CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

ANEXO A
GSM 11.11 Y SIM APPLICATION TOOLKIT

1. ISO/IEC 7816

El título formal del estándar ISO/IEC 7816 [1] es “Tarjetas de Circuito Integrado con contactos eléctricos”. Es el estándar internacional más ampliamente usado y referenciado para tarjetas inteligentes de contactos, cualquiera que esté interesado en tener un conocimiento técnico de ellas, debe familiarizarse con este estándar.

El estándar actualmente esta dividido en trece partes:

- Parte 1 – Características físicas
- Parte 2 – Dimensión y ubicación de los contactos
- Parte 3 – Interfaz eléctrica y protocolos de transmisión
- Parte 4 – Comandos Inter-industria para intercambio.
- Parte 5 – Inscripción de proveedores de aplicaciones
- Parte 6 – Elementos dato Inter-industria para intercambio
- Parte 7 - Comandos para SCQL
- Parte 8 – Comandos Inter-industria relacionados a seguridad
- Parte 9 – Comandos adicionales Inter-industria y atributos de seguridad
- Parte 10 – Interfaz eléctrica para tarjetas sincrónicas
- Parte 11 – Verificación personal a través de métodos biométricos
- Parte 12 – Interfaz eléctrica USB y procedimientos operativos
- Parte 15 – Aplicación de información Cifrada

1.1. ISO/IEC 7816 parte 4

Describe los mensajes o unidades básicas de intercambio con una tarjeta inteligente, las llamadas APDU's (*Application Protocol Data Units*). Los APDU's pueden ir en dos sentidos, mensajes *command* enviados hacia la tarjeta, y mensajes *response* retornados por la tarjeta. Una APDU puede ser considerada un paquete de datos que contiene una completa instrucción o una completa respuesta desde una tarjeta. Para proporcionar esta funcionalidad, las APDU's tienen una estructura bien definida.

- Command APDU

Encabezado obligatorio				**Cuerpo opcional**		
CLA	INS	P1	P2	Lc	*Data field*	Le

Figura 1-1. Estructura *Command APDU*

- CLA (1 byte): Clase de instrucción – indica la estructura y formato para una categoría de *command* y *response* APDUs.
- INS (1 byte): código de instrucción, especifica la instrucción del *command*.
- P1 (1 byte), P2 (1 byte): parámetros 1 y 2 para la instrucción.
- Lc: la longitud en bytes del *Data field.*
- *Data field*: Datos que son enviados a la tarjeta para que ejecuten la instrucción especificada en el encabezado.
- Le: especifica el número de bytes esperados en la respuesta de la tarjeta.

- Response APDU

Cuerpo opcional	***Trailer* obligatorio**	
Data Field	SW1	SW2

Figura 1-2. Estructura *Response APDU*

- *Data field* (longitud variable): Datos en forma de secuencia de bytes.
- SW1 (1 byte) y SW2 (1 byte): *Status Words* – denotan el estado de éxito o fracaso producido después de procesar el *command* en la tarjeta.

Establece un conjunto de comandos a lo ancho de todas las industrias para proporcionar acceso, seguridad y transmisión de los datos de la tarjeta. Dentro de este núcleo básico, por ejemplo, están los comandos de lectura, escritura y actualización de registros. Contiene una enmienda relacionada a la construcción de mensajes electrónicos seguros sobre estructuras de mensajes APDU.

Especifica las maneras de recuperar y acceder a los archivos, estructuras y contenido de bytes históricos que describen características operativas de la tarjeta, estructuras para aplicaciones y datos en la tarjeta, como distinguir a la interfaz cuando se procesan *commands*, una arquitectura de seguridad que define los derechos de acceso a archivos y

datos en la tarjeta, maneras y mecanismos para aplicaciones identificadas y direccionadas, métodos para mensajería segura, métodos de acceso a los algoritmos procesados por la tarjeta. El estándar No cubre la implementación interna dentro de la tarjeta y/o del mundo externo.

Es independiente de la tecnología de interfaz física. Se aplica a tarjetas accedidas por uno o mas de los siguientes métodos: contactos, acoplamiento cercano o radio frecuencia.

1.2. ISO/IEC 7816 parte 3

Describe los protocolos de transporte para las APDU's. Las estructuras de datos intercambiadas entre un CAD y la tarjeta inteligente usando el protocolo de transporte son llamadas TPDU's (*Transmission Protocol Data Units*). Una APDU puede ser transportada por el protocolo de transmisión T=0 que es orientado a byte, o por el T=1, que es un protocolo orientado a bloque (secuencia de bytes) *half duplex* asíncrono. Otros protocolos pueden embeber una APDU en su propia estructura de transporte.

1.3. ISO/IEC 7816 parte 9

Especifica los comandos inter-industria de las Tarjetas Inteligentes, tanto de contactos como sin contactos, para gestión de archivos, por ejemplo creación y borrado. Estos comandos cubren el ciclo de vida total y por consiguiente algunos comandos pueden ser usados antes de que la tarjeta sea emitida a los vendedores minoristas o después de que la tarjeta haya expirado. En un anexo se muestra cómo controlar y cargar datos (descarga segura) en la tarjeta, verificando los derechos de acceso de la entidad que carga y la protección de los datos transmitidos con mensajería segura.

2. GSM 11.11 [2]

La tarjeta SIM (Módulo de Identificación del Suscriptor) es una clase particular de tarjeta inteligente de contactos que ha tenido gran aceptación dentro del mundo de la telefonía celular. Las principales razones por las que ha tenido este gran auge son las siguientes:

- Aunque es un módulo perteneciente a la arquitectura de la red de telefonía celular, es la única parte de ella que permanece con el usuario fortaleciendo así la relación del operador con el cliente.

- Su objetivo principal es ser un componente de seguridad e identidad, el cual a través de los años se ha ido mejorando y actualmente permite identificar al usuario no sólo ante el operador de telefonía sino también ante un gran número de proveedores de servicios de valor agregado.

- Brinda la capacidad de almacenar información importante (como contactos, mensajes de texto, etc) de forma segura y portable [3], lo cual le facilita al usuario

el proceso de cambio de terminal, sin que esto implique la pérdida de dicha información o el cambio de su número telefónico.

- Es utilizada para el despliegue de servicios y aplicaciones donde la seguridad es un factor clave, ayudando a simplificar la agitada vida del ser humano. Ejemplos son actividades bancarias, m-commerce, servicios de pago y servicios basados en PKI (Public Key Infrastructure) brindando la posibilidad de mantener un gran control tanto de las llamadas y los datos salientes como entrantes.

2.1. Características físicas de la SIM

El tamaño de la tarjeta SIM es conocido como " ID-1 ". Las dimensiones físicas de la ranura para conectar la SIM en el ME, son: 15 mm de ancho y 25 mm de largo.

2.2. Contactos

Según el estándar GSM 11.11 una tarjeta SIM tiene 8 contactos (C1, C2,…, C8), pero en el teléfono móvil se deja opcional el soporte a los contactos C4 y C8. Los contactos tienen las siguientes características:

C1: es Vcc, su valor puede variar entre 4.5 V – 5.5 V, $I_{C\ Max}$ es 10 mA
C2: Reset (RST)
C3: Clock, puede tener una frecuencia de 1 – 5MHz la cual es proporcionada por el ME.
C5: Ground
C6: Vpp
C7: I / O, a un Baudrate = (frecuencia del Clock) / 372.

2.3. Estados

Mientras haya suministro de potencia, la SIM puede estar en dos estados:

- Estado "operating": cuando la SIM está ejecutando un comando. Este estado además incluye la transmisión desde y hacia el ME (Equipo Móvil).

- Estado "Idle": en cualquier otro instante en que no se ejecute un comando. La SIM debe retener todos los datos pertinentes durante este estado.

2.4. ATR (Answer To Reset)

El ATR es la información presentada por la SIM al ME en el inicio de la Card Session, la cual brinda requerimientos operacionales. La Card Session es un enlace entre la tarjeta y el mundo exterior empezando con un ATR y terminando con un subsecuente reset o una desactivación de la tarjeta.

La siguiente tabla da una explicación de los caracteres y requerimientos para el uso de ATR en GSM. La ATR consiste de a lo mucho 33 caracteres. El ME debe ser capaz de recibir por el protocolo T=0 (aunque el ME puede ser capaz de recibir usando otro protocolo distinto a T=0).

Caracter	**Contenido**	**Enivado por la SIM**	**a) evaluación por el ME b) reacción por el ME**
1. caracter inicial TS	Codificación acordada para todos los siguientes caracteres (conversión directa o inversa)	Siempre	a) Siempre b) usando la convención apropiada
2. formato del caracter T0	Caracteres Interfaz subsecuentes, número de caracteres históricos	Siempre	a) siempre b) Identica el acordado caracter subsecuente
3. caracter de interfaz (global) TA1	Parámetros para calcular el trabajo etu	Opcional	a) siempre si se presenta b) Si TA1 no es '11' o '01', el procedimiento PPS debe ser usado
4. caracter de interfaz (global) TB1	Parámetros para calcular el voltaje y corriente de programación	opcional	a) siempre si se presenta b) Si PI1 no es 0, entonces se rechaza la SIM
5. caracter de interfaz (global) TC1	Parámetros para calcular el tiempo de guarda extra solicitado por la tarjeta; el tiempo de guarda extra no es usado para enviar caracteres desde la tarjeta al ME	opcional	a) siempre si se presenta b) Si TC1 nunca es ni 0 ni 255, entonces se rechaza la SIM
6. caracter de interfaz TD1	Tipo de protocolo; indicador para la presencia de caracteres de interfaz, especificando las reglas a ser usadas para la transmisión con el tipo de protocolo dado	Siempre, si T=15 indicado en Tdi (i>1)	a) siempre si se presenta b) identificando los acordados caracteres subsecuentes
7. carácter de interfaz (especific)TA2	No usada para el protocolo T=0	Opcional	a) opcional b) --------
8. caracter de interfaz (global) TB2	Parámetro para calcular el voltaje de programación	Nunca	El valor permitido arriba de TB1 define que un voltaje de programación externo no es aplicable
9. carácter de interfaz (especifico) TC2	Parámetros para calcular el tiempo de espera de trabajo	opcional	a) siempre si se presenta b) usando el tiempo de espera de trabajo acordado
10. caracter de interfaz TDi (i>1)	Tipo de protocolo; indicador para la presencia de caracteres de interfaz, especificando las reglas a ser usadas para transmisión con el tipo de protocolo dado	opcional	a) siempre si se presenta b) identificando los acordados caracteres subsecuentes

Caracter	Contenido	Enivado por la SIM	a) evaluación por el ME b) reacción por el ME
11. caracter de interfaz TAi, TBi, TCi (i>2)	Caracteres que contienen caracteres de interfaz para otros protocolos de transmisión. Si TD(i-1) indica T=15, TAi es interpretado como carácter de interfaz global	Siempre si TD(i-1) indica T=15. Opcional de otra manera.	a) siempre b) Si T=15 es indicado en TD(i-1), TAi indica: XI indicador clock stop (b8 a b7) UI indicador de clase (b6 a b1)
12. caracter historico T1,...,TK	Contenido no se especifica en ISO/IEC	Opcional	a) opcional b) --------
13. caracter de chequeo TCK	Byte de chequeo (exclusivo -ORing)	No se envia si solo T=0 es indicado en el ATR. Si T=0 y T=15 están presentes y en todos los otros casos, TCK debe ser enviado	a) opcional b) --------

Tabla 2-1. Answer To Reset

2.5 Modelo lógico

La figura 2-1 muestra las relaciones estructurales generales que pueden existir entre archivos. Los archivos están organizados en una estructura jerárquica y son de uno de los tres tipos definidos abajo. Estos archivos pueden ser administrativos o específicos de aplicación. El sistema operativo maneja el acceso a los datos almacenados en diferentes archivos.

Los archivos están compuestos de un encabezado, el cual es internamente manejado por la SIM, y opcionalmente de un cuerpo. La información del encabezado está relacionada a la estructura y atributos del archivo y puede ser obtenida por el uso del comando GET RESPONSE o STATUS. La información es fijada durante la fase administrativa. El cuerpo contiene los datos del archivo.

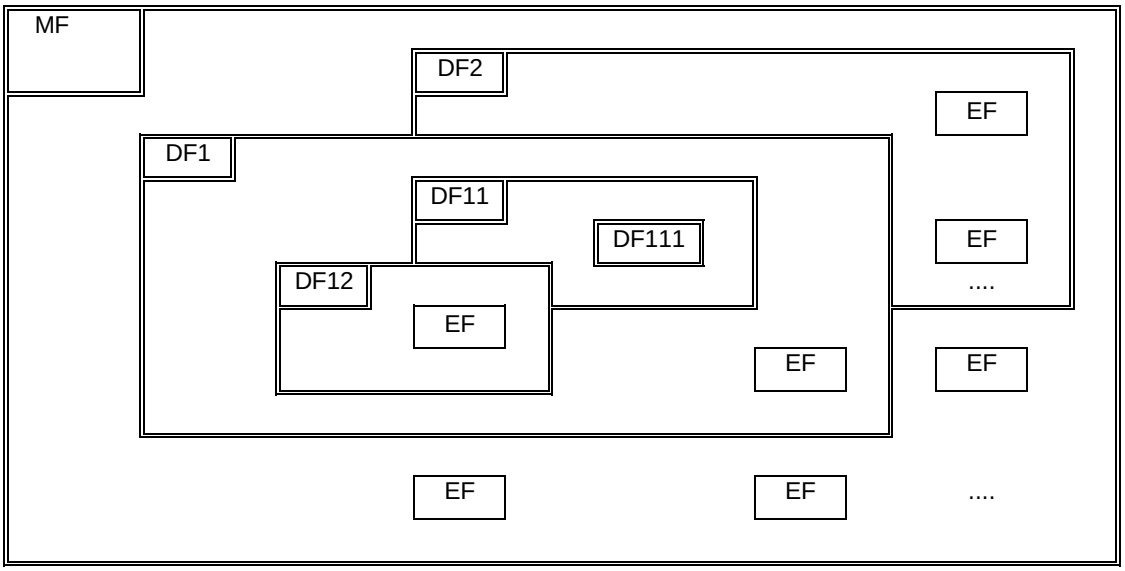

Figura 2-1. Organización de la memoria

2.5.1. Identificador de archivo

Un file ID es usado para dirigirse o identificar cada archivo específico. El file ID consiste de dos bytes los cuales serán codificados en notación Hexadecimal.

El primer byte identifica el tipo de archivo, y para GSM es:

- '3F': archivo maestro (Master File);
- '7F': archivo dedicado (Dedicated File) de 1er nivel;
- '5F': archivo dedicado de 2° nivel;
- '2F': Archivo elemental (Elementary File) bajo el archivo maestro;
- '6F': Archivo elemental bajo un archivo dedicado de 1er nivel;
- '4F': Archivo elemental bajo un archivo dedicado de 2° nivel.

Los file IDs estarán sujetos a las siguientes condiciones:

- El file ID será asignado en el tiempo de creación del archivo concerniente;
- Dos archivos que estén bajo el mismo padre no tendrán el mismo ID;
- Un hijo y algún padre, inmediato o remoto en la jerarquía, por ejemplo abuelo, nunca tendrán el mismo file ID.

De esta forma cada archivo es únicamente identificado.

2.5.2. Archivos dedicados (DF)

Un DF es una agrupación funcional de archivos que consisten de ellos mismos y todos aquellos archivos contenidos en este DF en su jerarquía padre (es decir consiste del DF y todos sus "subárboles"). Un DF "consiste" sólo de un encabezado.

Los tres primeros niveles DFs son definidos en la especificación GSM 11.11:

- DF_{GSM} los cuales contienen las aplicaciones para GSM y/o DCS 1800;
- DF_{IS41} los cuales contienen las aplicaciones para IS-41 como se especifica por ANSI T1P1;
- $DF_{TELECOM}$ los cuales contienen características de servicios de telecomunicaciones.

Todos estos tres archivos son hijos inmediatos del archivo maestro (MF) y pueden coexistir sobre una tarjeta multi-aplicación.

Los DFs de 2° nivel son definidos en la especificación debajo del DF_{GSM}.

Todos los DFs de 2° nivel son hijos inmediatos del DF_{GSM} y pueden existir sobre una tarjeta multi-aplicación.

2.5.3. Archivos elementales (EF)

Un EF está compuesto de un encabezado y un cuerpo. Las siguientes tres estructuras de un EF son usadas por GSM.

- **EF transparente**

  Un EF con una estructura transparente consiste de una secuencia de bytes. Cuando se está leyendo o actualizando, la secuencia de bytes a ser sobre actuada es referenciada por una dirección relativa (offset), la cual indica la posición de inicio (en bytes), y el número de bytes a ser leídos o actualizados. El primer byte de un EF transparente tiene la dirección relativa '00 00'. La longitud del dato total del cuerpo del EF es indicada en el encabezado del EF.

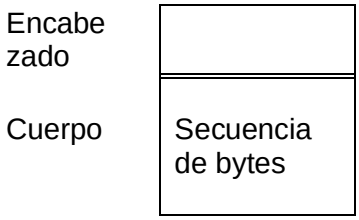

Figura 2-2. Estructura de un EF transparente

NOTA: esta estructura fue previamente referida como "binary" en GSM.

- **EF Fijado Lineal**

Un EF con estructura fijada lineal consiste de una secuencia de registros todos de la misma longitud (fijada). El primer registro es el registro número 1. La longitud de un registro así como también este valor multiplicado por el número de registros son indicados en el encabezado del EF.

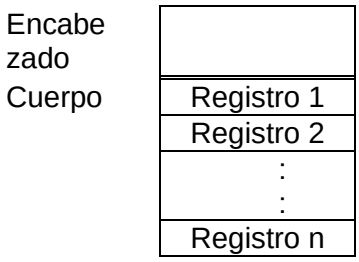

Figura 2-3. Estructura de un Archivo fijado lineal

Hay varios métodos para acceder a los registros dentro de un EF de este tipo:

- Absolutamente usando el número del registro;
- Cuando el puntero al registro no está fijado será posible ejecutar una acción sobre el primer o el último registro por usar el modo NEXT o PREVIOUS;
- Cuando el puntero del registro está fijado será posible ejecutar una acción sobre este registro, el siguiente registro (a menos que el puntero del registro esté fijado en el último registro) o el anterior registro (a menos que el puntero del registro esté fijado en el primer registro);
- Por identificar un registro usando patrones buscadores iniciando:
  - Hacia delante desde el inicio del archivo
  - Hacia delante desde el registro siguiente a uno del cual el puntero del registro es fijado (a menos de que el puntero del registro esté fijado en el último registro)
  - Hacia atrás desde el final del archivo
  - Hacia atrás desde el registro precedente a uno del cual el puntero del registro es fijado (a menos de que el puntero del registro esté fijado en el primer registro)

Si una acción siguiendo la selección de un registro es abortada, entonces el puntero del registro permanecerá fijado en el registro en el cual fue fijado anterior a la acción.

NOTA 1: no es posible, tener más de 255 registros en un archivo de este tipo, y cada registro no puede ser de más de 255 bytes.

NOTA 2: Esta estructura fue previamente referida como “formatted” en GSM

- **EF Cíclico**

Archivo cíclicos son usados para almacenar registros en orden cronológico. Cuando todos los registros han sido usados para almacenar, entonces el siguiente almacén de datos sobrescribirá la información antigua.

Un EF con una estructura cíclica consiste de un número fijado de registros con la misma longitud (fijada). En esta estructura de archivo está un enlace entre el último registro (n) y el primer registro. Cuando el puntero del registro es fijado al último registro n, entonces el siguiente registro es el registro 1. Similarmente, cuando el puntero del registro es fijado a el registro 1, entonces el registro previo es el registro n. El último registro actualizado que contiene los datos mas nuevos es el registro número 1, y los datos mas viejos son mantenidos en el registro número n.

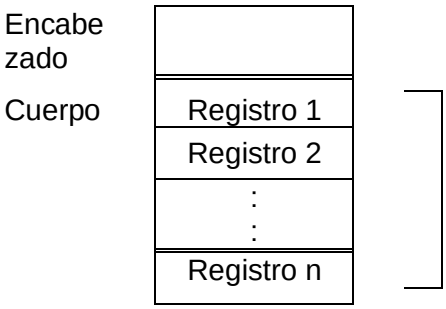

Figura 2-4. Estructura de un archivo cíclico

Para operaciones de actualización sólo registros PREVIOS serán usados. Para operaciones de lectura, los métodos para dirigirse son Next, Previous, Current y Record Number.

Después de la selección de un archivo cíclico (para cualquier operación), el puntero del registro apuntará al registro actualizado o último incrementado. Si una acción de selección siguiente a un registro es abortada, entonces el puntero del registro permanecerá fijado al registro el cual fue fijado previamente a la acción.

NOTA: no se permite, tener más de 255 registros en un archivo de este tipo, y cada registro no puede ser de mas de 255 bytes.

2.5.4 Métodos para seleccionar un archivo

Después del Answer To Reset (ATR), el archivo maestro (MF) es implícitamente seleccionado y se convierte en el directorio actual. Cada archivo puede entonces ser seleccionado mediante el uso de la función SELECT de acuerdo con las siguientes reglas.

Seleccionando un DF o el MF fija el directorio actual. Después de tal selección no queda seleccionado algún EF. Seleccionando un EF se fija el actual EF y en el actual directorio

permanece el DF o MF el cual es el padre de este EF. El actual EF es siempre un hijo del directorio actual.

Cualquier comando específico de aplicación solo será operable si este es específico al actual directorio.

Los siguientes archivos pueden ser seleccionados desde el último archivo seleccionado:

- Cualquier archivo hijo inmediato del actual directorio;
- Cualquier DF hijo inmediato del padre del actual DF;
- El padre del actual directorio;
- El actual DF;
- El MF.

Esto significa en particular que un DF será previamente seleccionado a la selección de alguno de sus EFs. Todas las selecciones son hechas usando el file ID.

La siguiente figura muestra la estructura lógica para la aplicación GSM. GSM define solo dos niveles de DFs debajo del MF.

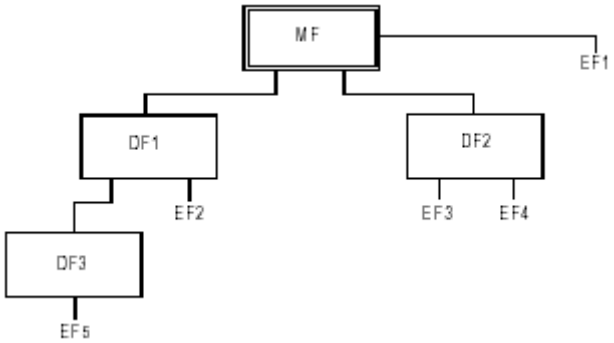

Figura 2-5. Estructura lógica

La siguiente tabla brinda las selecciones validas para GSM para la estructura lógica en la anterior figura. La reselección del último archivo seleccionado es además permitida pero no se muestra.

Ultimo archivo seleccionado	Selecciones válidas
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
EF4	MF, DF1, DF2, EF3
EF5	MF, DF1, DF3

Tabla 2-2. Selección de archivos

2.5.5 Reservación de file IDs

En adición a los identificadores usados para los archivos expresados en la especificación GSM 11.11, los siguientes file IDs son reservados para uso por GSM.

Archivos dedicados:

- uso administrativo:
  '7F 4X', '5F1X', '5F2X'

- uso operacional:
  '7F 10' ($DF_{TELECOM}$), '7F 20' (DF_{GSM}), '7F 21' ($DF_{DCS1800}$), '7F 22' (DF_{IS41}), and '7F 2X', donde X tiene un rango desde '3' a 'F'.

- reservado debajo de '7F20':
  '5F30' ($DF_{IRIDIUM}$), '5F31' ($DF_{Globalstar}$), '5F32' (DF_{ICO}), '5F33' (DF_{ACeS}), '5F3X', donde X tiene un rango desde '4' a 'F' para otro MSS.
  '5F40'($DF_{PCS-1900}$), '5F4Y' donde Y tiene un rango desde '1' a 'F' y, '5FYX' donde Y tiene un rango desde '5' a 'F'.

Archivos elementales:

- uso administrativo:
  '6F XX' en los DFs '7F 4X'; '4F XX' en los DFs '5F 1X', '5F2X'
  '6F 1X' en los DFs '7F 10', '7F 20', '7F 21';
  '4F 1X' en todos los DFs de 2° nivel
  '2F 01', '2F EX' en el MF '3F 00';

- uso operacional:
  '6F 2X', '6F 3X', '6F 4X' en '7F 10' y '7F 2X';
  '4F YX', donde Y tiene un rango desde '2' a 'F' en todos los DFs de 2° nivel.
  '2F 1X' en el MF '3F 00'.

En los anteriores archivos, el rango de X, a menos que se afirme otra cosa, va de '0' a 'F'.

2.6. Aspectos de seguridad en GSM

Los aspectos de seguridad de GSM son descritos en las referencias normativas GSM 02.09 y GSM 03.20 [4]. Las características de seguridad soportadas por la SIM habilitan, entre otras, lo siguiente: autenticación de la identidad del suscriptor a la red; confidencialidad de los datos sobre la interfaz de radio; condiciones de acceso a archivos.

- **Autenticación y procedimiento de generación de llave cifrada**

  El mecanismo de autenticación y generación de llave cifrada es invocado por la red. La red envía un número aleatorio (RAND) al MS. El ME pasa el RAND a la SIM en el command RUN GSM ALGORITHM. La SIM retorna el valor SRES y Kc al ME los

cuales son obtenidos usando algoritmos y procesos dados abajo. El ME envía el SRES a la red. La red compara este valor con el valor del SRES que es calculado por ella misma. La comparación de estos valores SRES proporciona la autenticación. El valor Kc es usado por el ME en alguna futura comunicación cifrada con la red hasta la próxima invocación de este mecanismo.

Una llave de autenticación de suscriptor Ki es usada en este procedimiento. Esta llave Ki tiene una longitud de 128 bits y es almacenada dentro de la SIM para usar en el algoritmo descrito abajo.

- **Algoritmos y procesos**

El nombre y parámetros de los algoritmos soportados por la SIM son definidos en GSM 03.20. Estos son:

- Algoritmo A3 para autenticar el MS a la red
- Algoritmo A8 para generar la llave de cifrado

Estos algoritmos pueden existir separadamente o combinados (en A38) dentro de la SIM. En cualquier caso la salida sobre la interfaz SIM/ME es de 12 bytes. Las entradas a ambos A3 y A8, o A38, son Ki (128 bits) internamente producidas en la SIM, y RAND (128 bits) a través de la interfaz SIM/ME. La salida es SRES (32 bits)/ Kc (64 bits) codificación que es definida en el command RUN GSM ALGORITHM.

- **Condiciones de acceso a archivos**

Cada archivo tiene su propia condición de acceso para cada comando. La condición de acceso relevante del último archivo seleccionado debe ser cumplida a cabalidad antes de que la acción pedida pueda tomar lugar.

Para cada archivo:

- Las condiciones de acceso para los comandos READ y SEEK son idénticas;
- Las condiciones de acceso para los comandos SELECT y STATUS son ALWays.

Las condiciones de acceso a archivos no son actualmente asignadas por GSM al MF ni a los DFs. Los niveles de condiciones de acceso son definidos en la siguiente tabla:

Nivel	**Condición de acceso**
0	ALWays
1	CHV1
2	CHV2
3	Reservado para uso futuro de GSM
4 a 14	ADM
15	NEVer

Tabla 2-3. Codificación de los niveles de condiciones de acceso

El significado de las condiciones de acceso a los archivos son las siguientes:

- **ALWays:** La acción puede ser ejecutada sin alguna restricción;
- **CHV1** (Card Holder Verification 1): La acción sólo será posible si una de las siguientes tres condiciones es cumplida a cabalidad:
  - Un correcto valor CHV1 ha sido ya presentado a la SIM durante la sesión actual.
  - El indicador CHV1 enabled/disabled está fijado a "disabled";
  - UNBLOCK CHV1 ha sido exitosamente ejecutado durante la sesión actual
- **CHV2:** La acción sólo será posible si una de las dos siguientes condiciones es cumplida a cabalidad:
  - Un correcto valor CHV2 ya ha sido presentado a la SIM durante la sesión actual.
  - UNBLOCK CHV2 ha sido exitosamente ejecutado durante la sesión actual
- **ADM:** Asignación de estos niveles y los respectivos requerimientos para su cumplimiento son la responsabilidad de la apropiada autoridad administrativa

La definición de la condición de acceso ADM no excluye a la autoridad administrativa de usar ALW, CHV1, CHV2 y NEV si se requiere.

- **NEVer:** La acción no puede ser ejecutada sobre la interfaz SIM/ME. La SIM puede ejecutar la acción internamente.

Los niveles de condiciones no son jerárquicos. Por ejemplo, la correcta presentación de CHV2 no quiere decir que acciones que requieran la presentación de CHV1 puedan ser ejecutadas. Un nivel de condición que ha sido satisfecho permanece válido hasta el final de la sesión GSM siempre y cuando el correspondiente código secreto permanezca desbloqueado, esto es después de tres consecutivos intentos equivocados, no necesariamente en la misma card session, los derechos de acceso previamente otorgados por el código secreto son perdidos inmediatamente. Un nivel de condición CHV satisfecho aplica a ambos DF_{GSM} y $DF_{TELECOM}$.

El ME determinará si el CHV2 está habilitado para usar la respuesta al comando STATUS. Si CHV2 está "not initialized" entonces comandos CHV2, por ejemplo VERIFY CHV2, no serían ejecutables.

2.7. Descripción de funciones

La siguiente tabla lista los tipos de archivos y estructuras junto con las funciones que pueden actuar sobre ellos durante una sesión GSM. Estos son indicados por un asterisco (*).

	File				
Función	**MF**	**DF**	**EF transparente**	**EF fijado lineal**	**EF cíclico**
SELECT	*	*	*	*	*
STATUS	*	*	*	*	*
READ BINARY			*		
UPDATE BINARY			*		
READ RECORD				*	*
UPDATE RECORD				*	*
SEEK				*	
INCREASE					*
INVALIDATE			*	*	*
REHABILITATE			*	*	*

Tabla 2-4. funciones para actuar sobre diferentes archivos

- **SELECT:** Esta función selecciona un archivo acorde con los métodos descritos en el modelo lógico. Después de una selección exitosa el puntero del registro en un archivo fijado lineal es indefinido. El puntero del registro en un archivo cíclico apuntará al último registro que fue actualizado o incrementado.

  Entrada: file ID.

  Salida:

  Si el archivo seleccionado está en el MF o un DF la salida es: file ID, espacio total de memoria disponible, CHV enabled/disabled indicator, CHV status y otros datos específicos GSM.

  Si el archivo seleccionado es un EF la salida es: file ID, tamaño del archivo, condiciones de acceso, invalidated/not invalidated indicator, estructura de EF y longitud de los registros en caso que sea fijado lineal o de estructura cíclica.

- **STATUS:** Esta función retorna información concerniente al directorio actual. Un EF actual no es afectado por la función STATUS. Este es además usado para dar una oportunidad a una pro-activa SIM que indique que la SIM quiere emitir un comando SAT al ME

  Entrada: nada.

Salida: file ID, espacio total de memoria disponible, CHV enabled/disabled indicator, CHV status y otros datos específicos GSM. (Idéntico al SELECT)

- **TERMINAL PROFILE:** Esta función es usada por el ME para transmitir a la SIM sus capacidades concernientes a la funcionalidad SIM Application Toolkit (SAT).

  Entrada: terminal profile.

  Salida: nada.

- **ENVELOPE:** Esta función es usada para transferir datos a la aplicación SAT en la SIM.

  Entrada: cadena de datos.

  Salida: la estructura del dato es definida en GSM 11.14.

- **FETCH:** Esta función es usada para transferir un comando SAT desde la SIM a el ME.

  Entrada: nada.

  Salida: cadena de datos conteniendo un comando SAT para el ME.

- **TERMINAL RESPONSE:** Esta función es usada para transferir desde el ME a la SIM la respuesta a un previamente retomado comando SAT.

  Entrada: cadena de datos conteniendo la respuesta.

  Salida: nada.

Como se mencionó en anteriormente, una SIM (que es una tipo particular de tarjeta inteligente) se comunica con un CAD (que se encuentra embebido en el ME) mediante las APDUs, la cuales son transportadas por el protocolo T=0.

La siguiente tabla muestra como se codifican las funciones mencionadas anteriormente.

COMANDO	**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

Tabla 2-5. Codificación de funciones

Anteriormente también se dijo que las APDUs pueden ser de dos tipos: command o response. Para ilustrar un poco más, a continuación se describe que es lo que se envía cuando el ME desea enviar un ENVELOPE APDU a la SIM (la función ENVELOPE es usada para transferir datos a una aplicación SAT en la SIM).

COMANDO	CLASS	INS	P1	P2	P3
ENVELOPE	‘A0’	‘C2’	‘00’	‘00’	lght

Parámetros/datos command: Longitud lght.

Parámetros/datos response: La estructura de los datos es definida en GSM 11.14 (ver siguiente capítulo).

CLASS = ‘A0’ es usado para aplicaciones GSM.

2.8. Contenido de los archivos elementales (EF) y parámetros accesibles en la SIM

Debido a las funciones mencionadas anteriormente, cualquier archivo puede ser leído y por tanto acceder a sus parámetros.

- **EFs del nivel MF**

  En este nivel, hay dos EF: EF_{ICCID} y el EF_{ELP}. Es decir se puede acceder a los parámetros: ICCID (Identificación ICC) y ELP (Extended Language Preference)

- **EFs del nivel de aplicación GSM**

En este nivel (DF_{GSM}) están los siguientes EF_S: EF_{LP} (Language Preference), $EFEF_{IMSI}$ (IMSI), EF_{Kc} (Ciphering key Kc), $EF_{PLMNsel}$ (PLMN selector), EF_{HPLMN} (HPLMN search period), EF_{ACMmax} (ACM maximum value), EF_{SST} (SIM service table), EF_{ACM} (Accumulated call meter), EF_{GID1} (Group Identifier Level 1), EF_{GID2} (Group Identifier Level 2), EF_{SPN} (Service Provider Name), EF_{PUCT} (Price per unit and currency table), EF_{CBMI} (Cell broadcast message identifier selection), EF_{BCCH} (Broadcast control channels), EF_{ACC} (Access control class), EF_{FPLMN} (Forbidden PLMNs), EF_{LOCI} (Location information), EF_{AD} (Administrative data), EF_{Phase} (Phase identification), EF_{VGCS} (Voice Group Call Service), EF_{VGCSS} (Voice Group Call Service Status), EF_{VBS} (Voice Broadcast Service), EF_{VBSS} (Voice Broadcast Service Status), EF_{eMLPP} (enhanced Multi Level Pre-emption and Priority), EF_{AAeM} (Automatic Answer for eMLPP Service), EF_{CBMID} (Cell Broadcast Message Identifier for Data Download), EF_{ECC} (Emergency Call Codes), EF_{CBMIR} (Cell broadcast message identifier range selection), EF_{DCK} (De-personalization Control Keys), EF_{CNL}(Co-operative Network List), EF_{NIA}(Network's Indication of Alerting), EF_{KcGPRS} (GPRS Ciphering key KcGPRS), $EF_{LOCIGPRS}$ (GPRS location information). Es decir se puede acceder a los parámetros:

- Language Preference
- IMSI
- Ciphering key Kc
- PLMN selector
- HPLMN search period
- ACM maximum value
- SIM service table
- Accumulated call meter
- Group Identifier Level 1
- Group Identifier Level 2
- Service Provider Name
- Price per unit and currency table
- Cell broadcast message identifier selection
- Broadcast control channels
- Access control class
- Forbidden PLMNs
- Location information
- Administrative data
- Phase identification
- Voice Group Call Service
- Voice Group Call Service Status
- Voice Broadcast Service
- Voice Broadcast Service Status
- enhanced Multi Level Pre-emption and Priority
- Automatic Answer for eMLPP Service
- Cell Broadcast Message Identifier for Data Download
- Emergency Call Codes
- Cell broadcast message identifier range selection
- De-personalization Control Keys
- Co-operative Network List

- Network's Indication of Alerting
- GPRS Ciphering key KcGPRS
- GPRS location information

➢ **EFs del nivel telecom**

En este nivel ($DF_{TELECOM}$) se encuentran los siguientes EFs: EF_{ADN} (Abbreviated dialling numbers), EF_{FDN} (Fixed dialling numbers), EF_{SMS} (Short messages), EF_{CCP} (Capability configuration parameters), EF_{MSISDN} (MSISDN), EF_{SMSP} (Short message service parameters) , EF_{SMSS} (SMS status) , EF_{LND} (Last number dialled), EF_{SDN} (Service Dialling Numbers), EF_{EXT1} (Extension1), EF_{EXT2} (Extension2), EF_{EXT3} (Extension3), EF_{BDN} (Barred Dialling Numbers), EF_{EXT4} (Extension4), EF_{SMSR} (Short message status reports). Es decir se puede acceder a los parámetros:

- Abbreviated dialling numbers
- Fixed dialling numbers
- Short messages
- Capability configuration parameters
- MSISDN
- Short message service parameters
- SMS status
- Last number dialled
- Service Dialling Numbers
- Extension1
- Extension2
- Extension3
- Barred Dialling Numbers
- Extension4
- Short message status reports

A continuación se describen con mayor detalle algunos archivos elementales.

EF_{ICCID} (ICC Identification)

Este EF provee un número de identificación único para la SIM.

Identifier: '2FE2'	Structure: transparent		Mandatory
File size: 10 bytes		Update activity: low	
Condiciones de acceso: READ ALWAYS UPDATE NEVER INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/ O	Length
1 to 10	Identification number	M	10 bytes

Contenido:

El contenido debe estar acorde con la recomendación del CCITT E.118, sin embargo, los operadores de red que se encuentren usando actualmente tarjetas de GSM fase 1 con un número de identificación de 20 dígitos de longitud pueden conservar esta longitud.

EF_{IMSI} (IMSI)

Este EF Contiene el IMSI (International Mobile Subscriber Identity)

Identifier: '6F07'	Structure: transparent		Mandatory
File size: 9 bytes		Update activity: low	
Condiciones de acceso: READ CHV1 UPDATE ADM INVALIDATE ADM REHABILITATE CHV1			
Bytes	Description	M/ O	Length
1	length of IMSI	M	1 byte
2 to 9	IMSI	M	8 bytes

Contenido:

El indicador de longitud hace referencia al número de bytes significativos, sin incluir la longitud de este byte, requeridos para el IMSI.

EF_{LOCI} (Location information)

Este EF contiene la siguiente información de localización: Temporary Mobile Subscriber Identity (TMSI), Location Area Information (LAI), TMSI TIME, Location update status.

Identifier: '6F7E'	Structure: transparent	Mandatory
File size: 11 bytes	Update activity: high	
Condicones de acceso: READ CHV1 UPDATE CHV1 INVALIDATE ADM REHABILITATE CHV1		

Bytes	Description	M/O	Length
1 to 4	TMSI	M	4 bytes
5 to 9	LAI	M	5 bytes
10	TMSI TIME	M	1 byte
11	Location update status	M	1 byte

3. SIM APPLICATION TOOLKIT [5]

Los operadores de las redes de telefonía celular, en el transcurso del tiempo, han mejorado sus redes y sus servicios en función de las necesidades, demandas y preferencias de los usuarios. Para un operador es muy importante tener servicios y aplicaciones que requieren un tiempo de desarrollo y despliegue muy cortos por las cuestiones de competencia existente, las cuales condicionan el mercado.

El desarrollo de los servicios y aplicaciones debe realizarse en tiempos muy cortos para que los operadores puedan mantener a sus suscriptores, además, se debe mantener flexibilidad para cambiar, modificar y mejorar estos servicios a través de su ciclo de vida.

Por tales razones, el 3GPP ha especificado el SIM Application Toolkit, el cual es un conjunto de comandos y procedimientos utilizados en las redes GSM por parte del operador y un equipo móvil que tenga soporte para dicho conjunto. SIM Application Toolkit especifica y define una serie de interfaces que garantizan la interoperabilidad entre la SIM y el equipo móvil independientemente del fabricante de uno u otro elemento.

La tecnología SIM Toolkit está también disponible en el estándar UMTS con una compatibilidad hacia atrás que ha tenido en cuenta su previa estandarización en GSM. SIM Toolkit puede ser también el habilitador de servicios de valor agregado en las tarjetas inteligentes de las redes 2.5G y 3G.

Con el desarrollo del SIM Toolkit la SIM puede ser programada con una aplicación que puede ver y oír en el teléfono móvil. Las aplicaciones pueden ser definidas totalmente por el operador y además adicionar menús que se instalan en la SIM del móvil del usuario. Esto posibilita la utilización de servicios GSM con operaciones específicas definidas en los menús del operador como por ejemplo Banca Móvil (para conectarnos a nuestra cuenta bancaria), Información bajo demanda (para conectarnos a proveedores de contenido mediante una fácil navegación a través de una lista de tipos de información).

SIM Toolkit es una útil herramienta para instalar servicios de valor agregado sobre los servicios portadores (llamar, recibir llamadas, enviar mensajes).

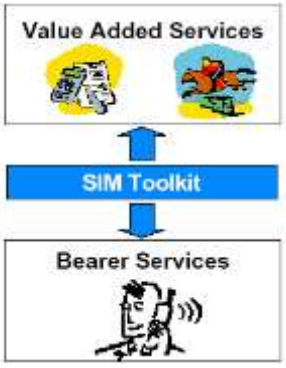

Figura 3-1. Estructura de aplicación SAT

Existen muchas razones para desplegar los servicios directamente sobre la SIM, la más importante es que la tarjeta SIM pertenece al operador, la tarjeta es definida y personalizada por el operador convirtiéndola en el único enlace entre los servicios de red y los usuarios finales. Además, con herramientas de gestión remota la tarjeta puede ser controlada remotamente en cualquier momento. El operador mantiene total control de la aplicación, él la descarga y él la elimina.

Como las tarjetas SIM son dispositivos seguros, los operadores tienen la disponibilidad para controlar y certificar las aplicaciones introducidas a y extraídas desde la SIM. así mismo el proceso de ejecución puede ser completamente seguro. Sólo la SIM puede ofrecer este nivel de seguridad.

Mecanismos de SIM Application Toolkit

SIM Application Toolkit provee una serie de mecanismos que permiten a las aplicaciones residentes en la SIM interactuar y operar con el equipo móvil. Si se soporta el SIM Application Toolkit clase “a”, se tiene la posibilidad de comunicación con tarjetas adicionales en el equipo móvil, pero generalmente este tipo de dispositivos son poco comunes sobre todo en nuestro medio.

A continuación se enumeran los mecanismos definidos por SIM Application Toolkit los que posteriormente se describen con más detalle.

- Profile Downlad
- Proactive SIM
- Data Download to SIM
- Menu Selection
- Call Control by SIM
- Event Download
- Security
- Multiple Card

- Time Expiration
- Bearer Independent Protocol

3.1. Profile Download

La instrucción Profile Download es enviada por el equipo móvil a la SIM como parte del procedimiento de inicialización. En este procedimiento el móvil lee los requerimientos de la SIM, si ese requerimiento es el procedimiento profile download, el móvil con una previa verificación, comprobación del comando y selección de canales para la comunicación, envía el comando TERMINAL PROFILE a la SIM. El perfil enviado por el móvil a la SIM especifica las capacidades que el soporta del SIM Application Toolkit.

La importancia de este procedimiento radica en que a través de este la SIM conoce que capacidades tiene el móvil que es su portador y gracias a eso la SIM puede limitar el uso de las instrucciones del SIM Application Toolkit de acuerdo al perfil obtenido. Si en el procedimiento no se recibe ningún comando por parte del móvil se asume que el móvil portador de la SIM no soporta SIM Application Toolkit.

El ME conoce que capacidades posee la SIM a través de la SIM Service Table y el EF_{PHASE}. A continuación se explica el procedimiento:

Paso	Dirección	Mensaje / Acción	Comentarios
1	USER → ME	Se enciende el ME	
...			
2	ME → USER	Solicitud del PIN	
3	USER → ME	Entrada “1111”	
...			
4	ME → SIM	VERIFY CHV1 1.1A	[CHV1 codigo: “1111”]
5	SIM → ME	Intento de VERIFY CHV no exitoso 1.1A	
...			
6	ME → USER	Nueva solicitud del PIN	
7	USER → ME	Entrada “1234”	
....			
8	ME → SIM	VERIFY CHV1 1.1B	[CHV1 codigo: “1234”]
9	SIM → ME	NORMAL ENDING OF COMMAND 1.1A	
...			
10	ME → SIM	TERMINAL PROFILE 1.1A	
11	SIM → ME	NORMAL ENDING OF COMMAND 1.1A	
...			
12	ME → SIM	SELECT EF IMSI o SELECT EF LOCI	

Tabla 3-1. Profile Download

3.2. PROACTIVE SIM

La especificación del 3GPP define que el móvil debe comunicarse con la SIM utilizando el protocolo T=0, el cual esta especificado en ISO/IEC 7816-3, bajo esta condición, el equipo móvil desempeña un rol de “maestro” iniciando la comunicación con la SIM siempre preparando y enviando comandos de forma tal que no haya la posibilidad de que la SIM envíe comandos hacia el móvil y por tanto limitando la posibilidad de la utilización de las capacidades del móvil.

Los comandos proactivos de SIM Application Toolkit proveen mecanismos con los cuales podemos permanecer dentro del protocolo T=0 pero añaden una nueva respuesta de estado SW1, esta respuesta de estado es similar en su significado a la de terminación normal (’90 00’) y se utiliza con muchos comandos para especificar una terminación normal pero además permite a la SIM decir al móvil “tengo información para enviarte”, es entonces cuando el móvil utiliza la función FETCH para encontrar la información.

Estos comandos proactivos pueden ser utilizados únicamente en móviles que soporten estas capacidades dadas las características de incompatibilidad que existe con móviles que no soporten este tipo de comandos.

Todos los comandos proactivos de SIM Application Toolkit que ejecute la SIM deben evitar la suspensión de los servicios prestados por el operador al móvil, esto puede ocurrir si por ejemplo de la actividad interna de la SIM se solicita la ejecución del comando RUN GSM ALGORITHM y este provoca un retardo que impida el acceso del operador a la SIM causando una suspensión del servicio al usuario. En la especificación del 3GPP se refiere enfáticamente al comando MORE TIME el cual debe ser usado cuantas veces sea necesario para permitir al equipo móvil acceder las funcionalidades GSM en la SIM si una aplicación SIM Toolkit a tomado demasiado tiempo para completar su ejecución.

A continuación se listan los comandos proactivos:

- **CLOSE CHANNEL** Mediante el cual se le solicita al móvil cerrar un canal de comunicaciones que se encuentra actualmente abierto.

- **DISPLAY TEXT** Mediante el cual se despliega texto o un icono en pantalla reemplazando el contenido actual de ella.

- **GET CHANNEL STATUS** Mediante el cual el móvil retorna el estado de un canal de comunicación específico.

- **GET INKEY** Mediante el cual se envía texto o iconos a la pantalla del móvil y se espera una respuesta de entrada consistente en un simple carácter, este tipo de comando es utilizado para mantener diálogos entre el usuario y la aplicación SIM, seleccionando un ítem o acción determinada en un menú de opciones.

- **GET INPUT** Este comando es básicamente igual al anterior, se diferencia en el tipo de respuesta de retorno que se entrega a la aplicación SIM

- **GET READER STATUS** Mediante este comando es posible obtener el estado de lectores adicionales que posea el móvil, pero como se mencionó anteriormente este tipo de dispositivos con más de un lector no son tan comunes en nuestro medio.

- **LANGUAGE NOTIFICATION** Mediante el cual la SIM puede informar al móvil del lenguaje utilizado en las cadenas de texto que están siendo enviadas por la aplicación de SIM Application Toolkit

- **LAUNCH BROWSER** Mediante el cual se solicita al móvil la ejecución de un browser, si es que este móvil soporta alguno, para que procese una URL determinada.

- **MORE TIME** Mediante el cual un proceso o tarea que se ejecuta en la SIM puede solicitar más tiempo de procesamiento para terminar su ejecución. Cuando un proceso es demasiado largo su ejecución puede traer problemas afectando el normal desempeño de las operaciones GSM. Este comando no afecta los demás procesos que se ejecutan y termina con un comando de OK por parte del móvil hacia la SIM y dejando el procesamiento de la tarea en background.

- **OPEN CHANNEL** Mediante el cual se solicita al móvil la apertura de un canal con los parámetros especificados en el comando.

- **PERFORM CARD APDU** Mediante el cual se solicita al móvil el envío de una APDU hacia alguna tarjeta adicional que este disponga, siendo este comando con el protocolo de comunicación entre la SIM y el móvil (generalmente T=0).

- **PLAY TONE** Mediante el cual se solicita al móvil que reproduzca tonos en alguno de los dispositivos de salida de sonido que este disponga.

- **POLL INTERVAL** Mediante el cual se realiza la negociación de cómo se enviará el comando STATUS desde le móvil a la SIM.

- **POWER OFF CARD** Mediante el cual se cierra la sesión de comunicación entre el móvil y alguna tarjeta adicional que esta posea.

- **POWER ON CARD** Mediante el cual se inicia la sesión de comunicación entre el móvil y alguna tarjeta adicional que este posea.

- **PROVIDE LOCAL INFORMATION** Mediante el cual se solicita al móvil que transfiera información local a la SIM. Al presente esta información se encuentra restringida a:

- Informacion local: el MCC (mobile country code), el MNC (mobile network code), el LAC (location area code) y el cell ID de la celda de servicio actual
- El IMEI del ME
- El Network Measurement Results y el BCCH channel list
- La fecha, hora y zona horaria actual
- La configuración actual del lenguaje del ME
- Timing Advance.

- **RECEIVE DATA** Mediante el cual se solicita al móvil el envío de información que esta llegando por algún canal de comunicaciones específico.
- **REFRESH** Este comando hace posible el reinicio de la sesión de la tarjeta mediante un reset de la tarjeta misma.
- **RUN AT COMMAND** Mediante el cual se realiza el paso de un comando AT hacia el móvil para que sea ejecutado y se entregue el resultado de este comando a la aplicación SIM.
- **SELECT ITEM** Utilizado para cuando se muestre al usuario una serie de opciones y se espera que el seleccione una.
- **SEND DATA** Mediante el cual se solicita al móvil la transmisión de datos proveídos por la SIM a través de un canal de comunicación determinado.
- **SEND DTMF** Mediante el cual se solicita al móvil el envío de tonos DTMF en una llamada establecida.
- **SEND SHORT MESSAGE** Mediante el cual se puede enviar un mensaje SMS o un comando SMS a la red. Para este comando se definen dos tipos.

  Uno es cuando un mensaje SMS se envía a la red en un mensaje SMS-SUBMIT o un mensaje SMS-COMMAND donde los datos de usuario son pasados de forma transparente.

  Otro cuando un mensaje SMS se envía a la red en un mensaje SMS-SUBMIT donde el texto necesariamente es empaquetado por el móvil.

  Cualquiera que sea el tipo, la cadena de texto resultante no debe exceder los 160 caracteres. La codificación de este texto debe ser acorde al TS23.038

- **SEND SS** Mediante el cual se envía una petición de SS (Supplementary Service) a la red.

- **SEND USSD** Mediante el cual se envía una cadena USSD (Unstructured Supplementary Service Data) a la red.

- **SET UP CALL** mediante el cual se establece una llamada telefónica.

- **SET UP EVENT LIST** Utilizado por la SIM para especificar al móvil que tipo de eventos quiere que se de detallen de su ocurrencia.

- **SET UP IDLE MODE TEXT** Utilizado para dar al móvil una cadena con el texto que debe ser desplegado por este cuando se encuentre en el modo idle.

- **SET UP MENU** Utilizado cuando la SIM brinda al móvil una lista de ítems que deben ser incorporados a la estructura de menús que este maneja.

- **TIMER MANAGEMENT** Mediante el cual se solicita al móvil el manejo del timer para administrar el tiempo como una forma de describir el comportamiento de un comando, pues la aplicación más lógica es determinar la duración de ejecución de un comando específico.

Las interacciones del equipo móvil con la SIM a través de los comandos y el manejo de excepciones y flujos alternos en caso de fallo en la ejecución de algunos comandos se encuentran a cargo de la aplicación SIM, sin embargo, la aplicación SIM necesita conocer el resultado del procesamiento de un comando y para esto se utilizan respuestas indicando el resultado de la ejecución del comando, estas respuestas se agrupan en 3 tipos principales:

OK.
Tempory problem.
Permanent problem.

Para realizar la identificación de un móvil que soporte los comandos proactivos de SIM Application Toolkit se envía, por parte del móvil, a la SIM el comando TERMINAL PROFILE durante el proceso de inicialización de esta.

3.3. DATA DOWNLOAD TO SIM

La descarga de datos a la SIM a través de SMS es un servicio que debe ser desplegado y activado por el operador de red y permite que los datos lleguen a las aplicaciones SIM directamente desde la red de telefonía a través de SMS de dos formas:

- SMS-PP (Descarga de datos con SMS point-to-point).

- Cell Broadcast Data Download.

Estos servicios como se mencionó anteriormente dependen en gran medida del operador, de que tan sofisticada es la red de telefonía móvil que posee este operador y es él quien se encarga del manejo y control de estos servicios mediante OTA.

3.4. MENU SELECTION

Como se describió en los comandos proactivos, la SIM puede brindar al móvil un conjunto de menús de opciones usando el comando proactivo SET UP MENU. Si la SIM ha enviado este comando con los diferentes ítems de los menús de opciones y luego el usuario solicita la acción en alguno de estos ítems el móvil debe informar a la SIM de tal evento y será la aplicación SIM quien se encargará del procesamiento de esta entrada mediante los procedimientos adecuados.

3.5. CALL CONTROL BY SIM

El control de llamada por la SIM es un servicio que debe ser desplegado y activado por el operador de red, mediante estos mecanismos se permite a la SIM el manejo de detalles de las llamadas que se realicen en el móvil. La especificación del 3GPP define de una forma muy detallada todos los procedimientos, mensajes y respuestas que se manejan tanto en el móvil como en la SIM para poder llevar a cabo tareas de control de llamada.

3.6. EVENT DOWNLOAD

Mediante el uso de los comandos proactivos de SIM Application Toolkit la SIM puede especificar al móvil que tipo de eventos desea que el monitoree, esto se hace a través del comando SET UP EVENT LIST, así pues, cuando un evento de los listados ocurra el móvil debe proveer esta información a la SIM intentando toda una serie de mecanismos y flujos alternos dependiendo de las condiciones del móvil y de la interfaz móvil-SIM. Los detalles se encuentran en la especificación del 3GPP.

3.7. SECURITY

Los mecanismos de seguridad para SAT se describen en el estándar GSM 02.48 [6]. Para comprender dichos mecanismos se deben tener claras las siguientes definiciones:

- **Aplicación Sending:** entidad que genera un mensaje de aplicación a ser enviado.
- **Aplicación Receiving:** esta es la entidad a la cual es destinado el mensaje de aplicación.
- **Capa de Aplicación:** capa encima de la capa de transporte sobre la cual los mensajes de aplicación son intercambiados entre las aplicaciones Sending y Receiving.

- **Capa de Transporte:** esta es la capa responsable para transportar paquetes asegurados a través de la red GSM. La capa de transporte implementa uno o más mecanismos de transporte (por ejemplo SMS o USSD).

- **Chequeo de redundancia:** cadena de bits derivada del mensaje de aplicación provista con información adicional cuyo propósito es detectar cambios accidentales del mensaje, sin el uso de alguna clave secreta.

- **Código de estado:** indicación de que un mensaje ha sido recibido (correctamente o incorrectamente, indicando la razón de la falla).

- **Contador:** mecanismo o campo de datos usado para llevar la pista de una secuencia de mensaje. Este puede estar realizado como una secuencia orientada o como una estampa de tiempo de valor derivado manteniendo un nivel de sincronización**.**

- **Encabezado de seguridad:** parte del paquete asegurado que consiste de toda la información de seguridad (por ejemplo contador, clave de identificación, indicación del nivel de seguridad, suma de chequeo o firma Digital).

- **Entidad Receiving:** esta es la entidad donde los paquetes asegurados son recibidos (por ejemplo SMS-SC, SIM, punto de entrada USSD, o un servidor dedicado SIM Toolkit) y donde los mecanismos de seguridad son utilizados. La entidad Receiving procesa los paquetes asegurados.

- **Entidad Sending:** esta es la entidad desde la cual el paquete asegurado se origina (por ejemplo SMS-SC, SIM, punto de entrada USSD, o un servidor dedicado SIM Toolkit) y donde los mecanismos de seguridad son invocados. La entidad Sending genera el paquete de seguridad a ser enviado.

- **Firma Digital:** cadena de bits derivada de alguna información secreta (por ejemplo una clave secreta), el completo mensaje de aplicación, y posible información adicional (por ejemplo parte del encabezado de seguridad). La información secreta es conocida sólo por la entidad Sending. Aunque la autenticidad de la firma Digital puede ser comprobada por la entidad Receiving, la entidad Receiving no es capaz de reproducir la firma digital sin conocimiento de la información secreta propia de la entidad Sending.

- **Identificación del emisor:** esta es la simple verificación de la identidad de la entidad Sending por la entidad Receiving comparando la identidad del emisor con una identidad almacenada a priori del emisor en la entidad Receiving.

- **Mensaje de Aplicación:** paquete de comandos o datos enviados desde la aplicación Sending a la aplicación Receiving, o viceversa, independientemente del mecanismo de transporte. Un mensaje de aplicación es transformado con respecto a una capa de transporte elegida y a un nivel de seguridad elegido en uno o más paquetes asegurados.

- **Paquete asegurado:** flujo de información por encima del cual el nivel de seguridad requerida ha sido aplicado. Un mensaje de aplicación es transformado con respecto a una capa de transporte elegida y a un nivel de seguridad elegido de uno o más paquetes asegurados.

- **Reconocimiento inseguro:** este es un Código de estado incluido en un mensaje de respuesta**.**

- **Suma de chequeo Criptográfica:** cadena de bits derivada de alguna información secreta (por ejemplo una clave secreta), parte o todo el mensaje de aplicación, y posible información adicional (por ejemplo parte del encabezado de seguridad). La clave secreta es conocida a la entidad Sending y a la entidad Receiving. La suma de chequeo criptográfica es a menudo referenciada como un código de autenticación de mensaje.

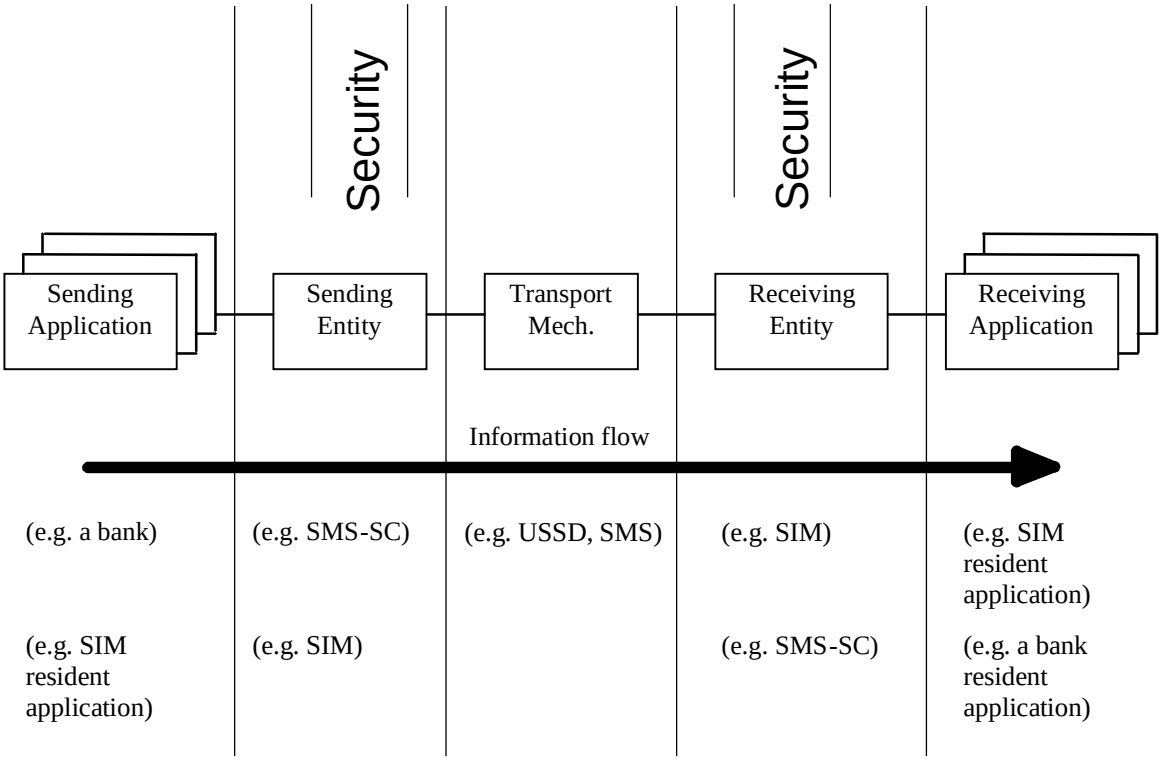

Figura 3-2. Ejemplo de una aplicación con seguridad

3.7.1. Autenticación

- **Definición**

La autenticación es la verificación de la identidad demandada de una entidad por otra entidad. Un primer nivel de autenticación es la “autenticación unilateral” la cual proporciona al receptor la prueba de la identidad del emisor. A un alto nivel esta la

“autenticación mutua”, en donde ambas entidades son provistas con pruebas de la identidad de la otra.

Para propósito de autenticación mutua las entidades Sending y/o Receiving tienen que generar e intercambiar mensajes de autenticación dedicados. Debido a la naturaleza unidireccional de los mecanismos de transporte actuales la autenticación mutua no es considerada en la especificación GSM 02.48.

- **Propósito**

El propósito de la autenticación es el de proteger la entidades Sending y Receiving y a las Aplicaciones contra el uso inautorizado. La autenticación asegura que sólo partes autorizadas pueden ejecutar acciones en la SIM, y esto evita que partes inautorizadas tengan acceso a entidades sobre parte de la red (o incluso detrás de esta) por medio de una característica SAT.

- **Requerimientos funcionales**

Para el propósito de enviar la Identificación y autenticación unilateral la entidad Sending será únicamente definida y destinada (por ejemplo una SIM GSM ya satisface este requerimiento).

La autenticación unilateral puede ser lograda por el uso de una Suma de chequeo criptográfica o Firma digital adherida al mensaje. La identificación distintiva de las entidades Receiving y Sending será enlazada a ellas para todo el tiempo de vida de estas entidades (si por alguna razón, la identidad de alguna de estas entidades es cambiada, entonces todas las otras entidades en el procedimiento de autenticación serán informadas de la nueva identidad).

3.7.2. Integridad del Mensaje

- **Definición**

La integridad del mensaje asegura que la no corrupción, accidental o intencional, del contenido de ese mensaje ha ocurrido.

- **Propósito**

El propósito de este mecanismo es el de detectar alguna corrupción del mensaje de aplicación de todo el paquete asegurado.

- **Requerimientos funcionales**

La integridad del mensaje de aplicación o todo el paquete asegurado puede ser lograda como sigue:

  - Por adherir un Chequeo de redundancia en el encabezado de seguridad para protegerlo contra corrupción accidental (el mecanismo de Chequeo de

redundancia en sí sólo protege contra corrupción accidental. En conjunción con cifrado puede ser usado para proporcionar integridad al mensaje)

- Por adherir una suma de chequeo criptográfica en el encabezado de seguridad. En ciertas circunstancias la autenticación de la entidad Sending es lograda implícitamente por la verificación de la suma de chequeo criptográfica

- Por calcular y verificar una Firma digital sobre el mensaje de aplicación a ser transferido. En este caso la autenticación de la entidad Sending es lograda implícitamente por la verificación de la firma digital.

3.7.3. Detección de Repetición e integridad de Secuencia

➢ **Definición**

La detección de Repetición es un mecanismo que le proporciona a la entidad Receiving unas formas de reconocer que se ha recibido el mismo paquete(s) asegurado previamente.

La integridad de secuencia es un mecanismo que asegura que no han ocurrido cambios, accidentales o intencionales, en la pretendida secuencia de los paquetes asegurados.

➢ **Propósito**

La detección de repetición protege a la entidad Receiving contra ataques de repetición y duplicación de paquetes asegurados. La integridad de secuencia protege la entidad Receiving contra supresión de mensajes y pérdida de paquetes asegurados.

➢ **Requerimientos funcionales**

La implementación de estos mecanismos será lograda por incluir un contador en el encabezado de seguridad. La protección del contador será lograda por incluirlo en el cálculo de la suma de chequeo (suma de chequeo criptográfica o chequeo de redundancia cifrada) o firma digital cuando sea usada.

La entidad Sending y la entidad Receiving mantendrán la sincronización para sus contadores.

3.7.4. Acuse de recibo y prueba de ejecución

➢ **Definición**

El acuse de recibo le dice a la entidad Sending que la entidad Receiving ha recibido correctamente un paquete asegurado, ha ejecutado los chequeos de seguridad necesarios y ha enviado el contenido a la aplicación Receiving.

La prueba de ejecución le dice a la aplicación Sending que la aplicación Receiving ha ejecutado una acción que la aplicación Sending inició. La prueba de ejecución no es aplicable a la capa de Transporte.

- **Propósito**

El propósito del acuse de recibo es probar la entrega de un paquete asegurado a la entidad Receiving en una forma inambigua. Esto permite la detección de los paquetes no entregados debido a errores de red, corrupción del mensaje, validación fallida etc. ser indicado a la entidad Sending usando un código de estado en la respuesta acuse de recibo.

- **Requerimientos funcionales**

El acuse de recibo debe ser pedido por la entidad Sending. El acuse de recibo es retornado desde la entidad Receiving en un reconocimiento de un paquete asegurado transmitido por la entidad Sending. El reconocimiento tomará la forma de un código de estado en un mensaje de respuesta, el cual puede ser asegurado por una suma de chequeo criptográfica o por una firma digital.

La entidad Sending enviará una indicación de acuse de recibo a la aplicación Sending sobre la entrega exitosa del mensaje de aplicación, o indicando la razón del fallo sobre el fracaso en la entrega del mensaje de aplicación.

La entidad Sending y Receiving estarán únicamente definidas y destinadas. En el caso de transporte SMS, el acuse de recibo podría ser llevado en el reconocimiento del short message como es definido en GSM 11.14 (SMS mecanismo data download).

3.7.5. Confidencialidad del mensaje

- **Definición**

La confidencialidad del mensaje asegura que el mensaje intercambiado no se hace disponible o se revela a individuos, entidades, o procesos desautorizados.

- **Propósito**

Esta función de seguridad evita que cualquier parte externa extraiga cualquier información útil de un paquete asegurado.

- **Requerimientos funcionales**

La confidencialidad del mensaje es lograda por el cifrado del mensaje. Para que el receptor use el contenido del mensaje éste tiene que ser descifrado.

Algunos de los parámetros que constituyen el encabezado de seguridad (firmas digitales, contadores y otros parámetros de seguridad) pueden ser cifrados.

3.7.6. Gestión de seguridad

Los mecanismos de seguridad aplicados a los paquetes asegurados serán indicados en el encabezado de seguridad, y esta indicación puede ser de integridad protegida para prevenirla de alteración maliciosa.

Los parámetros de seguridad (por ejemplo contadores, claves) en la entidad Receiving y Sending serán almacenados de una manera segura tal que partes inautorizadas no puedan leer, modificar o usar estos parámetros. Los procedimientos de manejo de claves (por ejemplo key update) deben ser previstos por la capa de Transporte.

3.7.6.1. Procedimientos normales

- **Mecanismos de seguridad**

Desde los requerimientos de seguridad, los siguientes subpuntos definen los mecanismos de seguridad sobre la capa de Transporte.

Algunos de los mecanismos de seguridad cumplen mas de un requerimiento de seguridad.

- **Mecanismos de autenticación**

Los mecanismos que aseguran la autenticación son:

- Suma de chequeo criptográfica (b1)
- Firma digital (b2)

El mecanismo de Suma de chequeo criptográfica es adecuado para autenticación cuando la información secreta es compartida sólo por las entidades que se comunican.

- **Mecanismos de integridad del mensaje**

Los mecanismos que aseguran la integridad del mensaje son:

- Chequeo de redundancia
- Suma de chequeo criptográfica (b1)
- Firma digital (b2).

El mecanismo de chequeo de redundancia en sí solo protege contra corrupción accidental. En conjunción con Cifrado este puede ser usado para proporcionar integridad al mensaje.

- **Detección de repetición y mecanismos de integridad de secuencia**

Los mecanismos que aseguran la detección de repetición e integridad de secuencia son:

- Contador simple

- Un contador incluido en el cálculo de la suma de chequeo criptográfico (d1)
- Un contador incluido en el cálculo de la firma digital (d2).

El mecanismo de contador simple protege contra pérdida accidental o repetición. En conjunción con cifrado este puede ser usado para proteger contra perdida maliciosa o repetición. Allí existirá un valor de contador específico el cual indica que los mecanismos de detección de repetición e integridad de secuencia están inactivos.

➢ **Mecanismos de acuse de recibo**

Los mecanismos de acuse de recibo pueden frecuentemente ser usados en conjunción con detección de repetición e integridad de secuencia.

Los mecanismos que aseguran el acuse de recibo son:

- reconocimiento inseguro;
- reconocimiento incluido en el cálculo de la suma de chequeo criptográfica (f1)
- reconocimiento incluido en el cálculo de la firma Digital (f2).

➢ **Mecanismos de confidencialidad del mensaje**

Se logra con el mecanismo de cifrado (g).

3.7.6.2. Mecanismos de seguridad y combinaciones recomendadas

➢ **Mecanismos no-criptográficos**

A continuación un número de mecanismos son listados los cuales se basan sobre mecanismos no-criptográficos. Estos mecanismos no ofrecen seguridad contra algún ataque deliverado, sólo contra detección de corrupción accidental.

- Chequeo de redundancia
- Reconocimiento inseguro;
- Contador simple.

➢ **Mecanismos criptográficos**

El encabezado de seguridad, excepto la suma de chequeo criptográfica/Firma digital, siempre será incluido en el cálculo de la suma de chequeo criptográfica/Firma digital.

- Suma de chequeo criptográfica (d1) o firma digital (d2)

Este mecanismo de seguridad va dirigido a los siguientes requerimientos de seguridad: autenticación, integridad del mensaje, detección de repetición e integridad de secuencia.

- Reconocimiento como Suma de chequeo criptográfica (f1) o firma digital (f2);

Este mecanismo de seguridad satisface el requerimiento de seguridad de acuse de recibo.

- Cifrado de los datos de aplicación y partes posibles del encabezado de seguridad (g);

El cifrado de los datos de aplicación y partes posibles del encabezado de seguridad corresponde al requerimiento de confidencialidad del mensaje.

3.7.6.3. Procedimientos excepcionales

- **Autenticación o integridad fallida**

En el caso de autenticación o integridad fallida, el mensaje recibido será descartado. Si el acuse de recibo ha sido pedido, entonces un código de estado indicando la razón por el fallo será retornado a la entidad Sending.

- **Detección de secuencia y repetición fallida**

Hay varios mecanismos con los cuales la sincronización del valor del contador puede ser mantenida, o recuperada si la sincronización es perdida. Si la sincronización no puede ser recuperada, la entidad Receiving descartará cualquier paquete asegurado con un valor del contador desincronizado. En adición, si el acuse de recibo ha sido pedido, entonces un código de estado indicando la razón por el fallo será retornado a la entidad Sending**.**

- **Acuse de recibo fallido**

La entidad Sending informará a la aplicación Sending del fallo en la entrega del mensaje de aplicación, indicando la razón por el fallo.

3.8. Múltiple card

Este mecanismo se encuentra disponible únicamente si un ME tiene soporte para lectores y/o módulos SIM adicionales y si además manifiesta conformidad con SIM Application Toolkit clase “a”. Un ME que manifiesta conformidad con SIM Application Toolkit clase “a” esta obligado a implementar los siguientes comandos proactivos:

- GET READER STATUS
- PERFORM CARD APDU
- POWER ON CARD
- POWER OFF CARD

REFERENCIAS BIBLIOGRÁFICAS

[1] Estándar ISO 7816, http://www.ttfn.net/techno/smartcards/iso7816_4.html

[2] Estándar GSM 11.11 ó 3GPP TS 11.11: Descripción de la interfaz SIM-ME [doc]. Disponible en http://www.3gpp.org/ftp/Specs/html-info/1111.htm

[3] ETSI (European Telecommunications Standardization Institute). http://www.etsi.org

[4] (Especificación Técnica) GSM 03.20 (igual a 3GPP TS 43.020): Funciones de red relacionadas a seguridad. Disponible en http://www.3gpp.org/ftp/Specs/html-info/43020.htm

[5] (Especificación Técnica) 3GPP 11.14. SIM Application Toolkit [doc]. Disponible en http://www.3gpp.org/ftp/Specs/html-info/1114.htm

[6] GSM 02.48 Disponible en http://www.3gpp.org/ftp/Specs/html-info/0248.htm

GLOSARIO

3GPP 3rd Generation Partnership Project

A
ADM: Administrator
APDU: Application Protocol Data Unit
APPLET Aplicación para Tarjetas Inteligentes.
ATR Answer To Reset

C
CAD Card Acceptance Device
CARD OS Sistema operativo de tarjeta
CDSA Common Data Security Architecture
CHV1 Card Holder Verification 1, tambien es llamado PIN
CID Cell ID
CPU Central Process Unit

D
DES Data Encryption Standard
DF Dedicated File
DTMF Dual Tone Multi-Frequency

E
EF Elementary File
ELP Extended Language Preference
ETSI European Telecommunications Standard Institute

G
GSM Global System for Mobile Communications

I
IMEI International Mobile Equipment Identifier
IMSI International Mobile Subscriber Identity
ISO International Standard Organization

M
MCC Mobile Country Code
ME Mobile Equipment
MF Master File
MS Mobile Station

O
OTA Over the Air

P

PIN	Personal Identification Number
PKCS#11	Cryptographic Token Interface Standard # 11
PKI	Public Key Infrastructure
R	
RSA	(algoritmo Rivest-Shamir-Adleman
S	
SAT	SIM Application Toolkit
SIM	Subscriber Identity Module
SMS	Short Message Service
SMS-PP	Short Message Service Point to Point
Smart Card	Tarjeta inteligente
SS	Suplementary Service
SW	Status Word
T	
TA	Time Advance
TPDU	Transport Protocol Data Unit
TS	Technical Specification
U	
USIM	Universal Subscriber Identity Module
USSD	Unstructured Supplementary Service Data