record at which it was set prior to the action. According to ISO/IEC 7816-4 [35] it is not possible to have more than 254 records in a file of this type, and each record can not be more than 255 bytes using the short command APDU format.

NOTE: This structure was previously referred to as "formatted" in GSM.

6.4.3 Cyclic EF

Cyclic files are used for storing records in chronological order. When all records have been used for storage, then the next storage of data shall overwrite the oldest information.

An EF with a cyclic structure consists of a fixed number of records with the same (fixed) length. In this file structure there is a link between the last record (n) and the first record. When the record pointer is set to the last record n, then the next record is record 1. Similarly, when the record pointer is set to record 1, then the previous record is record n. The last updated record containing the newest data is record number 1, and the oldest data is held in record number n.

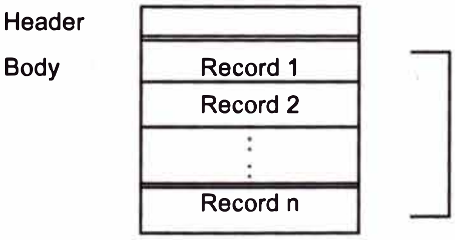


Figure 6: Structure of a cyclic file

For update operations only PREVIOUS record shall be used. For reading operations, the methods of addressing are Next, Previous, Current and Record Number.

After selection of a cyclic file (for either operation), the record pointer shall address the record updated or increased last. If an action following selection of a record is aborted, then the record pointer shall remain set at the record at which it was set prior to the action.

NOTE: It is not possible, at present, to have more than 255 records in a file of this type, and each record cannot be greater than 255 bytes.

6.5 Methods for selecting a file

After the Answer To Reset (ATR), the Master File (MF) is implicitly selected and becomes the Current Directory. Each file may then be selected by using the SELECT function in accordance with the following rules.

Selecting a DF or the MF sets the Current Directory. After such a selection there is no current EF. Selecting an EF sets the current EF and the Current Directory remains the DF or MF which is the parent of this EF. The current EF is always a child of the Current Directory.

Any application specific command shall only be operable if it is specific to the Current Directory.

The following files may be selected from the last selected file:

- any file which is an immediate child of the Current Directory;
- any DF which is an immediate child of the parent of the current DF;
- the parent of the Current Directory;
- the current DF;
- the MF.

This means in particular that a DF shall be selected prior to the selection of any of its EFs. All selections are made using the file ID.

The following figure gives the logical structure for the GSM application. GSM defines only two levels of DFs under the MF.

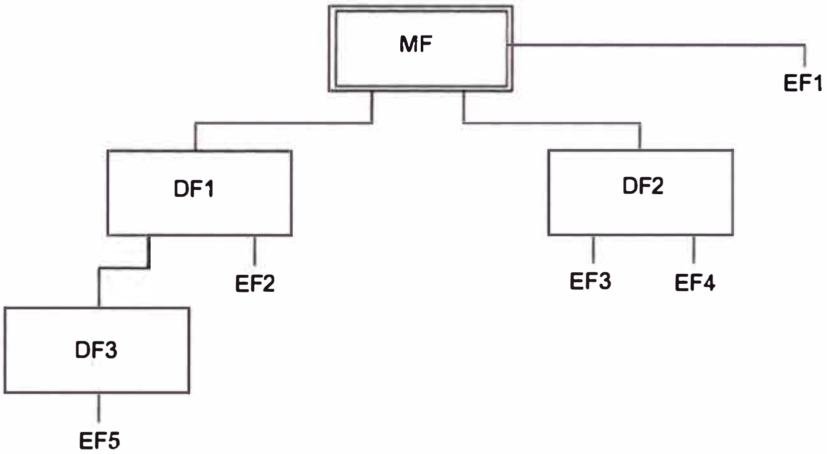


Figure 7: Logical structure

The following table gives the valid selections for GSM for the logical structure in figure 7. Reselection of the last selected file is also allowed but not shown.

Table 6: File selection

Last selected file	Valid Selections
MF	DF1, DF2, EF1
DF1	MF, DF2, DF3, EF2
DF2	MF, DF1, EF3, EF4
DF3	MF, DF1, EF5
EF1	MF, DF1, DF2
EF2	MF, DF1, DF2, DF3
EF3	MF, DF1, DF2, EF4
EF5	MF, DF1, DF3

6.6 Reservation of file IDs

In addition to the identifiers used for the files specified in the present document, the following file IDs are reserved for use by GSM.

Dedicated Files:

- administrative use:

  '7F 4X', '5F1X', '5F2X'

- operational use:

  '7F 10' ($DF_{TELECOM}$), '7F 20' (DF_{GSM}), '7F 21' ($DF_{DCS1800}$), '7F 22' (DF_{IS-41}), '7F 23' (DF_{FP-CTS}) (see GSM 11.19 [34]), '7F 24' ($DF_{TIA/EIA-136}$), '7F 25' ($DF_{TIA/EIA-95}$), and '7F 2X', where X ranges from '6' to 'F'.

NOTE: '7F 80' (DF_{PDC}) is used in the Japanese PDC specification.
'7F 90' (DF_{TETRA}) is used in the ETSI TETRA specification [44].

- reserved under '7F10':

  '5F50' ($DF_{GRAPHICS}$)

  reserved under '7F20':

  '5F30' ($DF_{IRIDIUM}$), '5F31' ($DF_{Globalstar}$), '5F32' (DF_{ICO}), '5F33' (DF_{ACeS}), '5F3C' (DF_{MExE}), '5F3X', where X ranges from '4' to 'B' and 'D' to 'F';

  '5F40'($DF_{EIA/TIA-553}$), '5F4Y' where Y ranges from '1' to 'F';

  '5F5X' where X ranges from '0' to 'F';

  '5F60'(DF_{CTS}), '5F6Y' where Y ranges from '1' to 'F';

  '5F70' (DF_{SoLSA}), '5F7Y' where Y ranges from '1' to 'F';

  '5FYX' where Y ranges from '8' to 'F' and X from '0' to 'F'.

Elementary files:

- administrative use:

  '6F XX' in the DFs '7F 4X'; '4F XX' in the DFs '5F 1X', '5F2X'

  '6F 1X' in the DFs '7F 10', '7F 20', '7F 21';

  '4F 1X' in all 2nd level DFs

  '2F 01', '2F EX' in the MF '3F 00';

- operational use:

  '6F 2X', '6F 3X', '6F 4X' in '7F 10' and '7F 2X';

'4F YX', where Y ranges from '2' to 'F' in all 2nd level DFs.

'2F 1X' in the MF '3F 00'.

In all the above, X ranges, unless otherwise stated, from '0' to 'F'.

7 Security features

The security aspects of GSM are described in the normative references GSM 02.09 [4] and GSM 03.20 [11]. This clause gives information related to security features supported by the SIM to enable the following:

- authentication of the subscriber identity to the network;
- data confidentiality over the radio interface;
- file access conditions.

7.1 Authentication and cipher key generation procedure

This subclause describes the authentication mechanism and cipher key generation which are invoked by the network. For the specification of the corresponding procedures across the SIM/ME interface see clause 11.

The network sends a Random Number (RAND) to the MS. The ME passes the RAND to the SIM in the command RUN GSM ALGORITHM. The SIM returns the values SRES and Kc to the ME which are derived using the algorithms and processes given below. The ME sends SRES to the network. The network compares this value with the value of SRES which it calculates for itself. The comparison of these SRES values provides the authentication. The value Kc is used by the ME in any future enciphered communications with the network until the next invocation of this mechanism.

A subscriber authentication key Ki is used in this procedure. This key Ki has a length of 128 bits and is stored within the SIM for use in the algorithms described below.

7.2 Algorithms and processes

The names and parameters of the algorithms supported by the SIM are defined in GSM 03.20 [11]. These are:

- Algorithm A3 to authenticate the MS to the network;
- Algorithm A8 to generate the encryption key.

These algorithms may exist either discretely or combined (into A38) within the SIM. In either case the output on the SIM/ME interface is 12 bytes. The inputs to both A3 and A8, or A38, are Ki (128 bits) internally derived in the SIM, and RAND (128 bits) across the SIM/ME interface. The output is SRES (32 bits)/Kc (64 bits) the coding of which is defined in the command RUN GSM ALGORITHM in clause 9.

7.3 File access conditions

Every file has its own specific access condition for each command. The relevant access condition of the last selected file shall be fulfilled before the requested action can take place.

For each file:

- the access conditions for the commands READ and SEEK are identical;
- the access conditions for the commands SELECT and STATUS are ALWays.

No file access conditions are currently assigned by GSM to the MF and the DFs.

The access condition levels are defined in the following table:

Table 7: Access condition level coding

Level	Access Condition
0	ALWays
1	CHV1
2	CHV2
3	Reserved for GSM Future Use
4 to 14	ADM
15	NEVer

The meaning of the file access conditions is as follows:

ALWAYS: The action can be performed without any restriction;

CHV1 (card holder verification 1): The action shall only be possible if one of the following three conditions is fulfilled:

a correct CHV1 value has already been presented to the SIM during the current session;

the CHV1 enabled/disabled indicator is set to "disabled";

NOTE: Some Phase 1 and Phase 2 SIMs do not necessarily grant access when CHV1 is "disabled" and "blocked".

- UNBLOCK CHV1 has been successfully performed during the current session;

CHV2: The action shall only be possible if one of the following two conditions is fulfilled:

a correct CHV2 value has already been presented to the SIM during the current session;

- UNBLOCK CHV2 has been successfully performed during the current session;

ADM: Allocation of these levels and the respective requirements for their fulfilment are the responsibility of the appropriate administrative authority

The definition of access condition ADM does not preclude the administrative authority from using ALW, CHV1, CHV2 and NEV if required.

NEVER: The action cannot be performed over the SIM/ME interface. The SIM may perform the action internally.

Condition levels are not hierarchical. For instance, correct presentation of CHV2 does not allow actions to be performed which require presentation of CHV1. A condition level which has been satisfied remains valid until the end of the GSM session as long as the corresponding secret code remains unblocked, i.e. after three consecutive wrong attempts, not necessarily in the same card session, the access rights previously granted by this secret code are lost immediately. A satisfied CHV condition level applies to both DF_{GSM} and $DF_{TELECOM}$.

The ME shall determine whether CHV2 is available by using the response to the STATUS command. If CHV2 is "not initialized" then CHV2 commands, e.g. VERIFY CHV2, shall not be executable.

8 Description of the functions

This clause gives a functional description of the commands and their respective responses. Associated status conditions, error codes and their corresponding coding are specified in clause 9.

It shall be mandatory for all cards complying with this Standard to support all functions described in this Standard. The command GET RESPONSE which is needed for the protocol T=0 is specified in clause 9.

The following table lists the file types and structures together with the functions which may act on them during a GSM session. These are indicated by an asterisk (*).

Table 8: Functions on files in GSM session

	File				
Function	MF	DF	EF transparent	EF linear fixed	EF cyclic
SELECT	*	*	*	*	*
STATUS	*	*	*	*	*
READ BINARY			*		
UPDATE BINARY			*		
READ RECORD				*	*
UPDATE RECORD				*	*
SEEK				*	
INCREASE					*
INVALIDATE			*	*	*
REHABILITATE			*	*	*

8.1 SELECT

This function selects a file according to the methods described in clause 6. After a successful selection the record pointer in a linear fixed file is undefined. The record pointer in a cyclic file shall address the last record which has been updated or increased.

Input:

- file ID.

Output:

- if the selected file is the MF or a DF:

  file ID, total memory space available, CHV enabled/disabled indicator, CHV status and other GSM specific data;

- if the selected file is an EF:

  file ID, file size, access conditions, invalidated/not invalidated indicator, structure of EF and length of the records in case of linear fixed structure or cyclic structure.

8.2 STATUS

This function returns information concerning the current directory. A current EF is not affected by the STATUS function. It is also used to give an opportunity for a pro-active SIM to indicate that the SIM wants to issue a SIM Application Toolkit command to the ME.

Input:

- none.

Output:

- file ID, total memory space available, CHV enabled/disabled indicator, CHV status and other GSM specific data (identical to SELECT above).

8.3 READ BINARY

This function reads a string of bytes from the current transparent EF. This function shall only be performed if the READ access condition for this EF is satisfied.

Input:

- relative address and the length of the string.

Output:

- string of bytes.

8.4 UPDATE BINARY

This function updates the current transparent EF with a string of bytes. This function shall only be performed if the UPDATE access condition for this EF is satisfied. An update can be considered as a replacement of the string already present in the EF by the string given in the update command.

Input:

- relative address and the length of the string;
- string of bytes.

Output:

- none.

8.5 READ RECORD

This function reads one complete record in the current linear fixed or cyclic EF. The record to be read is described by the modes below. This function shall only be performed if the READ access condition for this EF is satisfied. The record pointer shall not be changed by an unsuccessful READ RECORD function.

Four modes are defined:

CURRENT: The current record is read. The record pointer is not affected.

ABSOLUTE: The record given by the record number is read. The record pointer is not affected.

NEXT: The record pointer is incremented before the READ RECORD function is performed and the pointed record is read. If the record pointer has not been previously set within the selected EF, then READ RECORD (next) shall read the first record and set the record pointer to this record.

If the record pointer addresses the last record in a linear fixed EF, READ RECORD (next) shall not cause the record pointer to be changed, and no data shall be read.

If the record pointer addresses the last record in a cyclic EF, READ RECORD (next) shall set the record pointer to the first record in this EF and this record shall be read.

PREVIOUS: The record pointer is decremented before the READ RECORD function is performed and the pointed record is read. If the record pointer has not been previously set within the selected EF, then READ RECORD (previous) shall read the last record and set the record pointer to this record.

If the record pointer addresses the first record in a linear fixed EF, READ RECORD (previous) shall not cause the record pointer to be changed, and no data shall be read.

If the record pointer addresses the first record in a cyclic EF, READ RECORD (previous) shall set the record pointer to the last record in this EF and this record shall be read.

Input:

- mode, record number (absolute mode only) and the length of the record.

Output:

the record.

8.6 UPDATE RECORD

This function updates one complete record in the current linear fixed or cyclic EF. This function shall only be performed if the UPDATE access condition for this EF is satisfied. The UPDATE can be considered as a replacement of the relevant record data of the EF by the record data given in the command. The record pointer shall not be changed by an unsuccessful UPDATE RECORD function.

The record to be updated is described by the modes below. Four modes are defined of which only PREVIOUS is allowed for cyclic files:

CURRENT: The current record is updated. The record pointer is not affected.

ABSOLUTE: The record given by the record number is updated. The record pointer is not affected.

NEXT: The record pointer is incremented before the UPDATE RECORD function is performed and the pointed record is updated. If the record pointer has not been previously set within the selected EF, then UPDATE RECORD (next) shall set the record pointer to the first record in this EF and this record shall be updated. If the record pointer addresses the last record in a linear fixed EF, UPDATE RECORD (next) shall not cause the record pointer to be changed, and no record shall be updated.

PREVIOUS: For a linear fixed EF the record pointer is decremented before the UPDATE RECORD function is performed and the pointed record is updated. If the record pointer has not been previously set within the selected EF, then UPDATE RECORD (previous) shall set the record pointer to the last record in this EF and this record shall be updated. If the record pointer addresses the first record in a linear fixed EF, UPDATE RECORD (previous) shall not cause the record pointer to be changed, and no record shall be updated.

For a cyclic EF the record containing the oldest data is updated, the record pointer is set to this record and this record becomes record number 1.

Input:

mode, record number (absolute mode only) and the length of the record;

the data used for updating the record.

Output:

none.

8.7 SEEK

This function searches through the current linear fixed EF to find a record starting with the given pattern. This function shall only be performed if the READ access condition for this EF is satisfied. Two types of SEEK are defined:

Type 1 The record pointer is set to the record containing the pattern, no output is available.

Type 2 The record pointer is set to the record containing the pattern, the output is the record number.

NOTE: A Phase 1 SIM only executes type 1 of the SEEK function.

The SIM shall be able to accept any pattern length from 1 to 16 bytes inclusive. The length of the pattern shall not exceed the record length.

Four modes are defined:

from the beginning forwards;

from the end backwards;

from the next location forwards;

from the previous location backwards.

If the record pointer has not been previously set (its status is undefined) within the selected linear fixed EF, then the search begins:

with the first record in the case of SEEK from the next location forwards; or

with the last record in the case of SEEK from the previous location backwards.

After a successful SEEK, the record pointer is set to the record in which the pattern was found. The record pointer shall not be changed by an unsuccessful SEEK function.

Input:

type and mode;

- pattern;

length of the pattern.

Output:

type 1: none;

type 2: status/record number

8.8 INCREASE

This function adds the value given by the ME to the value of the last increased/updated record of the current cyclic EF, and stores the result into the oldest record. The record pointer is set to this record and this record becomes record number 1. This function shall be used only if this EF has an INCREASE access condition assigned and this condition is fulfilled (see bytes 8 and 10 in the response parameters/data of the current EF, clause 9). The SIM shall not perform the increase if the result would exceed the maximum value of the record (represented by all bytes set to 'FF').

Input:

the value to be added.

Output:

value of the increased record;

value which has been added.

8.9 VERIFY CHV

This function verifies the CHV presented by the ME by comparing it with the relevant one stored in the SIM. The verification process is subject to the following conditions being fulfilled:

CHV is not disabled;

CHV is not blocked.

If the access condition for a function to be performed on the last selected file is CHV1 or CHV2, then a successful verification of the relevant CHV is required prior to the use of the function on this file unless the CHV is disabled.

If the CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3.

If the CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented. After 3 consecutive false CHV presentations, not necessarily in the same card session, the respective CHV shall be blocked and the access condition can never be fulfilled until the UNBLOCK CHV function has been successfully performed on the respective CHV.

Input:

indication CHV1/CHV2, CHV.

Output:

- none.

8.10 CHANGE CHV

This function assigns a new value to the relevant CHV subject to the following conditions being fulfilled:

- CHV is not disabled;
- CHV is not blocked.

The old and new CHV shall be presented.

If the old CHV presented is correct, the number of remaining CHV attempts for that CHV shall be reset to its initial value 3 and the new value for the CHV becomes valid.

If the old CHV presented is false, the number of remaining CHV attempts for that CHV shall be decremented and the value of the CHV is unchanged. After 3 consecutive false CHV presentations, not necessarily in the same card session, the respective CHV shall be blocked and the access condition can never be fulfilled until the UNBLOCK CHV function has been performed successfully on the respective CHV.

Input:
- indication CHV1/CHV2, old CHV, new CHV.

Output:
- none.

8.11 DISABLE CHV

This function may only be applied to CHV1. The successful execution of this function has the effect that files protected by CHV1 are now accessible as if they were marked "ALWAYS". The function DISABLE CHV shall not be executed by the SIM when CHV1 is already disabled or blocked.

If the CHV1 presented is correct, the number of remaining CHV1 attempts shall be reset to its initial value 3 and CHV1 shall be disabled.

If the CHV1 presented is false, the number of remaining CHV1 attempts shall be decremented and CHV1 remains enabled. After 3 consecutive false CHV1 presentations, not necessarily in the same card session, CHV1 shall be blocked and the access condition can never be fulfilled until the UNBLOCK CHV function has been successfully performed on CHV1.

Input:

- CHV1.

Output:

- none.

8.12 ENABLE CHV

This function may only be applied to CHV1. It is the reverse function of DISABLE CHV. The function ENABLE CHV shall not be executed by the SIM when CHV1 is already enabled or blocked.

If the CHV1 presented is correct, the number of remaining CHV1 attempts shall be reset to its initial value 3 and CHV1 shall be enabled.

If the CHV1 presented is false, the number of remaining CHV1 attempts shall be decremented and CHVl remains disabled. After 3 consecutive false CHV1 presentations, not necessarily in the same card session, CHVl shall be blocked and may optionally be set to "enabled". Once blocked, the CHV1 can only be unblocked using the UNBLOCK CHV function. If the CHV1 is blocked and "disabled", the access condition shall remain granted. If the CHV1 is blocked and "enabled", the access condition can never be fulfilled until the UNBLOCK CHV function has been successfully performed on CHV1.

8.13 UNBLOCK CHV

This function unblocks a CHV which has been blocked by 3 consecutive wrong CHV presentations. This function may be performed whether or not the relevant CHV is blocked.

If the UNBLOCK CHV presented is correct, the value of the CHV, presented together with the UNBLOCK CHV, is assigned to that CHV, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV is reset to its initial value 10 and the number of remaining CHV attempts for that CHV is reset to its initial value 3. After a successful unblocking attempt the CHV is enabled and the relevant access condition level is satisfied.

If the presented UNBLOCK CHV is false, the number of remaining UNBLOCK CHV attempts for that UNBLOCK CHV shall be decremented. After 10 consecutive false UNBLOCK CHV presentations, not necessarily in the same card session, the respective UNBLOCK CHV shall be blocked. A false UNBLOCK CHV shall have no effect on the status of the respective CHV itself.

Input:

- indication CHV1/CHV2, the UNBLOCK CHV and the new CHV.

Output:

- none.

8.14 INVALIDATE

This function invalidates the current EF. After an INVALIDATE function the respective flag in the file status shall be changed accordingly. This function shall only be performed if the INVALIDATE access condition for the current EF is satisfied.

An invalidated file shall no longer be available within the application for any function except for the SELECT and the REHABILITATE functions unless the file status of the EF indicates that READ and UPDATE may also be performed.

Input:

- none.

Output:

- none.

8.15 REHABILITATE

This function rehabilitates the invalidated current EF. After a REHABILITATE function the respective flag in the file status shall be changed accordingly. This function shall only be performed if the REHABILITATE access condition for the current EF is satisfied.

If BDN is enabled (see subclause 11.5.1) then the REHABILITATE function shall not rehabilitate the invalidated EF_{IMSI} and EF_{LOCI} until the PROFILE DOWNLOAD procedure is performed indicating that the ME supports the "Call control by SIM" facility (see GSM 11.14 [27]).

Input:

- none.

Output:

- none.

8.16 RUN GSM ALGORITHM

This function is used during the procedure for authenticating the SIM to a GSM network and to calculate a cipher key. The card runs the specified algorithms A3 and A8 using a 16 byte random number and the subscriber authentication key Ki, which is stored in the SIM. The function returns the calculated response SRES and the cipher key Kc.

The function shall not be executable unless DF_{GSM} or any sub-directory under DF_{GSM} has been selected as the Current Directory and a successful CHV1 verification procedure has been performed (see subclause 11.3.1).

Input:

- RAND.

Output:

- SRES, Kc.

The contents of Kc shall be presented to algorithm A5 by the ME in its full 64 bit format as delivered by the SIM.

8.17 SLEEP

This is an obsolete GSM function which was issued by Phase 1 MEs. The function shall not be used by an ME of Phase 2 or later.

8.18 TERMINAL PROFILE

This function is used by the ME to transmit to the SIM its capabilities concerning the SIM Application Toolkit functionality.

Input:

- terminal profile.

Output:

- none.

8.19 ENVELOPE

This function is used to transfer data to the SIM Application Toolkit applications in the SIM.

Input:

- data string.

Output:

- The structure of the data is defined in GSM 11.14 [27].

8.20 FETCH

This function is used to transfer an Application Toolkit command from the SIM to the ME.

Input:

- none.

Output:

- data string containing an SIM Application Toolkit command for the ME.

8.21 TERMINAL RESPONSE

This function is used to transfer from the ME to the SIM the response to a previously fetched SIM Application Toolkit command.

Input:

- data string containing the response.

Output:

- none.

9 Description of the commands

This clause states the general principles for mapping the functions described in clause 8 onto Application Protocol Data Units which are used by the transmission protocol.

9.1 Mapping principles

An APDU can be a command APDU or a response APDU.

A command APDU has the following general format:

CLA	INS	P1	P2	P3	Data

The response APDU has the following general format:

Data	SW1	SW2

An APDU is transported by the T=0 transmission protocol without any change. Other protocols might embed an APDU into their own transport structure (ISO/IEC 7816-3 [26]).

The bytes have the following meaning:

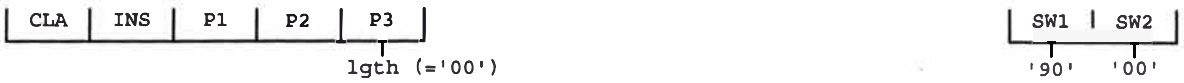
- CLA is the class of instruction (ISO/IEC 7816-3 [26]), 'A0' is used in the GSM application;
- INS is the instruction code (ISO/IEC 7816-3 [26]) as defined in this subclause for each command;
- P1, P2, P3 are parameters for the instruction. They are specified in table 9. 'FF' is a valid value for P1, P2 and P3. P3 gives the length of the data element. P3='00' introduces a 256 byte data transfer from the SIM in an outgoing data transfer command (response direction). In an ingoing data transfer command (command direction), P3='00' introduces no transfer of data;
- SW1 and SW2 are the status words indicating the successful or unsuccessful outcome of the command.

For some of the functions described in clause 8 it is necessary for T=0 to use a supplementary transport service command (GET RESPONSE) to obtain the output data. For example, the SELECT function needs the following two commands:

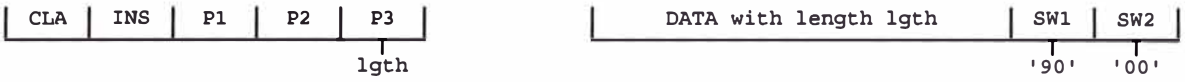
- the first command (SELECT) has both parameters and data serving as input for the function;
- the second command (GET RESPONSE) has a parameter indicating the length of the data to be returned.

If the length of the response data is not known beforehand, then its correct length may be obtained by applying the first command and interpreting the status words. SW1 shall be '9F' and SW2 shall give the total length of the data. Other status words may be present in case of an error. The various cases are:

Case 1: No input / No output

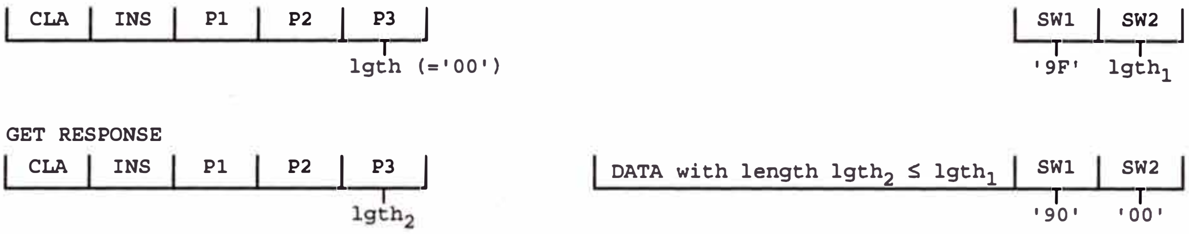


Case 2: No input / Output of known length

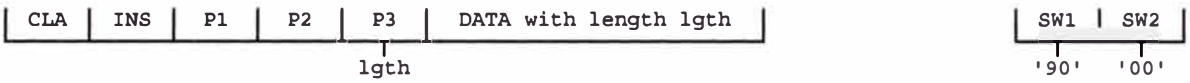


NOTE: lgth='00' causes a data transfer of 256 bytes.

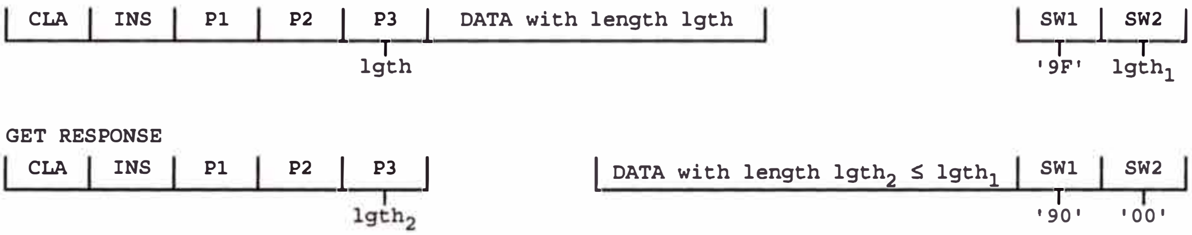
Case 3: No Input / Output of unknown length



Case 4: Input / No output



Case 5: Input / Output of known or unknown length



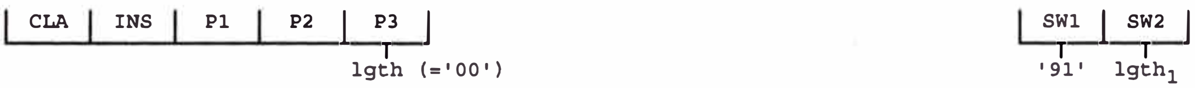
For cases 3 and 5, when SW1/SW2 indicates there is response data (i.e. SW1/SW2 = '9FXX'), then, if the ME requires to get this response data, it shall send a GET RESPONSE command as described in the relevant case above.

For case 5, in case of an ENVELOPE for SIM data download, SW1/SW2 may also indicate that there is response data with the value '9EXX', and the ME shall then send a GET RESPONSE command to get this response data.

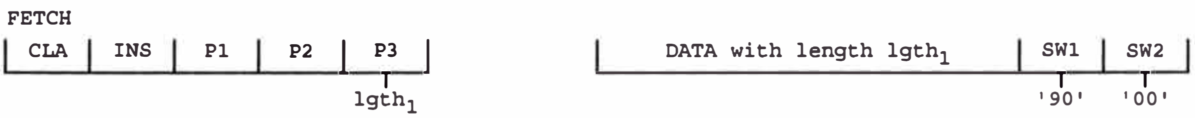
If the GSM application is one of several applications in a multi-application card, other commands with CLA not equal to 'A0' may be sent by the terminal. This shall not influence the state of the GSM application.

The following diagrams show how the five cases of transmission protocol identified in the above diagrams can all be used to send pro-active SIM commands. For further information on the diagrams below see GSM 11.14 [27].

Case 1: No input / "OK" response with no output, plus additional command from SIM



[Possible "normal GSM operation" command/response pairs]



NOTE: lgth$_1$='00' causes a data transfer of 256 bytes.

Case 2: No input / "OK" response with data of known length, plus additional command from SIM

CLA	INS	P1	P2	P3	DATA with length lgth	SW1	SW2
				lgth		'91'	lgth$_1$

[Possible "normal GSM operation" command/response pairs]

FETCH

CLA	INS	P1	P2	P3	DATA with length lgth$_1$	SW1	SW2
				lgth$_1$		'90'	'00'

NOTE: lgth='00' causes a data transfer of 256 bytes. The same applies to lgth$_1$.

Case 3: No Input / "OK" response with data of unknown length, plus additional command from SIM

CLA	INS	P1	P2	P3	SW1	SW2
				lgth (='00')	'9F'	lgth$_1$

GET RESPONSE

CLA	INS	P1	P2	P3	DATA with length lgth$_2$ ≤ lgth$_1$	SW1	SW2
				lgth$_2$		'91'	lgth$_3$

[Possible "normal GSM operation" command/response pairs]

FETCH

CLA	INS	P1	P2	P3	DATA with length lgth$_3$	SW1	SW2
				lgth$_3$		'90'	'00'

Case 4: Input / "OK" response with no output data, plus additional command from SIM

CLA	INS	P1	P2	P3	DATA with length lgth	SW1	SW2
				lgth		'91'	lgth$_1$

[Possible "normal GSM operation" command/response pairs]

FETCH

CLA	INS	P1	P2	P3	DATA with length lgth$_1$	SW1	SW2
				lgth$_1$		'90'	'00'

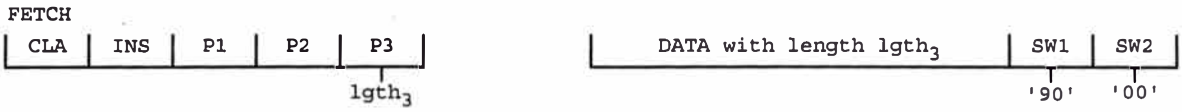
Case 5: Input / "OK" response with data of known or unknown length, plus additional command from SIM

CLA	INS	P1	P2	P3	DATA with length lgth	SW1	SW2
				lgth		'9F'	lgth$_1$

GET RESPONSE

CLA	INS	P1	P2	P3	DATA with length lgth$_2$≤lgth$_1$	SW1	SW2
				lgth$_2$		'91'	lgth$_3$

[Possible "normal GSM operation" command/response pairs]



9.2 Coding of the commands

Table 9 below gives the coding of the commands. The direction of the data is indicated by (S) and (R), where (S) stands for data sent by the ME while (R) stands for data received by the ME. Offset is coded on 2 bytes where P1 gives the high order byte and P2 the low order byte. '00 00' means no offset and reading/updating starts with the first byte while an offset of '00 01' means that reading/updating starts with the second byte.

In addition to the instruction codes specified in table 9 the following codes are reserved:

GSM operational phase:

'1X' with X even, from X=6 to X=E.

Administrative management phase:

'2A', 'D0', 'D2', 'DE', 'C4', 'C6', 'C8', 'CA', 'CC', 'B4', 'B6', 'B8', 'BA' and 'BC'.

Table 9: Coding of the commands

COMMAND	INS	P1	P2	P3	S/R
SELECT	'A4'	'00'	'00'	'02'	S/R
STATUS	'F2'	'00'	'00'	lgth	R
READ BINARY	'B0'	offset high	offset low	lgth	R
UPDATE BINARY	'D6'	offset high	offset low	lgth	S
READ RECORD	'B2'	rec No.	mode	lgth	R
UPDATE RECORD	'DC'	rec No.	mode	lgth	S
SEEK	'A2'	'00'	type/mode	lgth	S/R
INCREASE	'32'	'00'	'00'	'03'	S/R
VERIFY CHV	'20'	'00'	CHV No.	'08'	S
CHANGE CHV	'24'	'00'	CHV No.	'10'	S
DISABLE CHV	'26'	'00'	'01'	'08'	S
ENABLE CHV	'28'	'00'	'01'	'08'	S
UNBLOCK CHV	'2C'	'00'	see note	'10'	S
INVALIDATE	'04'	'00'	'00'	'00'	-
REHABILITATE	'44'	'00'	'00'	'00'	-
RUN GSM ALGORITHM	'88'	'00'	'00'	'10'	S/R
SLEEP	'FA'	'00'	'00'	'00'	-
GET RESPONSE	'C0'	'00'	'00'	lgth	R
TERMINAL PROFILE	'10'	'00'	'00'	lgth	S
ENVELOPE	'C2'	'00'	'00'	lgth	S/R
FETCH	'12'	'00'	'00'	lgth	R
TERMINAL RESPONSE	'14'	'00'	'00'	lgth	S

NOTE: If the UNBLOCK CHV command applies to CHV1 then P2 is coded '00'; if it applies to CHV2 then P2 is coded '02'.

Definitions and codings used in the response parameters/data of the commands are given in subclause 9.3.

9.2.1 SELECT

COMMAND	CLASS	INS	P1	P2	P3
SELECT	'A0'	'A4'	'00'	'00'	'02'

Command parameters/data:

Byte(s)	Description	Length
1 - 2	File ID	2

Response parameters/data in case of an MF or DF:

Byte(s)	Description	Length
1 - 2	RFU	2
3 - 4	Total amount of memory of the selected directory which is not allocated to any of the DFs or EFs under the selected directory	2
5 - 6	File ID	2
7	Type of file (see subclause 9.3)	1
8 - 12	RFU	5
13	Length of the following data (byte 14 to the end)	1
14 - 34	GSM specific data	21

GSM specific data:

Byte(s)	Description	Length
14	File characteristics (see detail 1)	1
15	Number of DFs which are a direct child of the current directory	1
16	Number of EFs which are a direct child of the current directory	1
17	Number of CHVs, UNBLOCK CHVs and administrative codes	1
18	RFU	1
19	CHV1 status (see detail 2)	1
20	UNBLOCK CHV1 status (see detail 2)	1
21	CHV2 status (see detail 2)	1
22	UNBLOCK CHV2 status (see detail 2)	1
23	RFU	1
24 - 34	Reserved for the administrative management	0 ≤ lgth ≤ 11

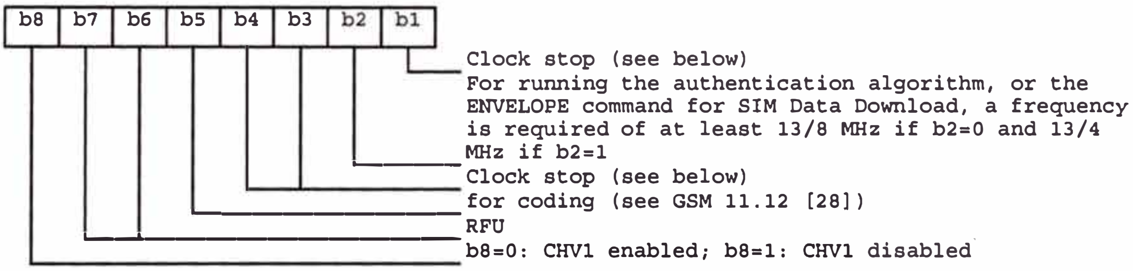
Bytes 1 - 22 are mandatory and shall be returned by the SIM. Bytes 23 and following are optional and may not be returned by the SIM.

NOTE 1: Byte 35 and following are RFU.

NOTE 2: The STATUS information of the MF, DF_{GSM} and $DF_{TELECOM}$ provide some identical application specific data, e.g. CHV status. On a multi-application card the MF should not contain any application specific data. Such data is obtained by terminals from the specific application directories. ME manufacturers should take this into account and therefore not use application specific data which may exist in the MF of a mono-application SIM.

Similarly, the VERIFY CHV command should not be executed in the MF but in the relevant application directory (e.g. DF_{GSM}).

Detail 1: File characteristics



Clock stop (see below)

For running the authentication algorithm, or the ENVELOPE command for SIM Data Download, a frequency is required of at least 13/8 MHz if b2=0 and 13/4 MHz if b2=1

Clock stop (see below)

for coding (see GSM 11.12 [28])

RFU

b8=0: CHV1 enabled; b8=1: CHV1 disabled

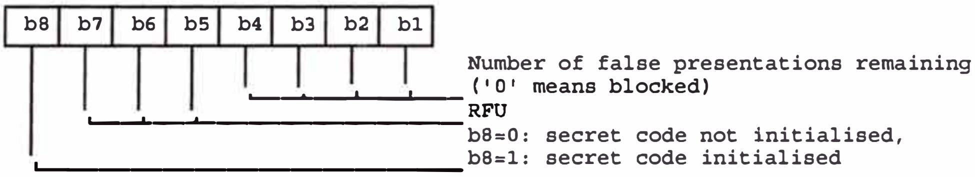
The coding of the conditions for stopping the clock is as follows:

Bit b1	Bit b3	Bit b4	
1	0	0	clock stop allowed, no preferred level
1	1	0	clock stop allowed, high level preferred
1	0	1	clock stop allowed, low level preferred
0	0	0	clock stop not allowed
0	1	0	clock stop not allowed, unless at high level
0	0	1	clock stop not allowed, unless at low level

If bit b1 (column 1) is coded 1, stopping the clock is allowed at high or low level. In this case columns 2 (bit b3) and 3 (bit b4) give information about the preferred level (high or low, respectively) at which the clock may be stopped.

If bit b1 is coded 0, the clock may be stopped only if the mandatory condition in column 2 (b3=1, i.e. stop at high level) or column 3 (b4=1, i.e. stop at low level) is fulfilled. If all 3 bits are coded 0, then the clock shall not be stopped.

Detail 2: Status byte of a secret code


b8
b7
b6
b5
b4
b3
b2
b1
Number of false presentations remaining
('0' means blocked)
RFU
b8=0: secret code not initialised,
b8=1: secret code initialised

Response parameters/data in case of an EF:

Byte(s)	Description	Length
1 - 2	RFU	2
3 - 4	File size (for transparent EF: the length of the body part of the EF) (for linear fixed or cyclic EF: record length multiplied by the number of records of the EF)	2
5 - 6	File ID	2
7	Type of file (see 9.3)	1
8	see detail 3	1
9 - 11	Access conditions (see 9.3)	3
12	File status (see 9.3)	1
13	Length of the following data (byte 14 to the end)	1
14	Structure of EF (see 9.3)	1
15	Length of a record (see detail 4)	1
16 and following	RFU	-

Bytes 1-14 are mandatory and shall be returned by the SIM.

Byte 15 is mandatory in case of linear fixed or cyclic EFs and shall be returned by the SIM.

Byte 15 is optional in case of transparent EFs and may not be returned by the SIM.

Byte 16 and following (when defined) are optional and may not be returned by the SIM.

Detail 3: Byte 8

For transparent and linear fixed EFs this byte is RFU. For a cyclic EF all bits except bit 7 are RFU; b7=1 indicates that the INCREASE command is allowed on the selected cyclic file.

Detail 4: Byte 15

For cyclic and linear fixed EFs this byte denotes the length of a record. For a transparent EF, this byte shall be coded '00', if this byte is sent by the SIM.

9.2.2 STATUS

COMMAND	CLASS	INS	P1	P2	P3
STATUS	'A0'	'F2'	'00'	'00'	lgth

The response parameters/data are identical to the response parameters/data of the SELECT command in case of an MF or DF.

9.2.3 READ BINARY

COMMAND	CLASS	INS	P1	P2	P3
READ BINARY	'A0'	'B0'	offset high	offset low	lgth

Response parameters/data:

Byte(s)	Description	Length
1 - lgth	Data to be read	lgth

9.2.4 UPDATE BINARY

COMMAND	CLASS	INS	P1	P2	P3
UPDATE BINARY	'A0'	'D6'	offset high	offset low	lgth

Command parameters/data:

Byte(s)	Description	Length
1 - lgth	Data	lgth

9.2.5 READ RECORD

COMMAND	CLASS	INS	P1	P2	P3
READ RECORD	'A0'	'B2'	Rec.No.	Mode	lgth

Parameter P2 specifies the mode:

- '02' = next record;
- '03' = previous record;
- '04' = absolute mode/current mode, the record number is given in P1 with P1='00' denoting the current record.

For the modes "next" and "previous" P1 has no significance and shall be set to '00' by the ME. To ensure phase compatibility between Phase 2 SIMs and Phase 1 MEs, the SIM shall not interpret the value given by the ME.

Response parameters/data:

Byte(s)	Description	Length
1 - lgth	The data of the record	lgth

9.2.6 UPDATE RECORD

COMMAND	CLASS	INS	P1	P2	P3
UPDATE RECORD	'A0'	'DC'	Rec.No.	Mode	lgth

Parameter P2 specifies the mode:

- '02' = next record;
- '03' = previous record;
- '04' = absolute mode/current mode; the record number is given in P1 with P1='00' denoting the current record.

For the modes "next" and "previous" P1 has no significance and shall be set to '00' by the ME. To ensure phase compatibility between Phase 2 SIMs and Phase 1 MEs, the SIM shall not interpret the value given by the ME.

Command parameters/data:

Byte(s)	Description	Length
1 - lgth	Data	lgth

9.2.7 SEEK

COMMAND	CLASS	INS	P1	P2	P3
SEEK	'A0'	'A2'	'00'	Type/Mode	lgth

Parameter P2 specifies type and mode:

- 'x0' = from the beginning forward;
- 'x1' = from the end backward;
- 'x2' = from the next location forward;
- 'x3' = from the previous location backward;

with x='0' specifies type 1 and x='1' specifies type 2 of the SEEK command.

Command parameters/data:

Byte(s)	Description	Length
1 - lgth	Pattern	lgth

There are no response parameters/data for a type 1 SEEK. A type 2 SEEK returns the following response parameters/data:

Byte(s)	Description	Length
	Record number	1

9.2.8 INCREASE

COMMAND	CLASS	INS	P1	P2	P3
INCREASE	'A0'	'32'	'00'	'00'	'03'

Command parameters/data:

Byte(s)	Description	Length
1 - 3	Value to be added	3

Response parameters/data:

Byte(s)	Description	Length
1 - X	Value of the increased record	X
X+1 - X+3	Value which has been added	3

NOTE: X denotes the length of the record.

9.2.9 VERIFY CHV

COMMAND	CLASS	INS	P1	P2	P3
VERIFY CHV	'A0'	'20'	'00'	CHV No.	'08'

Parameter P2 specifies the CHV:

- '01' = CHV1;
- '02' = CHV2.

Command parameters/data:

Byte(s)	Description	Length
1 - 8	CHV value	8

9.2.10 CHANGE CHV

COMMAND	CLASS	INS	P1	P2	P3
CHANGE CHV	'A0'	'24'	'00'	CHV No.	'10'

Parameter P2 specifies the CHV:

- '01' = CHV1;
- '02' = CHV2.

Command parameters/data:

Byte(s)	Description	Length
1 - 8	Old CHV value	8
9 - 16	New CHV value	8

9.2.11 DISABLE CHV

COMMAND	CLASS	INS	P1	P2	P3
DISABLE CHV	'A0'	'26'	'00'	'01'	'08'

Command parameters/data:

Byte(s)	Description	Length
1 - 8	CHV1 value	8

9.2.12 ENABLE CHV

COMMAND	CLASS	INS	P1	P2	P3
ENABLE CHV	'A0'	'28'	'00'	'01'	'08'

Command parameters/data:

Byte(s)	Description	Length
1 - 8	CHV1 value	8

9.2.13 UNBLOCK CHV

COMMAND	CLASS	INS	P1	P2	P3
UNBLOCK CHV	'A0'	'2C'	'00'	CHV No.	'10'

Parameter P2 specifies the CHV:

00 = CHV1;

- 02 = CHV2.

NOTE: The coding '00' for CHV1 differs from the coding of CHV1 used for other commands.

Command parameters/data:

Byte(s)	Description	Length
1 - 8	UNBLOCK CHV value	
9 - 16	New CHV value	8

9.2.14 INVALIDATE

COMMAND	CLASS	INS	P1	P2	P3
INVALIDATE	'A0'	'04'	'00'	'00'	'00'

9.2.15 REHABILITATE

COMMAND	CLASS	INS	P1	P2	P3
REHABILITATE	'A0'	'44'	'00'	'00'	'00'

9.2.16 RUN GSM ALGORITHM

COMMAND	CLASS	INS	P1	P2	P3
RUN GSM ALGORITHM	'A0'	'88'	'00'	'00'	'10'

Command parameters/data:

Byte(s)	Description	Length
1 - 16		16

Response parameters/data:

Byte(s)	Description	Length
1 - 4	SRES	4
5 - 12	Cipher Key Kc	8

The most significant bit of SRES is coded on bit 8 of byte 1. The most significant bit of Kc is coded on bit 8 of byte 5.

9.2.17 SLEEP

COMMAND	CLASS	INS	P1	P2	P3
SLEEP	'A0'	'FA'	'00'	'00'	'00'

NOTE: This command is used by Phase 1 MEs only.

9.2.18 GET RESPONSE

COMMAND	CLASS	INS	P1	P2	P3
GET RESPONSE	'A0'	'C0'	'00'	'00'	lgth

The response data depends on the preceding command. Response data is available after the commands RUN GSM ALGORITHM, SEEK (type 2), SELECT, INCREASE, and ENVELOPE. If the command GET RESPONSE is executed, it is required that it is executed immediately after the command it is related to (no other command shall come between the command/response pair and the command GET RESPONSE). If the sequence is not respected, the SIM shall send the status information "technical problem with no diagnostic given" as a reaction to the GET RESPONSE.

Since the MF is implicitly selected after activation of the SIM, GET RESPONSE is also allowed as the first command after activation.

The response data itself is defined in the subclause for the corresponding command.

9.2.19 TERMINAL PROFILE

COMMAND	CLASS	INS	P1	P2	P3
TERMINAL PROFILE	'A0'	'10'	'00'	'00'	lgth

Command parameters/data:

length `lgth`. The structure of the command parameters is defined in GSM 11.14 [27].

Response parameters/data:

none available

9.2.20 ENVELOPE

COMMAND	CLASS	INS	P1	P2	P3
ENVELOPE	'A0'	'C2'	'00'	'00'	lgth

Command parameters/data:

length `lgth`. The structure of the command parameters is defined in GSM 11.14 [27].

Response parameters/data:

The structure of the data is defined in GSM 11.14 [27].

9.2.21 FETCH

COMMAND	CLASS	INS	P1	P2	P3
FETCH	'A0'	'12'	'00'	'00'	lgth

Command parameters/data:

none.

Response parameters/data:

length `lgth`. The structure of the data is defined in GSM 11.14 [27].

9.2.22 TERMINAL RESPONSE

COMMAND	CLASS	INS	P1	P2	P3
TERMINAL RESPONSE	'A0'	'14'	'00'	'00'	lgth

Command parameters/data:

length `lgth`. The structure of the command parameters is defined in GSM 11.14 [27].

Response parameters/data:

none available.

9.3 Definitions and coding

The following definitions and coding are used in the response parameters/data of the commands.

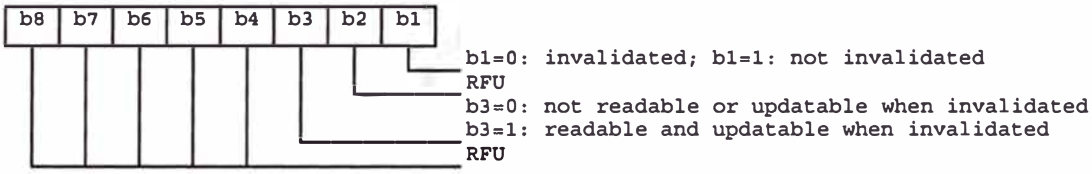
Coding

Each byte is represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB). In each representation the leftmost bit is the MSB.

RFU

In a GSM specific card all bytes which are RFU shall be set to '00' and RFU bits to 0. Where the GSM application exists on a multiapplication card or is built on a generic telecommunications card (e.g. TE9) then other values may apply. The values will be defined in the appropriate specifications for such cards. These bytes and bits shall not be interpreted by an ME in a GSM session.

File status


b8
b7
b6
b5
b4
b3
b2
b1
b1=0: invalidated; b1=1: not invalidated
RFU
b3=0: not readable or updatable when invalidated
b3=1: readable and updatable when invalidated
RFU

Bit b3 may be set to 1 in special circumstances when it is required that the EF can be read and updated even if the EF is invalidated, e.g. reading and updating the EF$_{ADN}$ when the FDN feature is enabled, or reading and updating the EF$_{BDN}$ when the BDN feature is disabled.

Structure of file

- '00' transparent;
- '01' linear fixed;
- '03' cyclic.

Type of File

- '00' RFU;
- '01' MF;
- '02' DF;
- '04' EF.

Coding of CHVs and UNBLOCK CHVs

A CHV is coded on 8 bytes. Only (decimal) digits (0-9) shall be used, coded in CCITT T.50 [20] with bit 8 set to zero. The minimum number of digits is 4. If the number of digits presented by the user is less than 8 then the ME shall pad the presented CHV with 'FF' before sending it to the SIM.

The coding of the UNBLOCK CHVs is identical to the coding of the CHVs. However, the number of (decimal) digits is always 8.

Coding of Access Conditions

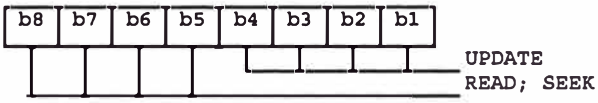
The access conditions for the commands are coded on bytes 9, 10 and 11 of the response data of the SELECT command. Each condition is coded on 4 bits as shown in table 10.

Table 10: Access conditions

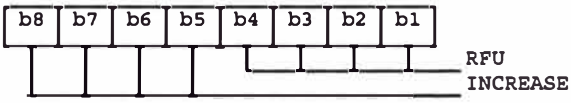
ALW	'0' *
CHV1	'1' *
CHV2	'2' *
RFU	'3'
ADM	'4'
.....	..
ADM	'E'
NEW	'F' *

Entries marked "*" in the table above, are also available for use as administrative codes in addition to the ADM access levels '4' to 'E' (refer to subclause 7.3) if required by the appropriate administrative authority. If any of these access conditions are used, the code returned in the Access Condition bytes in the response data shall be the code applicable to that particular level.

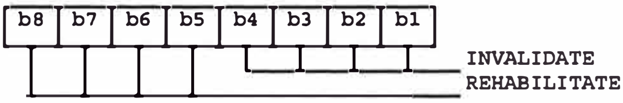
Byte 9:



Byte 10:



Byte 11:



9.4 Status conditions returned by the card

This subclause specifies the coding of the status words SW1 and SW2.

9.4.1 Responses to commands which are correctly executed

SW1	SW2	Description
'90'	'00'	- normal ending of the command
'91'	'XX'	- normal ending of the command, with extra information from the proactive SIM containing a command for the ME. Length 'XX' of the response data
'9E'	'XX'	- length 'XX' of the response data given in case of a SIM data download error
'9F'	'XX'	- length 'XX' of the response data

9.4.2 Responses to commands which are postponed

SW1	SW2	Error description
'93'	'00'	- SIM Application Toolkit is busy. Command cannot be executed at present, further normal commands are allowed.

9.4.3 Memory management

SW1	SW2	Error description
'92'	'0X'	- command successful but after using an internal update retry routine 'X' times
'92'	'40'	- memory problem

9.4.4 Referencing management

SW1	SW2	Error description
'94'	'00'	- no EF selected
'94'	'02'	- out of range (invalid address)
'94'	'04'	- file ID not found - pattern not found
'94'	'08'	- file is inconsistent with the command

9.4.5 Security management

SW1	SW2	Error description
'98'	'02'	- no CHV initialized
'98'	'04'	- access condition not fulfilled - unsuccessful CHV verification, at least one attempt left - unsuccessful UNBLOCK CHV verification, at least one attempt left - authentication failed (see note)
'98'	'08'	- in contradiction with CHV status
'98'	'10'	- in contradiction with invalidation status
'98'	'40'	- unsuccessful CHV verification, no attempt left - unsuccessful UNBLOCK CHV verification, no attempt left - CHV blocked - UNBLOCK CHV blocked
'98'	'50'	- increase cannot be performed, Max value reached

NOTE: A Phase 1 SIM may send this error code after the third consecutive unsuccessful CHV verification attempt or the tenth consecutive unsuccessful unblocking attempt.

9.4.6 Application independent errors

<table>
<tr><th>SW1</th><th>SW2</th><th>Error description</th></tr>
<tr><td>'67'</td><td>'XX'</td><td>- incorrect parameter P3 (see note)</td></tr>
<tr><td>'6B'</td><td>'XX'#</td><td>- incorrect parameter P1 or P2 (see ##)</td></tr>
<tr><td>'6D'</td><td>'XX'#</td><td>- unknown instruction code given in the command</td></tr>
<tr><td>'6E'</td><td>'XX'#</td><td>- wrong instruction class given in the command</td></tr>
<tr><td>'6F'</td><td>'XX'#</td><td>- technical problem with no diagnostic given</td></tr>
<tr><td colspan="3">NOTE 1: # These values of 'XX' are specified by ISO/IEC; at present the default value 'XX'='00' is the only one defined.
NOTE 2: ## When the error in P1 or P2 is caused by the addressed record being out of range, then the return code '94 02' shall be used.</td></tr>
</table>

NOTE: 'XX' gives the correct length or states that no additional information is given ('XX' = '00').

9.4.7 Commands versus possible status responses

The following table shows for each command the possible status conditions returned (marked by an asterisk *).

Table 11: Commands and status words

	OK				**Busy**	**Mem Sta**		**Refer. Status**				**Security Status**						**Application Independent Errors**				
Commands	90 00	91 XX	9E XX	9F XX	93 00	92 0X	92 40	94 00	94 02	94 04	94 08	98 02	98 04	98 08	98 10	98 40	98 50	67 XX	6B XX	6D XX	6E XX	6F XX
Select				*			*			*								*	*		*	*
Status	*	*					*											*	*		*	*
Update Binary	*	*				*	*	*			*		*		*			*	*		*	*
Update Record	*	*				*	*	*	*		*		*		*			*	*		*	*
Read Binary	*	*					*	*			*		*		*			*	*		*	*
Read Record	*	*					*	*	*		*		*		*			*	*		*	*
Seek	*			*			*	*		*	*		*		*			*	*		*	*
Increase				*		*	*	*			*		*		*		*	*	*		*	*
Verify CHV	*	*				*	*					*	*	*		*		*	*		*	*
Change CHV	*	*				*	*					*	*	*		*		*	*		*	*
Disable CHV	*	*				*	*					*	*	*		*		*	*		*	*
Enable CHV	*	*				*	*					*	*	*		*		*	*		*	*
Unblock CHV	*	*				*	*					*	*	*		*		*	*		*	*
Invalidate	*	*				*	*	*					*		*			*	*		*	*
Rehabilitate	*	*				*	*	*					*		*			*	*		*	*
Run GSM Algorithm				*			*				*		*					*	*		*	*
Sleep	*																	*	*		*	*
Get Response	*	*					*											*	*		*	*
Terminal Profile	*	*				*	*											*	*		*	*
Envelope	*	*	*	*	*	*	*											*	*		*	*
Fetch	*						*											*	*		*	*
Terminal Response	*	*				*	*											*	*		*	*

The responses '91 XX', and '93 00' and '9E XX' can only be given by a SIM supporting SIM Application Toolkit, to an ME also supporting SIM Application Toolkit.

For the SEEK command the response '91 XX' can be given directly after a Type 1 SEEK command. Following the Type 2 SEEK command the SIM can give the response '91 XX' only after the GET RESPONSE command.

10 Contents of the Elementary Files (EF)

This clause specifies the EFs for the GSM session defining access conditions, data items and coding. A data item is a part of an EF which represents a complete logical entity, e.g. the alpha tag in a EF_{ADN} record.

EFs or data items having an unassigned value, or, which during the GSM session, are cleared by the ME, shall have their bytes set to 'FF'. After the administrative phase all data items shall have a defined value or have their bytes set to 'FF'. If a data item is 'deleted' during a GSM session by the allocation of a value specified in another GSM TS, then this value shall be used, and the data item is not unassigned; e.g. for a deleted LAI in EF_{LOCI} the last byte takes the value 'FE' (GSM 04.08 [15] refers).

EFs are mandatory (M) or optional (O). The file size of an optional EF may be zero. All implemented EFs with a file size greater than zero shall contain all mandatory data items. Optional data items may either be filled with 'F', or, if located at the end of an EF, need not exist.

When the coding is according to CCITT Recommendation T.50 [20], bit 8 of every byte shall be set to 0.

For an overview containing all files see figure 8.

10.1 Contents of the EFs at the MF level

There are only two EFs at the MF level.

10.1.1 EF$_{ICCID}$ (ICC Identification)

This EF provides a unique identification number for the SIM.

<table>
<tr><td colspan="2">Identifier: '2FE2'</td><td>Structure: transparent</td><td>Mandatory</td></tr>
<tr><td colspan="2">File size: 10 bytes</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="4">Access Conditions:
READ ALWAYS
UPDATE NEVER
INVALIDATE ADM
REHABILITATE ADM</td></tr>
<tr><td>Bytes</td><td>Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 10</td><td>Identification number</td><td>M</td><td>10 bytes</td></tr>
</table>

- Identification number

  Contents:

  according to CCITT Recommendation E.118 [18]. However, network operators who are already issuing Phase 1 SIM cards with an identification number length of 20 digits may retain this length.

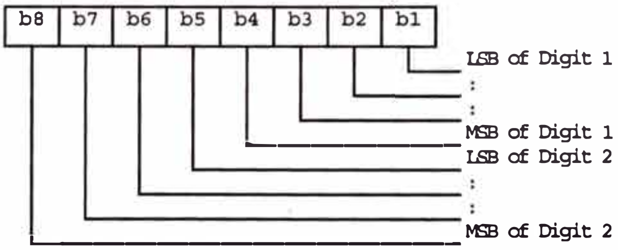
  Purpose:

  card identification number.

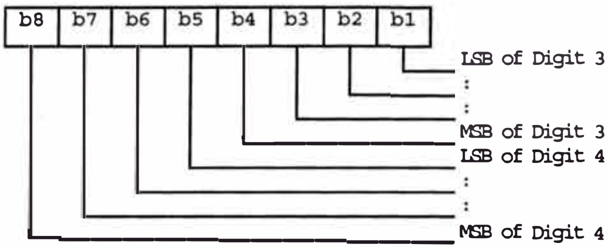
  Coding:

  BCD, left justified and padded with 'F'; after padding the digits within a byte are swapped (see below). However, network operators who are already issuing Phase 1 SIM cards where the digits within a byte are not swapped may retain this configuration.

  Byte 1:



Byte 2:



etc.

10.1.2 EF$_{ELP}$ (Extended language preference)

This EF contains the codes for up to n languages. This information, determined by the user/operator, defines the preferred languages of the user in order of priority. This information may be used by the ME for MMI purposes.

This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows.

When the CB Message Identifier capability is both allocated and activated, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in EF$_{LP}$, whichever of these EFs is used (see subclause 11.2.1). The CB message language is defined by the Data Coding Scheme (DCS: see GSM 03.38 [12]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in GSM 03.38 [12]) to the language coding as defined in ISO 639 [30] if it is necessary to check the language coding in EF$_{ELP}$.

Identifier: '2F 05'	Structure: transparent		Optional
File size: 2n bytes		Update activity: low	
Access Conditions: READ ALW UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 2	1st language code (highest prior.)	O	2 bytes
3 - 4	2nd language code	O	2 bytes
2n-1 - 2n	nth language code (lowest prior.)	O	2 bytes

Coding:

each language code is a pair of alpha-numeric characters, as defined in ISO 639 [30]. Each alpha-numeric character shall be coded on one byte using the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] with bit 8 set to 0.

Unused language entries shall be set to 'FF FF'.

10.2 DFs at the GSM application level

For compatibility with other systems based on the GSM switching platform and for special GSM services, DFs may be present as child directories of DF$_{GSM}$. The following have been defined:

DF$_{IRIDIUM}$	'5F30'
DF$_{GLOBALSTAR}$	'5F31'
DF$_{ICO}$	'5F32'
DF$_{ACeS}$	'5F33'
DF$_{MExE}$	'5F3C'
DF$_{EIA/TIA-553}$	'5F40'
DF$_{CTS}$	'5F60'
DF$_{SoLSA}$	'5F70'

Only the contents of DF_{SoLSA} and DF_{MExE} are specified in the present document. For details of the EFs contained in the DF_{CTS}, see GSM 11.19 [34].

10.3 Contents of files at the GSM application level

The EFs in the Dedicated File DF_{GSM} contain network related information.

10.3.1 EF_{LP} (Language preference)

This EF contains the codes for one or more languages. This information, determined by the user/operator, defines the preferred languages of the user in order of priority. This information may be used by the ME for MMI purposes.

This information may also be used for the screening of Cell Broadcast messages in a preferred language, as follows. When the CB Message Identifier capability is both allocated and activated, the ME selects only those CB messages the language of which corresponds to an entry in this EF or in EF_{ELP}, whichever of these EFs is used (see subclause 11.2.1). The CB message language is defined by the Data Coding Scheme (DCS: see GSM 03.38 [12]) received with the CB message. The ME shall be responsible for translating the language coding indicated in the Data Coding Scheme for the Cell Broadcast Service (as defined in GSM 03.38 [12]) to the language coding as defined in ISO 639 [30] if it is necessary to check the language coding in EF_{ELP}.

Identifier: '6F05'	Structure: transparent		Mandatory
File size: 1-n bytes		Update activity: low	
Access Conditions: READ ALW UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	1st language code (highest prior.)	M	1 byte
2	2nd language code	O	1 byte
n	nth language code (lowest prior.)	O	1 byte

Coding: according to language codings contained in the Data Coding Scheme (see GSM 03.38 [12]).

Using the command GET RESPONSE, the ME can determine the size of the EF.

10.3.2 EF_{IMSI} (IMSI)

This EF contains the International Mobile Subscriber Identity (IMSI).

Identifier: '6F07'	Structure: transparent		Mandatory
File size: 9 bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE CHV1			
Bytes	Description	M/O	Length
1	length of IMSI	M	1 byte
2 - 9	IMSI	M	8 bytes

- length of IMSI

  Contents:

The length indicator refers to the number of significant bytes, not including this length byte, required for the IMSI.

Coding: according to GSM 04.08 [15].

- IMSI

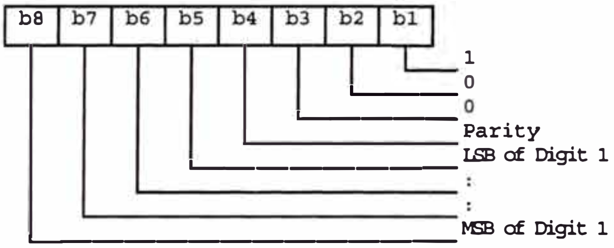
Contents:

International Mobile Subscriber Identity.

Coding:

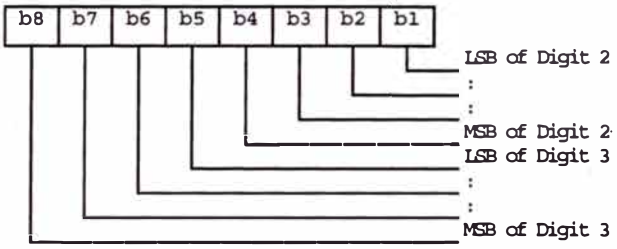
This information element is of variable length. If a network operator chooses an IMSI of less than 15 digits, unused nibbles shall be set to 'F'.

Byte 2:



For the parity bit, see GSM 04.08 [15].

Byte 3:



etc.

10.3.3 EF$_{Kc}$ (Ciphering key Kc)

This EF contains the ciphering key Kc and the ciphering key sequence number n.

Identifier: '6F20'	Structure: transparent		Mandatory
File size: 9 bytes		Update activity: high	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 8	Ciphering key Kc	M	8 bytes
9	Ciphering key sequence number n	M	1 byte

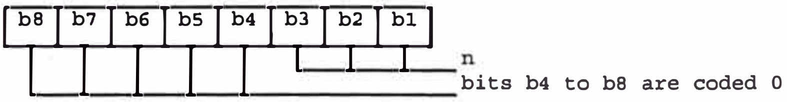
Ciphering key Kc

Coding:

The least significant bit of Kc is the least significant bit of the eighth byte. The most significant bit of Kc is the most significant bit of the first byte.

- Ciphering key sequence number n

  Coding:



NOTE: GSM 04.08 [15] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

10.3.4 EF$_{PLMNsel}$ (PLMN selector)

This EF contains the coding for n PLMNs, where n is at least eight. This information determined by the user/operator defines the preferred PLMNs of the user in priority order.

Identifier: '6F30'	Structure: transparent	Optional
File size: 3n (n ≥ 8) bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 - 3	1st PLMN (highest priority)	M	3 bytes
22 - 24	8th PLMN	M	3 bytes
25 - 27	9th PLMN	O	3 bytes
(3n-2)-3n	nth PLMN (lowest priority)	O	3 bytes

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to GSM 04.08 [15].

  If storage for fewer than the maximum possible number n is required, the excess bytes shall be set to 'FF'.

  For instance, using 246 for the MCC and 81 for the MNC and if this is the first and only PLMN, the contents reads as follows:

  Bytes 1-3: '42' 'F6' '18'

  Bytes 4-6: 'FF' 'FF' 'FF'

  etc.

10.3.5 EF$_{HPLMN}$ (HPLMN search period)

This EF contains the interval of time between searches for the HPLMN (see GSM 02.11 [5]).

Identifier: '6F31'	Structure: transparent	Mandatory
File size: 1 byte	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Time interval	M	1 byte

- Time interval

  Contents:

  The time interval between two searches.

  Coding:

  The time interval is coded in integer multiples of n minutes. The range is from n minutes to a maximum value. The value '00' indicates that no attempts shall be made to search for the HPLMN. The encoding is:

  - '00': No HPLMN search attempts
  - '01': n minutes
  - '02': 2n minutes
  - : :
  - 'YZ': (16Y+Z)n minutes (maximum value)

  All other values shall be interpreted by the ME as a default period.

For specification of the integer timer interval n, the maximum value and the default period refer to GSM 02.11 [5].

10.3.6 EF_{ACMmax} (ACM maximum value)

This EF contains the maximum value of the accumulated call meter. This EF shall always be allocated if EF_{ACM} is allocated.

Identifier: '6F37'	Structure: transparent	Optional
File size: 3 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1/CHV2 (fixed during administrative management) INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 - 3	Maximum value	M	3 bytes

- Maximum value

  Contents:

  maximum value of the Accumulated Call Meter (ACM)

  Coding:

First byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{23}	2^{22}	2^{21}	2^{20}	2^{19}	2^{18}	2^{17}	2^{16}

Second byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{15}	2^{14}	2^{13}	2^{12}	2^{11}	2^{10}	2^{9}	2^{8}

Third byte:

b8	b7	b6	b5	b4	b3	b2	b1
2^{7}	2^{6}	2^{5}	2^{4}	2^{3}	2^{2}	2^{1}	2^{0}

For instance, '00' '00' '30' represents 2^5+2^4.

All ACM data is stored in the SIM and transmitted over the SIM/ME interface as binary.

ACMmax is not valid, as defined in GSM 02.24 [7], if it is coded '000000'.

10.3.7 EF_{SST} (SIM service table)

This EF indicates which services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the SIM, the ME shall not select this service.

Identifier: '6F38'	Structure: transparent		Mandatory
File size: X bytes, X ≥ 2		Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Services n° 1 to n°4	M	1 byte
2	Services n°5 to n°8	M	1 byte
3	Services n°9 to n° 12	O	1 byte
4	Services n° 13 to n° 16	O	1 byte
5	Services n° 17 to n°20	O	1 byte
6	Services n°21 to n°24	O	1 byte
7	Services n°25 to n°28	O	1 byte
8	Services n°29 to n°32	O	1 byte
etc.			
X	Services (4X-3) to (4X)	O	1 byte

-Services

Contents:	Service n°1 :	CHV1 disable function
	Service n°2 :	Abbreviated Dialling Numbers (ADN)
	Service n°3 :	Fixed Dialling Numbers (FDN)
	Service n°4 :	Short Message Storage (SMS)
	Service n°5 :	Advice of Charge (AoC)
	Service n°6 :	Capability Configuration Parameters (CCP)
	Service n°7 :	PLMN selector
	Service n°8 :	RFU
	Service n°9 :	MSISDN
	Service n°10:	Extension1
	Service n°11:	Extension2
	Service n°12:	SMS Parameters
	Service n°13:	Last Number Dialled (LND)
	Service n°14:	Cell Broadcast Message Identifier
	Service n°15:	Group Identifier Level 1
	Service n°16:	Group Identifier Level 2
	Service n°17:	Service Provider Name
	Service n°18:	Service Dialling Numbers (SDN)
	Service n°19:	Extension3
	Service n°20:	RFU
	Service n°21:	VGCS Group Identifier List (EF_{VGCS} and EF_{VGCSS})
	Service n°22:	VBS Group Identifier List (EF_{VBS} and EF_{VBSS})
	Service n°23:	enhanced Multi-Level Precedence and Pre-emption Service
	Service n°24:	Automatic Answer for eMLPP
	Service n°25:	Data download via SMS-CB
	Service n°26:	Data download via SMS-PP
	Service n°27:	Menu selection
	Service n°28:	Call control
	Service n°29:	Proactive SIM
	Service n°30:	Cell Broadcast Message Identifier Ranges
	Service n°31:	Barred Dialling Numbers (BDN)
	Service n°32:	Extension4
	Service n°33:	De-personalization Control Keys
	Service n°34:	Co-operative Network List
	Service n°35:	Short Message Status Reports
	Service n°36:	Network's indication of alerting in the MS
	Service n°37:	Mobile Originated Short Message control by SIM
	Service n°38:	GPRS
	Service n°39:	Image (IMG)
	Service n°40:	SoLSA (Support of Local Service Area)
	Service n°41:	USSD string data object supported in Call Control
	Service n°42:	RUN AT COMMAND command
	Service n 43:	PLMN Selector List with Access Technology
	Service n 44:	OPLMN Selector List with Access Technology
	Service n 45	HPLMN Access Technology
	Service n 46:	CPBCCH Information
	Service n 47:	Investigation Scan
	Service n°48:	Extended Capability Configuration Parameters
	Service n°49:	MExE

For a phase 2 SIM, the EF shall contain at least two bytes which correspond to the Phase 1 services. Further bytes may be included, but if the EF includes an optional byte, then it is mandatory for the EF to also contain all bytes before that byte. Other services are possible in the future and will be coded on further bytes in the EF. The coding falls under the responsibility of ETSI.

NOTE 1: Service N°8 was used in Phase 1 for Called Party Subaddress. To prevent any risk of incompatibility Service N°8 should not be reallocated.

NOTE 2: As the BDN service relies on the Call Control feature, service n°31 (BDN) should only be allocated and activated if service n°28 (Call control) is allocated and activated.

Coding:

2 bits are used to code each service:

first bit = 1: service allocated

first bit = 0: service not allocated

where the first bit is b1, b3, b5 or b7;

second bit = 1: service activated

second bit = 0: service not activated

where the second bit is b2, b4, b6 or b8.

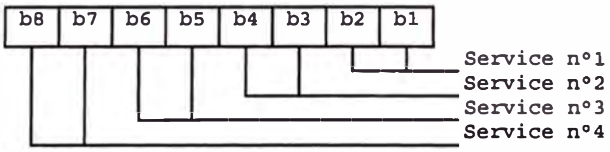
Service allocated means that the SIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

The following codings are possible:

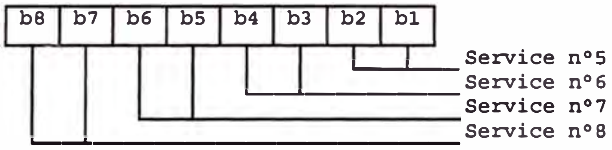
- first bit = 0: service not allocated, second bit has no meaning;
- first bit = 1 and second bit = 0: service allocated but not activated;
- first bit = 1 and second bit = 1: service allocated and activated.

The bits for services not yet defined shall be set to RFU. For coding of RFU see subclause 9.3.

First byte:

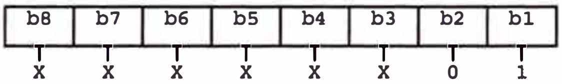


Second byte:



etc.

The following example of coding for the first byte means that service n°1 "CHV1-Disabling" is allocated but not activated:



If the SIM supports the FDN feature (FDN allocated and activated) a special mechanism shall exist in the SIM which invalidates both EF$_{\text{IMSI}}$ and EF$_{\text{LOCI}}$ once during each GSM session. This mechanism shall be invoked by the SIM automatically if FDN is enabled. This invalidation shall occur at least before the next command following selection of either EF. FDN is enabled when the ADN is invalidated or not activated.

If the SIM supports the BDN feature (BDN allocated and activated) a special mechanism shall exist in the SIM which invalidates both EF$_{\text{IMSI}}$ and EF$_{\text{LOCI}}$ once during each GSM session and which forbids the REHABILITATE command to rehabilitate both EF$_{\text{IMSI}}$ and EF$_{\text{LOCI}}$ until the PROFILE DOWNLOAD procedure is performed indicating that the ME supports the "Call control by SIM" facility. This mechanism shall be invoked by the SIM automatically if BDN is enabled. The invalidation of EF$_{\text{IMSI}}$ and EF$_{\text{LOCI}}$ shall occur at least before the next command following selection of either EF. BDN is enabled when the EF$_{\text{BDN}}$ is not invalidated.

10.3.8 EF$_{\text{ACM}}$ (Accumulated call meter)

This EF contains the total number of units for both the current call and the preceding calls.

NOTE: The information may be used to provide an indication to the user for advice or as a basis for the calculation of the monetary cost of calls (see GSM 02.86 [9]).

Identifier: '6F39'	Structure: cyclic	Optional
Record length: 3 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1/CHV2 (fixed during administrative management)
INCREASE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 3	Accumulated count of units	M	3 bytes

- Accumulated count of units

  Contents: value of the ACM

  Coding: see the coding of EF_{ACMmax}

10.3.9 EF_{GID1} (Group Identifier Level 1)

This EF contains identifiers for particular SIM-ME associations. It can be used to identify a group of SIMs for a particular application.

Identifier: '6F3E'	Structure: transparent	Optional
File size: 1-n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - n	SIM group identifier(s)	O	n bytes

10.3.10 EF_{GID2} (Group Identifier Level 2)

This EF contains identifiers for particular SIM-ME associations. It can be used to identify a group of SIMs for a particular application.

Identifier: '6F3F'	Structure: transparent	Optional
File size: 1-n bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - n	SIM group identifier(s)	O	n bytes

NOTE: The structure of EF_{GID1} and EF_{GID2} are identical. They are provided to allow the network operator to enforce different levels of security dependant on application.

10.3.11 EF_{SPN} (Service Provider Name)

This EF contains the service provider name and appropriate requirements for the display by the ME.

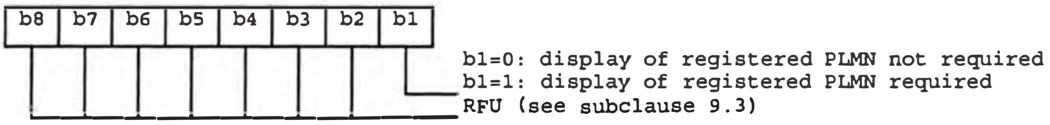
Identifier: '6F46'	Structure: transparent		Optional
File Size: 17 bytes		Update activity: low	
Access Conditions: READ ALWAYS UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Display Condition	M	1 byte
2 - 17	Service Provider Name	M	16 bytes

- Display Condition

  Contents: display condition for the service provider name in respect to the registered PLMN (see GSM 02.07 [3]).

  Coding: see below

  Byte 1:


b8
b7
b6
b5
b4
b3
b2
b1
b1=0: display of registered PLMN not required
b1=1: display of registered PLMN required
RFU (see subclause 9.3)

- Service Provider Name

  Contents: service provider string to be displayed

  Coding: the string shall use either

  - the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] with bit 8 set to 0. The string shall be left justified. Unused bytes shall be set to 'FF'; or
  - one of the UCS2 code options defined in annex B.

10.3.12 EF_{PUCT} (Price per unit and currency table)

This EF contains the Price per Unit and Currency Table (PUCT). The PUCT is Advice of Charge related information which may be used by the ME in conjunction with EF_{ACM} to compute the cost of calls in the currency chosen by the subscriber, as specified in GSM 02.24 [7]. This EF shall always be allocated if EF_{ACM} is allocated.

Identifier: '6F41'	Structure: transparent		Optional
File size: 5 bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1/CHV2 (fixed during administrative management) INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 3	Currency code	M	3 bytes
4 - 5	Price per unit	M	2 bytes

- Currency code

  Contents:

  the alpha-identifier of the currency code.

  Coding:

bytes 1, 2 and 3 are the respective first, second and third character of the alpha identifier. This alpha-tagging shall use the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] with bit 8 set to 0.

- Price per unit

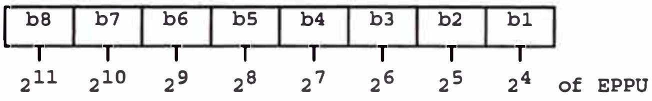
Contents:

price per unit expressed in the currency coded by bytes 1-3.

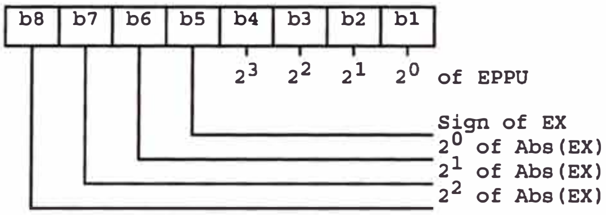
Coding:

Byte 4 and bits b1 to b4 of byte 5 represent the Elementary Price per Unit (EPPU) in the currency coded by bytes 1-3. Bits b5 to b8 of byte 5 are the decimal logarithm of the multiplicative factor represented by the absolute value of its decimal logarithm (EX) and the sign of EX, which is coded 0 for a positive sign and 1 for a negative sign.

Byte 4:



Byte 5:



The computation of the price per unit value is made by the ME in compliance with GSM 02.24 [7] by the following formula:

price per unit = EPPU * 10^{EX}.

The price has to be understood as expressed in the coded currency.

10.3.13 EF_{CBMI} (Cell broadcast message identifier selection)

This EF contains the Message Identifier Parameters which specify the type of content of the cell broadcast messages that the subscriber wishes the MS to accept.

Any number of CB Message Identifier Parameters may be stored in the SIM. No order of priority is applicable.

Identifier: '6F45'	Structure: transparent		Optional
File size: 2n bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 2	CB Message Identifier 1	O	2 bytes
3 - 4	CB Message Identifier 2	O	2 bytes
2n-1 - 2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier

Coding:

as in GSM 03.41, "Message Format on BTS-MS Interface - Message Identifier".

Values listed show the types of message which shall be accepted by the MS.

Unused entries shall be set to 'FF FF'.

10.3.14 EF$_{BCCH}$ (Broadcast control channels)

This EF contains information concerning the BCCH according to GSM 04.08 [15].

BCCH storage may reduce the extent of a Mobile Station's search of BCCH carriers when selecting a cell. The BCCH carrier lists in an MS shall be in accordance with the procedures specified in GSM 04.08 [15]. The MS shall only store BCCH information from the System Information 2 message and not the 2bis extension message.

Identifier: '6F74'	Structure: transparent		Mandatory
File size: 16 bytes		Update activity: high	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 16	BCCH information	M	16 bytes

- BCCH information

Coding:

The information is coded as octets 2-17 of the "neighbour cells description information element" in GSM 04.08 [15].

10.3.15 EF$_{ACC}$ (Access control class)

This EF contains the assigned access control class(es). GSM 02.11 [5] refers. The access control class is a parameter to control the RACH utilization. 15 classes are split into 10 classes randomly allocated to normal subscribers and 5 classes allocated to specific high priority users. For more information see GSM 02.11 [5].

Identifier: '6F78'	Structure: transparent		Mandatory
File size: 2 bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 2	Access control classes	M	2 bytes

- Access control classes

Coding:

Each ACC is coded on one bit. An ACC is "allocated" if the corresponding bit is set to 1 and "not allocated" if this bit is set to 0. Bit b3 of byte 1 is set to 0.

Byte 1:

b8	b7	b6	b5	b4	b3	b2	b1	
15	14	13	12	11	10	09	08	Number of the ACC (except for bit b3)

Byte 2:

b8	b7	b6	b5	b4	b3	b2	b1	
07	06	05	04	03	02	01	00	Number of the ACC

10.3.16 EF_{FPLMN} (Forbidden PLMNs)

This EF contains the coding for four Forbidden PLMNs (FPLMN). It is read by the ME as part of the SIM initialization procedure and indicates PLMNs which the MS shall not automatically attempt to access.

A PLMN is written to the EF if a network rejects a Location Update with the cause "PLMN not allowed". The ME shall manage the list as follows.

When four FPLMNs are held in the EF, and rejection of a further PLMN is received by the ME from the network, the ME shall modify the EF using the UPDATE command. This new PLMN shall be stored in the fourth position, and the existing list "shifted" causing the previous contents of the first position to be lost.

When less than four FPLMNs exist in the EF, storage of an additional FPLMN shall not cause any existing FPLMN to be lost.

Dependent upon procedures used to manage storage and deletion of FPLMNs in the EF, it is possible, when less than four FPLMNs exist in the EF, for 'FFFFFF' to occur in any position. The ME shall analyse all the EF for FPLMNs in any position, and not regard 'FFFFFF' as a termination of valid data.

Identifier: '6F7B'	Structure: transparent		Mandatory
File size: 12 bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 3	PLMN 1	M	3 bytes
4 - 6	PLMN 2	M	3 bytes
7 - 9	PLMN 3	M	3 bytes
10 - 12	PLMN 4	M	3 bytes

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

  Coding:

  according to GSM 04.08 [15].

  For instance, using 246 for the MCC and 81 for the MNC and if this is stored in PLMN 3 the contents is as follows:

  Bytes 7-9:'42' 'F6' '18'

  If storage for fewer than 4 PLMNs is required, the unused bytes shall be set to 'FF'.

10.3.17 EF_{LOCI} (Location information)

This EF contains the following Location Information:

- Temporary Mobile Subscriber Identity (TMSI);
- Location Area Information (LAI);
- TMSI TIME;
- Location update status.

See clause 11.1.2 for special requirements when updating EF_{LOCI}.

<table>
<tr><td colspan="2">Identifier: '6F7E'</td><td colspan="2">Structure: transparent</td><td>Mandatory</td></tr>
<tr><td colspan="3">File size: 11 bytes</td><td colspan="2">Update activity: high</td></tr>
<tr><td colspan="5">Access Conditions:
READ CHV1
UPDATE CHV1
INVALIDATE ADM
REHABILITATE CHV1</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1 - 4</td><td colspan="2">TMSI</td><td>M</td><td>4 bytes</td></tr>
<tr><td>5 - 9</td><td colspan="2">LAI</td><td>M</td><td>5 bytes</td></tr>
<tr><td>10</td><td colspan="2">TMSI TIME</td><td>M</td><td>1 byte</td></tr>
<tr><td>11</td><td colspan="2">Location update status</td><td>M</td><td>1 byte</td></tr>
</table>

- TMSI

  Contents: Temporary Mobile Subscriber Identity

  Coding: according to GSM 04.08 [15].

  Byte 1: first byte of TMSI

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- LAI

  Contents: Location Area Information

  Coding: according to GSM 04.08 [15].

  Byte 5: first byte of LAI

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- TMSI TIME

  Contents: Current value of Periodic Location Updating Timer (T3212).

  This byte is used by Phase 1 MEs, but it shall not be used by Phase 2 MEs.

- Location update status

  Contents: status of location update according to GSM 04.08 [15].

  Coding:

Byte 11:

Bits:	b3	b2	b1	
0	0	0	:	updated
0	0	1	:	not updated
0	1	0	:	PLMN not allowed
0	1	1	:	Location Area not allowed
1	1	1	:	reserved

Bits b4 to b8 are RFU (see subclause 9.3).

10.3.18 EF_{AD} (Administrative data)

This EF contains information concerning the mode of operation according to the type of SIM, such as normal (to be used by PLMN subscribers for GSM operations), type approval (to allow specific use of the ME during type approval procedures of e.g. the radio equipment), cell testing (to allow testing of a cell before commercial use of this cell), manufacturer specific (to allow the ME manufacturer to perform specific proprietary auto-test in its ME during e.g. maintenance phases).

It also provides an indication of whether some ME features should be activated during normal operation as well as information about the length of the MNC, which is part of the International Mobile Subscriber Identity (IMSI).

Identifier: '6FAD'	Structure: transparent		Mandatory
File size: 3+X bytes		Update activity: low	
Access Conditions: READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	MS operation mode	M	1 byte
2 to 3	Additional information	M	2 bytes
4	length of MNC in the IMSI	O	1 byte
5 to 4+X	RFU	O	X bytes

- MS operation mode

  Contents: mode of operation for the MS

  Coding:

  Initial value

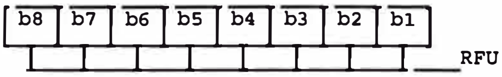
- normal operation	'00'
- type approval operations	'80'
- normal operation + specific facilities	'01'
- type approval operations + specific facilities	'81'
- maintenance (off line)	'02'
- cell test operation	'04'

- Additional information

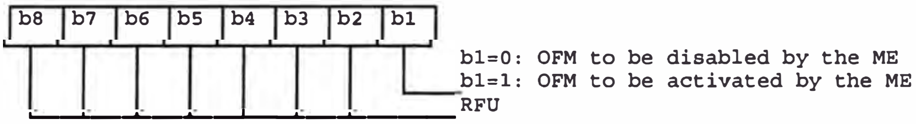
  Coding:

  - specific facilities (if b1=1 in byte 1);

Byte 2 (first byte of additional information):



Byte 3:


b8
b7
b6
b5
b4
b3
b2
b1
b1=0: OFM to be disabled by the ME
b1=1: OFM to be activated by the ME
RFU

The OFM bit is used to control the Ciphering Indicator as specified in GSM 02.07 [3]

- ME manufacturer specific information (if b2=1 in byte 1).

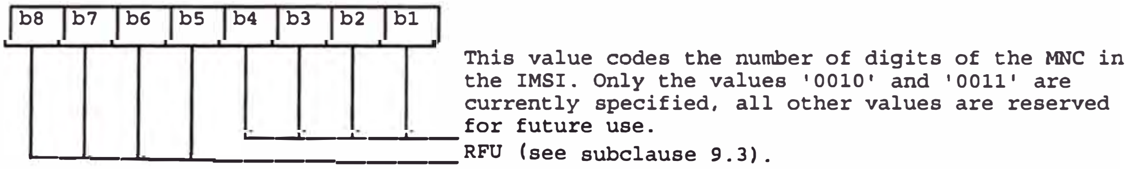
Length of MNC in the IMSI :

Contents:

The length indicator refers to the number of digits, used for extracting the MNC from the IMSI

Coding:

Byte 4:


b8
b7
b6
b5
b4
b3
b2
b1
This value codes the number of digits of the MNC in the IMSI. Only the values '0010' and '0011' are currently specified, all other values are reserved for future use.
RFU (see subclause 9.3).

10.3.19 EF$_{Phase}$ (Phase identification)

This EF contains information concerning the phase of the SIM.

Identifier: '6FAE'	Structure: transparent		Mandatory
File size: 1 byte		Update activity: low	
Access Conditions: READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	**Description**	**M/O**	**Length**
1	SIM Phase	M	1 byte

SIM Phase

Coding:

'00': phase 1

'02': phase 2

'03': phase 2 and PROFILE DOWNLOAD required (see GSM 11.14 [27]).

All other codings are reserved for specification by ETSI TC SMG. Codings '04' to '0F' indicate that the SIM supports, as a minimum, the mandatory requirements defined in this specification.

This phase identification does not preclude a SIM to support some features of a phase later than the one indicated in EF$_{Phase}$. For example : if EF$_{Phase}$ is coded '00', it may be assumed by the ME that some Phase 2 or Phase 2+ features are supported by this SIM; if EF$_{Phase}$ is coded '02' or '03', it may be assumed by the ME that some Phase 2+ features are supported by this SIM.

However, the services n°3 (FDN) and/or n°5 (AoC) shall only be allocated and activated in SIMs of phase 2 or later with EF$_{\text{Phase}}$ being coded '02' or greater. Similarly, service n°31 (BDN) shall only be allocated and activated in SIMs with EF$_{\text{Phase}}$ being coded '03' or greater.

If EF$_{\text{Phase}}$ is coded '03' or greater, an ME supporting SIM Application Toolkit shall perform the PROFILE DOWNLOAD procedure, as defined in GSM 11.14 [27].

10.3.20 EF$_{\text{VGCS}}$ (Voice Group Call Service)

This EF contains a list of those VGCS group identifiers the user has subscribed to. The elementary file is used by the ME for group call establishment and group call reception.

Identifier: '6FB1'	Structure: transparent	Optional
File size: 4n bytes (n <= 50)	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 - 4	Group ID 1	M	4 bytes
5 - 8	Group ID 2	O	4 bytes
:	:	:	:
(4n-3)-4n	Group ID n	O	4 bytes

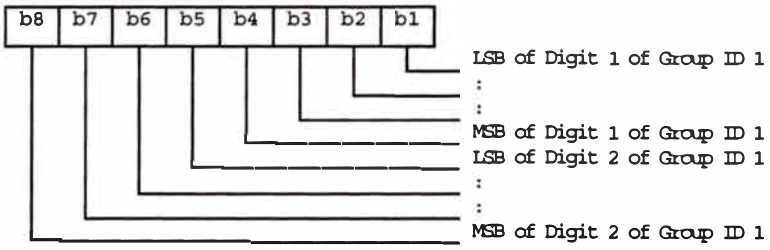
- Group ID

  Contents: VGCS Group ID, according to GSM 03.03 [10]

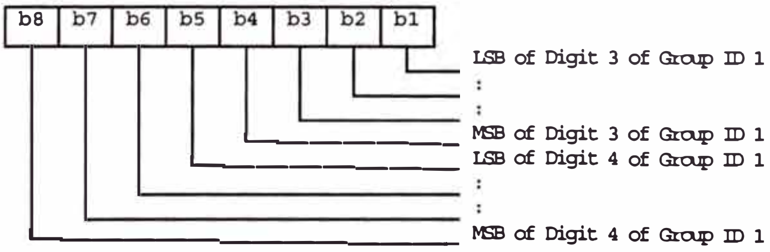
  Coding:

  The VGCS Group ID is of a variable length with a maximum length of 8 digits. Each VGCS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code. If a VGCS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VGCS Group ID Digit 1 is the most significant digit of the Group ID.

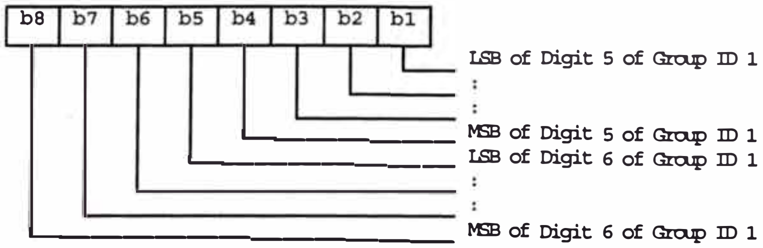
Byte 1:


b8
b7
b6
b5
b4
b3
b2
b1
LSB of Digit 1 of Group ID 1
:
:
MSB of Digit 1 of Group ID 1
LSB of Digit 2 of Group ID 1
:
:
MSB of Digit 2 of Group ID 1

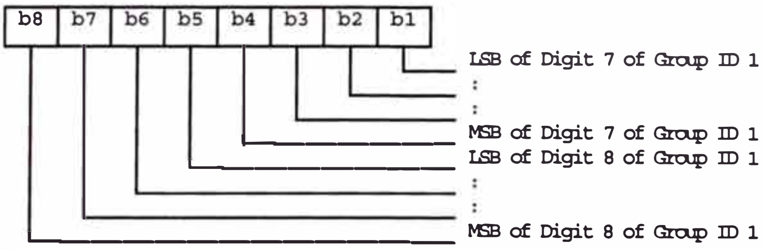
Byte 2:


b8
b7
b6
b5
b4
b3
b2
b1
LSB of Digit 3 of Group ID 1
:
:
MSB of Digit 3 of Group ID 1
LSB of Digit 4 of Group ID 1
:
:
MSB of Digit 4 of Group ID 1

Byte 3:


b8 b7 b6 b5 b4 b3 b2 b1
LSB of Digit 5 of Group ID 1
:
:
MSB of Digit 5 of Group ID 1
LSB of Digit 6 of Group ID 1
:
:
MSB of Digit 6 of Group ID 1

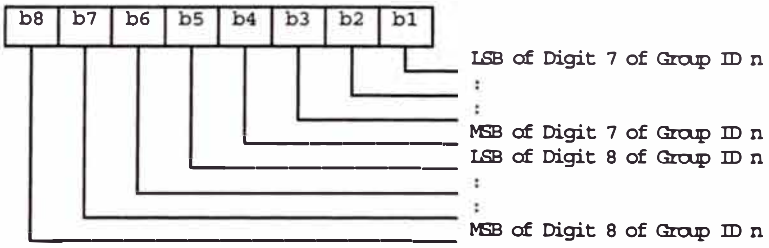
Byte 4:


b8 b7 b6 b5 b4 b3 b2 b1
LSB of Digit 7 of Group ID 1
:
:
MSB of Digit 7 of Group ID 1
LSB of Digit 8 of Group ID 1
:
:
MSB of Digit 8 of Group ID 1

:

: etc........

Byte (4n-3)-4n:


b8 b7 b6 b5 b4 b3 b2 b1
LSB of Digit 7 of Group ID n
:
:
MSB of Digit 7 of Group ID n
LSB of Digit 8 of Group ID n
:
:
MSB of Digit 8 of Group ID n

If storage for fewer than the maximum possible number *n* of VGCS Group IDs, is required, the excess bytes shall be set to 'FF'.

10.3.21 EF$_{VGCSS}$ (Voice Group Call Service Status)

This EF contains the status of activation for the VGCS group identifiers. The elementary file is directly related to the EF$_{VGCS}$. This EF shall always be allocated if EF$_{VGCS}$ is allocated.

Identifier: '6FB2'	Structure: transparent		Optional
File size: 7 bytes	Update activity: low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 7	Activation/Deactivation Flags	M	7 bytes

- Activation/Deactivation Flags

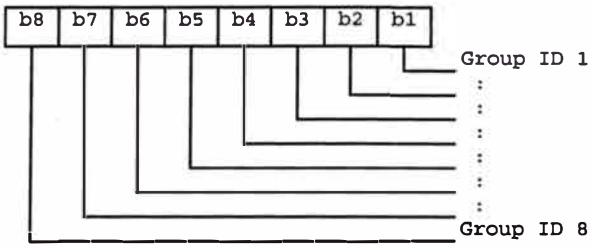
Contents: Activation/Deactivation Flags of the appropriate Group IDs

Coding:

bit = 0 means - Group ID deactivated

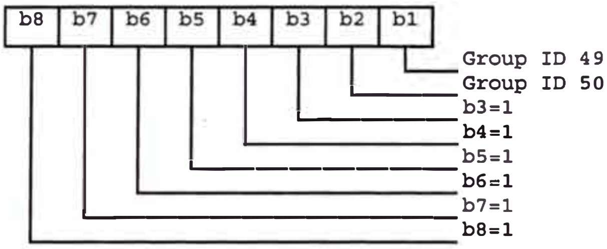
bit = 1 means - Group ID activated

Byte 1:



etc : : : : : : : :

Byte 7:



10.3.22 EF$_{VBS}$ (Voice Broadcast Service)

This EF contains a list of those VBS group identifiers the user has subscribed to. The elementary file is used by the ME for broadcast call establishment and broadcast call reception.

Identifier: '6FB3'	Structure: transparent		Optional
File size: 4n bytes (n <= 50)	Update activity: low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 4	Group ID 1	M	4 bytes
5 - 2	Group ID 2	O	4 bytes
:	:	:	:
(4n-3)-4n	Group ID n	O	4 bytes

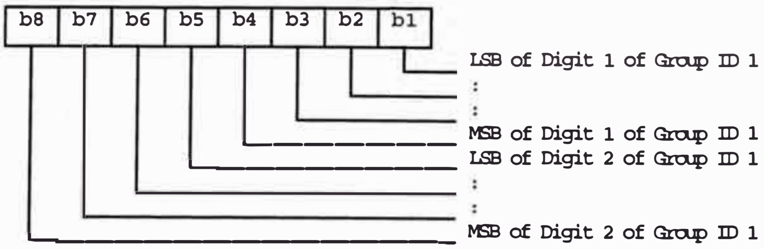
- Group ID

Contents: VBS Group ID, according to GSM 03.03 [10]

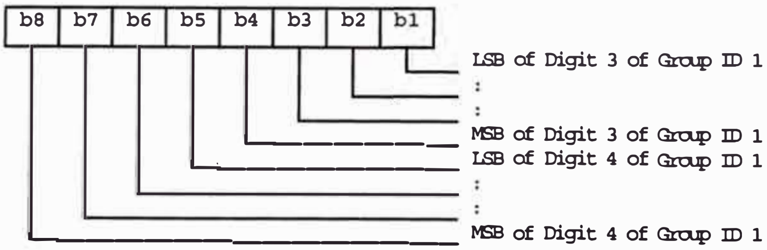
Coding:

The VBS Group ID is of a variable length with a maximum length of 8 digits. Each VBS Group ID is coded on four bytes, with each digit within the code being coded on four bits corresponding to BCD code. If a VBS Group ID of less than 8 digits is chosen, then the unused nibbles shall be set to 'F'. VBS Group ID Digit 1 is the most significant digit of the Group ID.

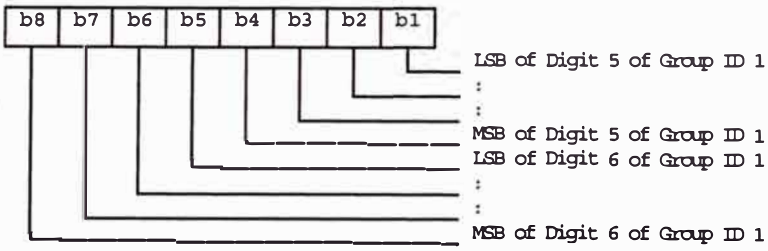
Byte 1:


b8
b7
b6
b5
b4
b3
b2
b1
LSB of Digit 1 of Group ID 1
:
:
MSB of Digit 1 of Group ID 1
LSB of Digit 2 of Group ID 1
:
:
MSB of Digit 2 of Group ID 1

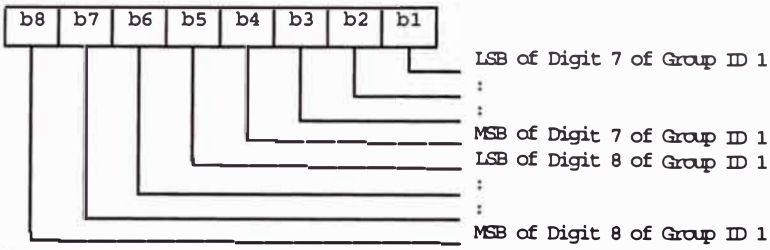
Byte 2:


b8
b7
b6
b5
b4
b3
b2
b1
LSB of Digit 3 of Group ID 1
:
:
MSB of Digit 3 of Group ID 1
LSB of Digit 4 of Group ID 1
:
:
MSB of Digit 4 of Group ID 1

Byte 3:


b8
b7
b6
b5
b4
b3
b2
b1
LSB of Digit 5 of Group ID 1
:
:
MSB of Digit 5 of Group ID 1
LSB of Digit 6 of Group ID 1
:
:
MSB of Digit 6 of Group ID 1

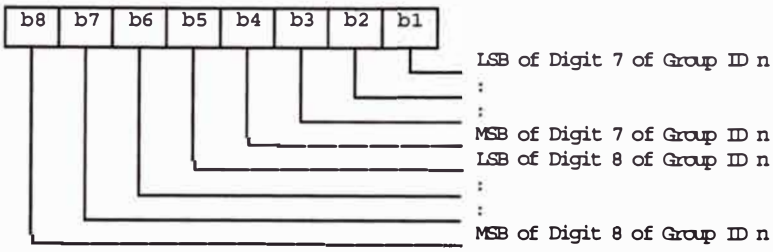
Byte 4:


b8
b7
b6
b5
b4
b3
b2
b1
LSB of Digit 7 of Group ID 1
:
:
MSB of Digit 7 of Group ID 1
LSB of Digit 8 of Group ID 1
:
:
MSB of Digit 8 of Group ID 1

:

: etc........

Byte (4n-3)-4n:


b8
b7
b6
b5
b4
b3
b2
b1
LSB of Digit 7 of Group ID n
:
:
MSB of Digit 7 of Group ID n
LSB of Digit 8 of Group ID n
:
:
MSB of Digit 8 of Group ID n

If storage for fewer than the maximum possible number *n* of VBS Group IDs, is required, the excess bytes shall be set to 'FF'.

10.3.23 EF_{VBSS} (Voice Broadcast Service Status)

This EF contains the status of activation for the VBS group identifiers. The elementary file is directly related to the EF_{VBS}. This EF shall always be allocated if EF_{VBS} is allocated.

Identifier: '6FB4'	Structure: transparent		Optional
File size: 7 bytes	Update activity: low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 7	Activation/Deactivation Flags	M	7 bytes

- Activation/Deactivation Flags

Contents: Activation/Deactivation Flags of the appropriate Group IDs

Coding:

see coding of EF_{VGCS}

10.3.24 EF_{eMLPP} (enhanced Multi Level Pre-emption and Priority)

This EF contains information about priority levels and fast call set-up conditions for the enhanced Multi Level Pre-emption and Priority service that which can be used by the subscriber.

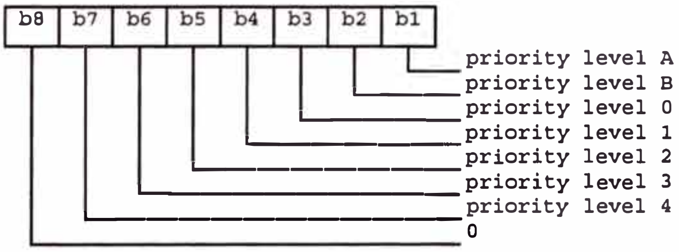
Identifier: '6FB5'	Structure: transparent		Optional
File size: 2 bytes	Update activity: low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Priority levels	M	1 byte
2	Fast call set-up conditions	M	1 byte

- Priority levels

Contents: The eMLPP priority levels subscribed to.

Coding: Each eMLPP priority level is coded on one bit. Priority levels subscribed to have their corresponding bits set to 1. Priority levels not subscribed to have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

Byte 1:



NOTE: Priority levels A and B can not be subscribed to (see GSM 02.67 [42] for details).

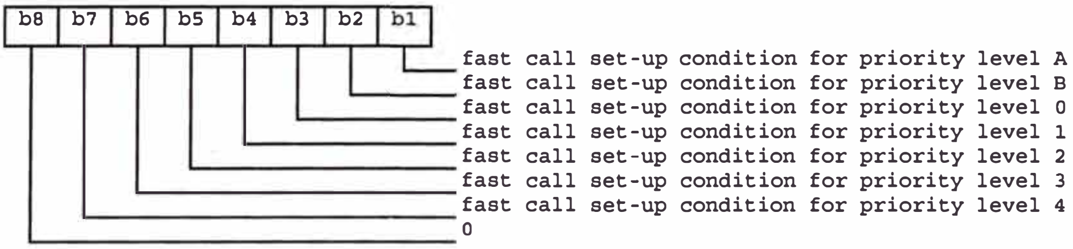
EXAMPLE 1: If priority levels 0, 1 and 2 are subscribed to, EF$_{eMLPP}$ shall be coded '1C'.

- Fast call set-up conditions

  Contents: For each eMLPP priority level, the capability to use a fast call set-up procedure.

  Coding: Each eMLPP priority level is coded on one bit. Priority levels for which fast call set-up is allowed have their corresponding bits set to 1. Priority levels for which fast call set-up is not allowed have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

  Byte 2: fast call set-up condition for:


b8
b7
b6
b5
b4
b3
b2
b1
fast call set-up condition for priority level A
fast call set-up condition for priority level B
fast call set-up condition for priority level 0
fast call set-up condition for priority level 1
fast call set-up condition for priority level 2
fast call set-up condition for priority level 3
fast call set-up condition for priority level 4
0

EXAMPLE 2: If fast call set-up is allowed for priority levels 0 and 1, then byte 2 of EF$_{eMLPP}$ is coded '0C'.

10.3.25 EF$_{AAeM}$ (Automatic Answer for eMLPP Service)

This EF contains those priority levels (of the Multi Level Pre-emption and Priority service) for which the mobile station shall answer automatically to incoming calls.

Identifier: '6FB6'	Structure: transparent		Optional
File size: 1 byte	Update activity: low		
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Automatic answer priority levels	M	1 byte

- Automatic answer priority levels

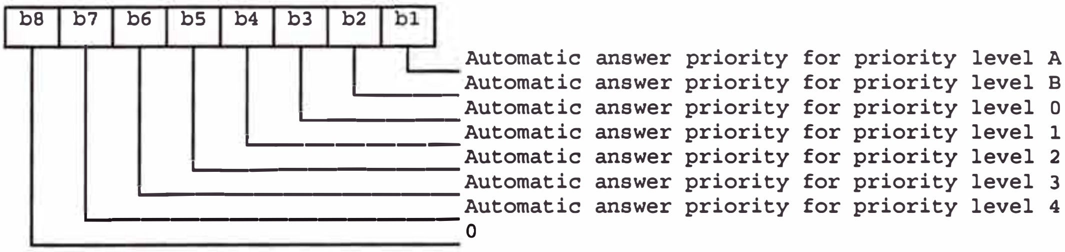
  Contents:

  For each eMLPP priority level, the capability for the mobile station to answer automatically to incoming calls (with the corresponding eMLPP priority level).

  Coding:

  Each eMLPP priority level is coded on one bit. Priority levels allowing an automatic answer from the mobile station have their corresponding bits set to 1. Priority levels not allowing an automatic answer from the mobile station have their corresponding bits set to 0. Bit b8 is reserved and set to 0.

  Byte 1:


b8
b7
b6
b5
b4
b3
b2
b1
Automatic answer priority for priority level A
Automatic answer priority for priority level B
Automatic answer priority for priority level 0
Automatic answer priority for priority level 1
Automatic answer priority for priority level 2
Automatic answer priority for priority level 3
Automatic answer priority for priority level 4
0

EXAMPLE: If automatic answer is allowed for incoming calls with priority levels A, 0 and 1, then $EF_{AAeMLPP}$ is coded '0D'.

10.3.26 EF_{CBMID} (Cell Broadcast Message Identifier for Data Download)

This EF contains the message identifier parameters which specify the type of content of the cell broadcast messages which are to be passed to the SIM.

Any number of CB message identifier parameters may be stored in the SIM. No order of priority is applicable.

Identifier: '6F48'	Structure: transparent		Optional
File size: 2n bytes	Update activity: low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1-2	CB Message Identifier 1	O	2 bytes
3-4	CB Message Identifier 2	O	2 bytes
2n-1-2n	CB Message Identifier n	O	2 bytes

- Cell Broadcast Message Identifier

  Coding:

  as in GSM 03.41 [14]. Values listed show the identifiers of messages which shall be accepted by the MS to be passed to the SIM.

  Unused entries shall be set to 'FF FF'.

10.3.27 EF_{ECC} (Emergency Call Codes)

This EF contains up to 5 emergency call codes.

Identifier: '6FB7'	Structure: transparent		Optional
File size: 3n (n ≤ 5) bytes	Update activity: low		
Access Conditions: READ ALW UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 3	Emergency Call Code 1	O	3 bytes
4 - 6	Emergency Call Code 2	O	3 bytes
(3n-2) - 3n	Emergency Call Code n	O	3 bytes

- Emergency Call Code

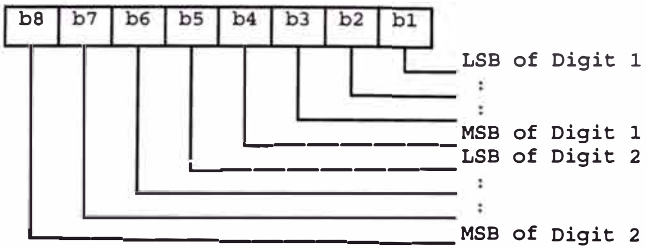
  Contents:

  Emergency Call Code

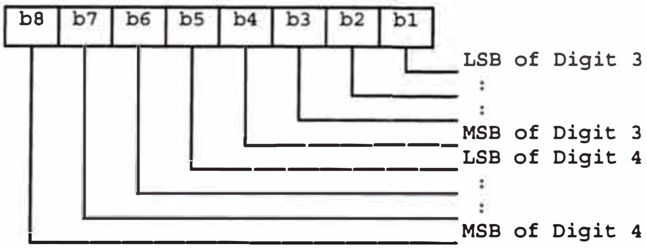
  Coding:

The emergency call code is of a variable length with a maximum length of 6 digits. Each emergency call code is coded on three bytes, with each digit within the code being coded on four bits as shown below. If a code of less that 6 digits is chosen, then the unused nibbles shall be set to 'F'.

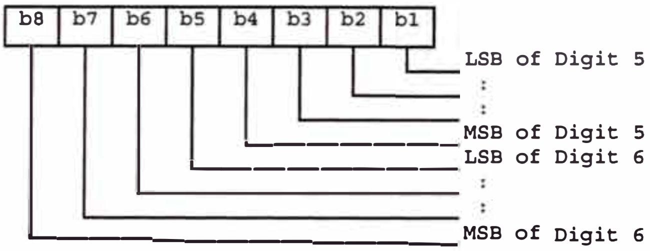
Byte 1:



Byte 2:



Byte 3:



10.3.28 EF$_{CBMIR}$ (Cell broadcast message identifier range selection)

This EF contains ranges of cell broadcast message identifiers that the subscriber wishes the MS to accept.

Any number of CB Message Identifier Parameter ranges may be stored in the SIM. No order of priority is applicable.

Identifier: '6F50'	Structure: transparent		Optional
File size: 4n bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 4	CB Message Identifier Range 1	O	4 bytes
5 - 8	CB Message Identifier Range 2	O	4 bytes
(4n-3) - 4n	CB Message Identifier Range n	O	4 bytes

- Cell Broadcast Message Identifier Ranges

  Contents:

  CB Message Identifier ranges:

Coding:

bytes one and two of each range identifier equal the lower value of a cell broadcast range, bytes three and four equal the upper value of a cell broadcast range, both values are coded as in GSM 03.41 [14] "Message Format on BTS-MS Interface - Message Identifier". Values listed show the ranges of messages which shall be accepted by the MS.

Unused entries shall be set to 'FF FF FF FF'.

10.3.29 EF$_{DCK}$ De-personalization Control Keys

This EF provides storage for the de-personalization control keys associated with the OTA de-personalization cycle of GSM 02.22.

Identifier: '6F2C'	Structure: transparent		Optional
File size: 16 bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 to 4	8 digits of network de-personalization control key	M	4 bytes
5 to 8	8 digits of network subset de-personalization control key	M	4 bytes
9 to 12	8 digits of service provider de-personalization control key	M	4 bytes
13 to 16	8 digits of corporate de-personalization control key	M	4 bytes

Empty control key records shall be coded 'FFFFFFFF'.

10.3.30 EF$_{CNL}$ (Co-operative Network List)

This EF contains the Co-operative Network List for the multiple network personalization services defined in GSM 02.22.

Identifier: '6F32'	Structure: transparent		Optional
File size: 6n bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 to 6	Element 1 of co-operative net list	O	6 bytes
6n-5 to 6n	Element n of co-operative net list	O	6 bytes

- Co-operative Network List

Contents:

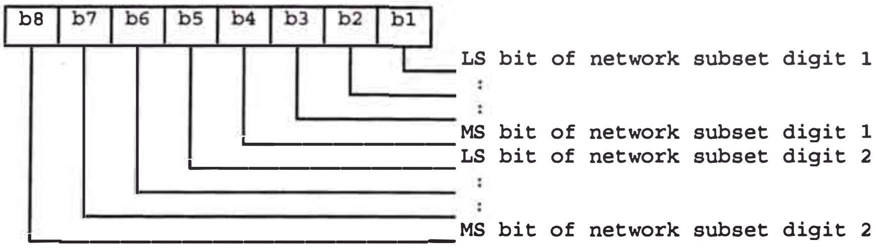
PLMN network subset, service provider ID and corporate ID of co-operative networks.

Coding:

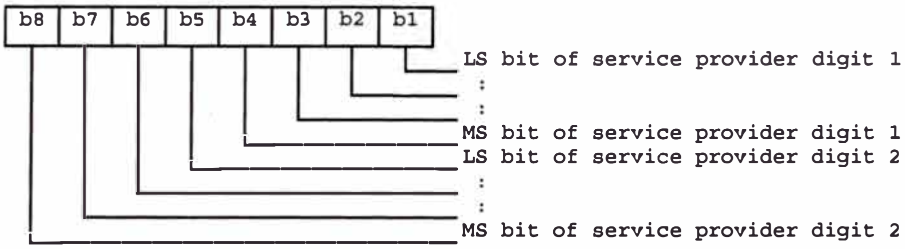
For each 6 byte list element

Byte 1 to 3 : PLMN (MCC + MNC) : according to GSM 04.08 [15].

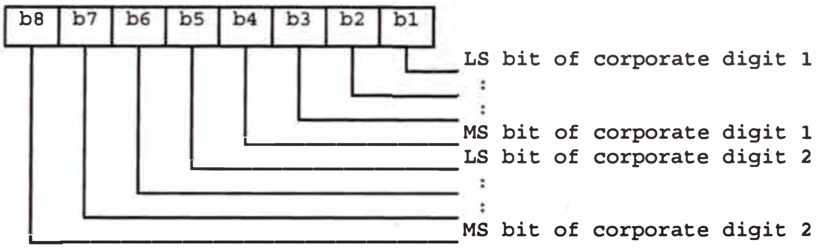
Byte 4:


b8
b7
b6
b5
b4
b3
b2
b1
LS bit of network subset digit 1
:
:
MS bit of network subset digit 1
LS bit of network subset digit 2
:
:
MS bit of network subset digit 2

Byte 5:


b8
b7
b6
b5
b4
b3
b2
b1
LS bit of service provider digit 1
:
:
MS bit of service provider digit 1
LS bit of service provider digit 2
:
:
MS bit of service provider digit 2

Byte 6:


b8
b7
b6
b5
b4
b3
b2
b1
LS bit of corporate digit 1
:
:
MS bit of corporate digit 1
LS bit of corporate digit 2
:
:
MS bit of corporate digit 2

Empty fields shall be coded with 'FF'.

The end of the list is delimited by the first MCC field coded 'FFF'.

10.3.31 EF$_{NIA}$ (Network's Indication of Alerting)

This EF contains categories and associated text related to the Network's indication of alerting in the MS service defined in GSM 02.07 [3].

Identifier: '6F51'	Structure: linear fixed		Optional
Record length : X+1 bytes	Update activity: low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Alerting category	M	1 byte
2 to X+1	Informative text	M	X bytes

- Alerting category

Contents:

category of alerting for terminating traffic.

Coding:

according to GSM 04.08 [15]. Value 'FF' means that no information on alerting category is available.

- Informative text

Contents:

text describing the type of terminating traffic associated with the category.

Coding:

see the coding of the Alpha Identifier item of the EF$_{ADN}$ (subclause 10.5.1). The maximum number of characters for this informative text is indicated in GSM 02.07 [3].

10.3.32 EF$_{KcGPRS}$ (GPRS Ciphering key KcGPRS)

This EF contains the ciphering key KcGPRS and the ciphering key sequence number n for GPRS (see GSM 03.60 [32]).

Identifier: '6F52'	Structure: transparent		Optional
File size: 9 bytes		Update activity: high	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1 - 8	Ciphering key KcGPRS	M	8 bytes
9	Ciphering key sequence number n for GPRS	M	1 byte

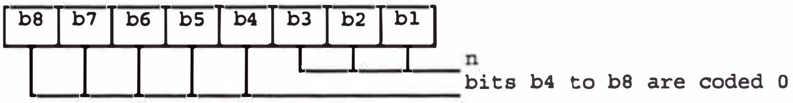
- Ciphering key KcGPRS

Coding:

The least significant bit of KcGPRS is the least significant bit of the eighth byte. The most significant bit of KcGPRS is the most significant bit of the first byte.

- Ciphering key sequence number n for GPRS

Coding:



NOTE: GSM 04.08 [15] defines the value of n=111 as "key not available". Therefore the value '07' and not 'FF' should be present following the administrative phase.

10.3.33 EF$_{LOCIGPRS}$ (GPRS location information)

This EF contains the following Location Information:

- Packet Temporary Mobile Subscriber Identity (P-TMSI);
- Packet Temporary Mobile Subscriber Identity signature value (P-TMSI signature value);
- Routing Area Information (RAI);
- Routing Area update status.

Identifier: '6F53'	Structure: transparent	Optional
File size: 14 bytes	Update activity: high	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 - 4	P-TMSI	M	4 bytes
5 – 7	P-TMSI signature value	M	3 bytes
8 - 13	RAI	M	6 bytes
14	Routing Area update status	M	1 byte

- P-TMSI

Contents: Packet Temporary Mobile Subscriber Identity

Coding: according to GSM 04.08 [15].

Byte 1: first byte of P-TMSI

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- P-TMSI signature value

Contents: Packet Temporary Mobile Subscriber Identity signature value

Coding: according to GSM 04.08 [15].

Byte 5: first byte of P-TMSI signature value

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- RAI

Contents: Routing Area Information

Coding: according to GSM 04.08 [15].

Byte 8: first byte of RAI

b8	b7	b6	b5	b4	b3	b2	b1
MSB							

- Routing area update status

Contents: status of routing area update according to GSM 04.08 [15].

Coding:

Byte 14:

Bits:	b3	b2	b1	
	0	0	0	: updated
	0	0	1	: not updated
	0	1	0	: PLMN not allowed
	0	1	1	: Routing Area not allowed
	1	1	1	: reserved

Bits b4 to b8 are RFU (see subclause 9.3).

10.3.34 EF$_{SUME}$ (SetUpMenu Elements)

This EF contains Simple TLVs related to the menu title to be used by a SIM card supporting the SIM API when issuing a SET UP MENU proactive command.

Identifier: '6F54'	Structure: transparent	Optional
File size: X+Y bytes	Update activity: low	
Access Conditions: READ ADM UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 - X	Title Alpha Identifier	M	X bytes
1+X - X+Y	Title Icon Identifier	O	Y bytes

- Title Alpha Identifier

Contents:

this field contains the Alpha Identifier Simple TLV defining the menu title text.

Coding:

according to GSM 11.14 [27].

Title Icon Identifier

Contents:

this field contains the Icon Identifier Simple TLV defining the menu title icon.

Coding:

according to GSM 11.14 [27].
If not present the field shall be set to 'FF'.

Unused bytes of this file shall be set to 'FF'.

10.3.35 EF$_{PLMNwACT}$ (PLMN Selector with Access Technology)

This EF contains coding for n PLMNs, where n is at least eight. This information, determined by the user, defines the preferred PLMNs of the user in priority order. The EF also contains the Access Technologies for each PLMN in this list. The MS use this information to determine what type of channels to scan for when searching for a specific PLMN (see GSM 03.22 [45]).

Identifier:'6F60'	Structure: transparent	Optional
File size: 4n (n ≥ 8) bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 – 3	1st PLMN (highest priority)	M	3 bytes
4	Access Technologies of 1st PLMN in PLMN selector with Access Technology	M	1 byte
5–7	2nd PLMN	M	3 bytes
8	Access Technologies of 2nd PLMN in PLMN selector with Access Technology	M	1 byte
(4n–3)--(4n–1)	nth PLMN (lowest priority)	O	3 bytes
4n	Access Technologies of nth PLMN in PLMN selector with Access Technology	O	1 byte

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

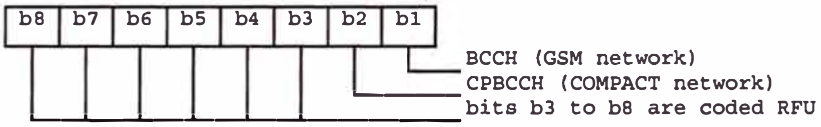
  Coding:

  according to TS 24.008 [47].

- Access Technologies

  Contents: The Access Technologies of a PLMN that the MS will assume when searching for a listed PLMN.

  Coding:



A '1' in a bit position indicates that the Access Technology corresponding to that bit position is supported and a '0' that it is not supported. The RFU bits are coded with '0' in the bit positions.

The default coding of the Access Technologies field shall be '01'.

A user initiated update of a PLMN shall automatically initiate an update of the associated Access Technologies field, according to the Access Technologies identified by the MS for the respective PLMN. If no Access Technologies are identified, the default coding value shall apply for the associated Access Technologies field.

If storage for fewer than the maximum possible number n is required, the excess bytes shall be set to 'FF'.

For instance, using 246 for the MCC and 81 for the MNC for a GSM-only PLMN, and if this is the first and only PLMN in the list, the contents reads as follows:

Bytes 1-3: '42' 'F6' '18'

Byte 4 : '01'

Bytes 5-7: 'FF' 'FF' 'FF'

Byte 8 : 'FF'

etc.

10.3.36 $EF_{OPLMNwACT}$ (Operator controlled PLMN Selector with Access Technology)

This EF contains coding for n PLMNs, where n is at least eight. This information, determined by the operator, defines the preferred PLMNs of the operator in priority order. The EF also contains the Access Technologies for each PLMN in this list. The MS uses this information to determine what type of channels to scan for when searching for a specific PLMN (see GSM 03.22 [45]).

Identifier: '6F61'	Structure: transparent	Optional
File size: 4n (n ≥ 8) bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 – 3	1st PLMN (highest priority)	M	3 bytes
4	Access Technologies of 1st PLMN in Operator controlled PLMN selector with Access Technology	M	1 byte
5–7	2nd PLMN	M	3 bytes
8	Access Technologies of 2nd PLMN in Operator controlled PLMN selector with Access Technology	M	1 byte
(4n–3)–(4n–1)	nth PLMN (lowest priority)	O	3 bytes
4n	Access Technologies of nth PLMN in Operator controlled PLMN selector with Access Technology	O	1 byte

- PLMN

  Contents:

  Mobile Country Code (MCC) followed by the Mobile Network Code (MNC).

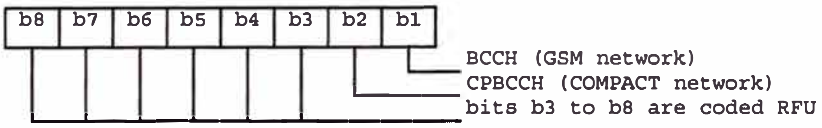
  Coding:

  according to TS 24.008 [47].

- Access Technologies

  Contents: The Access Technologies of a PLMN that the MS will assume when searching for a listed PLMN.

  Coding:



A '1' in a bit position indicates that the Access Technology corresponding to that bit position is supported and a '0' that it is not supported. The RFU bits are coded with '0' in the bit positions.

The default coding of the Access Technologies field shall be '01'.

If storage for fewer than the maximum possible number n is required, the excess bytes shall be set to 'FF'.

For instance, using 246 for the MCC and 81 for the MNC for a GSM-only PLMN and if this is the first and only PLMN in the list, the contents reads as follows:

Bytes 1-3: '42' 'F6' '18'

Byte 4 : '01'

Bytes 5-7: 'FF' 'FF' 'FF'

Byte 8 : 'FF'

etc.

10.3.37 EF$_{HPLMNACT}$ (HPLMN Access Technology)

This EF contains the Access Technology for the HPLMN (see EF$_{IMSI}$). The MS uses this information to determine what type of channels to scan for when searching for the HPLMN and in what priority order. (see GSM 03.22 [45]).

If this EF does not exist on the SIM then the MS shall assume that HPLMN use BCCH.

Identifier: '6F62'	Structure: transparent		Optional
File size: n bytes		Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			

Bytes	Description	M/O	Length
1	Access Technology 1 of HPLMN	O	1 byte
2	Access Technology 2 of HPLMN	O	1 byte
n	Access Technology n of HPLMN	O	1 byte

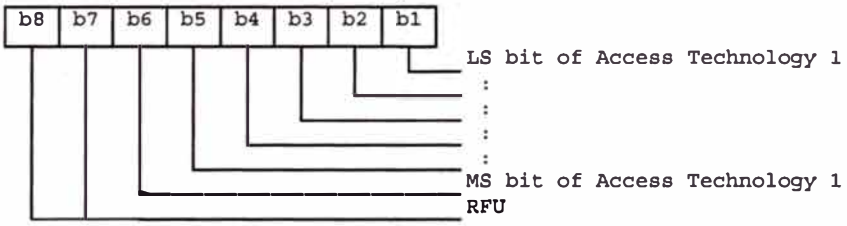
- Access Technology

Contents: The Access Technology of the HPLMN that the MS will assume when searching for the HPLMN, in priority order. The first Access Technology in the list has the highest priority.

Coding:

For each 1 byte list element

Byte 1:



Byte:

Bits:	b6	b5	b4	b31	b3	b2	b1	
	0	0	0	0	0	0	1	BCCH
	0	0	0	0	0	1	0	CPBCCH

The default coding of the Access Technology field shall be '000001'.

The RFU bit positions shall be set to '0'.

10.3.38 EF$_{CPBCCH}$ (CPBCCH Information)

This EF contains information concerning the CPBCCH according to GSM 04. 18[48] and GSM 03.22 [45].

CPBCCH storage may reduce the extent of a Mobile Station's search of CPBCCH carriers when selecting a cell. The CPBCCH carrier lists shall be in accordance with the procedures specified in GSM 04.18 [48], GSM 04.60 [49] and GSM 03.22 [45]. The MS stores CPBCCH information from the System Information 19 message, Packet System Information 3, and Packet System Information 3 bis on the SIM. The same CPBCCH carrier shall never occur twice in the list.

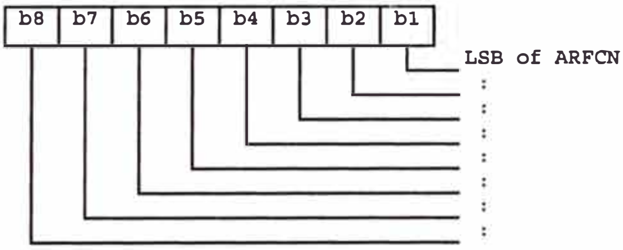
Identifier: '6F63'	Structure: transparent	Optional
File size: 2n bytes	Update activity: high	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to 2	Element 1 of CPBCCH carrier list	M	2 bytes
2n-1 to 2n	Element n of CPBCCH carrier list	M	2 bytes

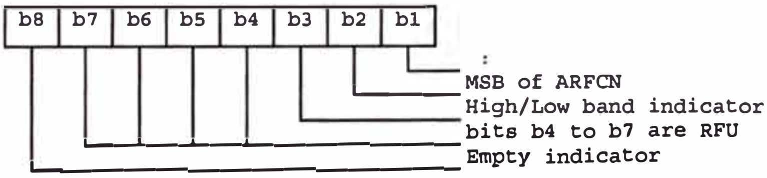
- Element in CPBCCH carrier list

  Coding:

  Byte 1: first byte of CPBCCH carrier list element



  Byte 2: second byte of CPBCCH carrier list element



  - ARFCN (10 bits) as defined in GSM 05.05 [46].
  - High/Low band indicator: If the ARFCN indicates possibly a channel in the DCS 1800 or a channel in the PCS 1900 band, if the bit is set to '1' the channel is in the higher band (GSM 1900). If the bit is set to '0', the lower band (GSM 1800) is indicated. If ARFCN indicates a unique channel, this indicator shall be set to '0'.
  - Empty indicator: If this bit is set to '1', no CPBCCH carrier is stored in this position. If the Empty Indicator is set to '1', the content of the CPBCCH carrier field shall be ignored. The empty indicator shall also be used, and set to '1', if storage of fewer than maximum number n, of CPBCCH carrier fields is required.

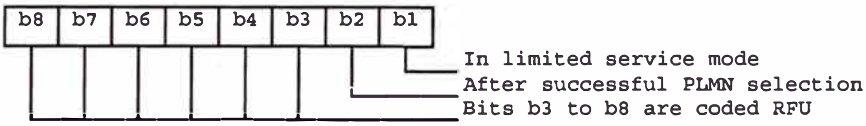
10.3.39 EF$_{\text{InvScan}}$ (Investigation PLMN Scan)

This EF contains two flags used to control the investigation scan for higher prioritized PLMNs not offering voice services.

Identifier: '6F64'	Structure: transparent		Optional
File size: 1 byte	Update activity: low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Investigation scan flags	M	1 bytes

- Investigation scan flags

  Coding:



A '1' in a bit position indicates that the investigation scan shall be performed for the condition corresponding to that bit position and a '0' that it shall not be performed.

If this elementary file is not present, no investigation scan shall be performed.

10.4 Contents of DFs at the GSM application level

10.4.1 Contents of files at the GSM SoLSA level

This subclause specifies the EFs in the dedicated file DF_{SoLSA}. It only applies if the SoLSA feature is supported (see GSM 03.73 [33]).

The EFs contain information about the users subscribed local service areas.

10.4.1.1 EF_{SAI} (SoLSA Access Indicator)

This EF contains the 'LSA only access indicator'. This EF shall always be allocated if DF_{SoLSA} is present.

If the indicator is set, the network will prevent terminated and/or originated calls when the MS is camped in cells that are not included in the list of allowed LSAs in EF_{SLL}. Emergency calls are, however, always allowed.

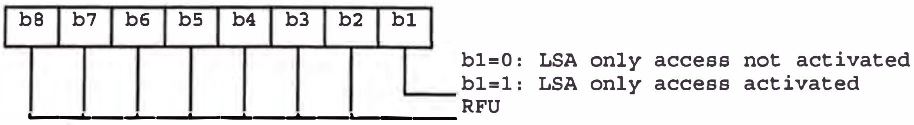
The EF also contains a text string which may be displayed when the MS is out of the served area(s).

Identifier: '4F30'	Structure: transparent		Optional
File size: X + 1 bytes	Update activity: low		
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	LSA only access indicator	M	1 byte
2 to X+1	LSA only access indication text	M	X bytes

- LSA only access indicator

  Contents: indicates whether the MS is restricted to use LSA cells only or not.

Coding:


b8
b7
b6
b5
b4
b3
b2
b1
b1=0: LSA only access not activated
b1=1: LSA only access activated
RFU

- LSA only access indication text

  Contents: text to be displayed by the ME when it's out of LSA area.

  Coding: the string shall use either

  - the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or

  - one of the UCS2 coded options as defined in annex B.

10.4.1.2 EF_{SLL} (SoLSA LSA List)

This EF contains information describing the LSAs that the user is subscribed to. This EF shall always be allocated if DF_{SoLSA} is present.

Each LSA is described by one record that is linked to a LSA Descriptor file. Each record contains information of the PLMN, priority of the LSA, information about the subscription and may also contain a text string and/or an icon that identifies the LSA to the user. The text string can be edited by the user.

Identifier: '4F31'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to X	LSA name	O	X bytes
X+1	Configuration parameters	M	1 byte
X+2	RFU	M	1 byte
X+3	Icon Identifier	M	1 byte
X+4	Priority	M	1 byte
X+5 to X+7	PLMN code	M	3 bytes
X+8 to X+9	LSA Descriptor File Identifier	M	2 byte
X+10	LSA Descriptor Record Identifier	M	1 byte

- LSA name

  Contents: LSA name string to be displayed when the ME is camped in the corresponding area, dependant on the contents of the LSA indication for idle mode field.

  Coding: the string shall use either

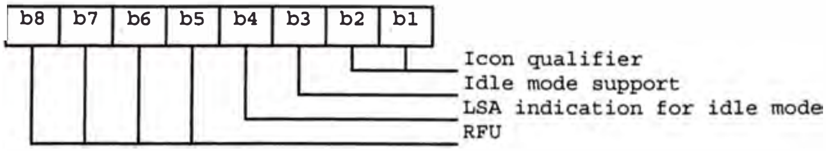
  - the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or

  - one of the UCS2 coded options as defined in annex B.

- Configuration parameters

  Contents: Icon qualifier, control of idle mode support and control of LSA indication for idle mode.

  Coding:



Icon qualifier:

Contents: The icon qualifier indicates to the ME how the icon is to be used.

b2, b1: 00: icon is not to be used and may not be present
01: icon is self-explanatory, i.e. if displayed, it replaces the LSA name
10: icon is not self-explanatory, i.e. if displayed, it shall be displayed together with the LSA name
11: RFU

Idle mode support:

Contents: The idle mode support is used to indicate whether the ME shall favour camping on the LSA cells in idle mode.

b3 = 0: Idle mode support disabled
b3 = 1: Idle mode support enabled

LSA indication for idle mode:

Contents: The LSA indication for idle mode is used to indicate whether or not the ME shall display the LSA name when the ME is camped on a cell within the LSA.

b4 = 0: LSA indication for idle mode disabled
b4 = 1: LSA indication for idle mode enabled

Bits b5 to b8 are RFU (see subclause 9.3).

Icon Identifier

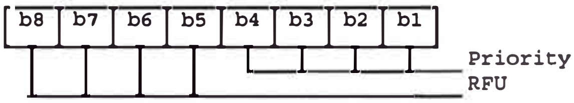
Contents: The icon identifier addresses a record in EF_{IMG}.

Coding: binary.

Priority

Contents: Priority of the LSA which gives the ME the preference of this LSA relative to the other LSAs.

Coding:



'0' is lowest priority, 'F' is highest.

- PLMN code

Contents: MCC + MNC for the LSA.

Coding: according to GSM 04.08 [15] and EF_{LOCI}.

- LSA Descriptor File Identifier:

Contents: these bytes identify the EF which contains the LSA Descriptors forming the LSA.

Coding: byte X+8: high byte of the LSA Descriptor file;
byte X+9: low byte of the LSA Descriptor file.

- LSA Descriptor Record Identifier:

Contents: this byte identifies the number of the first record in the LSA Descriptor file forming the LSA.

Coding: binary.

10.4.1.3 LSA Descriptor files

Residing under DF_{SoLSA}, there may be several LSA Descriptor files. These EFs contains one or more records again containing LSA Descriptors forming the LSAs. LSAs can be described in four different ways. As a list of LSA IDs, as a list of LAC + CIs, as a list of CIs or as a list of LACs. As the basic elements (LSA ID, LAC + CI, CI and LAC) of the four types of lists are of different length, they can not be mixed within one record. Different records may contain different kinds of lists within the EFs. Examples of codings of LSA Descriptor files can be found in annex F.

Identifier: '4FXX'	Structure: linear fixed	Optional
Record length: n*X+2 bytes	Update activity: low	

Access Conditions:

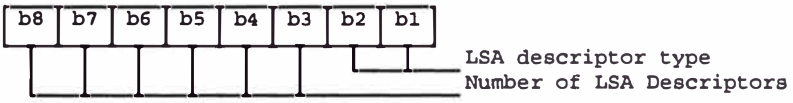
READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	LSA descriptor type and number	M	1 byte
2 to X+1	1st LSA Descriptor	M	X bytes
X+2 to 2X+1	2nd LSA Descriptor	M	X bytes
(n-1)*X+2 to n*X+1	nth LSA Descriptor	M	X bytes
n*X+2	Record Identifier	M	1 byte

- LSA descriptor type and number:

Contents: The LSA descriptor type gives the format of the LSA descriptor and the number of valid LSA Descriptors within the record.

Coding:



LSA descriptor type:

Contents: Gives the format of the LSA Descriptors.

b2, b1:	00: LSA ID.
	01: LAC + CI
	10: CI
	11: LAC

Number of LSA Descriptors:

Contents: Gives the number of valid LSA Descriptors in the record.

Coding: binary, with b8 as MSB and b3 as LSB leaving room for 64 LSA Descriptors per record.

- LSA Descriptor

Contents: Dependant of the coding indicated in the LSA descriptor type:

- in case of LSA ID the field length 'X' is 3 bytes;
- in case of LAC + CI the field length 'X' is 4 bytes;
- in case of CI the field length 'X' is 2 bytes;

- in case of LAC the field length 'X' is 2 bytes.

Coding: according to GSM 04.08 [15].

- Record Identifier:

Contents: This byte identifies the number of the next record containing the LSA Descriptors forming the LSA.

Coding: record number of next record. 'FF' identifies the end of the chain.

This file utilises the concept of chaining as for EF_{EXT1}.

The identifier '4FXX' shall be different from one LSA Descriptor file to the other and different from the identifiers of EF_{SAI} and EF_{SLL}. For the range of 'XX', see subclause 6.6.

10.4.2 Contents of files at the MExE level

This subclause specifies the EFs in the dedicated file DFMExE. It only applies if support of MExE by the SIM is supported (see TS 23.057 [50]).

The EFs in the Dedicated File DFMExE contain execution environment related information.

10.4.2.1 $EF_{MExE-ST}$ (MExE Service table)

This EF indicates which MExE services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the SIM, the ME shall not select this service.

Identifier: '4F40'	Structure: transparent		Optional
File size: X bytes, X ≥ 1		Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Services n°1 to n°4	M	1 byte
2	Services n°5 to n°8	O	1 byte
etc.			
X	Services (4X-3) to (4X)	O	1 byte

-Services

Contents:

Service n°1 :	Operator root public key
Service n°2 :	Administrator root public key
Service n°3 :	Third party root public key
Service n°4 :	RFU

Coding:

2 bits are used to code each service:
first bit = 1: service allocated
first bit = 0: service not allocated
where the first bit is b1, b3, b5 or b7;
second bit = 1: service activated
second bit = 0: service not activated
where the second bit is b2, b4, b6 or b8.

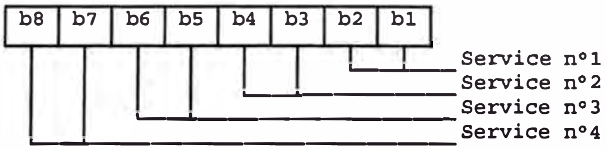
Service allocated means that the SIM has the capability to support the service. Service activated means that the service is available for the card holder (only valid if the service is allocated).

The following codings are possible:

- first bit = 0: service not allocated, second bit has no meaning;
- first bit = 1 and second bit = 0: service allocated but not activated;
- first bit = 1 and second bit = 1: service allocated and activated.

The bits for services not yet defined shall be set to RFU. For coding of RFU see subclause 9.3.

First byte:



etc.

For an example of coding see sub-clause 10.3.7

10.4.2.2 EF$_{ORPK}$ (Operator Root Public Key)

This EF contains the descriptor(s) of certificates containing the Operator Root Public Key. This EF shall only be allocated if the operator wishes to verify applications and certificates in the MExE operator domain using a root public key held on the SIM. Each record of this EF contains one certificate descriptor.

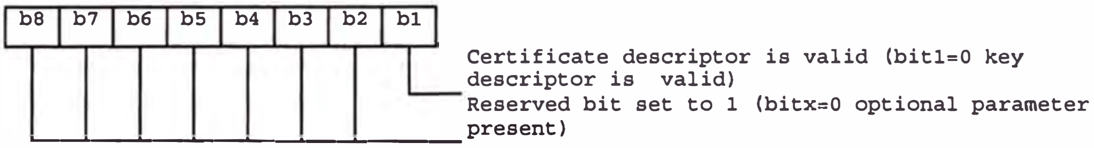
For example, Operator may provide a second key for recover disaster procedure in order to limit OTA data to load.

Identifier: '4F41'	Structure: linear fixed	Optional
Record length : X + 10 bytes	Update activity: low	

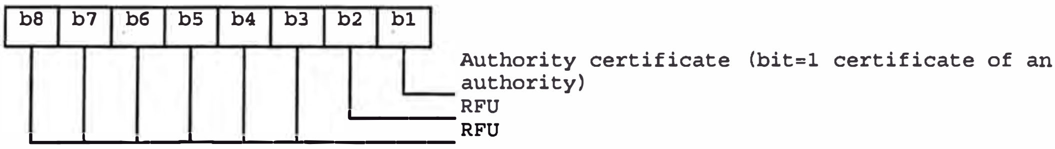
Access Conditions:
READ CHV1
UPDATE ADM
INVALIDATE ADM
REHABILITATE ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (k)	M	1 byte
11 to 10+k	Key identifier	M	k bytes

- Parameter indicator
  Contents:
  The parameter indicator indicates if record is full and which optional parameters are present
  Coding: bit string


b8
b7
b6
b5
b4
b3
b2
b1
Certificate descriptor is valid (bit1=0 key descriptor is valid)
Reserved bit set to 1 (bitx=0 optional parameter present)

- Flags
  Contents:
  The authority flag indicates whether the certificate identify an authority (i.e. CA or AA) or not.
  Coding: bit string



- Type of certificate
  Contents:
  This field indicates the type of certificate containing the key.
  Coding: binary :
  0 : WTLS
  1 : X509
  2 : X9.68
  Other values are reserved for further use

- Key/certificate File Identifier
  Contents:
  these bytes identify an EF which is the key/certificate data file (see subclause 10.7.5), holding the actual key/certificate data for this record.
  Coding:
  byte 4: high byte of Key/certificate File Identifier;
  byte 5: low byte of Key/certificate File Identifier.

- Offset into Key/certificate File
  Contents:
  these bytes specify an offset into the transparent key/certificate data File identified in bytes 4 and 5.
  Coding:
  byte 6: high byte of offset into Key/certificate Data File;
  byte 7: low byte of offset into Key/certificate Data File

- Length of Key/certificate Data
  Contents:
  these bytes yield the length of the key/certificate data, starting at the offset identified in "Offset into Key/certificate File" field.
  Coding:
  byte 8: high byte of Key/certificate Data length;
  byte 9: low byte of Key/certificate Data length.

- Key identifier length
  Contents:
  This field gives length of key identifier
  Coding:
  binary

- Key identifier
  Contents:
  This field provides a means of identifying certificates that contain a particular public key (chain building) and linking the public key to its corresponding private key. For more information about value and using see TS 23.057 [50].
  Coding:
  octet string

Note: transparent key/certificate data longer than 256 bytes may be read using successive READ BINARY commands.

10.4.2.3 EF$_{\text{ARPK}}$ (Administrator Root Public Key)

This EF contains the descriptor(s) of certificates containing the Administrator Root Public Key. This EF shall only be allocated if the SIM issuer wishes to control the Third Party certificates on the terminal using an Administrator Root Public Key held on the SIM. Each record of this EF contains one certificate descriptor.

This file shall contain only one record.

Identifier: '4F42'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (k)	M	1 byte
11 to 10+k	Key identifier	M	k bytes

For contents and coding of all data items see the respective data items of the EF$_{\text{ORPK}}$ (sub-clause 10.4. 2. 1).

10.4.2.4 EF$_{\text{TPRPK}}$ (Third Party Root Public key)

This EF contains descriptor(s) of certificates containing the Third Party Root Public key (s). This EF shall only be allocated if the SIM issuer wishes to verify applications and certificates in the MExE Third Party domain using root public key(s) held on the SIM. This EF can contain one or more root public keys. Each record of this EF contains one certificate descriptor.

For example, an operator may provide several Third Party root public keys.

Identifier: '4F43'	Structure: linear fixed	Optional
Record length : X + 10 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (k)	M	1 byte
11 to 10+k	Key identifier	M	k bytes
11+k to11+k	Certificate identifier length (m)	M	1 byte
12+k to11+k+m	Certificate identifier	M	m bytes

- Certificate identifier length
  Contents:
    This field gives length of certificate identifier
  Coding:
    binary

- Certificate identifier
  Contents:
    This field identify the issuer and provide a easy way to find a certificate. For more information about value and usage, see TS 23.057 [50].
  Coding:
    Octet string

For contents and coding of all other data items see the respective data items of the EF$_{ORPK}$ (sub-clause 10.7.1).

10.4.2.5 Trusted Key/Certificates Data Files

Residing under DF$_{MExE}$, there may be several key/certificates data files. These EFs containing key/certificates data shall have the following attributes:

Identifier: '4FXX'	Structure: transparent	Optional
Record length: Y bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to Y	Key/Certicates Data	M	Y bytes

Contents and coding:

Key/certificate data are accessed using the key/certificates descriptors provided by EF$_{TPRPK}$ (see sub-clause 10.4.2.4).

The identifier '4FXX' shall be different from one key/certificate data file to the other. For the range of 'XX', see sub-clause 6.6. The length Y may be different from one key/certificate data file to the other.

10.5 Contents of files at the telecom level

The EFs in the Dedicated File DF$_{TELECOM}$ contain service related information.

10.5.1 EF$_{ADN}$ (Abbreviated dialling numbers)

This EF contains Abbreviated Dialling Numbers (ADN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F3A'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	CHV2
REHABILITATE	CHV2

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

- Alpha Identifier

Contents:

Alpha-tagging of the associated dialling number.

Coding:

this alpha-tagging shall use either

- the SMS default 7-bit coded alphabet as defined in GSM 03.38 [12] with bit 8 set to 0. The alpha identifier shall be left justified. Unused bytes shall be set to 'FF'; or
- one of the UCS2 coded options as defined in annex B.

NOTE 1: The value of X may be from zero to 241. Using the command GET RESPONSE the ME can determine the value of X.

- Length of BCD number/SSC contents

Contents:

this byte gives the number of bytes of the following two data items containing actual BCD number/SSC information. This means that the maximum value is 11, even when the actual ADN/SSC information length is greater than 11. When an ADN/SSC has extension, it is indicated by the extension1 identifier being unequal to 'FF'. The remainder is stored in the EF_{EXT1} with the remaining length of the additional data being coded in the appropriate additional record itself (see subclause 10.5.10).

Coding:

according to GSM 04.08 [15].

- TON and NPI

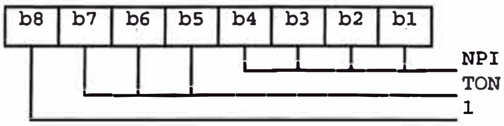
Contents:

Type of number (TON) and numbering plan identification (NPI).

Coding:

according to GSM 04.08 [15]. If the Dialling Number/SSC String does not contain a dialling number, e.g. a control string deactivating a service, the TON/NPI byte shall be set to 'FF' by the ME (see note 2).

NOTE 2: If a dialling number is absent, no TON/NPI byte is transmitted over the radio interface (see GSM 04.08 [15]). Accordingly, the ME should not interpret the value 'FF' and not send it over the radio interface.



- Dialling Number/SSC String

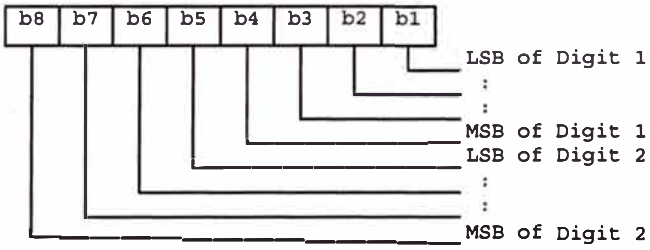
Contents:

up to 20 digits of the telephone number and/or SSC information.

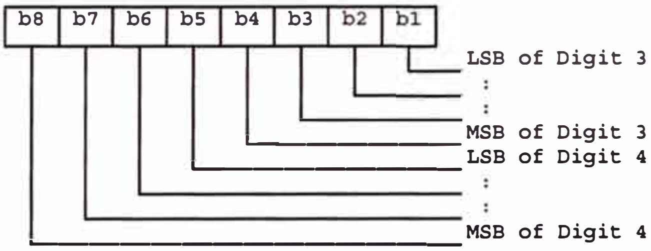
Coding:

according to GSM 04.08 [15] , GSM 02.30 [8] and the extended BCD-coding (see table 12). If the telephone number or SSC is longer than 20 digits, the first 20 digits are stored in this data item and the remainder is stored in an associated record in the EF_{EXT1}. The record is identified by the Extension1 Record Identifier. If ADN/SSC require less than 20 digits, excess nibbles at the end of the data item shall be set to 'F'. Where individual dialled numbers, in one or more records, of less than 20 digits share a common appended digit string the first digits are stored in this data item and the common digits stored in an associated record in the EF_{EXT1}. The record is identified by the Extension 1 Record Identifier. Excess nibbles at the end of the data item shall be set to 'F'.

Byte X+3



Byte X+4:



etc.

- Capability/Configuration Identifier

Contents:

capability/configuration identification byte. This byte identifies the number of a record in the EF_{CCP} containing associated capability/configuration parameters required for the call. The use of this byte is optional. If it is not used it shall be set to 'FF'.

Coding:

binary.

- Extension1 Record Identifier

Contents:

extension1 record identification byte. This byte identifies the number of a record in the EF_{EXT1} containing an associated called party subaddress or additional data. The use of this byte is optional. If it is not used it shall be set to 'FF'.

If the ADN/SSC requires both additional data and called party subaddress, this byte identifies the additional record. A chaining mechanism inside EF_{EXT1} identifies the record of the appropriate called party subaddress (see subclause 10.5.10).

Coding:

binary.

NOTE 3: As EF_{ADN} is part of the $DF_{TELECOM}$ it may be used by GSM and also other applications in a multi-application card. If the non-GSM application does not recognize the use of Type of Number (TON) and Number Plan Identification (NPI), then the information relating to the national dialling plan must be held within the data item dialling number/SSC and the TON and NPI fields set to UNKNOWN. This format would be acceptable for GSM operation and also for the non-GSM application where the TON and NPI fields shall be ignored.

EXAMPLE: SIM storage of an International Number using E.164 [19] numbering plan.

	TON	NPI	Digit field
GSM application	001	0001	abc...
Other application compatible with GSM	000	0000	xxx...abc...

where "abc..." denotes the subscriber number digits (including its country code), and "xxx..." denotes escape digits or a national prefix replacing TON and NPI.

NOTE 4: When the ME acts upon the EF_{ADN} with a SEEK command in order to identify a character string in the alpha-identifier, it is the responsibility of the ME to ensure that the number of characters used as SEEK parameters are less than or equal to the value of X if the MMI allows the user to offer a greater number.

Table 12: Extended BCD coding

BCD Value	Character/Meaning
'0'	"0"
...	...
'9'	"9"
'A'	"*"
'B'	"#"
'C'	DTMF Control digit separator (GSM 02.07 [3])
'D'	"Wild" value This will cause the MMI to prompt the user for a single digit (see GSM 02.07 [3]).
'E'	Expansion digit ("Shift Key"). It has the effect of adding '10' to the following digit. The following BCD digit will hence be interpreted in the range of '10'-'1E'. The purpose of digits in this range is for further study.
'F'	Endmark e.g. in case of an odd number of digits

BCD values 'C', 'D' and 'E' are never sent across the radio interface.

NOTE 5: The interpretation of values 'D', 'E' and 'F' as DTMF digits is for further study.

NOTE 6: A second or subsequent 'C' BCD value will be interpreted as a 3 second PAUSE (see GSM 02.07 [3]).

10.5.2 EF$_{FDN}$ (Fixed dialling numbers)

This EF contains Fixed Dialling Numbers (FDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F3B'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:
READ CHV1
UPDATE CHV2
INVALIDATE ADM
REHABILITATE ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension2 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF$_{ADN}$ (subclause 10.5.1), with the exception that extension records are stored in the EF$_{EXT2}$.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF$_{ADN}$.

10.5.3 EF$_{SMS}$ (Short messages)

This EF contains information in accordance with GSM 03.40 [13] comprising short messages (and associated parameters) which have either been received by the MS from the network, or are to be used as an MS originated message.

Identifier: '6F3C'	Structure: linear fixed	Optional
Record length: 176 bytes	Update activity: low	

Access Conditions:
READ CHV1
UPDATE CHV1
INVALIDATE ADM
REHABILITATE ADM

Bytes	Description	M/O	Length
1	Status	M	1 byte
2 to 176	Remainder	M	175 bytes

- Status

Contents:

Status byte of the record which can be used as a pattern in the SEEK command. For MS originating messages sent to the network, the status shall be updated when the MS receives a status report, or sends a successful SMS Command relating to the status report.

Coding:

```
b8  b7  b6  b5  b4  b3  b2  b1
                    X   X   0   free space
                    X   X   1   used space
                    0   0   1   message received by MS from network; message read
                    0   1   1   message received by MS from network; message to be
                                read
                    1   1   1   MS originating message; message to be sent

|___|___|___|___|______________ RFU (see subclause 9.3)
```

```
b8  b7  b6  b5  b4  b3  b2  b1
            X   X   1   0   1   MS originating message; message sent to the network:
            0   0   1   0   1     status report not requested
            0   1   1   0   1     status report requested but not (yet) received;
            1   0   1   0   1     status report requested, received but not stored
                                       in EF-SMSR;
            1   1   1   0   1     status report requested, received and stored
                                       in EF-SMSR;

|___|___|______________________ RFU (see subclause 9.3)
```

- Remainder

Contents:

This data item commences with the TS-Service-Centre-Address as specified in GSM 04.11 [16]. The bytes immediately following the TS-Service-Centre-Address contain an appropriate short message TPDU as specified in GSM 03.40 [13], with identical coding and ordering of parameters.

Coding:

according to GSM 03.40 [13] and GSM 04.11 [16]. Any TP-message reference contained in an MS originated message stored in the SIM, shall have a value as follows:

	Value of the TP-message-reference:
message to be sent:	'FF'
message sent to the network:	the value of TP-Message-Reference used in the message sent to the network.

Any bytes in the record following the TPDU shall be filled with 'FF'.

It is possible for a TS-Service-Centre-Address of maximum permitted length, e.g. containing more than 18 address digits, to be associated with a maximum length TPDU such that their combined length is 176 bytes. In this case the ME shall store in the SIM the TS-Service-Centre-Address and the TPDU in bytes 2-176 without modification, except for the last byte of the TPDU, which shall not be stored.

10.5.4 Capability configuration parameters

10.5.4.1 EF_{CCP} (Capability configuration parameters)

This EF contains parameters of required network and bearer capabilities and ME configurations associated with a call established using an abbreviated dialling number, a fixed dialling number, an MSISDN, a last number dialled, a service dialling number or a barred dialling number.

For compatibility reasons, this file may be present for release 98 or earlier MEs in order to support Capability Configuration Parameters service.

Identifier: '6F3D'	Structure: linear fixed	Optional
Record length: 14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to 10	Bearer capability information element	M	10 bytes
11 to 14	Bytes reserved - see below	M	4 bytes

- Bearer capability information element

  Contents and Coding:

  - see GSM 04.08 [15]. The Information Element Identity (IEI) shall be excluded. i.e. the first byte of the EF$_{\text{CCP}}$ record shall be Length of the bearer capability contents.

  - Bytes 11-14 shall be set to 'FF' and shall not be interpreted by the ME.

10.5.4.2 EF$_{\text{ECCP}}$ (Extended Capability configuration parameters)

This EF contains parameters of required network and bearer capabilities and ME configurations associated with a call established using an abbreviated dialling number, a fixed dialling number, an MSISDN, a last number dialled, a service dialling number or a barred dialling number.

The number of records of the EF$_{\text{ECCP}}$ shall be equal to the number of records of the EF$_{\text{CCP}}$. Each record of the EF$_{\text{CCP}}$ shall have a corresponding record in the EF$_{\text{ECCP}}$ with the same record number.

If an ME has to update a record, then the ME shall update each record of both files, EF$_{\text{CCP}}$ with 10 bytes and EF$_{\text{ECCP}}$ with X bytes ($X \geq 15$).

If an ME has to read a record, then the ME shall check the consistency between the record of the EF$_{\text{ECCP}}$ and the corresponding record of the EF$_{\text{CCP}}$ and update the record of the EF$_{\text{ECCP}}$ with the value of the corresponding record of the EF$_{\text{CPP}}$.

Identifier: '6F4F'	Structure: linear fixed	Optional
Record length: X ($X \geq 15$)	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Bearer capability information element	M	X bytes

- Bearer capability information element

  Contents and Coding:

  see TS 24.008 [47]. The Information Element Identity (IEI) shall be excluded, i.e. the first byte of the EF$_{\text{ECCP}}$ record shall be Length of the bearer capability contents.

  Unused bytes are filled with 'FF'.

10.5.5 EF$_{\text{MSISDN}}$ (MSISDN)

This EF contains MSISDN(s) related to the subscriber. In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F40'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of EF_{ADN}.

NOTE 1: If the SIM stores more than one MSISDN number and the ME displays the MSISDN number(s) within the initialization procedure then the one stored in the first record shall be displayed with priority.

NOTE 2: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.5.6 EF_{SMSP} (Short message service parameters)

This EF contains values for Short Message Service header Parameters (SMSP), which can be used by the ME for user assistance in preparation of mobile originated short messages. For example, a service centre address will often be common to many short messages sent by the subscriber.

The EF consists of one or more records, with each record able to hold a set of SMS parameters. The first (or only) record in the EF shall be used as a default set of parameters, if no other record is selected.

To distinguish between records, an alpha-identifier may be included within each record, coded on Y bytes.

The SMS parameters stored within a record may be present or absent independently. When a short message is to be sent from the MS, the parameter in the SIM record, if present, shall be used when a value is not supplied by the user.

Identifier: '6F42'	Structure: linear fixed	Optional
Record length: 28+Y bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to Y	Alpha-Identifier	O	Y bytes
Y+1	Parameter Indicators	M	1 byte
Y+2 to Y+13	TP-Destination Address	M	12 bytes
Y+14 to Y+25	TS-Service Centre Address	M	12 bytes
Y+26	TP-Protocol Identifier	M	1 byte
Y+27	TP-Data Coding Scheme	M	1 byte
Y+28	TP-Validity Period	M	1 byte

Storage is allocated for all of the possible SMS parameters, regardless of whether they are present or absent. Any bytes unused, due to parameters not requiring all of the bytes, or due to absent parameters, shall be set to 'FF'.

- Alpha-Identifier

Contents:

Alpha Tag of the associated SMS-parameter.

Coding:

see subclause 10.5.1 (EF$_{ADN}$).

NOTE: The value of Y may be zero, i.e. the alpha-identifier facility is not used. By using the command GET RESPONSE the ME can determine the value of Y.

- Parameter Indicators

Contents:

Each of the default SMS parameters which can be stored in the remainder of the record are marked absent or present by individual bits within this byte.

Coding:

Allocation of bits:

Bit number	Parameter indicated
1	TP-Destination Address
2	TS-Service Centre Address
3	TP-Protocol Identifier
4	TP-Data Coding Scheme
5	TP-Validity Period
6	reserved, set to 1
7	reserved, set to 1
8	reserved, set to 1

Bit value	Meaning
0	Parameter present
1	Parameter absent

- TP-Destination Address

Contents and Coding: As defined for SM-TL address fields in GSM 03.40 [13].

- TP-Service Centre Address

Contents and Coding: As defined for RP-Destination address Centre Address in GSM 04.11 [16].

- TP-Protocol Identifier

Contents and Coding: As defined in GSM 03.40 [13].

- TP-Data Coding Scheme

Contents and Coding: As defined in GSM 03.38 [12].

- TP-Validity Period

Contents and Coding: As defined in GSM 03.40 [13] for the relative time format.

10.5.7 EF$_{SMSS}$ (SMS status)

This EF contains status information relating to the short message service.

The provision of this EF is associated with EF$_{SMS}$. Both files shall be present together, or both absent from the SIM.

Identifier: '6F43'	Structure: transparent	Optional
File size: 2+X bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Last Used TP-MR	M	1 byte
2	SMS "Memory Cap. Exceeded" Not. Flag	M	1 byte
3 to 2+X	RFU	O	X bytes

Last Used TP-MR.

Contents:

the value of the TP-Message-Reference parameter in the last mobile originated short message, as defined in GSM 03.40 [13].

Coding:

as defined in GSM 03.40 [13].

SMS "Memory Capacity Exceeded" Notification Flag.

Contents:

This flag is required to allow a process of flow control, so that as memory capacity in the MS becomes available, the Network can be informed. The process for this is described in GSM 03.40 [13].

Coding:

b1=1 means flag unset; memory capacity available

b1=0 means flag set

b2 to b8 are reserved and set to 1.

10.5.8 EF_{LND} (Last number dialled)

This EF contains the last numbers dialled (LND) and/or the respective supplementary service control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain associated alpha-tagging.

Identifier: '6F44'	Structure: cyclic	Optional
Record length: X+14 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE CHV1 INCREASE NEVER INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension1 Record Identifier	M	1 byte

For contents and coding, see subclause 10.5.1 EF_{ADN}.

The value of X in EF_{LND} may be different to both the value of X in EF_{ADN} and of X in EF_{FDN}.

If the value of X in EF_{LND} is longer than the length of the α-tag of the number to be stored, then the ME shall pad the α-tag with 'FF'. If the value of X in EF_{LND} is shorter than the length of the α-tag of the number to be stored, then the ME shall cut off excessive bytes.

10.5.9 EF_{SDN} (Service Dialling Numbers)

This EF contains special service numbers (SDN) and/or the respective supplementary service control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain associated alpha-tagging.

Identifier: '6F49'	Structure: linear fixed	Optional
Record length: X+14 bytes	Update activity: low	

Access Conditions:
READ CHV1
UPDATE ADM
INVALIDATE ADM
REHABILITATE ADM

Bytes	Description	M/O	Length
1-X	Alpha identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 bytes
X+2	TON and NPI	M	1 byte
X+3-X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension3 Record Identifier	M	1 byte

For contents and coding of all data items see the respective data items of the EF_{ADN} (subclause 10.5.1), with the exception that extension records are stored in the EF_{EXT3}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.5.10 EF_{EXT1} (Extension1)

This EF contains extension data of an ADN/SSC, an MSISDN, or an LND. Extension data is caused by:

- an ADN/SSC (MSISDN, LND) which is greater than the 20 digit capacity of the ADN/SSC (MSISDN, LND) Elementary File or where common digits are required to follow an ADN/SSC string of less than 20 digits. The remainder is stored in this EF as a record, which is identified by a specified identification byte inside the ADN/SSC (MSISDN, LND) Elementary File. The EXT1 record in this case is specified as additional data;
- an associated called party subaddress. The EXT1 record in this case is specified as subaddress data.

Identifier: '6F4A'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

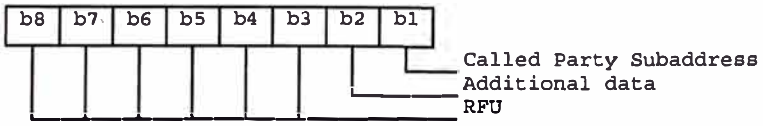
Access Conditions:
READ CHV1
UPDATE CHV1
INVALIDATE ADM
REHABILITATE ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

- Record type

Contents: type of the record

Coding:



b3-b8 are reserved and set to 0;
a bit set to 1 identifies the type of record;
only one type can be set;
'00' indicates the type "unknown".

The following example of coding means that the type of extension data is "additional data":

b8	b7	b6	b5	b4	b3	b2	b1
0	0	0	0	0	0	1	0

- Extension data

Contents: Additional data or Called Party Subaddress depending on record type.

Coding:

Case 1, Extension1 record is additional data:

The first byte of the extension data gives the number of bytes of the remainder of ADN/SSC (respectively MSISDN, LND). The coding of remaining bytes is BCD, according to the coding of ADN/SSC (MSISDN, LND). Unused nibbles at the end have to be set to 'F'. It is possible if the number of additional digits exceeds the capacity of the additional record to chain another record inside the EXT1 Elementary File by the identifier in byte 13.

Case 2, Extension1 record is Called Party Subaddress:

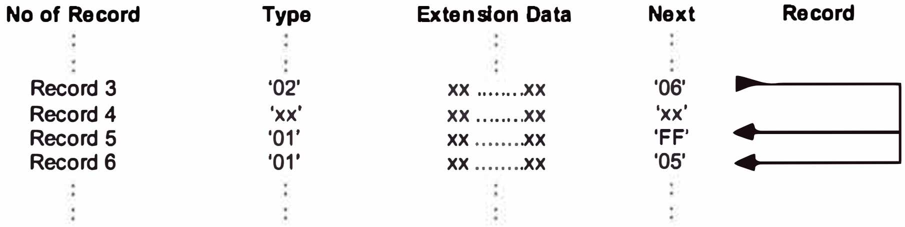
The subaddress data contains information as defined for this purpose in GSM 04.08 [15]. All information defined in GSM 04.08, except the information element identifier, shall be stored in the SIM. The length of this subaddress data can be up to 22 bytes. In those cases where two extension records are needed, these records are chained by the identifier field. The extension record containing the first part of the called party subaddress points to the record which contains the second part of the subaddress.

- Identifier

Contents: identifier of the next extension record to enable storage of information longer than 11 bytes.

Coding: record number of next record. 'FF' identifies the end of the chain.

EXAMPLE: Of a chain of extension records being associated to an ADN/SSC. The extension1 record identifier (Byte 14+X) of ADN/SSC is set to 3.



No of Record	Type	Extension Data	Next	Record
⋮	⋮	⋮	⋮	
Record 3	'02'	xx xx	'06'	
Record 4	'xx'	xx xx	'xx'	
Record 5	'01'	xx xx	'FF'	
Record 6	'01'	xx xx	'05'	
⋮	⋮	⋮	⋮	

In this example ADN/SSC is associated to additional data (record 3) and a called party subaddress whose length is more than 11 bytes (records 6 and 5).

10.5.11 EF$_{EXT2}$ (Extension2)

This EF contains extension data of an FDN/SSC (see EXT2 in subclause 10.5.2).

Identifier: '6F4B'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:	
READ	CHV1
UPDATE	CHV2
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see subclause 10.5.10 EF$_{EXT1}$.

10.5.12 EF$_{EXT3}$ (Extension3)

This EF contains extension data of an SDN (see EXT3 in subclause 10.5.9).

Identifier: '6F4C'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:	
READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see subclause 10.5.10 EF$_{EXT1}$.

10.5.13 EF$_{BDN}$ (Barred Dialling Numbers)

This EF contains Barred Dialling Numbers (BDN) and/or Supplementary Service Control strings (SSC). In addition it contains identifiers of associated network/bearer capabilities and identifiers of extension records. It may also contain an associated alpha-tagging.

Identifier: '6F4D'	Structure: linear fixed	Optional
Record length: X+15 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV2
INVALIDATE	CHV2 / ADM (set at personalisation)
REHABILITATE	CHV2 / ADM (set at personalisation)

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	O	X bytes
X+1	Length of BCD number/SSC contents	M	1 byte
X+2	TON and NPI	M	1 byte
X+3 to X+12	Dialling Number/SSC String	M	10 bytes
X+13	Capability/Configuration Identifier	M	1 byte
X+14	Extension4 Record Identifier	M	1 byte
X+15	Comparison Method Pointer	M	1 byte

For contents and coding of all data items, except for the Comparison Method Pointer, see the respective data items of the EF_{ADN} (subclause 10.5.1), with the exception that extension records are stored in the EF_{EXT4}. The Comparison Method Pointer refers to a record number in EF_{CMI}.

NOTE: The value of X (the number of bytes in the alpha-identifier) may be different to the length denoted X in EF_{ADN}.

10.5.14 EF_{EXT4} (Extension4)

This EF contains extension data of an BDN/SSC (see EXT4 in subclause 10.5.13).

Identifier: '6F4E'	Structure: linear fixed	Optional
Record length: 13 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV2
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Record type	M	1 byte
2 to 12	Extension data	M	11 bytes
13	Identifier	M	1 byte

For contents and coding see subclause 10.5.10 EF_{EXT1}.

10.5.15 EF_{SMSR} (Short message status reports)

This EF contains information in accordance with GSM 03.40 [13] comprising short message status reports which have been received by the MS from the network.

Each record is used to store the status report of a short message in a record of EF_{SMS}. The first byte of each record is the link between the status report and the corresponding short message in EF_{SMS}.

Identifier: '6F47'	Structure: linear fixed	Optional
Record length: 30 bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	CHV1
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	SMS record identifier	M	1
2 - 30	SMS status report	M	29 bytes

- SMS record identifier

  Contents:

  This data item identifies the corresponding SMS record in EF_{SMS}, e.g. if this byte is coded '05' then this status report corresponds to the short message in record #5 of EF_{SMS}.

  Coding:

  '00' - empty record

  '01' - 'FF' - record number of the corresponding SMS in EF_{SMS}.

- SMS status report

  Contents:

  This data item contains the SMS-STATUS-REPORT TPDU as specified in GSM 03.40 [13], with identical coding and ordering of parameters.

  Coding:

  according to GSM 03.40 [13]. Any bytes in the record following the TPDU shall be filled with 'FF'.

10.5.16 EF_{CMI} (Comparison Method Information)

This EF contains a list of Comparison Method Identifiers and alpha-tagging associated with BDN entries (see EF_{BDN}). This EF shall always be present if EF_{BDN} is present.

Identifier: '6F58'	Structure: linear fixed	Optional
Record length: X+1 bytes	Update activity: low	

Access Conditions:

READ	PIN1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to X	Alpha Identifier	M	X bytes
X+1	Comparison Method Identifier	M	1 byte

- Alpha Identifier

  Contents:

  Alpha-tagging of the associated Comparison Method Identifier

  Coding:

Same as the alpha identifier in EF_{ADN}.

- Comparison Method Identifier

Contents:

this byte describes the comparison method which is associated with a BDN record. Its interpretation is not specified but it shall be defined by the operators implementing the BDN feature.

Coding:

'00' - 'FE' = Comparison Method Identifier.

'FF' = Default method.

10.6 DFs at the telecom level

DFs may be present as child directories of $DF_{TELECOM}$. The following has been defined.

$DF_{GRAPHICS}$ '5F50'

10.6.1 Contents of files at the telecom graphics level

The EFs in the Dedicated File $DF_{GRAPHICS}$ contain graphical information.

10.6.1.1 EF_{IMG} (Image)

Each record of this EF identifies instances of one particular graphical image, which graphical image is identified by this EF's record number.

Image instances may differ as to their size, having different resolutions, and the way they are coded, using one of several image coding schemes.

As an example, image k may represent a company logo, of which there are i instances on SIM, of various resolutions and perhaps encoded in several image coding schemes. Then, the i instances of the company's logo are described in record k of this EF.

Identifier: '4F20'	Structure: linear fixed	Optional
Record length: 9n+2 bytes	Update activity: low	
Access Conditions: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1	Number of Actual Image Instances	M	1 byte
2 to 10	Descriptor of Image Instance 1	M	9 bytes
11 to 19	Descriptor of Image Instance 2	O	9 bytes
:			
9 (n-1) + 2 to 9n + 1	Descriptor of Image Instance n	O	9 bytes
9n + 2	RFU	O	1 byte

- Number of Actual Image Instances

Contents: this byte gives the number of actual image instances described in the following data items (i.e. unused descriptors are not counted).

Coding: binary

Image Instance Descriptor

Contents: a description of an image instance

Coding: see below

Byte 1: Image Instance Width

Contents:

this byte specifies the image instance width, expressed in raster image points.

Coding:

binary.

Byte 2: Image Instance Height

Contents:

this byte specifies the image instance height, expressed in raster image points.

Coding:

binary.

Byte 3: Image Coding Scheme

Contents:

this byte identifies the image coding scheme that has been used in encoding the image instance.

Coding:

'11' - basic image coding scheme as defined in annex G;

'21' - colour image coding scheme as defined in annex G;

other values are reserved for future use.

Bytes 4 and 5: Image Instance File Identifier

Contents:

these bytes identify an EF which is the image instance data file (see subclause 10.6.1.2), holding the actual image data for this particular instance.

Coding:

byte 4: high byte of Image Instance File Identifier;

byte 5: low byte of Image Instance File Identifier.

Bytes 6 and 7: Offset into Image Instance File

Contents:

these bytes specify an offset into the transparent Image Instance File identified in bytes 4 and 5.

Coding:

byte 6: high byte of offset into Image Instance File;

byte 7: low byte of offset into Image Instance File

Bytes 8 and 9: Length of Image Instance Data

Contents:

these bytes yield the length of the image instance data, starting at the offset identified in bytes 6 and 7.

Coding:

byte 8: high byte of Image Instance Data length;

byte 9: low byte of Image Instance Data length.

NOTE: Transparent image instance data longer than 256 bytes may be read using successive READ BINARY commands.

10.6.1.2 Image Instance Data Files

Residing under DF$_{GRAPHICS}$, there may be several image instance data files. These EFs containing image instance data shall have the following attributes.

Identifier: '4FXX'	Structure: transparent	Optional
Record length: Y bytes	Update activity: low	

Access Conditions:

READ	CHV1
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1 to Y	Image Instance Data	M	Y bytes

Contents and coding:

Image instance data are accessed using the image instance descriptors provided by EF$_{IMG}$ (see subclause 10.6.1.1).

The identifier '4FXX' shall be different from one image instance data file to the other. For the range of 'XX', see subclause 6.6. The length Y may be different from one image instance data file to the other.

10.7 Files of GSM

This subclause contains a figure depicting the file structure of the SIM. DF$_{GSM}$ shall be selected using the identifier '7F20'. If selection by this means fails, then DCS 1800 MEs shall, and optionally GSM MEs may then select DF$_{GSM}$ with '7F21'.

NOTE 1: The selection of the GSM application using the identifier '7F21', if selection by means of the identifier '7F20' fails, is to ensure backwards compatibility with those Phase 1 SIMs which only support the DCS 1800 application using the Phase 1 directory DF$_{DCS1800}$ coded '7F21'.

NOTE 2: To ensure backwards compatibility with those Phase 1 DCS 1800 MEs which have no means to select DF$_{GSM}$ two options have been specified. These options are given in GSM 09.91 [17].

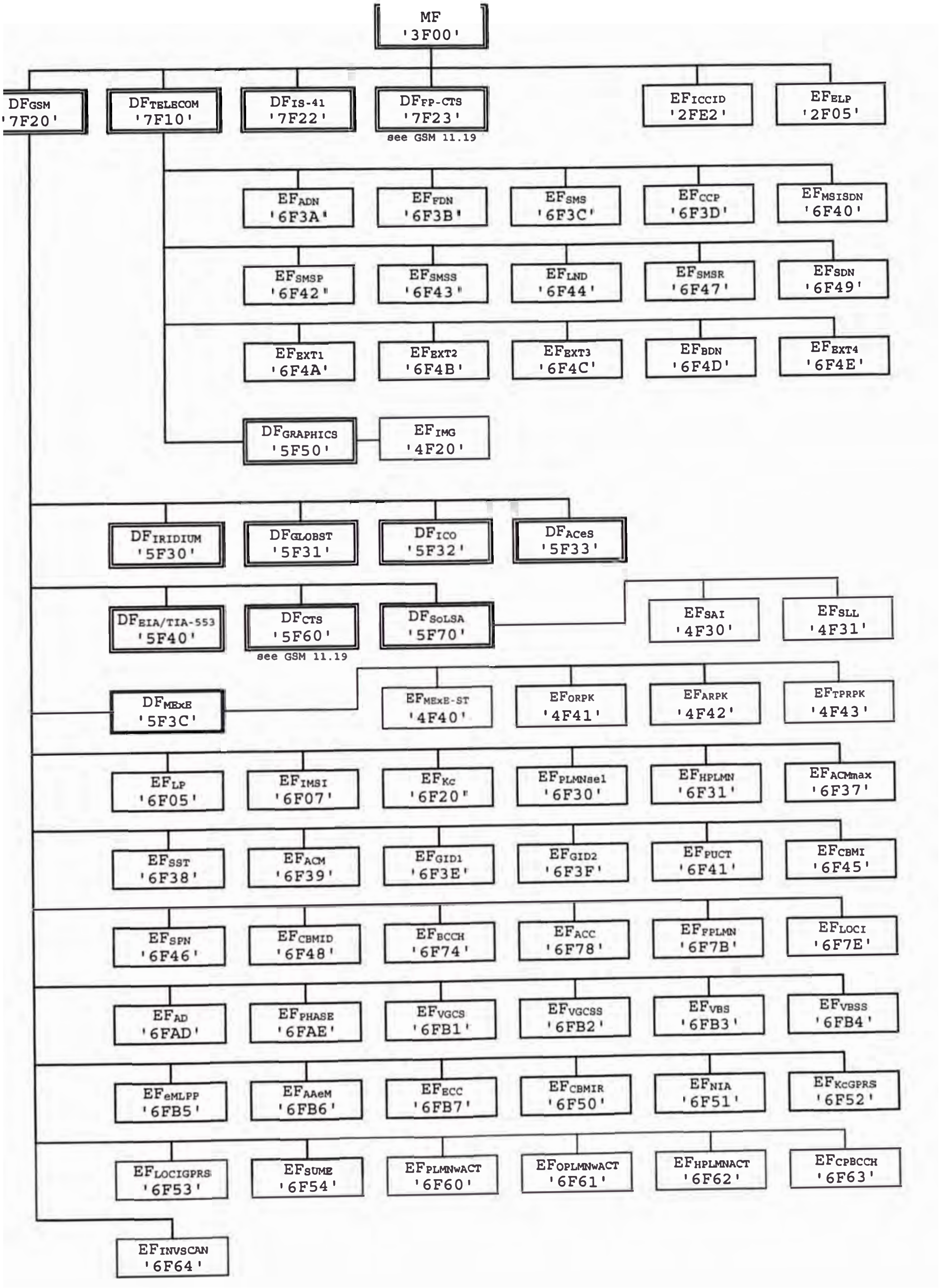


Figure 8: File identifiers and directory structures of GSM

11 Application protocol

When involved in GSM administrative management operations, the SIM interfaces with appropriate terminal equipment. These operations are outside the scope of this standard.

When involved in GSM network operations the SIM interfaces with an ME with which messages are exchanged. A message can be a command or a response.

> A GSM command/response pair is a sequence consisting of a command and the associated response.
>
> A GSM procedure consists of one or more GSM command/response pairs which are used to perform all or part of an application-oriented task. A procedure shall be considered as a whole, that is to say that the corresponding task is achieved if and only if the procedure is completed. The ME shall ensure that, when operated according to the manufacturer's manual, any unspecified interruption of the sequence of command/response pairs which realize the procedure, leads to the abortion of the procedure itself.
>
> A GSM session of the SIM in the GSM application is the interval of time starting at the completion of the SIM initialization procedure and ending either with the start of the GSM session termination procedure, or at the first instant the link between the SIM and the ME is interrupted.

During the GSM network operation phase, the ME plays the role of the master and the SIM plays the role of the slave.

The SIM shall execute all GSM and SIM Application Toolkit commands or procedures in such a way as not to jeopardise, or cause suspension, of service provisioning to the user. This could occur if, for example, execution of the RUN GSM ALGORITHM is delayed in such a way which would result in the network denying or suspending service to the user.

Some procedures at the SIM/ME interface require MMI interactions. The descriptions hereafter do not intend to infer any specific implementation of the corresponding MMI. When MMI interaction is required, it is marked "MMI" in the list given below.

Some procedures are not clearly user dependent. They are directly caused by the interaction of the MS and the network. Such procedures are marked "NET" in the list given below.

Some procedures are automatically initiated by the ME. They are marked "ME" in the list given below.

The list of procedures at the SIM/ME interface in GSM network operation is as follows:

General Procedures:

- Reading an EF	ME
Updating an EF	ME
Increasing an EF	ME

SIM management procedures:

SIM initialization	ME
GSM session termination	ME
Emergency call codes request	ME
Extended language preference request	ME
Language preference request	ME
Administrative information request	ME
SIM service table request	ME
SIM phase request	ME

CHV related procedures:

- CHV verification	MMI
- CHV value substitution	MMI
- CHV disabling	MMI
- CHV enabling	MMI
- CHV unblocking	MMI

GSM security related procedures:

GSM algorithms computation	NET
- IMSI request	NET
- Access control information request	NET
- HPLMN search period request	NET
- Investigation PLMN scan request	NET
- Location Information	NET
- Cipher key	NET
- BCCH information	NET
- CPBCCH information	NET
- Forbidden PLMN information	NET
- LSA information	NET

Subscription related procedures:

- Dialling Numbers (ADN, FDN, MSISDN, LND, SDN, BDN)	MMI/ME
- Short messages (SMS)	MMI
- Advice of Charge (AoC)	MMI
- Capability Configuration Parameters (CCP)	MMI
- PLMN Selector	MMI
- HPLMN Access Technology	MMI
- PLMN Selector with Access Technology	MMI
- OPLMN Selector with Access Technology	MMI
- Cell Broadcast Message Identifier (CBMI)	MMI
- Group Identifier Level 1 (GID1)	MMI/ME
- Group Identifier Level 2 (GID2)	MMI/ME
- Service Provider Name (SPN)	ME
- Voice Group Call Service (VGCS)	MMI/ME
- Voice Broadcast Service (VBS)	MMI/ME
Enhanced Multi Level Pre-emption and Priority (eMLPP)	MMI/ME

- Depersonalisation Control Keys	ME
Short message status reports (SMSR)	MMI
- Network's indication of alerting	ME
SIM Application Toolkit related procedures:	
- Data Download via SMS-CB (CBMID)	NET
- Data Download via SMS-PP	NET
- Menu selection	MMI
Call Control	MMI/ME/NET
- Proactive SIM	MMI/ME/NET
- Mobile Originated Short Message control by SIM	MMI/ME/NET
- Image Request	MMI/ME
MExE related procedures:	
- Reading of MExE_ST	ME
- Reading of root public keys on the SIM (ORPK, ARPK,TPRPK)	ME/NET

The procedures listed in subclause 11.2 are basically required for execution of the procedures in subclauses 11.3, 11.4 and 11.5. The procedures listed in subclauses 11.3 and 11.4 are mandatory (see GSM 02.17 [6]). The procedures listed in subclause 11.5 are only executable if the associated services, which are optional, are provided in the SIM. However, if the procedures are implemented, it shall be in accordance with subclause 11.5.

If a procedure is related to a specific service indicated in the SIM Service Table, it shall only be executed if the corresponding bits denote this service as "allocated and activated" (see subclause 10.3.7). In all other cases this procedure shall not start.

11.1 General procedures

11.1.1 Reading an EF

The ME selects the EF and sends a READ command. This contains the location of the data to be read. If the access condition for READ is fulfilled, the SIM sends the requested data contained in the EF to the ME. If the access condition is not fulfilled, no data will be sent and an error code will be returned.

11.1.2 Updating an EF

The ME selects the EF and sends an UPDATE command. This contains the location of the data to be updated and the new data to be stored. If the access condition for UPDATE is fulfilled, the SIM updates the selected EF by replacing the existing data in the EF with that contained in the command. If the access condition is not fulfilled, the data existing in the EF will be unchanged, the new data will not be stored, and an error code will be returned.

In the case when updating EF_{LOCI} with data containing the TMSI value and the card reports the error '92 40' (Memory Problem), the ME shall terminate GSM operation.

11.1.3 Increasing an EF

The ME selects the EF and sends an INCREASE command. This contains the value which has to be added to the contents of the last updated/increased record. If the access condition for INCREASE is fulfilled, the SIM increases the existing value of the EF by the data contained in the command, and stores the result. If the access condition is not fulfilled, the data existing in the EF will be unchanged and an error code will be returned.

NOTE: The identification of the data within an EF to be acted upon by the above procedures is specified within the command. For the procedures in subclauses 11.1.1 and 11.1.2 this data may have been previously identified using a SEEK command, e.g. searching for an alphanumeric pattern.

11.2 SIM management procedures

Phase 2 MEs shall support all SIMs which comply with the mandatory requirements of Phase 1, even if these SIMs do not comply with all the mandatory requirements of Phase 2. Furthermore, Phase 2 MEs shall take care of potential incompatibilities with Phase 1 SIMs which could arise through use of inappropriate commands or misinterpretation of response data. Particular note should be taken of making a false interpretation of RFU bytes in a Phase 1 SIM having contradictory meaning in Phase 2; e.g. indication of EF invalidation state.

11.2.1 SIM initialization

After SIM activation (see subclause 4.3.2), the ME selects the Dedicated File DF_{GSM} and optionally attempts to select EF_{ECC} If EF_{ECC} is available, the ME requests the emergency call codes.

The ME requests the Extended Language Preference. The ME only requests the Language Preference (EF_{LP}) if at least one of the following conditions holds:

EF_{ELP} is not available;

EF_{ELP} does not contain an entry corresponding to a language specified in ISO 639[30];

the ME does not support any of the languages in EF_{ELP}.

If both EFs are not available or none of the languages in the EFs is supported then the ME selects a default language. It then runs the CHV1 verification procedure.

If the CHV1 verification procedure is performed successfully, the ME then runs the SIM Phase request procedure.

For a SIM requiring PROFILE DOWNLOAD, then the ME shall perform the PROFILE DOWNLOAD procedure in accordance with GSM 11.14 [27]. When BDN is enabled on a SIM, the PROFILE DOWNLOAD procedure is used to indicate to the SIM whether the ME supports the "Call Control by SIM" facility. If so, then the SIM is able to allow the REHABILITATE command to rehabilitate EF_{IMSI} and EF_{LOCI}.

If the ME detects a SIM of Phase 1, it shall omit the following procedures relating to FDN and continue with the Administrative Information request. The ME may omit procedures not defined in Phase 1 such as HPLMN Search Period request.

For a SIM of Phase 2 or greater, GSM operation shall only start if one of the two following conditions is fulfilled:

if EF_{IMSI} and EF_{LOCI} are not invalidated, the GSM operation shall start immediately;

if EF_{IMSI} and EF_{LOCI} are invalidated, the ME rehabilitates these two EFs.

MEs without FDN capability but with Call control by SIM facility shall not rehabilitate EF_{IMSI} and/or EF_{LOCI} if FDN is enabled in the SIM and therefore have no access to these EFs. GSM operation will therefore be prohibited;

MEs without FDN capability and without Call control by SIM facility shall not rehabilitate EF_{IMSI} and/or EF_{LOCI} and therefore have no access to these EFs. GSM operation will therefore be prohibited.

It is these mechanisms which are used for control of services n°3 and n°31 by the use of SIMs for these services which always invalidate these two EFs at least before the next command following selection of either EF.

NOTE: When FDN and BDN are both enabled, and if the ME supports FDN but does not support the Call control by SIM facility, the rehabilitation of EF_{IMSI} and EF_{LOCI} will not be successful because of a restriction mechanism of the REHABILITATE command linked to the BDN feature.

When EF_{IMSI} and EF_{LOCI} are successfully rehabilitated, if the FDN capability procedure indicates that:

i) FDN is allocated and activated in the SIM; and FDN is set "enabled", i.e. ADN "invalidated" or not activated; and the ME supports FDN; or

ii) FDN is allocated and activated in the SIM; and FDN is set "disabled", i.e. ADN "not invalidated"; or

iii) FDN is not allocated or not activated;

then GSM operation shall start.

In all other cases GSM operation shall not start.

Afterwards, the ME runs the following procedures:

Administrative Information request;

SIM Service Table request;

IMSI request;

- Access Control request;

HPLMN Search Period request;

Investigation PLMN scan request;

PLMN selector request;

HPLMN Access Technology request;

- PLMN Selector with Access Technology request;

OPLMN Selector with Access Technology request;

Location Information request;

Cipher Key request;

BCCH information request;

CPBCCH information request;

Forbidden PLMN request;

LSA information request;

CBMID request;

Depersonalisation Control Keys request;

- Network's indication of alerting request.

If the SIM service table indicates that the proactive SIM service is active, then from this point onwards, the ME, if it supports the proactive SIM service, shall send STATUS commands at least every 30s during idle mode as well as during calls, in order to enable the proactive SIM to respond with a command. The SIM may send proactive commands (see GSM 11.14 [27]), including a command to change the interval between STATUS commands from the ME, when in idle mode. In-call requirements for STATUS for SIM Presence Detection are unchanged by this command.

After the SIM initialization has been completed successfully, the MS is ready for a GSM session.

11.2.2 GSM session termination

NOTE 1: This procedure is not to be confused with the deactivation procedure in subclause 4.3.2.

The GSM session is terminated by the ME as follows.

The ME runs all the procedures which are necessary to transfer the following subscriber related information to the SIM:

- Location Information update;
- Cipher Key update;
- BCCH information update;
- CPBCCH information update;
- Advice of Charge increase;
- Forbidden PLMN update.

As soon as the SIM indicates that these procedures are completed, the ME/SIM link may be deactivated.

Finally, the ME deletes all these subscriber related information elements from its memory.

NOTE 2: If the ME has already updated any of the subscriber related information during the GSM Session, and the value has not changed until GSM session termination, the ME may omit the respective update procedure.

11.2.3 Emergency Call Codes

Request: The ME performs the reading procedure with EF_{ECC}.

Update: The ME performs the updating procedure with EF_{ECC}.

NOTE: The update procedure is only applicable when access conditions of ADM for update is set to ALW, CHV1 or CHV2.

11.2.4 Language preference

Request: The ME performs the reading procedure with EF_{LP}.

Update: The ME performs the updating procedure with EF_{LP}.

11.2.5 Administrative information request;

The ME performs the reading procedure with EF_{AD}.

11.2.6 SIM service table request

The ME performs the reading procedure with EF_{SST}.

11.2.7 SIM phase request

The ME performs the reading procedure with EF_{Phase}.

11.2.8 SIM Presence Detection and Proactive Polling

As an additional mechanism, to ensure that the SIM has not been removed during a card session, the ME sends, at frequent intervals, a STATUS command during each call. A STATUS command shall be issued within all 30 second periods of inactivity on the SIM-ME interface during a call. Inactivity in this case is defined as starting at the end of the last communication or the last issued STATUS command. If no response data is received to this STATUS command, then the call shall be terminated as soon as possible but at least within 5 seconds after the STATUS command has been sent. If the DF indicated in response to a STATUS command is not the same as that which was indicated in the previous response, or accessed by the previous command, then the call shall be terminated as soon as possible but at least within 5 seconds after the response data has been received. This procedure shall be used in addition to a mechanical or other device used to detect the removal of a SIM.

If the ME supports the proactive SIM service, and the SIM has this service activated in its Service Table, then during idle mode the ME shall send STATUS commands to the SIM at intervals no longer than the interval negotiated with the SIM (see GSM 11.14 [27]).

11.2.9 Extended Language preference

Request: The ME performs the reading procedure with EF_{ELP}.

Update: The ME performs the updating procedure with EF_{ELP}.

11.3 CHV related procedures

A successful completion of one of the following procedures grants the access right of the corresponding CHV for the GSM session. This right is valid for all files within the GSM application protected by this CHV.

After a third consecutive presentation of a wrong CHV to the SIM, not necessarily in the same GSM session, the CHV status becomes "blocked" and if the CHV is "enabled", the access right previously granted by this CHV is lost immediately.

An access right is not granted if any of the following procedures are unsuccessfully completed or aborted.

11.3.1 CHV verification

The ME checks the CHV status.

In the case of CHV1 the following procedure applies:

- if the CHV1 status is "blocked" and CHV1 is "enabled", the procedure ends and is finished unsuccessfully;
- if the CHV1 status is "blocked" but CHV1 is "disabled", the procedure ends and is finished successfully. The ME shall, however, accept SIMs which do not grant access rights when CHV1 is "blocked" and "disabled". In that case ME shall consider those SIMs as "blocked";
- if the CHV1 status is not "blocked" and CHV1 is "disabled", the procedure is finished successfully;
- if the CHV1 status is not "blocked" and CHV1 is "enabled", the ME uses the VERIFY CHV function. If the CHV1 presented by the ME is equal to the corresponding CHV1 stored in the SIM, the procedure is finished successfully. If the CHV1 presented by the ME is not equal to the corresponding CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

In the case of CHV2 the following procedure applies:

- if the CHV2 status is "blocked", the procedure ends and is finished unsuccessfully;
- if the CHV2 status is not "blocked", the ME uses the VERIFY CHV function. If the CHV2 presented by the ME is equal to the corresponding CHV2 stored in the SIM, the procedure is finished successfully. If the CHV2 presented by the ME is not equal to the corresponding CHV2 stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.2 CHV value substitution

The ME checks the CHV status. If the CHV status is "blocked" or "disabled", the procedure ends and is finished unsuccessfully.

If the CHV status is not "blocked" and the enabled/disabled indicator is set "enabled", the ME uses the CHANGE CHV function. If the old CHV presented by the ME is equal to the corresponding CHV stored in the SIM, the new CHV presented by the ME is stored in the SIM and the procedure is finished successfully.

If the old CHV and the CHV in memory are not identical, the procedure ends and is finished unsuccessfully.

11.3.3 CHV disabling

Requirement: Service n°1 "allocated and activated".

The ME checks the CHV1 status. If the CHV1 status is "blocked", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked", the ME reads the CHV1 enabled/disabled indicator. If this is set "disabled", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked" and the enabled/disabled indicator is set "enabled", the ME uses the DISABLE CHV function. If the CHV1 presented by the ME is equal to the CHV1 stored in the SIM, the status of CHV1 is set "disabled" and the procedure is finished successfully. If the CHV1 presented by the ME is not equal to the CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.4 CHV enabling

The ME checks the CHV1 status. If the CHV1 status is "blocked", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked", the ME reads the CHV1 enabled/disabled indicator. If this is set "enabled", the procedure ends and is finished unsuccessfully.

If the CHV1 status is not "blocked" and the enabled/disabled indicator is set "disabled", the ME uses the ENABLE CHV function. If the CHV1 presented by the ME is equal to the CHV1 stored in the SIM, the status of CHV1 is set "enabled" and the procedure is finished successfully. If the CHV presented by the ME is not equal to the CHV1 stored in the SIM, the procedure ends and is finished unsuccessfully.

11.3.5 CHV unblocking

The execution of the CHV unblocking procedure is independent of the corresponding CHV status, i.e. being blocked or not.

The ME checks the UNBLOCK CHV status. If the UNBLOCK CHV status is "blocked", the procedure ends and is finished unsuccessfully.

If the UNBLOCK CHV status is not "blocked", the ME uses the UNBLOCK CHV function. If the UNBLOCK CHV presented by the ME is equal to the corresponding UNBLOCK CHV stored in the SIM, the relevant CHV status becomes "unblocked" and the procedure is finished successfully. If the UNBLOCK CHV presented by the ME is not equal to the corresponding UNBLOCK CHV stored in the SIM, the procedure ends and is finished unsuccessfully.

11.4 GSM security related procedures

11.4.1 GSM algorithms computation

The ME selects DF_{GSM} and uses the RUN GSM ALGORITHM function (see subclause 8.16). The response SRES-Kc is sent to the ME when requested by a subsequent GET RESPONSE command.

11.4.2 IMSI request

The ME performs the reading procedure with EF_{IMSI}.

11.4.3 Access control request

The ME performs the reading procedure with EF_{ACC}.

11.4.4 HPLMN search period request

The ME performs the reading procedure with EF_{HPLMN}.

11.4.5 Location information

Request: The ME performs the reading procedure with EF_{LOCI}.

Update: The ME performs the updating procedure with EF_{LOCI}.

11.4.6 Cipher key

Request: The ME performs the reading procedure with EF_{Kc}.

Update: The ME performs the updating procedure with EF_{Kc}.

11.4.7 BCCH information

Request: The ME performs the reading procedure with EF_{BCCH}.

Update: The ME performs the updating procedure with EF_{BCCH}.

11.4.8 Forbidden PLMN

Request: The ME performs the reading procedure with EF_{PLMN}.

Update: The ME performs the updating procedure with EF_{PLMN}.

11.4.9 LSA information

Request: The ME performs the reading procedure with EF_{SAI}, EF_{SLL} and its associated LSA Descriptor files.

Update: The ME performs the updating procedure with EF_{SLL}.

11.4.10 PLMN Selector with Access Technology

Requirement: Service n°43"allocated and activated".

Request: The ME performs the reading procedure with $EF_{PLMNwACT}$.

Update: The ME performs the updating procedure with $EF_{PLMNwACT}$.

11.4.11 OPLMN Selector with Access Technology

Requirement: Service n°44 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{OPLMNwACT}$

Update: The ME performs the updating procedure with $EF_{OPLMNwACT}$

11.4.12 HPLMN Access Technology

Requirement: Service n°45 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{HPLMNACT}$.

11.4.13 CPBCCH information

Requirement: Service n°46 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CPBCCH}.

Update: The ME performs the updating procedure with EF_{CPBCCH}.

11.4.14 Investigation PLMN Scan Request

Request: The ME performs the reading procedure with $EF_{InvScan}$.

11.5 Subscription related procedures

11.5.1 Dialling numbers

The following procedures may not only be applied to EF_{ADN} and its associated extension files EF_{CCP} and EF_{EXT1} as described in the procedures below, but also to EF_{EDN}, EF_{MSISDN}, EF_{LND}, EF_{BDN} and EF_{SDN} and their associated extension files. If these files are not allocated and activated, as denoted in the SIM service table, the current procedure shall be aborted and the appropriate EFs shall remain unchanged.

As an example, the following procedures are described as applied to ADN.

Requirement: Service n°2 "allocated and activated"

(Service n°3 for FDN,

Service n°9 for MSISDN,

Service n°13 for LND,

Service n°18 for SDN),

Service n°31 for BDN)

Update: The ME analyses and assembles the information to be stored as follows (the byte identifiers used below correspond to those in the description of the EFs in subclauses 10.5.1, 10.5.4 and 10.5.10):

i) The ME identifies the Alpha-tagging, Capability/Configuration Identifier and Extension1 Record Identifier.

ii) The dialling number/SSC string shall be analysed and allocated to the bytes of the EF as follows:

if a "+" is found, the TON identifier is set to "International";

if 20 or less "digits" remain, they shall form the dialling number/SSC string;

if more than 20 "digits" remain, the procedure shall be as follows:

Requirement:

Service n°10 "allocated and activated";

(Service n°10 applies also for MSISDN and LND;

Service n°11 for FDN;

Service n°19 for SDN;

Service n°32 for BDN).

The ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted.

The first 20 "digits" are stored in the dialling number/SSC string. The value of the length of BCD number/SSC contents is set to the maximum value, which is 11. The Extension1 record identifier is coded with the associated record number in the EF_{EXT1}. The remaining digits are stored in the selected Extension1 record where the type of the record is set to "additional data". The first byte of the Extension1 record is set with the number of bytes of the remaining additional data. The number of bytes containing digit information is the sum of the length of BCD number/SSC contents of EF_{ADN} and byte 2 of all associated chained Extension1 records containing additional data (see subclauses 10.5.1 and 10.5.10).

iii) If a called party subaddress is associated to the ADN/SSC the procedure shall proceed as follows:

Requirement:

Service n°10 "allocated and activated"
(Service n°10 applies also for MSISDN and LND;
Service n°11 for FDN;
Service n°19 for SDN;
Service n°32 for BDN.)

If the length of the called party subaddress is less than or equal to 11 bytes (see GSM 04.08 [15] for coding):

the ME seeks for a free record in EF_{EXT1}. If an Extension1 record is not marked as "free", the ME runs the Purge procedure. If an Extension1 record is still unavailable, the procedure is aborted;

the ME stores the called party subaddress in the Extension1 record, and sets the Extension1 record type to "called party subaddress".

If the length of the called party subaddress is greater than 11 bytes (see GSM 04.08 [15] for coding):

the ME seeks for two free records in EF_{EXT1}. If no such two records are found, the ME runs the Purge procedure. If two Extension1 records are still unavailable, the procedure is aborted;

the ME stores the called party subaddress in the two Extension1 records. The identifier field in the Extension1 record containing the first part of the subaddress data is coded with the associated EF_{EXT1} record number containing the second part of the subaddress data. Both Extension1 record types are set to "called party subaddress".

Once i), ii), and iii) have been considered the ME performs the updating procedure with EF_{ADN}. If the SIM has no available empty space to store the received ADN/SSC, or if the procedure has been aborted, the ME advises the user.

NOTE 1: For reasons of memory efficiency the ME is allowed to analyse all Extension1 records to recognize if the additional or subaddress data to be stored is already existing in EF_{EXT1}. In this case the ME may use the existing chain or the last part of the existing chain from more than one ADN (LND, MSISDN). The ME is only allowed to store extension data in unused records. If existing records are used for multiple access, the ME shall not change any data in those records to prevent corruption of existing chains.

Erasure: The ME sends the identification of the information to be erased. The content of the identified record in EF_{ADN} is marked as "free".

Request: The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{ADN} (subclause 10.5.1) to ascertain, whether additional data is associated in EF_{EXT1} or EF_{CCP}. If necessary, then the ME performs the reading procedure on these EFs to assemble the complete ADN/SSC.

Purge: The ME shall access each EF which references EF_{EXT1} (EF_{EXT2}) for storage and shall identify records in these files using extension data (additional data or called party subaddress). Note that existing chains have to be followed to the end. All referred Extension1 (Extension2) records are noted by the ME. All Extension1 (Extension2) records not noted are then marked by the ME as "free" by setting the whole record to 'FF'.

NOTE 2: Dependent upon the implementation of the ME, and in particular the possibility of erasure of ADN/SSC records by Phase 1 MEs, which have no knowledge of the EF_{EXT1}, it is possible for Extension1 records to be marked as "used space" (not equal to 'FF'), although in fact they are no longer associated with an ADN/SSC record.

The following three procedures are only applicable to service n°3 (FDN).

FDN capability request. The ME has to check the state of service n°3, i.e. if FDN is "enabled" or "disabled". In case of enabled FDN, the ME has to switch to a restrictive terminal mode (see GSM 02.07). To ascertain the state of FDN, the ME checks in EF_{SST} whether or not ADN is activated. If ADN is not activated, service n°3 is enabled. If ADN is activated, the ME checks the response data of EF_{ADN}. If EF_{ADN} is invalidated, service n°3 is enabled. In all other cases service n°3 is disabled.

FDN disabling. The FDN disabling procedure requires that CHV2 verification procedure has been perfonned successfully and that ADN is activated. If not, FDN disabling procedure will not be executed successfully. To disable FDN capability, the ME rehabilitates EF_{ADN}. The invalidate/rehabilitate flag of EF_{ADN}, which is implicitly set by the REHABILITATE command, is at the same time the indicator for the state of the service n°3. If ADN is not activated, disabling of FDN is not possible and thus service n°3 is always enabled (see FDN capability request).

NOTE 3: If FDN is disabled (by rehabilitating EF_{ADN}) using an administrative terminal then the FDN disabling procedure of this administrative terminal need also to rehabilitate EF_{IMSI} and EF_{LOCI} to ensure normal operation of the SIM in a phase 1 ME or a phase 2 ME which does not support FDN.

FDN enabling. The FDN enabling procedure requires that CHV2 verification procedure has been performed successfully. If not, FDN enabling procedure will not be executed successfully. To enable FDN capability, the ME invalidates EF_{ADN}. The invalidate/rehabilitate flag of EF_{ADN}, which is implicitly cleared by the INVALIDATE command, is at the same time the indicator for the state of the service n°3 (see FDN capability request). If ADN is not activated, service n°3 is always enabled.

Invalidated ADNs may optionally still be readable and updatable depending on the file status (see subclause 9.3)

The following three procedures are only applicable to service n°31 (BDN).

BDN capability request. The ME has to check the state of service n°31, i.e. if BDN is "enabled" or "disabled". BDN service is "enabled" only if service n°31 is allocated and activated, and EF_{BDN} is not invalidated. In all other cases, the BDN service is "disabled".

BDN disabling. The BDN disabling procedure requires that CHV2 verification procedure has been performed successfully. If not, BDN disabling procedure will not be executed successfully. To disable BDN capability, the ME invalidates EF_{BDN}. The invalidate/rehabilitate flag of EF_{BDN}, which is implicitly cleared by the INVALIDATE command, is at the same time the indicator for the state of the service n°31 (see BDN capability request).

BDN enabling. The BDN enabling procedure requires that CHV2 verification procedure has been performed successfully. If not, BDN enabling procedure will not be executed successfully. To enable BDN capability, the ME rehabilitates EF_{BDN}. The invalidate/rehabilitate flag of EF_{BDN}, which is implicitly set by the REHABILITATE command, is at the same time the indicator for the state of the service n°31 (see BDN capability request).

Invalidated BDNs (when BDN capability is disabled) may optionally still be readable and updatable depending on the file status (see subclause 9.3).

11.5.2 Short messages

Requirement: Service n°4 "allocated and activated".

Request: The SIM seeks for the identified short message. If this message is found, the ME performs the reading procedure with EF_{SMS}.

If service n°35 is "allocated and activated" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the reading procedure with the corresponding record in EF_{SMSR}. If the ME does not find a corresponding record in EF_{SMSR}, then the ME shall update the status of the SMS with '19' (status report requested, received but not stored in EF_{SMSR}).

If the short message is not found within the SIM memory, the SIM indicates that to the ME.

Update: The ME looks for the next available area to store the short message. If such an area is available, it performs the updating procedure with EF_{SMS}.

If there is no available empty space in the SIM to store the received short message, a specific MMI will have to take place in order not to loose the message.

Erasure: The ME will select in the SIM the message area to be erased. Depending on the MMI, the message may be read before the area is marked as "free". After performing the updating procedure with EF_{SMS}, the memory allocated to this short message in the SIM is made available for a new incoming message. The memory of the SIM may still contain the old message until a new message is stored in this area.

If service n°35 is "allocated and activated" and the status of the SMS is '1D' (status report requested, received and stored in EF_{SMSR}), the ME performs the erasure procedure for EF_{SMSR} with the corresponding record in EF_{SMSR}.

11.5.3 Advice of Charge (AoC)

Requirement: Service n°5 "allocated and activated".

Accumulated Call Meter.

Request: The ME performs the reading procedure with EF_{ACM}. The SIM returns the last updated value of the ACM.

Initialization: The ME performs the updating procedure with EF_{ACM} using the new initial value.

Increasing: The ME performs the increasing procedure with EF_{ACM} sending the value which has to be added.

Accumulated Call Meter Maximum Value.

Request: The ME performs the reading procedure with EF_{ACMmax}.

Initialization: The ME performs the updating procedure with EF_{ACMmax} using the new initial maximum value.

Price per Unit and Currency Table (PUCT).

Request: The ME performs the reading procedure with EF_{PUCT}.

Update: The ME performs the updating procedure with EF_{PUCT}.

11.5.4 Capability configuration parameters

Requirement: Service n°6 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CCP}.

Update: The ME performs the updating procedure with EF_{CCP}.

Erasure: The ME sends the identification of the requested information to be erased. The content of the identified record in EF_{CCP} is marked as "free".

11.5.5 PLMN selector

Requirement: Service n°7 "allocated and activated".

Request: The ME performs the reading procedure with $EF_{PLMNsel}$.

Update: The ME performs the updating procedure with $EF_{PLMNsel}$.

11.5.6 Cell broadcast message identifier

Requirement: Service n°14 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CBMI}.

Update: The ME performs the updating procedure with EF_{CBMI}.

11.5.7 Group identifier level 1

Requirement: Service n°15 "allocated and activated".

Request: The ME performs the reading procedure with EF_{GID1}.

11.5.8 Group identifier level 2

Requirement: Service n°16 "allocated and activated".

Request: The ME performs the reading procedure with EF_{GID2}.

11.5.9 Service Provider Name

Requirement: Service n°17 "allocated and activated".

Request: The ME performs the reading procedure with EF_{SPN}.

11.5.10 Voice Group Call Services

Requirement: Service n°18 "allocated and activated".

Voice Group Call Service

Request: The ME performs the reading procedure with EF_{VGCS}.

Voice Group Call Service Status

Request: The ME performs the reading procedure with EF_{VGCSS}.

Update: The ME performs the updating procedure with EF_{VGCSS}.

11.5.11 Voice Broadcast Services

Requirement: Service n°19 "allocated and activated".

Voice Broadcast Service

Request: The ME performs the reading procedure with EF_{VBS}.

Voice Broadcast Service Status

Request: The ME performs the reading procedure with EF_{VBSS}.

Update: The ME performs the updating procedure with EF_{VBSS}.

11.5.12 Enhanced Multi Level Pre-emption and Priority Service

Requirement: Service n°18 "allocated and activated".

Enhanced Multi Level Pre-emption and Priority

Request: The ME performs the reading procedure with EF_{eMLPP}.

Automatic Answer on eMLPP service

Request: The ME performs the reading procedure with EF_{AAeM}.

Update: The ME performs the updating procedure with EF_{AAeM}.

11.5.13 Cell Broadcast Message range identifier

Requirement: Service n°30 "allocated and activated".

Request: The ME performs the reading procedure with EF_{CBMIR}.

Update: The ME performs the updating procedure with EF_{CBMIR}.

11.5.14 Depersonalisation Control Keys

Requirement: Service n°33 "allocated and activated".

Request: The ME performs the reading procedure with EF_{DCK}.

11.5.15 Short message status report

Requirement: Service n°35 "allocated and activated".

Request: If the status of a stored short message indicates that there is a corresponding status report, the ME performs the seek function with EF_{SMSR} to identify the record containing the appropriate status report. The ME performs the reading procedure with EF_{SMSR}.

Update: If a status report is received, the ME first seeks within the SMS record identifiers of EF_{SMSR} for the same record number it used for the short message in EF_{SMS}. If such a record identifier is found in EF_{SMSR}, it is used for storage. If such a record identifier is not found, then the ME seeks for a free entry in EF_{SMSR} for storage. If no free entry is found the ME runs the Purge procedure with EF_{SMSR}. If there is still no free entry, the status report is not stored.

If the ME found an appropriate record in EF_{SMSR} for storage, it updates the record with the status report setting the record identifier in EF_{SMSR} to the appropriate record number of the short message in EF_{SMS}.

The status in EF_{SMS} is updated accordingly (see subclause 10.5.3) by performing the update procedure with EF_{SMS}.

Erasure: The ME runs the update procedure with EF_{SMSR} by at least storing '00' in the first byte of the record. The ME may optionally update the following bytes with 'FF'.

Purge: The ME shall read the SMS record identifier (byte 1) of each record of EF_{SMSR}. With each record the ME checks the corresponding short messages in EF_{SMS}. If the status (byte 1) of the corresponding SMS is not equal '1D' (status report requested, received and stored in EF_{SMSR}), the ME shall perform the erasure procedure with the appropriate record in EF_{SMSR}.

11.5.16 Network's indication of alerting

Requirement: Service n°36 "allocated and activated".

Request: The ME performs the reading procedure with EF_{NIA}.

11.6 SIM Application Toolkit related procedures

SIM Application Toolkit is an optional feature. The higher level procedures, and contents and coding of the commands, are given in GSM 11.14 [27]. Procedures relating to the transmission of commands and responses across the SIM/ME interface are given in this section. A SIM or ME supporting SIM Application Toolkit shall conform to the requirements given in this section.

11.6.1 Initialization procedure

A SIM supporting SIM Application Toolkit shall indicate this through relevant data in EF_{Phase} and EF_{SST}, as defined in the relevant sections above.

An ME supporting SIM Application Toolkit shall perform initialization as defined in the SIM Initialization section above.

11.6.2 Proactive polling

An ME supporting proactive SIM (part of SIM Application Toolkit) shall support the polling procedure as defined above.

11.6.3 Support of commands

A SIM or ME supporting SIM Application Toolkit shall support the commands TERMINAL PROFILE, ENVELOPE, FETCH and TERMINAL RESPONSE.

These commands shall never be used if either the SIM or ME does not support SIM Application Toolkit. Therefore standard SIMs and MEs do not need to support these commands.

11.6.4 Support of response codes

A SIM or ME supporting SIM Application Toolkit shall support the response status words (SW1 SW2) '91 XX', and '93 00' and '9E XX'. The SIM shall send '9E XX' only to an ME indicating in TERMINAL PROFILE that it supports the handling of these status words.

These responses shall never be used if either the SIM or ME does not support SIM Application Toolkit. Therefore standard SIMs and MEs do not need to support them.

11.6.5 Command-response pairs

Using the terminology where the ME issues a command and the SIM a response, ending in status words SW1 SW2, a command-response pair is considered as a single transaction. Each transaction is initiated by the ME and terminated by the SIM. One transaction must be completed before the next one can be initiated. This protocol applies to SIM Application Toolkit in the same way as it does to normal operation.

11.6.6 Independence of normal GSM and SIM Application Toolkit tasks

Normal GSM operation (relating to general, CHV related, GSM security related, and subscription related procedures) and SIM Application Toolkit operation shall be logically independent, both in the SIM and in the ME.

Specifically, this means:

- the currently selected EF and current record pointer in the normal GSM task shall remain unchanged, if still valid, as seen by the ME, irrespective of any SIM Application Toolkit activity;
- between successive SIM Application Toolkit related command-response pairs, other normal GSM related command-response pairs can occur. The SIM Application Toolkit task status shall remain unchanged by these command-response pairs.

11.6.7 Use of BUSY status response

If for any reason the SIM Application Toolkit task of the SIM cannot process an ENVELOPE command issued by the ME at present (e.g. other SIM Application Toolkit processes are already running, and this additional one would cause an overload), the SIM can respond with a status response of '93 00'. The ME may re-issue the command at a later stage.

The BUSY status response has no impact on normal GSM operation.

11.6.8 Use of NULL procedure byte

The NULL procedure byte provides a mechanism for the SIM to obtain more time before supplying the response part of a command-response pair, during which time the ME is unable to send further commands to the SIM.

If a SIM Application Toolkit activity in the SIM runs for too long, this may prevent the ME from sending "normal GSM" commands which are time-critical, e.g. RUN GSM ALGORITHM. A MORE TIME command is defined in GSM 11.14 [27], which ensures that the SIM Application Toolkit task in the SIM gets more processing time, while at the same time freeing the SIM/ME interface. This should be used in preference to NULL procedure bytes ('60').

11.6.9 Using the TERMINAL PROFILE, ENVELOPE, and TERMINAL RESPONSE commands

These commands are part of the set used by SIM Application Toolkit. The use of the these commands, the occasions where they are required, and the command and response parameters associated with the commands, are specified in GSM 11.14 [27]. The ME completes the command parameters/data of the relevant command and sends the command to the SIM. The transmitted data is processed by the SIM in a specific way depending on the tag value in the command parameters.

A SIM or ME not supporting SIM Application Toolkit does not need to support these commands.

11.6.10 Using the FETCH command

This command is used by SIM Application Toolkit. The use of the this command, the occasions where it is required, and the command and response parameters associated with the command, are specified in GSM 11.14 [27]. It is similar in function to GET RESPONSE, in that it requests response parameters from the SIM, following a '91 XX' status response. The transmitted response data from the SIM is processed by the ME in a specific way depending on the tag value in the response parameters.

A SIM or ME not supporting SIM Application Toolkit does not need to support this command.

11.6.11 Data Download via SMS-CB

Requirement: Service n°25 "allocated and activated".

The ME shall perform the reading procedure with EF_{CBMID}. On receiving a cell broadcast message with an identifier which matches an identifier in EF_{CBMID}, the ME shall pass the CB message to the SIM using the ENVELOPE command. If a match is not found and service no. 14 is "allocated and activated", then the message identifier is checked against those in EF_{CBMI}.

11.6.12 Data Download via SMS-PP

Requirement: Service n°26 "allocated and activated".

The procedures and commands for Data Download via SMS-PP are defined in GSM 11.14 [27].

11.6.13 Menu selection

Requirement: Service n°27 "allocated and activated".

The procedures and commands for Menu Selection are defined in GSM 11.14 [27].

11.6.14 Call Control

Requirement: Service n°28 "allocated and activated".

The procedures and commands for Call Control are defined in GSM 11.14 [27]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Call Control in the TERMINAL PROFILE command. When BDN is enabled, the Call control facility of the ME is used by the SIM to support the BDN service.

11.6.15 Proactive SIM

Requirement: Service n°29 "allocated and activated".

The procedures and commands for Proactive SIM, at the application level, are defined in GSM 11.14 [27].

11.6.16 Mobile Originated Short Message control by SIM

Requirement: Service n°37 "allocated and activated".

The procedures and commands for Mobile Originated Short Message control by SIM are defined in GSM 11.14 [27]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Mobile Originated Short Message control by SIM in the TERMINAL PROFILE command.

11.6.17 SIM data download error

In case of an ENVELOPE for SIM data download, the SIM can respond with the status words '9E XX' to indicate that response data is available. The ME shall use the GET RESPONSE command to get the response data. The ME shall then send transparently to the network this response data, using the error procedure of the transport mechanism.

11.6.18 Image Request

Requirement: Service n°38 "allocated and activated".

The ME sends the identification of the information to be read. The ME shall analyse the data of EF_{IMG} (subclause 10.6.1.1) to identify the files containing the image's instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete image instance data.

11.7 MExE related procedures

MExE is an optional feature. The higher level procedures, and contents and coding of the commands, are given in TS 23.057 [50]. Procedures relating to the transmission of commands and responses across the SIM/ME interface are given in this section. A SIM or ME supporting MExE shall conform to the requirements given in this section.

11.7.1 MExE ST

Requirement: Service n°49 (MExE) "allocated and activated".

Request: The ME performs the reading procedure with $EF_{MExE\ ST}$.

11.7.2 Operator root public key

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°1 (EF_{ORPK})" allocated and activated".

Request: The ME performs the reading procedure with EF_{ORPK}. The ME shall analyse the data of EF_{ORPK} (sub-clause 10.7.2) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

11.7.3 Administrator root public key

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°2 (EF_{ARPK}) "allocated and activated".

Request: The ME performs the reading procedure with EF_{ARPK}. The ME shall analyse the data of EF_{ARPK} (sub-clause 10.7.3) to identify the file containing the certificate instance. If necessary, then the ME performs READ BINARY commands on this file to assemble the complete certificate instance data.

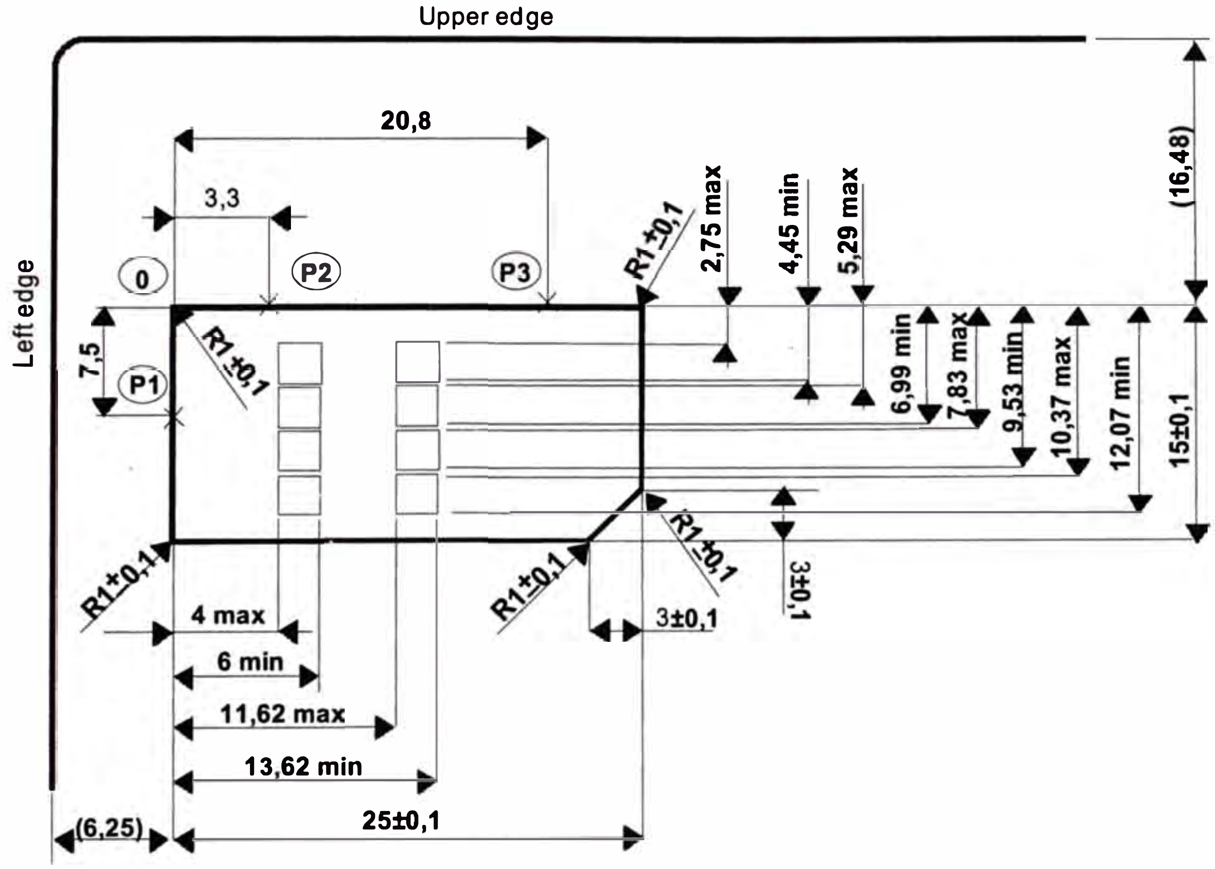
11.7.4 Third Party root public key(s)

Requirement: Service n°49 (MExE) "allocated and activated" and MExE ST service n°3 (EF_{TPRPK}) "allocated and activated".

Request: The ME performs the reading procedure with EF_{TPRPK}. The ME shall analyse the data of EF_{TPRPK} (sub-clause 10.7.4) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

Annex A (normative): Plug-in SIM

This annex specifies the dimensions of the Plug-in SIM as well as the dimensions and location of the contacts of the Plug-in SIM. For further details of the Plug-in SIM see clause 4.



NOTE: The Plug-in SIM may be "obtained" by cutting away excessive plastic of an ID-1 SIM. The values in parenthesis in figure A.1 show the positional relationship between the Plug-in and the ID-1 SIM and are for information only.

Figure A.1: Plug-in SIM

Annex B (normative): Coding of Alpha fields in the SIM for UCS2

If 16 bit UCS2 characters as defined in ISO/IEC 10646 [31] are being used in an alpha field, the coding can take one of three forms. If the ME supports UCS2 coding of alpha fields in the SIM, the ME shall support all three coding schemes for character sets containing 128 characters or less; for character sets containing more than 128 characters, the ME shall at least support the first coding scheme. If the alpha field record contains GSM default alphabet characters only, then none of these schemes shall be used in that record. Within a record, only one coding scheme, either GSM default alphabet, or one of the three described below, shall be used.

1) If the first octet in the alpha string is '80', then the remaining octets are 16 bit UCS2 characters, with the more significant octet (MSO) of the UCS2 character coded in the lower numbered octet of the alpha field, and the less significant octet (LSO) of the UCS2 character is coded in the higher numbered alpha field octet, i.e. octet 2 of the alpha field contains the more significant octet (MSO) of the first UCS2 character, and octet 3 of the alpha field contains the less significant octet (LSO) of the first UCS2 character (as shown below). Unused octets shall be set to 'FF', and if the alpha field is an even number of octets in length, then the last (unusable) octet shall be set to 'FF'.

Example 1

Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7	Octet 8	Octet 9
'80'	Ch1$_{MSO}$	Ch1$_{LSO}$	Ch2$_{MSO}$	Ch2$_{LSO}$	Ch3$_{MSO}$	Ch3$_{LSO}$	'FF'	'FF'

2) If the first octet of the alpha string is set to '81', then the second octet contains a value indicating the number of characters in the string, and the third octet contains an 8 bit number which defines bits 15 to 8 of a 16 bit base pointer, where bit 16 is set to zero, and bits 7 to 1 are also set to zero. These sixteen bits constitute a base pointer to a "half-page" in the UCS2 code space, to be used with some or all of the remaining octets in the string. The fourth and subsequent octets in the string contain codings as follows; if bit 8 of the octet is set to zero, the remaining 7 bits of the octet contain a GSM Default Alphabet character, whereas if bit 8 of the octet is set to one, then the remaining seven bits are an offset value added to the 16 bit base pointer defined earlier, and the resultant 16 bit value is a UCS2 code point, and completely defines a UCS2 character.

Example 2

Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7	Octet 8	Octet 9
'81'	'05'	'13'	'53'	'95'	'A6'	'XX'	'FF'	'FF'

In the above example;

Octet 2 indicates there 5 characters in the string.

Octet 3 indicates bits 15 to 8 of the base pointer, and indicates a bit pattern of 0hhh hhhh h000 0000 as the 16 bit base pointer number. Bengali characters for example start at code position 0980 (0*000 1001 1*000 0000), which is indicated by the coding '13' in octet 3 (shown by the italicised digits).

Octet 4 indicates GSM Default Alphabet character '53', i.e. "S".

Octet 5 indicates a UCS2 character offset to the base pointer of '15', expressed in binary as follows 001 0101, which, when added to the base pointer value results in a sixteen bit value of 0000 1001 1001 0101, i.e. '0995', which is the Bengali letter KA.

Octet 8 contains the value 'FF', but as the string length is 5, this a valid character in the string, where the bit pattern 111 1111 is added to the base pointer, yielding a sixteen bit value of 0000 1001 1111 1111 for the UCS2 character (i.e. '09FF').

3) If the first octet of the alpha string is set to '82', then the second octet contains a value indicating the number of characters in the string, and the third and fourth octets contain a 16 bit number which defines the complete 16 bit base pointer to a "half-page" in the UCS2 code space, for use with some or all of the remaining octets in the string. The fifth and subsequent octets in the string contain codings as follows; if bit 8 of the octet is set to zero, the remaining 7 bits of the octet contain a GSM Default Alphabet character, whereas if bit 8 of the octet is set to one, the remaining seven bits are an offset value added to the base pointer defined in octets three and four, and the resultant 16 bit value is a UCS2 code point, and defines a UCS2 character.

Example 3

Octet 1	Octet 2	Octet 3	Octet 4	Octet 5	Octet 6	Octet 7	Octet 8	Octet 9
'82'	'05'	'05'	'30'	'2D'	'82'	'D3'	'2D'	'31'

In the above example

- Octet 2 indicates there are 5 characters in the string.

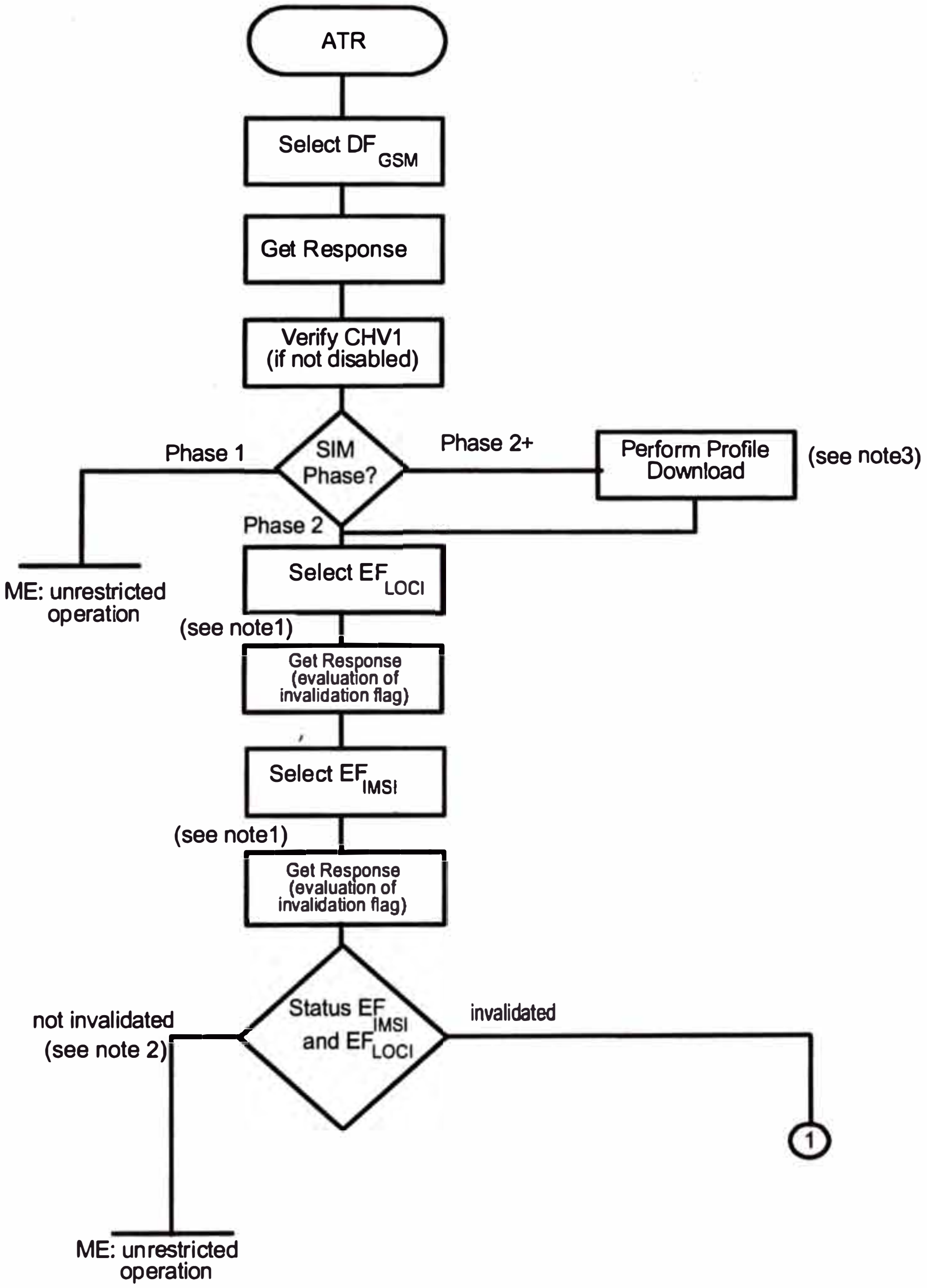
- Octets 3 and 4 contain a sixteen bit base pointer number of '0530', pointing to the first character of the Armenian character set.

Octet 5 contains a GSM Default Alphabet character of '2D', which is a dash "-".

Octet 6 contains a value '82', which indicates it is an offset of '02' added to the base pointer, resulting in a UCS2 character code of '0532', which represents Armenian character Capital BEN.

Octet 7 contains a value 'D3', an offset of '53', which when added to the base pointer results in a UCS2 code point of '0583', representing Armenian Character small PIWR.

Annex C (informative): FDN/BDN Procedures

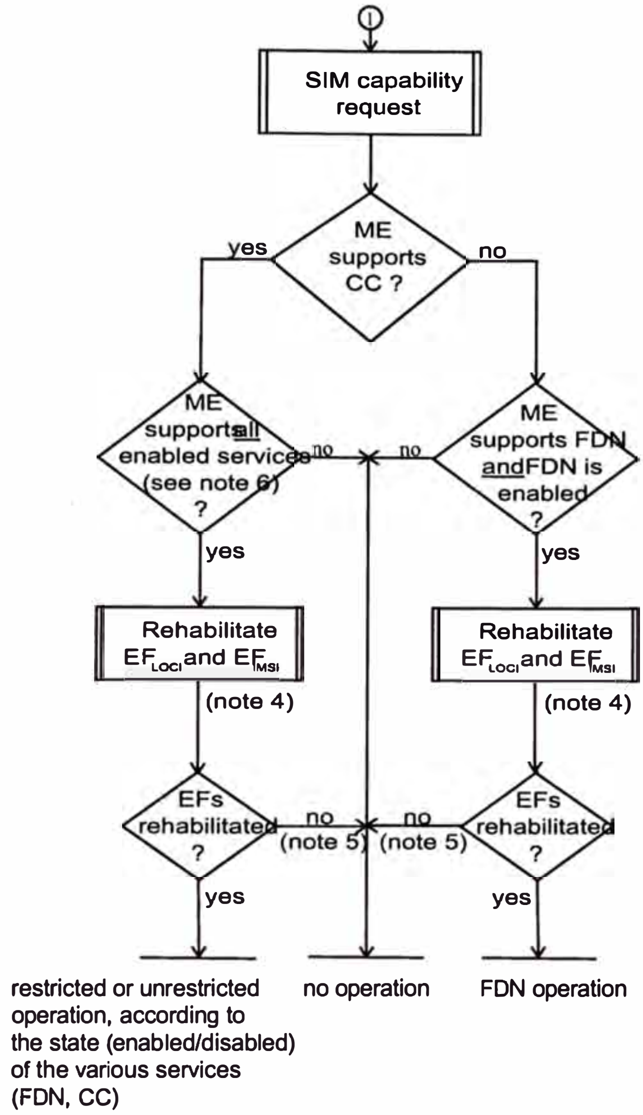

ATR
Select DF_{GSM}
Get Response
Verify CHV1 (if not disabled)
SIM Phase?
Phase 1
Phase 2+
Perform Profile Download
(see note3)
Phase 2
ME: unrestricted operation
Select EF_{LOCI}
(see note1)
Get Response (evaluation of invalidation flag)
Select EF_{IMSI}
(see note1)
Get Response (evaluation of invalidation flag)
Status EF_{IMSI} and EF_{LOCI}
not invalidated (see note 2)
invalidated
1
ME: unrestricted operation

NOTE 1: In case of enabled FDN and/or enabled BDN, the EF has been invalidated by the SIM at no later than this stage.

NOTE 2: Invalidation of only one of the two EFs is not allowed for FDN and BDN.

NOTE 3: For SIMs with enabled BDN this procedure is used to check whether the ME supports the Call Control by the SIM facility.

Figure C.1: Example of an Initialization Procedure of a FDN/BDN SIM (see subclause 11.2.1)


1
SIM capability request
ME supports CC ?
yes
no
ME supports all enabled services (see note 6) ?
no
no
ME supports FDN and FDN is enabled ?
yes
yes
Rehabilitate EF$_{LOCI}$ and EF$_{IMSI}$
Rehabilitate EF$_{LOCI}$ and EF$_{IMSI}$
(note 4)
(note 4)
EFs rehabilitated ?
no (note 5)
no (note 5)
EFs rehabilitated ?
yes
yes
restricted or unrestricted operation, according to the state (enabled/disabled) of the various services (FDN, CC)
no operation
FDN operation

NOTE 4: In case of "BDN enabled", the SIM only allows rehabilitation of the EF$_{IMSI}$ and EF$_{LOCI}$, if the ME has indicated its CC-capability to the SIM (by PROFILE_DOWNLOAD).

NOTE 5: Possibility for future "restricting" services to use the internal SIM mechanism of invalidation of EF$_{IMSI}$ and EF$_{LOCI}$.

NOTE 6: If the ME does not support all enabled services (e.g. FDN, BDN), it does not operate. In case of enabled BDN, the support of the "Call Control Feature" by the ME is sufficient for operation. For future use, there may be additional "restricting" services, which are not known to the ME. In that case the ME will perform the subsequent rehabilitation procedure but will fail to rehabilitate EF$_{IMSI}$ and EF$_{LOCI}$ (see note 4).

Figure C.1: Example of an Initialization Procedure of a FDN/BDN SIM (continued)

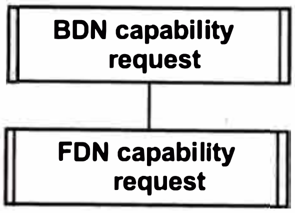


Figure C.2: SIM capability request

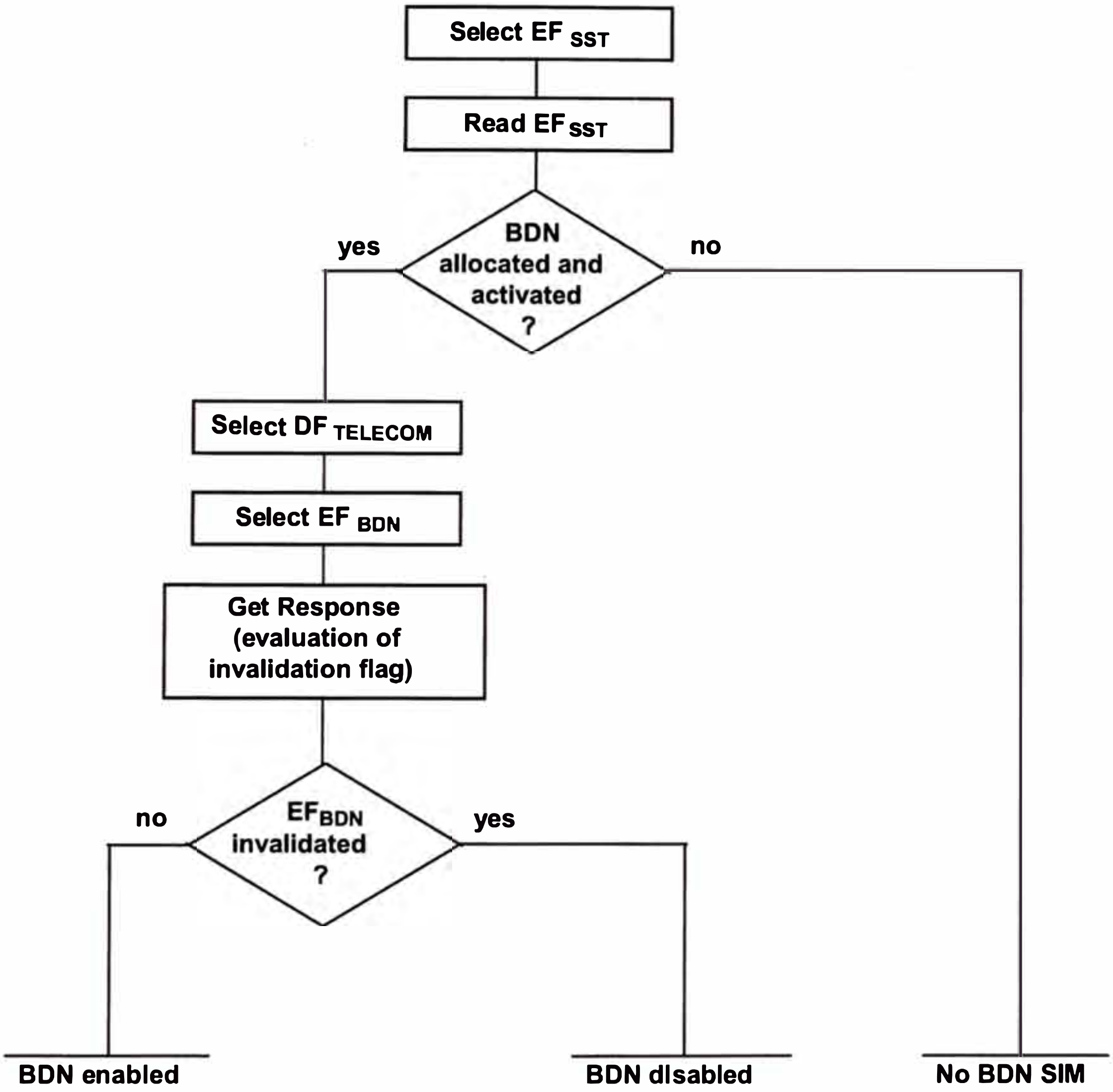
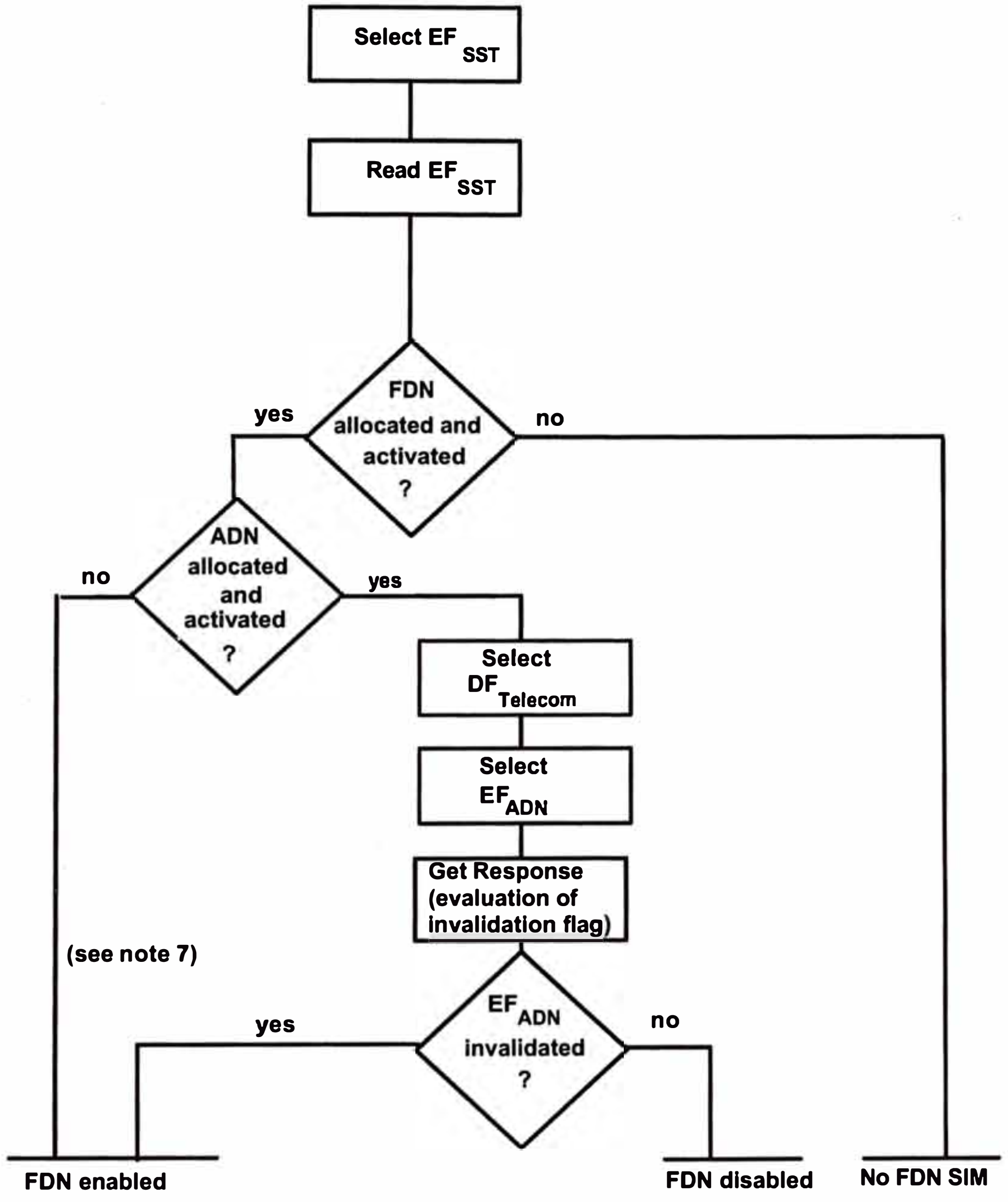
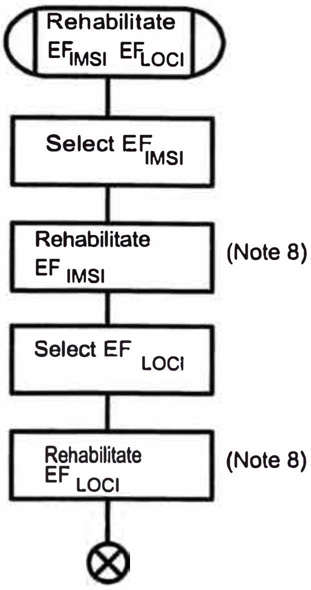


Figure C.3: BDN capability request (see subclause 11.5.1)



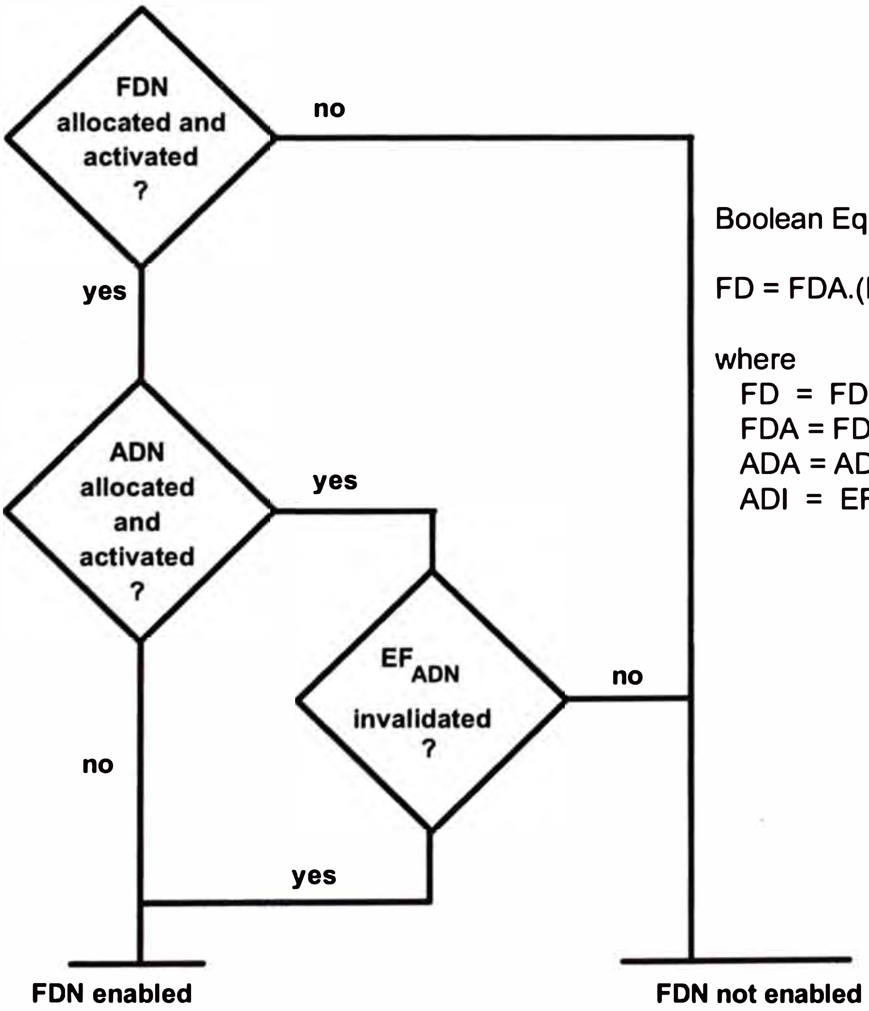
NOTE 7: In this case FDN is enabled without the possibility of disabling.

Figure C.4: FDN capability request (see subclause 11.5.1)



NOTE 8: If BDN is enabled in the SIM, and if the Profile download procedure has not indicated that the ME supports Call Control, the EF is not rehabilitated by the SIM.

Figure C.5: Procedure to rehabilitate GSM files



Boolean Equation:

FD = FDA.(NOT(ADA)+ADA.ADI)

where
FD = FDN enabled
FDA = FDN allocated and activated
ADA = ADN allocated and activated
ADI = EFADN invalidated

Figure C.6: Coding for state of FDN

Annex D (informative): Suggested contents of the EFs at pre-personalization

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

File Identification	Description	Value
'2FE2'	ICC identification	operator dependant (see 10.1.1)
'2F05'	Extended Language preference	'FF...FF'
'6F05'	Language preference	'FF'
'6F07'	IMSI	operator dependant (see 10.3.2)
'6F20'	Ciphering key Kc	'FF...FF07'
'6F30'	PLMN selector	'FF...FF'
'6F31'	HPLMN search period	'FF'
'6F37'	ACM maximum value	'000000' (see note 1)
'6F38'	SIM service table	operator dependant (see 10.3.7)
'6F39'	Accumulated call meter	'000000'
'6F3E'	Group identifier level 1	operator dependant
'6F3F'	Group identifier level 2	operator dependant
'6F41'	PUCT	'FFFFFF0000'
'6F45'	CBMI	'FF...FF'
'6F46'	Service provider name	'FF...FF'
'6F48'	CBMID	'FF...FF'
'6F49'	Service Dialling Numbers	'FF...FF'
'6F74'	BCCH information	'FF...FF'
'6F78'	Access control class	operator dependant (see 10.1.12)
'6F7B'	Forbidden PLMNs	'FF...FF'
'6F7E	Location information	'FFFFFFFF xxxxxx 0000 FF 01' (see note 2)
'6FAD'	Administrative data	operator dependant (see 10.3.15)
'6FAE'	Phase identification	see 10.3.16
'6F3A'	Abbreviated dialling numbers	'FF...FF'
'6F3B'	Fixed dialling numbers	'FF...FF'
'6F3C'	Short messages	'00FF...FF'
'6F3D'	Capability configuration parameters	'FF...FF'
'6F40'	MSISDN storage	'FF...FF'
'6F42'	SMS parameters	'FF...FF'
'6F43'	SMS status	'FF...FF'
'6F44'	Last number dialled	'FF...FF'
'6F47'	Short message status reports	'00FF…FF'
'6F4A'	Extension 1	'FF...FF'
'6F4B'	Extension 2	'FF...FF'
'6F4C'	Extension 3	'FF...FF'
'6F4D'	Barred dialling numbers	'FF...FF'
'6F4E'	Extension 4	'FF...FF'
'6F4F'	Extended capability configuration parameters	'FF...FF'
'6F51'	Network's indication of alerting	'FF...FF'
'6F52'	GPRS Ciphering key KcGPRS	'FF...FF07'
'6F53'	GPRS Location Information	'FFFFFFFF FFFFFF xxxxxx 0000 FF 01'
'6F54'	SetUpMenu Elements	operator dependant (see 10.3.34)
'6F58'	Comparison method information	'FF…FF'
'6F60'	PLMN Selector with Access Technology	'00…00'
'6F61'	OPLMN Selector with Access Technology	'00…00'
'6F62'	HPLMN Access Technology	'FF…FF'
'6F63'	CPBCCH information	'00'
'6F64'	Investigation PLMN Scan	'00'
'4F20'	Image data	'00FF...FF'
'4F30'	SoLSA Access Indicator)	'00FF...FF'
'4F31'	SoLSA LSA List	'FF...FF'

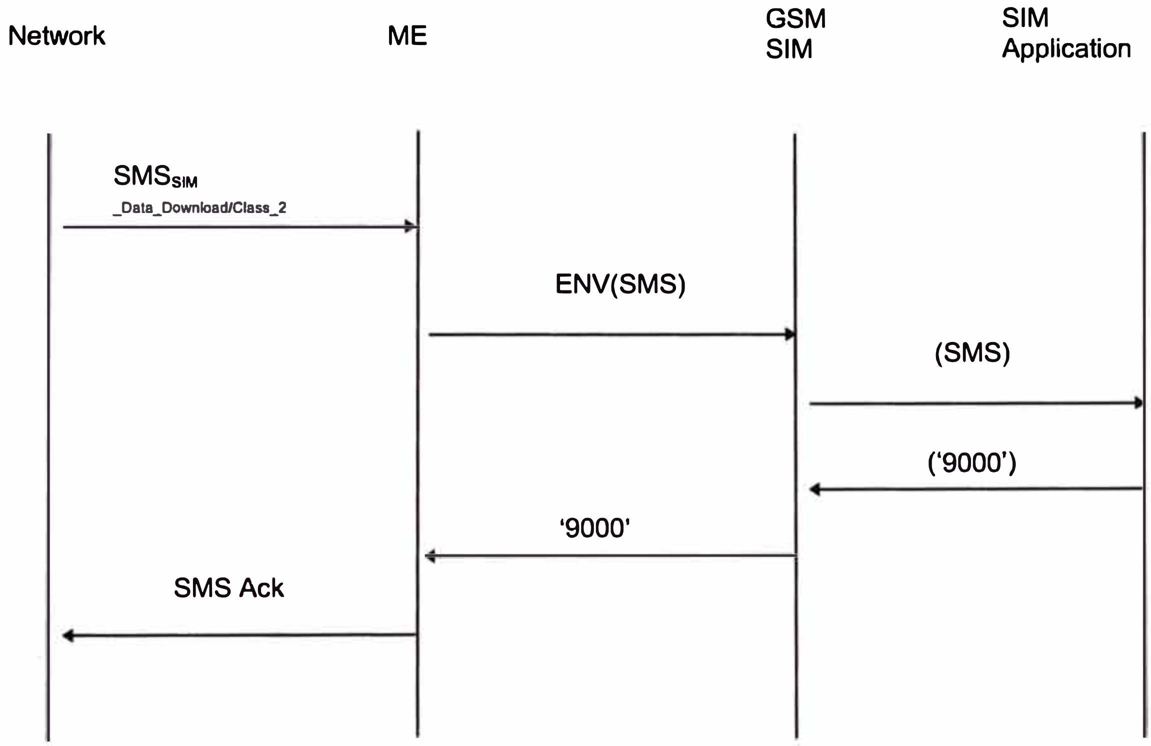
NOTE 1: The value '000000' means that ACMmax is not valid, i.e. there is no restriction on the ACM. When assigning a value to ACMmax, care should be taken not to use values too close to the maximum possible value 'FFFFFF', because the INCREASE command does not update EF_{ACM} if the units to be added would exceed 'FFFFFF'. This could affect the call termination procedure of the Advice of Charge function.

NOTE 2: xxxxxx stands for any valid MCC and MNC, coded according to GSM 04.08 [15].

Annex E (informative): SIM application Toolkit protocol diagrams

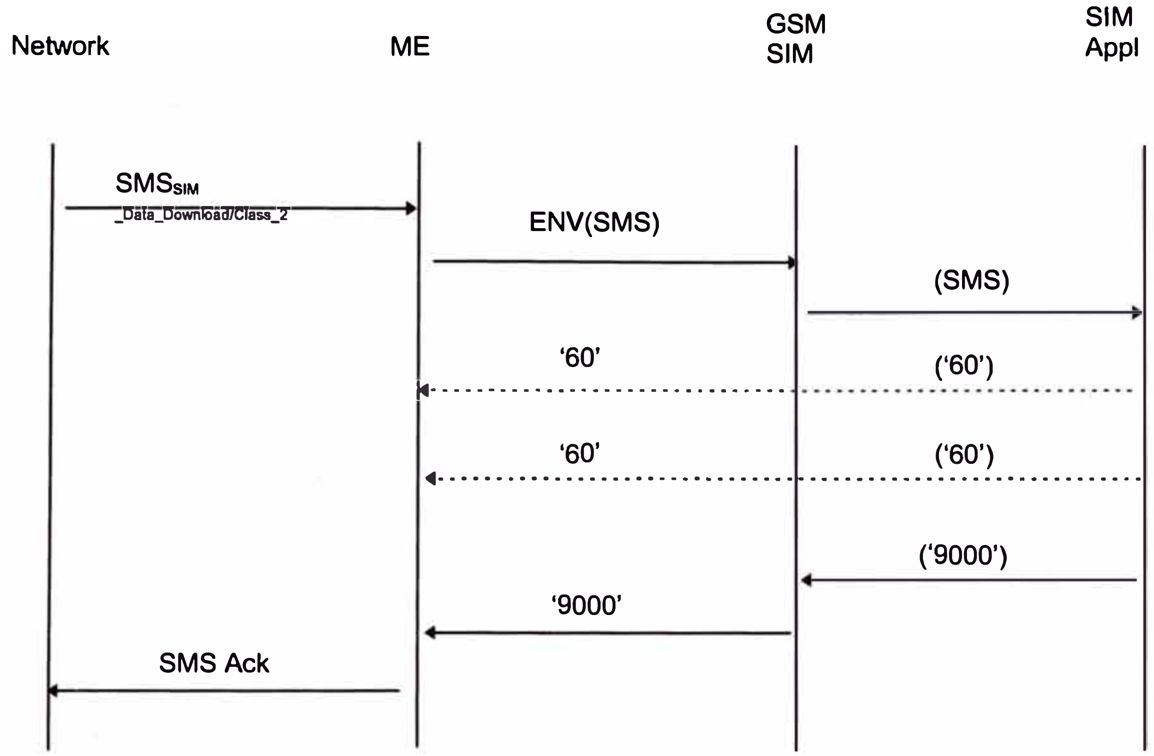
The diagrams in this annex are intended to illustrate the data protocols of the SIM toolkit application in various situations. The SIM application is shown as initiated by SMS Data Download messages. Other possibilities exist (as defined in GSM 11.14) such as data entry from a menu selection.

Case 1: Simple



This shows the simple case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed immediately by the SIM application. This requires no ME action except to ac■nowledge the SMS.

Case 2: Simple with short delay

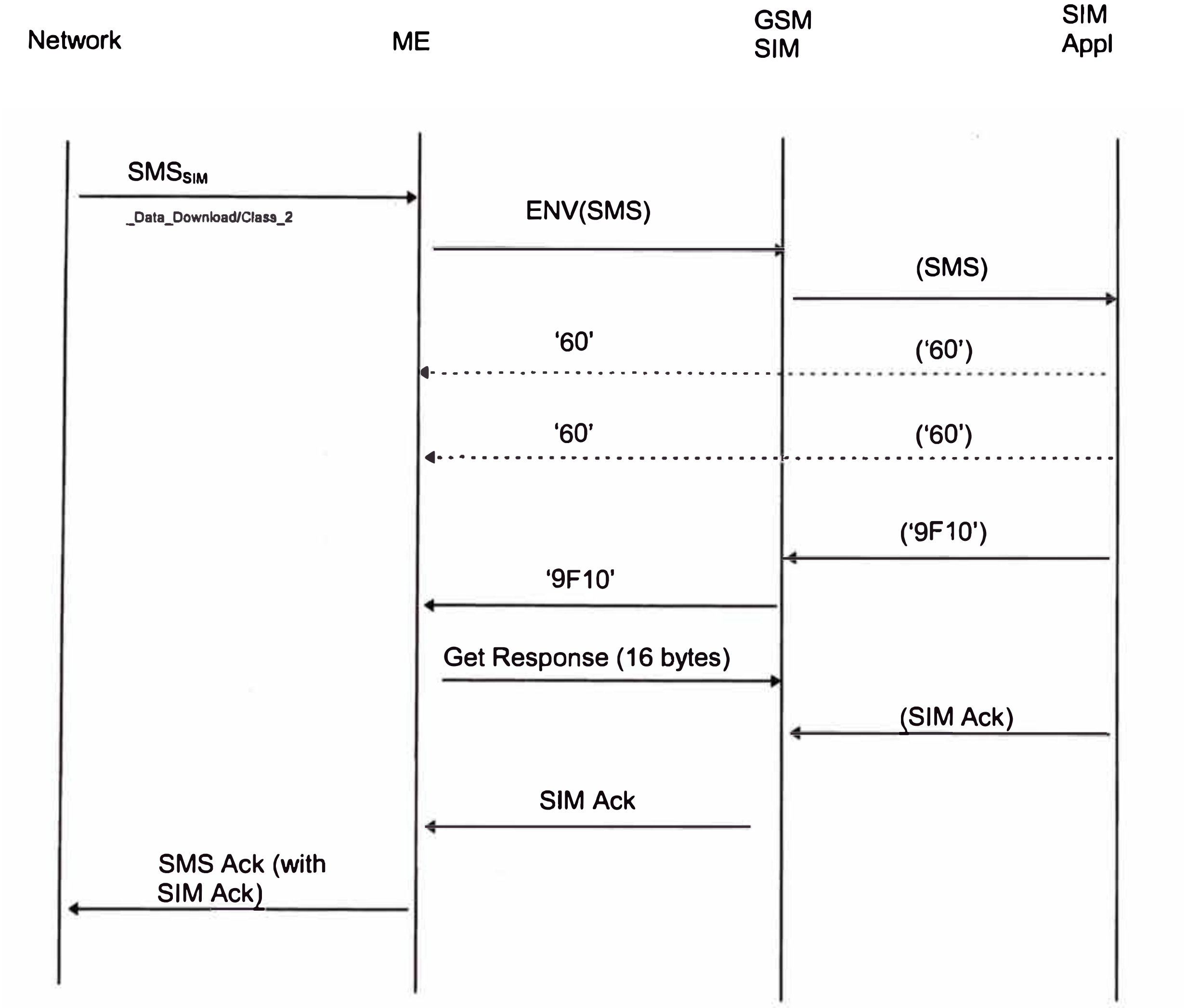


This shows the simple case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and which requires some time to process by the SIM application. The processing time is "not long" and is obtained by the SIM application sending "null procedure bytes" to the ME. Each byte has the effect of restarting the work waiting time so that the ME does not abort the transaction before the SIM application has finished processing the command(s) sent in the SMS.

Guidelines on timings:

1. The SMS Ack must be sent back before the network times out and sends the SMS again.
2. Use of null procedure bytes must not be excessive as during this time the ME is unable to issue normal GSM commands to the SIM.

Case 3: Simple with short delay and SIM Acknowledgement

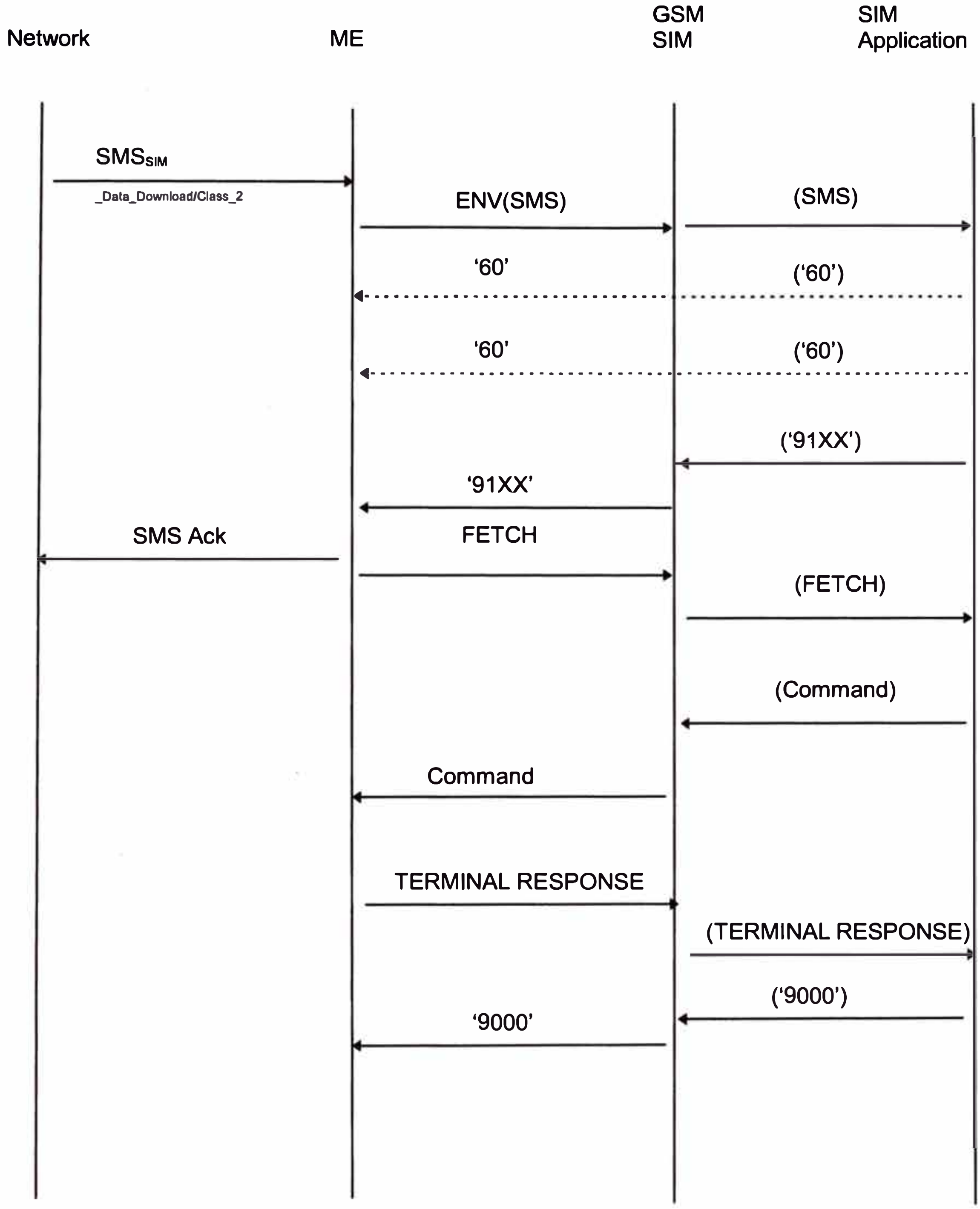


This shows the same case as previously where an SMS for SIM updating is received from the network, passed to the SIM by the ME and which requires some time to process by the SIM application. However in this case the SIM application has SIM acknowledgement data to include in the SMS acknowledgement being returned to the network by the ME.

Guideline on timings:

The SMS Ack must be sent back before the network times out and sends the SMS again.

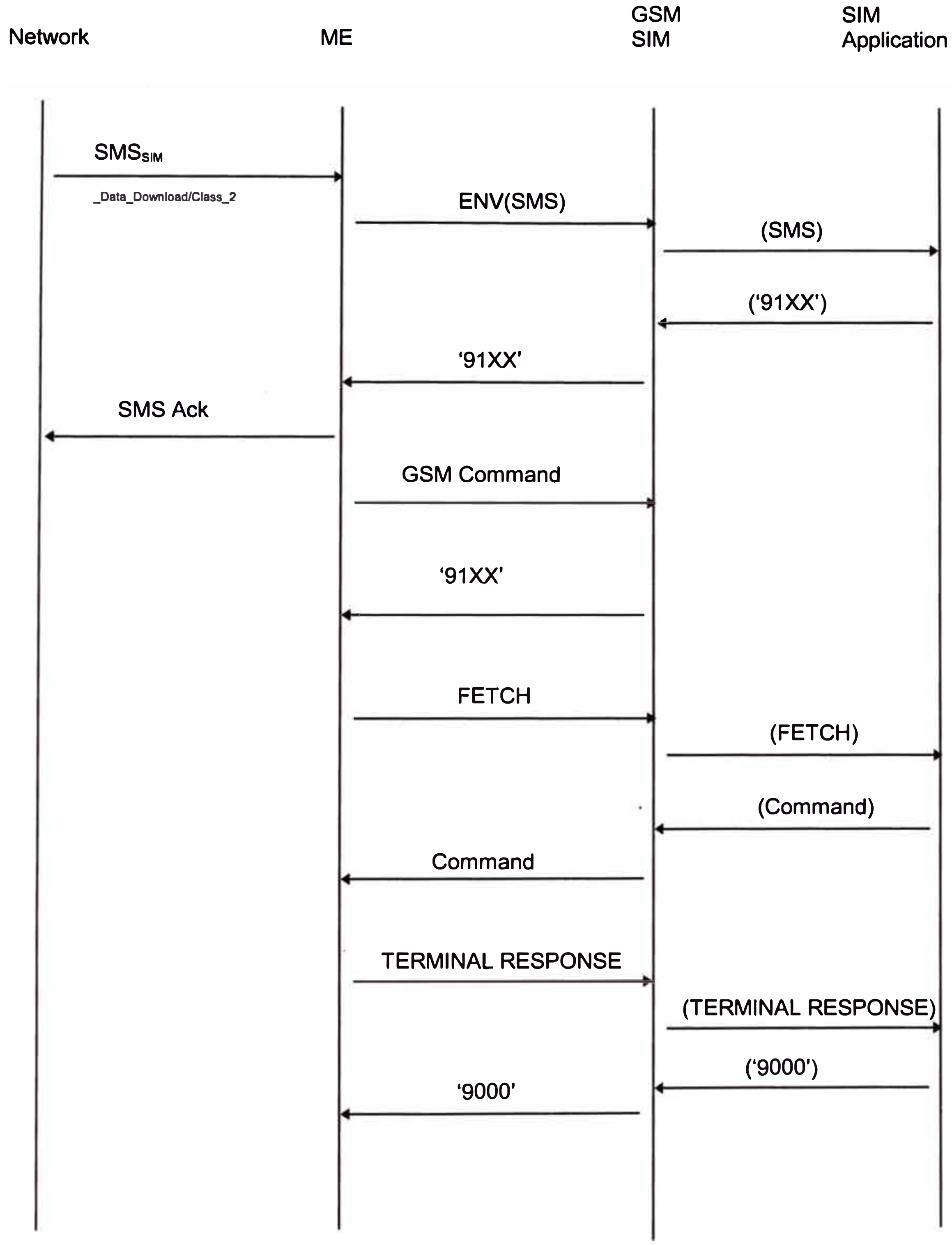
Case 4: A Toolkit command generated by the SIM application as a result of an SMS from the network



This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed by the SIM application which then generates a command for action by the ME (e.g. PLAYTONE).

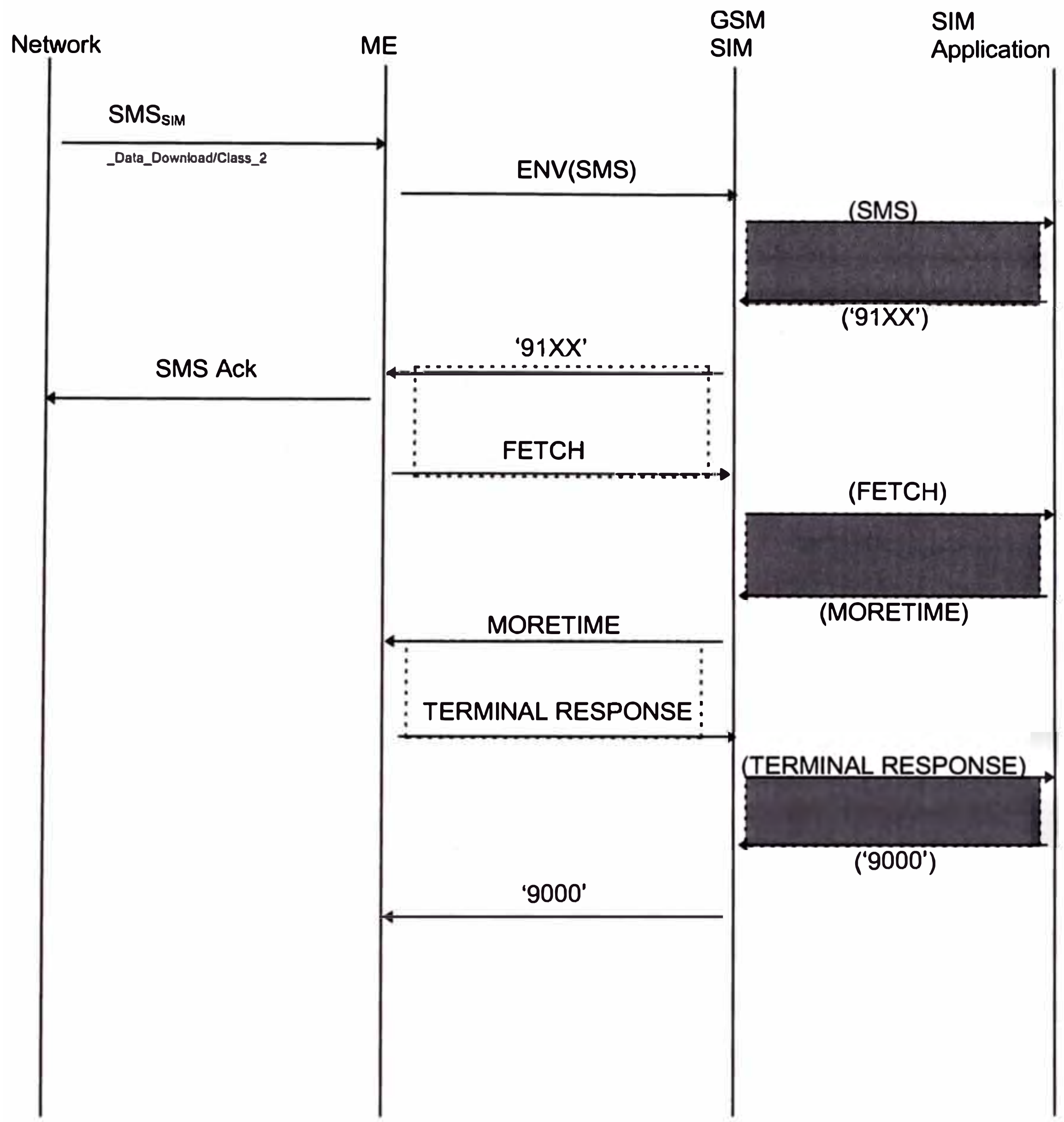
NOTE: If a positive acknowledgement to the network of completion of execution of the instructions given in the SMS message is required then the SIM application can issue a command to the ME to send a MO SMS.

Case 5: A normal GSM command requires processing before the ME can respond to the 91XX from the SIM



This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and processed by the SIM application which then generates a command for action by the ME (e.g. PLAYTONE). However a normal GSM command requires processing before the ME can FETCH the command which the SIM is waiting to give it. The response to the normal GSM command is '91XX' in this case to remind the ME of the outstanding SIM application command request.

Case 6: MORE TIME Command



This shows the case where an SMS for SIM updating is received from the network, passed to the SIM by the ME and requires a considerable period of time to be processed by the SIM application. In this case the use of null procedure bytes only is inappropriate as the ME must be given the opportunity to process normal GSM commands. The opportunities gained by the SIM application for processing, and the opportunities for normal GSM commands are shown in the diagram above. The sequence of 91XX, FETCH and MORETIME commands can be repeated if required.

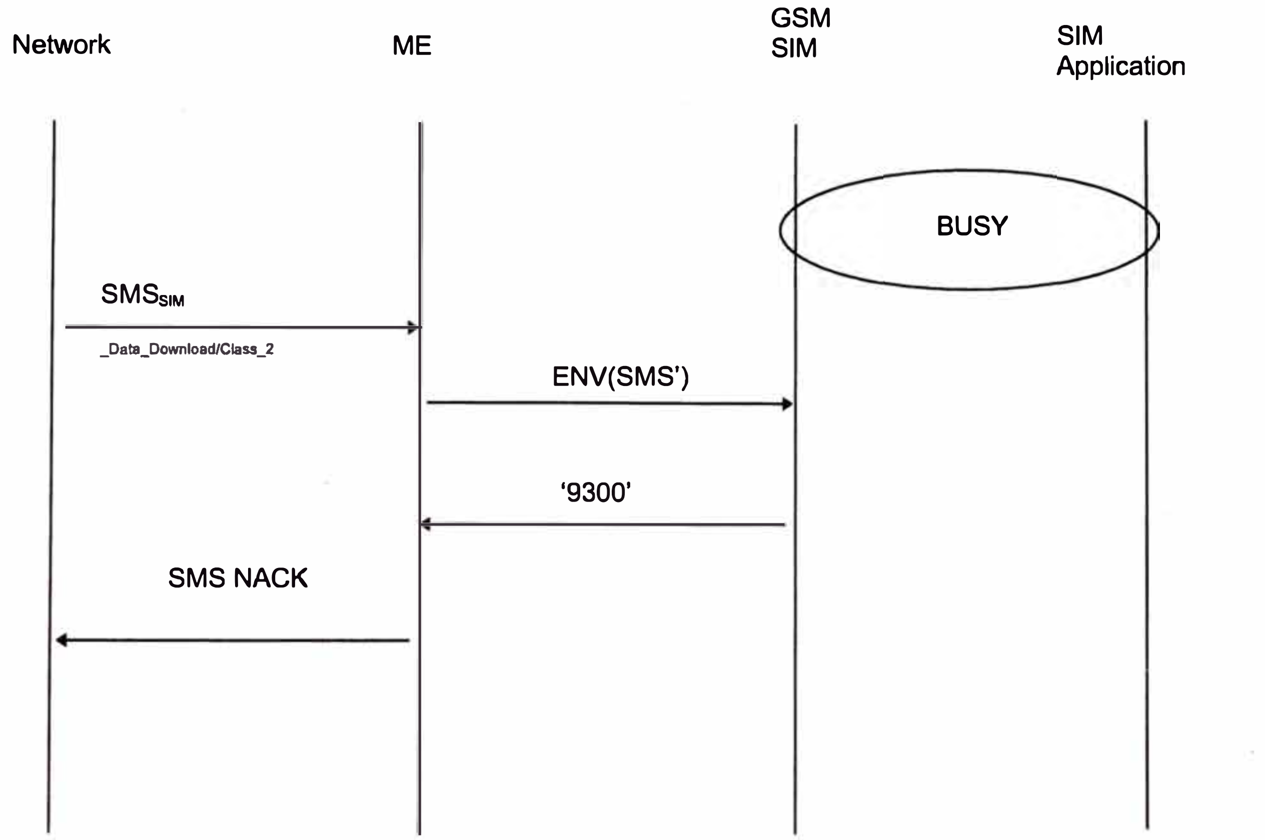
Opportunities to process normal GSM commands are shown thus:

⬚

Opportunities for SIM application processing are shown thus:

■

Case 7: SIM Application Busy



While the SIM application is busy processing a SMS for the SIM application arrives from the network and is sent to the SIM by the ME in the usual manner. The SIM operating system recognizes that the SIM application is busy, and it sends a busy response ('9300') to the ME. The ME then sends negative acknowledgement to the network. The responsibility for a retry rests with the network.

Annex F (informative): Examples of coding of LSA Descriptor files for SoLSA

The length of all the records is determined by the LSA descriptor containing the largest number of bytes. Combinations containing different numbers of LSA IDs, LAC+ CI and CI or LAC can therefore be done. Various examples are show. Due to the OTA management of the records it is recommended that the record length is maximum 100 bytes in order to leave room for command descriptor and signature information in the SMS.

This first example contains two LSAs, one described by two LSA IDs and another described by three Cell IDs, giving a record length of 8 bytes.

1st record:

LSA descriptor type = LSA ID and number = 2 (1 byte)	LSA ID (3 bytes)	LSA ID (3 bytes)	Identifier (1 byte)

2nd record:

LSA descriptor type = CI and number = 3 (1 byte)	CI (2 bytes)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

The second example contains two LSAs, one described by one LSA ID and one described by two Cell Ids, giving a record length of 6 bytes.

1st record:

LSA descriptor type = LSA ID and number = 1 (1 byte)	LSA ID (3 bytes)	'FF'	Identifier (1 byte)

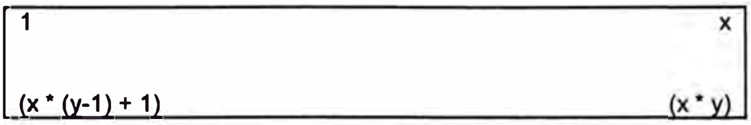
2nd record:

LSA descriptor type = CI and number = 2 (1 byte)	CI (2 bytes)	CI (2 bytes)	Identifier (1 byte)

Annex G (normative): Image Coding Schemes

The following image coding schemes are applicable to rectangular raster images. Raster image points are assumed to be of square shape. They are numbered sequentially from 1 onwards, starting at the upper left corner, proceeding line by line downwards, each line in turn proceeding from left to right, and ending at the image's lower right corner.

The following example illustrates the numbering scheme for raster image points by showing how the corner points are numbered, assuming an image length of x points and an image height of y points.



G.1 Basic Image Coding Scheme

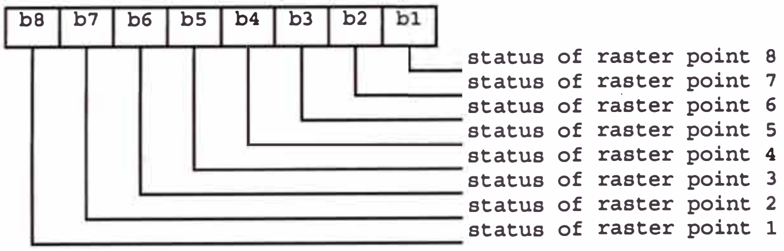
This coding scheme applies to rectangular raster images made up of raster points that are either set or not set. This coding scheme does not support any notion of colour. Image data are coded as follows:

Byte(s)	Description	Length
1	image width = X	1
2	image height = Y	1
3 to K+2	image body	K

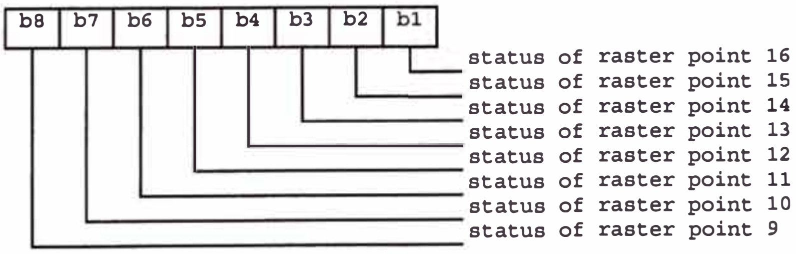
Coding of image body:

The status of each raster image point is coded in one bit, to indicate whether the point is set (status = 1) or not set (status = 0).

Byte 1:



Byte 2:


b8
b7
b6
b5
b4
b3
b2
b1
status of raster point 16
status of raster point 15
status of raster point 14
status of raster point 13
status of raster point 12
status of raster point 11
status of raster point 10
status of raster point 9

etc.

Unused bits shall be set to 1

G.2 Colour Image Coding Scheme

This coding scheme applies to coloured rectangular raster images. Raster image point colours are defined as references into a colour look-up table (CLUT), which contains a subset of the red-green-blue colour space. The CLUT in turn is located in the same transparent file as the image instance data themselves, at an offset defined within the image instance data.

Image data are coded as follows:

Byte(s)	Description	Length
1	Image width = X	1
2	Image height = Y	1
3	Bits per raster image point = B	1
4	Number of CLUT entries = C	1
5 to 6	Location of CLUT (Colour Look-up Table)	2
7 to K+6	Image body	K

Bits per raster image point:

Contents:

The number B of bits used to encode references into the CLUT, thus defining a raster image point's colour.

B shall have a value between 1 and 8.

Coding:

Binary.

- Number of entries in CLUT:

Contents:

The number C of entries in the CLUT which may be referenced from inside the image body. CLUT entries are numbered from 0 to C-1.

C shall have a value between 1 and 2**B.

Coding:

Binary. The value 0 shall be interpreted as 256.

Location of CLUT:

Contents:

This item specifies where the CLUT for this image instance may be found. The CLUT is always located in the same transparent file as the image instance data themselves, at an offset determined by these two bytes.

Coding:

Byte 1: high byte of offset into Image Instance File.

Byte 2: low byte of offset into Image Instance File.

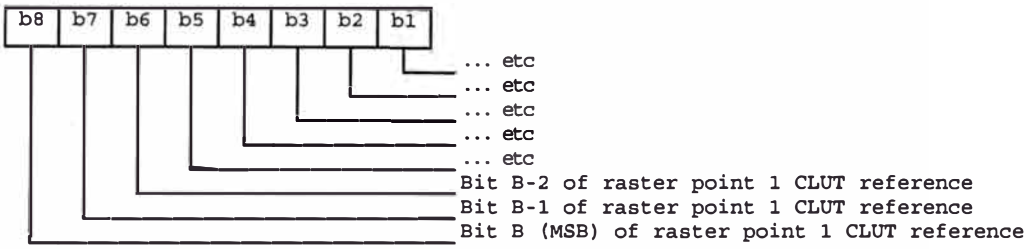
Image body:

Coding:

Each raster image point uses B bits to reference one of the C CLUT entries for this image instance. The CLUT entry being thus referenced yields the raster image point's colour.

The image body is arrayed as for the Basic Colour Image Coding Scheme, that is, starting with the highest bit of the first raster image point's colour information.

Byte 1:


b8
b7
b6
b5
b4
b3
b2
b1
... etc
... etc
... etc
... etc
... etc
Bit B-2 of raster point 1 CLUT reference
Bit B-1 of raster point 1 CLUT reference
Bit B (MSB) of raster point 1 CLUT reference

etc.

Unused bits shall be set to 1.

The CLUT (Colour Look-up Table) for an image instance with C colours is defined as follows:

Contents:

C CLUT entries defining one colour each.

Coding:

The C CLUT entries are arranged sequentially:

Byte(s) of CLUT	CLUT Entry
1-3	entry 0
...	...
3*(C-1) +1 to 3*C	Entry C-1

Each CLUT entry in turn comprises 3 bytes defining one colour in the red-green-blue colour space:

Byte(s) of CLUT enty	Intensity of Colour
1	Red
2	Green
3	Blue

A value of 'FF' means maximum intensity, so the definition 'FF' '00' 00' stands for fully saturated red.

NOTE 1: Two or more image instances located in the same file can share a single CLUT.

NOTE 2: Most MEs capable of displaying colour images are likely to support at least a basic palette of red, green, blue and white.

Annex H (normative): Coding of EFs for NAM and GSM-AMPS Operational Parameters

If the EIA/TIA-553 DF is provisioned on the SIM, then EFs specified in this annex and indicated as mandatory under the DF shall be provided. TIA/EIA-41 [40] based radio access systems should use this DF for storage of NAM parameters.

All quantities shown in the EF descriptions abide by the following rules unless otherwise specified:

- all unused bits of allocated parameters shall be set by default to 0;
- all unused bytes in a series of values (e.g. Partner, Favoured, or Forbidden SID List) should be set by default to 'FF'.

H.1 Elementary File Definitions and Contents

H.1.1 EF$_{MIN}$ (Mobile Identification Number)

This EF contains the Mobile Identification Number (MIN). The MIN is a 34-bit number used to address the mobile station across the AMPS and the TIA/EIA-136 air interfaces, and to identify the mobile station's home network. See TIA/EIA-136-005 [36] for further details on MIN.

Identifier: '4F88'	Structure: transparent		Mandatory
File size: 5 bytes	Update Activity: low		
Access Conditions: READ UPDATE INVALIDATE REHABILITATE	 CHV1 CHV2 ADM ADM		
Bytes	Description	M/O	Length
1 – 2	MIN2	M	2 bytes
3 – 5	MIN1	M	3 bytes

The MIN field is coded as follows:

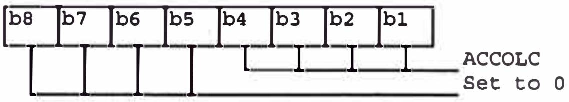
- 6 most significant bits are unused;
- next 10 bits are MIN2;
- 24 least significant bits are MIN1;
- default MIN is '00 00 00 00 00' or 'FF FF FF FF FF'. In either case the ME shall interpret this as an invalid MIN and shall not transmit this value over the radio interface.

H.1.2 EF$_{ACCOLC}$ (Access Overload Class)

This file contains the Access Overload Class (ACCOLC). The ACCOLC is a 4-bit indicator used to identify which overload class field controls the access attempts by the mobile station. See EIA/TIA-553 [41] for further details on ACCOLC.

Identifier: '4F89'		Structure: transparent	Mandatory
File size: 1 byte		Update Activity: low	
Access Conditions: READ UPDATE INVALIDATE REHABILITATE		 CHV1 CHV2 ADM ADM	
Bytes	Description	M/O	Length
1	ACCOLC (possible values from '00' to '0F')	M	1 byte

Byte 1:



Initial value shall be '00'.

H.1.3 EF$_{SID}$ (System ID Of Home System)

This file contains the system identity of the home system. The SID is a 15-bit number that uniquely identifies an AMPS or TIA/EIA-41 system. See EIA/TIA-553 [41] for further details on Home SID.

Identifier: '4F80'		Structure: transparent	Mandatory
File size: 2 bytes		Update Activity: low	
Access Conditions: READ UPDATE INVALIDATE REHABILITATE		 CHV1 CHV2 ADM ADM	
Bytes	Description	M/O	Length
1-2	System ID of Home System (SID) (Most significant bit = 0)	M	2 bytes

The default value shall be '0000'.

H.1.4 EF$_{IPC}$ (Initial Paging Channel)

The Initial (First) Paging Channel contains two 11-bit first paging channels (FIRSTCHP p-pri and FIRSTCHP p-sec) used to identify the channel number of the first paging channel when the mobile station is 'home'. See EIA/TIA-553 [41] for further details on First (Initial) Paging Channel.

Identifier: '4F82'	Structure: transparent	Mandatory
File size: 2-4 bytes	Update Activity: low	
Access Conditions: READ UPDATE INVALIDATE REHABILITATE	 CHV1 CHV2 ADM ADM	

Bytes	Description	M/O	Length
1 - 2	FIRSTCHPpri (Initial Paging Channel)	M	2 bytes
3 – 4	FIRSTCHPp-sec	O	2 bytes

- In the absence of the FIRSTCHPp-sec, the mobile station shall default to '02C4' if the primary channel = '014D' or '02E1' if the primary channel = '014E'
- A file size of 4 bytes may not be backwards compatible with the current dual-mode mobile equipment

The default of FISRTCHPpri value shall be '014D' for A systems, or '014E' for B systems.

H.1.5 EF$_{GPI}$ (Group ID)

This file defines a subset of the most significant bits of the system identification (SID) that is used to identify a group of cellular systems for local control purposes. If the local control option is enabled within the mobile station and the bits of the home system identification that comprise the group identification match the corresponding bits of the SID read by the mobile station over the air, then the Local Control status shall be enabled. Otherwise, the Local Control status shall be disabled. Refer to EIA/TIA-553 [41] for additional details.

Identifier: '4F81'	Structure: transparent	Mandatory
File size: 1 byte	Update Activity: low	
Access Conditions: READ UPDATE INVALIDATE REHABILITATE	 CHV1 CHV2 ADM ADM	

Bytes	Description	M/O	Length
1	Group ID	M	1 byte

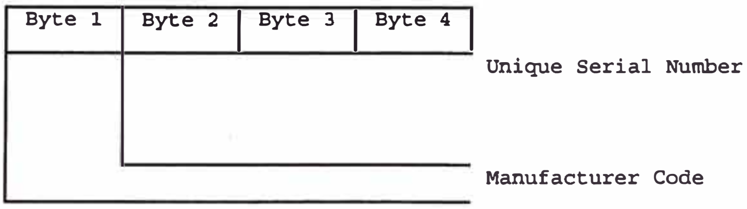
- Group ID default value for North America = '0A'.

H.1.6 EF$_{S\text{-}ESN}$ (SIM Electronic Serial Number)

This file stores a 32-bit electronic serial number (ESN) that is unique to the GSM-ANSI-136 SIM. The S-ESN can be unrelated to the ESN of any host equipment to which the GSM-ANSI-136 SIM may be attached. The S-ESN can be used for registration in conjunction with the MIN. The S-ESN may also be used in conjunction with the A-key and CAVE algorithm for authentication. See the ANSI-136 Usage Indicator file for details on the ESN usage indicator which specifies to the mobile equipment how the S-ESN should be used. See EIA/TIA-553 [41] for details on the ESN as it applies to registration and authentication.

The contents of this EF shall not be changed by any over-the-air procedures.

Identifier: '4F8B'	Structure: transparent		Mandatory
File size: 4 bytes	Update Activity: low		
Access Conditions: READ UPDATE INVALIDATE REHABILITATE	 CHV1 NEVER ADM ADM		
Bytes	Description	M/O	Length
1 – 4	SIM ESN	M	4 bytes



The default value shall be 'FF FF FF FF'.

H.1.7 EF$_{COUNT}$ (Call Count)

This file contains the CALL COUNT parameter. The CALL COUNT is used as a simple 'clone' detector in TIA/EIA-136 and AMPS modes. During the network access signalling in AMPS and other TIA/EIA-41 based networks, the SIM reports its CALL COUNT value to the network. If the value is consistent with the network perception of the CALL COUNT for that SIM, then the network will likely grant access based on the authentication process. During an AMPS or other TIA/EIA-41 based systems call, the value of the CALL COUNT may be incremented upon a command from the network. The value of the CALL COUNT, when incremented, is incremented by 1 using the INCREASE command. See EIA/TIA-553 [41] for further details on COUNTs-p.

Identifier: '4F83'	Structure: Cyclic		Mandatory
File size: 3*N bytes	Update Activity: high		
Access Conditions: READ UPDATE INVALIDATE REHABILITATE	 CHV1 ADM ADM ADM		
Bytes	Description	M/O	Length
Most Recent Record	CALL COUNT	M	3 bytes
—		...	...
Rec N	. . .	M	3 bytes

- File shall be initialised '00 00 00'
- Minimum file size is 2 records

H.1.8 EF$_{PSID}$ (Positive/Favoured SID list)

This file contains a list of Favoured SIDs for use in identifying Favoured service providers while performing network selection (intelligent roaming).

Identifier: '4F85'	Structure: transparent	Optional	
File size: 2*N bytes	Update Activity: low		
Access Conditions: READ UPDATE INVALIDATE REHABILITATE	 CHV1 ADM ADM ADM		
Bytes	Description	M/O	Length
1 – 2	Favoured SID 1	M	2 bytes
…	Favoured SID 2	O	…
(2N-1) – (2N)	Favoured SID N	O	2 bytes

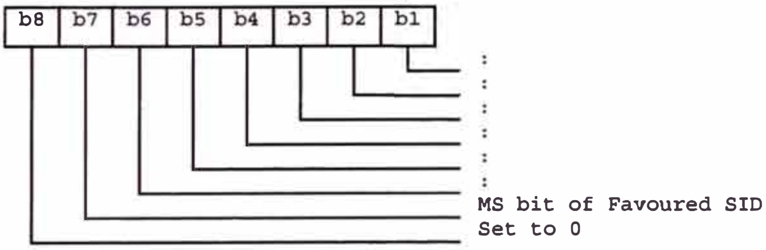
EOF (End of File) is indicated by 'FFFF'. An entry with all zeros is considered filler.

The most significant bit of the Favoured SID field is not used and it is set to 0.

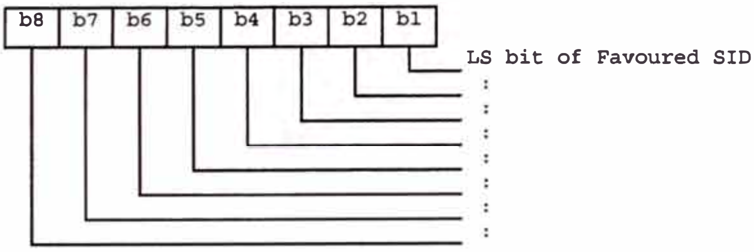
Coding of the Favoured SID field (2-byte coding)

The default value in the first two bytes shall be 'FFFF'.

Byte 1:



Byte 2:



H.1.9 EF$_{NSID}$ (Negative/Forbidden SID List)

This file contains a list of Forbidden SIDs, for use in identifying Forbidden service providers while performing network selection (intelligent roaming).

Identifier: '4F84'	Structure: transparent	Optional
File size: 2*N bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1 – 2	Forbidden SID 1	M	2 bytes
...	Forbidden SID 2	O	...
(2N-1) – (2N)	Forbidden SID N	O	2 bytes

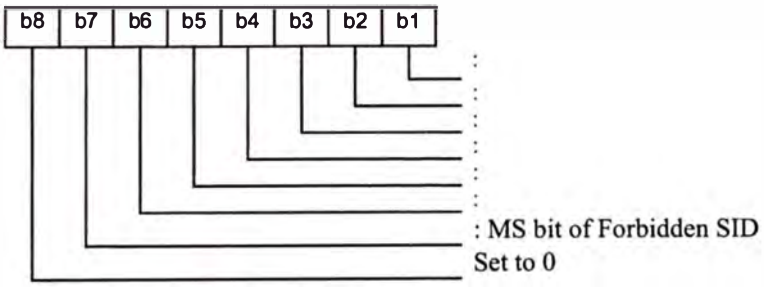
EOF (End of File) is indicated by 'FFFF.' An entry with all zeros is considered filler.

The most significant bit of the Forbidden SID field is not used and it is set to 0.

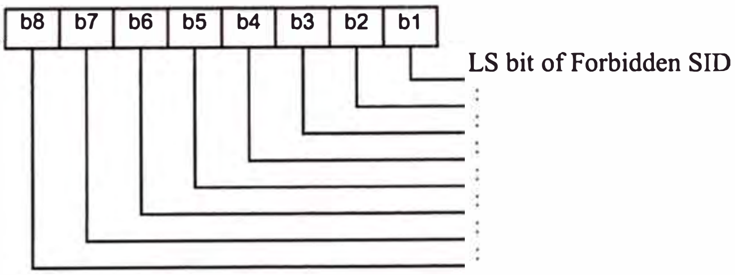
Coding of the Forbidden SID field (2-byte coding)

The default value in the first two bytes shall be 'FFFF'.

Byte 1:



Byte 2:



H.1.10 EF$_{SPL}$ (Scanning Priority List)

This file contains the Scanning Priority List. The Scanning Priority List is an array that defines the various types of systems that can be found. It also acts as a reference table, pointing to the various data structures in the SIM. This file is for backwards compatibility with GSM/AMPS mobile equipment. A Mobile Station supporting both TIA/EIA-136 and EIA/TIA-553 [41] is not expected to support this EF for network selection.

Identifier: '4F87'	Structure: transparent	Optional
File size: 27 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1	Value 1	M	1 byte
2 – 3	Pointer 1	M	2 bytes
…			
…			
25	Value 9	M	1 byte
26 – 27	Pointer 9	M	2 bytes

- The position of the pointers is fixed in this file. Highest priority level is 1, lowest priority level is 7. No two entries can have the same priority level with the exception the last two fields (Forbidden PLMNs and Negative SIDs) which both will have a value of 0. Default values are in parentheses. The values 1 or 2 shall reside in the first position (Home PLMN), and the second position (Last registered PLMN) shall contain a higher priority than position 3 (Preferred PLMNs List) and 4 (Any Other PLMNs).

Format:

Priority Value	Pointer	Reserved For
1 – 7 (2)	SIM ('6F07')	Home PLMN
1 – 7 (1)	SIM ('6F7E')	Last Registered PLMN
1 – 7 (3)	SIM ('6F30')	Preferred PLMNs List
1 – 7 (6)	0	Any Other PLMNs
1 – 7 (4)	SIM ('4F80')	Home SID
1 – 7 (5)	SIM ('4F85')	Positive SIDs List
1 – 7 (7)	0	Any Other SIDs
0	SIM ('6F7B')	Forbidden PLMNs List
0	SIM ('4F84')	Negative SIDs List

Constraints on the Priority List:

Mandatory PLMN priority order (highest to lowest):

Home PLMN or Last Registered PLMN, Preferred PLMNs, Any Other PLMNs

Mandatory SID priority order (highest to lowest):

Home SID, Positive SIs, Any Other SIDs.

H.1.11 EF$_{NETSEL}$ (Network Selection Activation Flag)

This file contains the Network Selection Activation Flag. This flag is used to enable/disable the Manual Mode and some MMI functionality within the ME.

Identifier: '4F86'		Structure: transparent	Mandatory
File size: 1 byte		Update Activity: low	
Access Conditions: READ UPDATE INVALIDATE REHABILITATE		 CHV1 CHV1 ADM ADM	
Bytes	Description	M/O	Length
1	Network Selection Activation Flag	M	1 byte

Enables / disables Manual Mode and some MMI functionality within the ME, in both AMPS and GSM modes.

Default value = 05 Hex.

Coding:

Bit 0 =0 GSM Manual Mode disabled

=1 GSM Manual Mode enabled (default)

Bit 1 =0 AMPS Manual Mode disabled (default)

=1 AMPS Manual Mode enabled

Bit 2 =0 Scanning Sequence Flags disabled

=1 Scanning Sequence Flags enabled (default)

Bit 3 =0 Disallow home only AMPS selection (default)

=1 Allow home only AMPS selection

Bits 4 through 7 are not used and set to zero.

H.1.12 EF$_{CSID}$ (Current/Last Registered SID)

This file contains the SIDsp value. The most significant bit is unused and set to 0.

Identifier: '4F8C'		Structure: transparent	Optional
File size: 2 bytes		Update Activity: low	
Access Conditions: READ UPDATE INVALIDATE REHABILITATE		 CHV1 CHV1 ADM ADM	
Bytes	Description	M/O	Length
1 -2	SIDsp	M	2 bytes

The default value shall be 'FFFF'.

H.1.13 EF$_{REG-THRESH}$ (Registration Threshold)

This file contains the NXTREGsp value, specified in EIA/TIA-553 [41]. The three most significant bits are unused and are set to 0.

Identifier: '4F8D'	Structure: transparent		Optional
File size: 3 bytes	Update Activity: low		
Access Conditions:			
READ	CHV1		
UPDATE	CHV1		
INVALIDATE	ADM		
REHABILITATE	ADM		
Bytes	Description	M/O	Length
1 – 3	NXTREGsp value	M	3 bytes

- (Default value = '00 00 00')

H.1.14 EF$_{CCCH}$ (Current Control Channel)

This file contains the Current Control Channel information related to the Last Paging Control Channel on which the AMPS phone camped on.

Identifier: '4F8E'	Structure: transparent		Optional
File size: 2 bytes	Update Activity: low		
Access Conditions:			
READ	CHV1		
UPDATE	CHV1		
INVALIDATE	ADM		
REHABILITATE	ADM		
Bytes	Description	M/O	Length
1 – 2	Current Control Channel	M	2 bytes

- (Default value = '0000')

H.1.15 EF$_{LDCC}$ (Latest DCC)

This file contains the DCC value associated with the saved Current Control Channel.

Identifier: '4F8F'	Structure: transparent		Optional
File size: 1 byte	Update Activity: low		
Access Conditions:			
READ	CHV1		
UPDATE	CHV1		
INVALIDATE	ADM		
REHABILITATE	ADM		
Bytes	Description	M/O	Length
1	DCC (Default value = '00')	M	1 byte

H.1.16 EF$_{GSM-RECON}$ (GSM Reconnect Timer)

This file specifies, in seconds, the time the ME should remain scanning the GSM-1900 spectrum, after loss of service from a GSM-1900 system, before any scanning of the AMPS spectrum is allowed.

Identifier: '4F90'	Structure: transparent	Optional
File size: 2 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1-2	GSM Reconnect Timer (Default value = '00 3C' = 60 seconds)	M	2 bytes

H.1.17 EF$_{\text{AMPS-2-GSM}}$ (AMPS to GSM Rescan Timing Table)

The EF specifies, in minutes, a series of (typically increasing) intervals for scanning the GSM-1900 spectrum, used while in-service on an AMPS network while in Dual-Mode operation. The time is measured from the end of the last GSM-1900 scan to the start of the next GSM-1900 scan. If the table is not completely filled (i.e. the end-of-table value 'FF' is found), the last filled value may be repeated indefinitely. If a value of 'F0' is encountered, the table is terminated, as are all rescans to GSM until the current AMPS system is lost.

Identifier: '4F91'	Structure: transparent	Optional
File size: 10 bytes	Update Activity: low	
Access Conditions:		
READ	CHV1	
UPDATE	ADM	
INVALIDATE	ADM	
REHABILITATE	ADM	

Bytes	Description	M/O	Length
1	First Rescan Attempt Interval (Default = '02')	M	1 byte
2	Second Rescan Attempt Interval (Default = '03')	M	1 byte
3	Third Rescan Attempt Interval (Default = '04')	M	1 byte
4	Fourth Rescan Attempt Interval (Default = '05')	M	1 byte
5	Fifth Rescan Attempt Interval (Default = '06')	M	1 byte
6	Sixth Rescan Attempt Interval (Default = 'FF')	M	1 byte
7	Seventh Rescan Attempt Interval (Default = 'FF')	M	1 byte
8	Eighth Rescan Attempt Interval (Default = 'FF')	M	1 byte
9	Ninth Rescan Attempt Interval (Default = 'FF')	M	1 byte
10	Tenth Rescan Attempt Interval (Default = 'FF')	M	1 byte

H.1.18 EF$_{\text{FC1}}$ (Feature Activation Codes)

This file contains the feature code table as specified in EIA/TIA-553 [41].

Identifier: '4F8A'	Structure: transparent		Optional
File size: 2 bytes	Update Activity: low		
Access Conditions: READ UPDATE INVALIDATE REHABILITATE	CHV1 ADM ADM ADM		
Bytes	Description	M/O	Length
1-2	Default value 'B990'.	M	2 bytes

H.1.19 EF$_{AMPS-UI}$ (AMPS USAGE INDICATORS)

This file contains usage indicators for local control and extended address method.

Identifier: 4F93	File Type: Transparent		Optional
File size: 2 bytes (minimum)	Update Activity: Low		
Access Conditions: READ UPDATE INVALIDATE REHABILITATE	CHV1 ADM ADM ADM		
Bytes	Description	M/O	Length
1	Number of Services (S)	M	1 byte
2	Services n°1 to n°8	M	1 byte

-Services:

Contents	Service n°1	Local Control Indicator (see Note 1)
	Service n°2 :	Extended Address Method indicator – included in any access attempts (see Note 2)
	Services n3°-n°8 :	RFU

- Number of Services

Contents:

This byte refers to the number of services defined in the following byte.

Coding:

This byte is coded as BCD

Services

Contents:

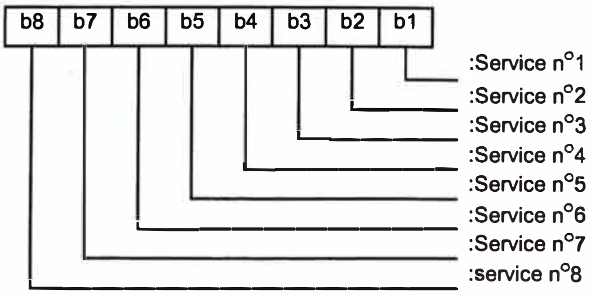
This byte describes the services

Coding:

- One bit is used to code each service
- If the bit = 0: service is not enabled
- If the bit = 1: service is enabled

- The bits for services not yet defined shall be set to RFU. For coding of RFU see subclause 9.3.

Byte 2:



NOTE 1: The Local Control Indicator is a means provided within the mobile station to enable or disable the local control option. Local Control is a mechanism that allows a cellular system to customise operation for home mobile stations, and for those roaming mobile stations whose home systems are members of a group, by sending local orders with the order field set to local control (which informs the mobile station to examine the local control field), and by sending one or both of two local control global action overhead messages.

A group of systems could be formed by participating systems agreeing to a common set of local control protocols and whose system identifications (SID) are recognised by mobile stations as a common group.

NOTE 2: The Extended Address Method indicator determines if the extended address word must be included in all access attempts.

H.2 Authentication Functionality

H.2.1 A-KEY (ANSI-41 Authentication Key)

The A-Key is only accessible to the algorithm used for Key generation. The A-Key may be programmed into the SIM directly by the service provider, or it may be programmed into the SIM through a specific over the air procedure. The A-Key is not accessible by the mobile equipment, therefore the method of storage on the SIM is not specified in this document. The SIM command A-KEY_VALIDATION is used to store the A-Key on the SIM.

H.2.2 SSD (Shared Secret Data)

The Shared Secret Data is accessible only to the Authentication and the Key Generation functions. SSD is not accessible by the mobile equipment, therefore the method of storage on the SIM is not specified in this document.

An additional Status Code is defined for SSD updating as follows:

98, 34 Error, Update SSD order sequence not respected (should be used if SSD Update commands are received out of sequence).

H.2.3 Validation and Storage of entered A-Key

The SIM only stores the A-Key after successful verification (see Common Cryptographic Algorithms, Revision C, October 27, 1998, TR45AHAG [43]). The following parameters are specified:

COMMAND	CLASS	INS	P1	P2	P3
A-KEY_VALIDATION	'A0'	'86'	'00'	'00'	'12'

Command parameters/data:

Byte(s)	Description	Length
1- 13	Authentication digits string (first digit in Most-Significant nibble of byte 1, last digit in Least-Significant nibble of Byte 12, for a total of 26 digits)	13
14	Use ME ESN = '00'	1
15-18	ESN	4

The following table specifies the coding of the status words SW1 and SW2 returned from the SIM.

SW1	SW2	Description
'90'	'00'	- Normal ending of the command
'98'	'04'	- Unsuccessful verification.

Annex I (informative): EF changes via Data Download or SIM Toolkit applications

This annex defines if changing the content of an EF by the network (e.g. by sending an SMS), or by SIM Toolkit Application (e.g. by using the SIM API), is advisable. Updating of certain EFs, "over the air" such as EF_{ACC} could result in unpredictable behaviour of the MS; these are marked "Caution" in the table below. Certain EFs are marked "No"; under no circumstances should "over the air" changes of these EFs be considered.

File identification	Description	Change advised
'2F05'	Extended Language preference	Yes
'2FE2'	ICC identification	No
'4F20'	Image data	Yes
'4Fxx'	Image Instance data Files	Yes
'6F05'	Language preference	Yes
'6F07'	IMSI	Caution (note)
'6F20'	Ciphering key Kc	No
'6F2C'	De-personalization Control Keys	Caution
'6F30'	PLMN selector	Caution
'6F31'	HPLMN search period	Caution
'6F32'	Co-operative network	Caution
'6F37'	ACM maximum value	Yes
'6F38'	SIM service table	Caution
'6F39'	Accumulated call meter	Yes
'6F3A'	Abbreviated dialling numbers	Yes
'6F3B'	Fixed dialling numbers	Yes
'6F3C'	Short messages	Yes
'6F3D'	Capability configuration parameters	Yes
'6F3E'	Group identifier level 1	Yes
'6F3F'	Group identifier level 2	Yes
'6F40'	MSISDN storage	Yes
'6F41'	PUCT	Yes
'6F42'	SMS parameters	Yes
'6F43'	SMS status	Yes
'6F44'	Last number dialled	Yes
'6F45'	CBMI	Caution
'6F46'	Service provider name	Yes
'6F47'	Short message status reports	Yes
'6F48'	CBMID	Yes
'6F49'	Service Dialling Numbers	Yes
'6F4A'	Extension 1	Yes
'6F4B'	Extension 2	Yes
'6F4C'	Extension 3	Yes
'6F4D'	Barred dialling numbers	Yes
'6F4E'	Extension 4	Yes
'6F50'	CBMIR	Yes
'6F51'	Network's indication of alerting	Caution
'6F52'	GPRS Ciphering key KcGPRS	No
'6F53'	GPRS Location Information	Caution
'6F58'	Comparison method information	
'6F60'	PLMN Selector with Access Technology	Caution
'6F61'	OPLMN Selector with Access Technology	Caution
'6F62'	HPLMN Access Technology	Caution
'6F63'	CPBCCH information	Caution
'6F64'	Investigation PLMN scan	Caution
'6F74'	BCCH information	No
'6F78'	Access control class	Caution
'6F7B'	Forbidden PLMNs	Caution
'6F7E'	Location information	No (note)
'6FAD'	Administrative data	Caution
'6FAE'	Phase identification	Caution

Continued.....

File identification	Description	Change advised
'6FB1'	Voice Group Call Service	Yes
'6FB2'	Voice Group Call Service Status	Yes
'6FB3'	Voice Broadcast Service	Yes
'6FB4'	Voice Broadcast Service Status	Yes
'6FB5'	Enhanced Multi Level Pre-emption and Priority	Yes
'6FB6'	Automatic Answer for eMLPP Service	Yes
'6FB7'	Emergency Call Codes	Caution
NOTE: If EF_{IMSI} is changed, the SIM should issue REFRESH as defined in GSM 11.14 [27] and update EF_{LOCI} accordingly.		

Annex J (informative): Change history

This annex lists all change requests approved for this document since the first phase2+ version was approved by ETSI SMG.

SMG#	SMG tdoc	SMG9 tdoc	VERS	CR	RV	PH	CAT	SUBJECT	Resulting Version
s16	709/95	154/95	4.15.0	A008		R96	1	SIM Speed Enhancement	5.0.0
s17	062/96	147/95	5.0.0	A006		R96	B	Service Dialling Numbers	5.1.0
	060/96	06/96		A009		R96	B	ASCI for VGCS and VBS	
	060/96	06/96		A010		R96	B	ASCI for eMLPP	
	059/96	204/95r		A013		R96	C	Interaction between FDNs and ADNs	
	061/96	05/96		A014		R96	D	Correction of baud rate for SIM Speed enhancement	
s18	263/96	57/96	5.1.0	A011	3	R96	B	SIM Application Toolkit protocol enhancements	5.2.0
	260/96	45/96		A016		R96	A	SIM presence detection clarification	
	261/96	54/96		A018		R96	A	Reponse codes and coding of SIM service table	
	262/96	55/96		A020		R96	A	Reference to International Standards	
s19	374/96	102/96	5.2.0	A012		R96	C	Contacting elements	5.3.0
	373/96	105/96		A023		R96	A	Clarification of clock stop timing	
	409/96	107/96		A024	1	R96	B	Emergency Call Codes (ECC)	
	374/96	108/96		A025		R96	C	Using ranges of CBMIs	
s20	580/96	206/96	5.3.0	A021		R96	B	Barred Dialling Numbers	5.4.0
	734/96	197/96		A026		R96	B	Addition of Cooperative Network List EF	
	734/96	197/96		A027		R96	B	Addition of ME Depersonalisation feature and EF	
	702/96	207/96		A031		R96	D	RFU bit taken into use in GSM 11.12	
s21	101/97	97/079	5.4.0	A032	2	R96	D	Ammendment to BDN diagrams in Annex B	5.5.0
	101/97	97/086		A033	1	R96	B	DFs for MSS/ PCS1900/other use	
	101/97	97/056		A034		R96	C	Reading of EFDCK during SIM initialisation	
	101/97	97/058		A036		R96	D	Administrative Access Conditions	
	101/97	97/059		A037		R96	B	Format of EFCNL to include fields for Corporate Personal. Code	
	101/97	97/089		A041		R96	B	Administrative Data field	
s22	356/97	183/97	5.5.0	A042		R97	B	Extended language preference	5.6.0
	356/97	163/97		A044	1	R96	A	Clarification of electrical/mechanical SIM/ME interface	
	356/97	179/97		A045		R96	D	Security procedures for 2nd level; DFs located under DF GSM	
	356/97	187/97		A047		R96	F	Number of bytes retumed after a SELECT command	
	356/97	093/97		A048		R96	D	Serivce table and "radio interface"	
	356/97	109/97		A049		R96	F	Update Access condition of EFDCK (aligns 11.11 & 02.22)	
s23	788/97	97/249	5.6.0	A046	2	R97	B	Short Message Status Reports	5.7.0
	788/97	97/243		A050		R96	F	Addition of SDN and BDN in the description of EFCCP	
	788/97	97/259		A051	1	R97	C	SIM and ME behaviour when SIM is disabled and blocked	
	788/97	97/262		A053		R96	F	Response data following an ENVELOPE command	
	788/97	97/260		A054		R96	F	Coding of EFPhase	
	788/97	97/271		A055		R97	C	Changes to Dialling Number Files and extensions	
	788/97	97/261		A056		R97	B	Network's indication of alerting in the MS	
s24	97-0886	97/365	5.7.0	A052	2	R97	b	Introduction of UCS2	5.8.0
	97-0886	97/383		A057		R97	c	MO SMS control by SIM	
At SMG #25, it was decided to create a version 6.0.0 of every specification that contained at least one release '97 work item and a version 7.0.0 of every specification that contained at least one release '98 work item.									
s25	98-0157	98p052	5.8.0	A058	2	R97	B	Addition of EFs for GPRS	6.0.0
	98-0157	98p108		A059		R97	F	Clarification regarding EFCCP records	
	98-0157	98p094		A061	1	R96	A	Clarification of removal of the SIM	
s26	98-0398	98p228	6.0.0	A062	2	R98	B	Icons - addition of EF IMG and DF GRAPHICS	7.0.0
	98-0398	98p227		A064		R98	B	Operation of ME with multiple card readers	
	98-0400	98p237		A065		R98	F	Deletion of all release 97 markers from the R98 version	
	98-0398	98p240		A066		R97	F	RP-ACK RP-ERROR for SIM data download error	
	98-0398	98p263		A069		R97	D	Allocation of file ID for IS-41	

(continued)

Change History (continued)

SMG#	SMG tdoc	SMG9 tdoc	VERS	CR	RV	PH	CAT	SUBJECT	Resulting Version
s27	98-0671	98p339	7.0.0	A071		R98	C	Enhanced image coding schemes (colour icons)	7.1.0
	98-0671			A072	1	R98	D	Addition of reference to PCS 1900	
s28	P-99-185	9-99-076	7.1.0	A073	1	R98	F	Alignment with 2^{nd} edition of ISO/IEC 7816-3 (1997)	7.2.0
	P-99-185	9-99-037		A074		R98	B	Addition of SoLSA data fields	
	P-99-185	9-99-066		A075	1	R98	B	Addition of CTS fields	
	P-99-185	9-99-095		A076	1	R98	B	Definition of a file containing the title of the main menu	
	P-99-185	9-99-072		A077		R98	C	USSD format indication in the SIM Service Table	
	P-99-185	0-99-093		A078		R98	B	Informative annex on EF changes	
	P-99-185	9-99-097		A080		R98	C	Additional GPRS field	
	P-99-188			A082		R98	D	Deletion of $(.......)$ release markers	
s29	P-99-412	9-99-163	7.2.0	A083	1	R98	C	EF IMSI changes via data download or SIM toolkit application	8.0.0
	P-99-412	9-99-180		A084		R98	F	Addition of RUN AT COMMAND to the SIM service table	
	P-99-412	9-99-208		A085		R99	C	Alignment of maximum of records in a linear fixed file in GSM	
s30	P-99-670	9-99-260	8.0.0	A089		R99	A	Correction for coding of SoLSA "Priority" field	8.1.0
	P-99-670	9-99-277		A090		R99	D	Clarification of the Ciphering Indicator disable bit in the EFad	
	P-99-670	9-99-281		A091		R99	F	Introduction of a new DF for the TIA/EIA-136 technology	
	P-99-670	9-99-294		A092	1	R99	B	Addition of EF definitions under the PCS 1900 DF	
	P-99-670	9-99-310		A093		R99	F	Clarification about "Memory Problem" error for EF_{LOCI} update	
	P-99-670	9-99-300		A094		R99	F	Execution time of SIM toolkit procedures	
	P-99-670	9-99-311		A095		R99	B	Introduction of a new DF for the TIA/EIA-95 technology	
	P-99-670	9-99-258		A097		R99	A	Clarification of Optional Status for GPRS files	
s31	P-00-137	9-00-0088	8.1.0	A098		R99	F	Clarification of interactions for CBS and the language files on	8.2.0
	P-00-137	9-00-0092		A101		R99	F	Correction to coding of ASCI EF eMLPP.	
	P-00-137	9-00-0095		A104		R99	F	Addition of coding for ASCI Efs (VGCS and VBS)	
	P-00-137	9-00-0098		A107		R99	F	Correction of the byte numbering related to EF LOCIGPRS	
	P-00-137	9-00-0133		A108		R99	F	Corrections and additions to DF-5F40	
	P-00-137	9-00-0146		A109	1	R99	F	Clarification of manual entry of the A-Key.	
	P-00-137	9-00-0151		A110		R99	D	Addition of reference to the File ID as used in the TETRA	
	P-00-137	9-00-0163		A111	1	R99	B	COMPACT Cell Selection	
	P-00-137	9-00-0155		A112		R99	B	COMPACT Cell Selection - Investigation Scan indicator for	
	P-00-139	9-00-0161		A113		R99	B	Enhancement to CCP coding (CR number incorrect in P-00-	
	P-00-139	9-00-0159		A114		R99	B	Enhancement of BDN feature (CR number incorrect in P-00-	
s32	P-00-296	9-00-0232	8.2.0	A120		R99	B	DFs for MExE	8.3.0
	P-00-296	9-00-0276		A122		R99	C	HPLM length	
	P-00-296	9-00-0275		A123		R99	A	LAI, RAI and CNL : alignment with GSM 04.08	
	P-00-296	9-00-0273		A124		R99	F	PLMN Selection Corrections regarding RFU bits	

History

Document history		
V8.2.0	May 2000	Publication
V8.3.0	August 2000	Publication

BIBLIOGRAFÍA

1. **Hernando Rábanos, José María**. “Comunicaciones Móviles GSM”. Fundación Airtel 1999.

2. **Huidobro Moya, Jose Manuel**. “Comunicaciones Móviles”. Thomson Editores Spain Paraninfo, S.A 2002.

3. **Bettstettet Christian**. “GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols and Air Interface”. IEEE Communications Surveys 1999.

4. **ETSI GSM 03.20**. “Security related network functions”.

5. **ETSI GSM 02.17** “European digital communication system – Subscriber Identity Modules (SIM) – Functional characteristics”.

6. **ETSI GSM 09.91** “Interworking aspects of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface”.

7. **ETSI GSM 11.11** “European digital telecommunications system – Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface”.

8. **ETSI GSM 11.12** “Specification of the 3 Volt Subscriber Identity Module – Mobile Equipment (SIM-ME) interface”.

9. **ETSI GSM 11.14** “Digital Cellular Telecommunication System (phase 2+): specification of SIM Application Toolkit for Subscriber Identity Module – Mobile Equipment (SIM-ME) interface”.

10. **ETSI GSM 11.17** “Digital Cellular Telecommunication System (phase 2+): SIM test specification”.

11. **ETSI GSM 03.19** “Digital Cellular Telecommunication System (phase 2+): SIM API for Java Cards”.

12. **ETSI GSM 03.48** “Digital Cellular Telecommunication System (phase 2+): Security Mechanisms for the SIM Application Toolkit”.

13. **3GPP TS 31.101** “UICC-Terminal Interface; Physical and Logical Characteristics”.

14. **Motorola**. Introducción al CDMA.

15. **Nokia**. SYSTRA

16. **Gemplus**. Cursos y Seminarios relacionados a las tarjetas SIM.

17. **SchlumbergerSema**. Simera^{TM} User's Guide.

18. **Referencias de Internet**

    http://www.gsmworld.com

    http://www.etsi.org

    http://www.3gpp.org

    http://www.nokia.com

    http://www.gemalto.com