ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

GLOSARIO

3GPP	Third Generation Partnership project
AID	Application Identifier
ADN	Abbreviated Dialling Number
API	Application Programmer Interface
S@T	Sim Application Toolkit
ASN.1	Abstract Syntax Notation.1
AuC	Authentication Centre, for authentication of mobile subscribers
BOA	Batch Order Assistant
BPM	Business Process Management
BOM	Trust Batch Order management
CCA	Customer Care Assistant
CDR	Charging Data Record
CRM	Customer Relationship Management
CSD	Circuited Switched Data
DBMS	Data Base Management System
DM	Device Management
DP	Delivery Platform
DPBF	DP Basic Framework
DTD	Document Type Definition
EAI	Enterprise Application Integration, a framework for integration
EDR	Event Data Records
EIS	Enterprise Information Services
EJB	Enterprise JavaBeans
ERP	Enterprise Resource Planning

ETSI European Telecommunications Standard institute

FDN Fixed Dialling Number

CAPíTULO I

1.1 INTRODUCCIÓN

El manejo de terminales y tarjetas SIM (*Subscriber Identity Module*) a través de una plataforma de aprovisionamiento asegura el correcto despliegue de servicios de datos y aplicaciones. Ayuda a maximizar la adopción de servicios, así como también reduce el costo de lanzamiento y operación de los mismos, ya que utiliza canales de comunicación como el SMS, SS7 o GPRS. Se basa en los estándares de la norma GSM 03.40 [1] y 03.48 [2].

Con una plataforma de aprovisionamiento, el operador podrá realizar servicios de activación, actualización de aplicaciones SIM TOOL KIT, descarga de *Applets*, actualización de parámetros y archivos GSM, entre otros servicios. Junto con las aplicaciones SIM *Tool Kit*, las plataformas OTA (*Over The Air*) son el corazón del grupo de nuevos servicios de valor agregado alrededor de las tarjetas

[1] Realización técnica del servicio de SMS, Doc. No. MPM05:0037, 2006, Smartrust

[2] 3GPP TS 23.048: Mecanismos de seguridad para aplicaciones Toolkit de tarjetas (U) SIM.

SIM. De hecho la tarjeta SIM en conjunto con la aplicación de detección automática de terminal, provee al operador una pieza de información relevante con respecto al tipo de terminal que el usuario se encuentra utilizando.

Ésta plataforma es clave para el despliegue e instalación de aplicaciones, servicios y configuraciones de manera remota. Proporciones las bases para la implementación de aplicaciones y servicios de Valor Agregado, tales como banca móvil, recargas prepago, comercio móvil, etc. Nuevos e innovadores servicios pueden ser propuestos a los usuarios finales dependiendo de las capacidades del terminal y aprovechando al máximo el ciclo de vida de las tarjetas SIM y la inversión realizada en las mismas sin tener que pasar a través de configuraciones complejas.

Este sistema de administración de configuración remota reduce los costos de atención y servicio al cliente, generados por la complejidad cada vez mayor de los servicios proporcionados por los Terminales y Tarjetas SIM, de esta manera se realiza un aprovisionamiento de las configuraciones y aplicaciones a los subscriptores incrementando la satisfacción para el cliente ya que los servicios y aplicaciones son rápidamente configurados con un mínimo de interacción del usuario.

La solución óptima para la demanda de servicios de valor agregado a través de interfaz aire es la implementación de una plataforma OTA dentro de una red celular, mediante la cual se puedan gestionar tanto equipos terminales como

tarjetas SIM, activando menús dinámicos o realizando descarga de aplicaciones dentro de la red inalámbrica.

Desde el punto de vista del usuario, en concepto OTA es el hecho de encontrar una aplicación interesante en la Web e iniciar su descarga sobre la red inalámbrica de manera totalmente transparente. Sin embargo, existen algunos elementos participantes dentro de este tipo de procesos tales como el tipo de terminal del usuario, el tipo de red, el servidor de descarga y el centro de proveedores de servicios a partir del cual se realizarán las descargas.

De hecho en la vida real, OTA no es un proceso simple, un aprovisionamiento generalmente abarca publicación y administración de contenidos, control de acceso, instalación y actualizaciones de aplicaciones, control de la utilización del contenido y las aplicaciones para propósitos de facturación.

Dependiendo de la implementación, la entrega de información OTA puede ser inicializado, a partir de una acción, tales como una llamada del usuario al centro de atención al cliente u otro servicio al que se pueda acceder vía telefónica. También el proceso de conexión y descarga de aplicaciones mediante OTA puede ser realizado automáticamente.

Para aprovisionar los parámetros en un equipo terminal mediante OTA, el equipo terminal necesita tener un cliente de aprovisionamiento capaz de recibir, procesar y configurar los parámetros.

En general, el término OTA implica el uso de mecanismos inalámbricos para enviar datos de aprovisionamiento o paquetes de actualización para *firmware* o *software* a un equipo terminal y en el caso de las tarjetas SIM implica el aprovisionamiento de nuevas aplicaciones que pueden encontrarse en modo ocultas dentro de las tarjetas.

Esto se lo realiza de manera que el usuario no tenga la necesidad de acercarse a algún centro de atención al cliente para tener su equipo terminal aprovisionado o cargado con nuevo *firmware* o *software*. Ya que en el caso de que la red inalámbrica no posea la plataforma OTA, el usuario deberá acercarse a un centro de atención al cliente, conectar el equipo al computador a través del cable y cambiar los parámetros o actualizaciones de *software* etc.

Este tipo de soluciones han sido implementadas en las operadoras más representativas a nivel mundial, como se indica en la figura 1.1

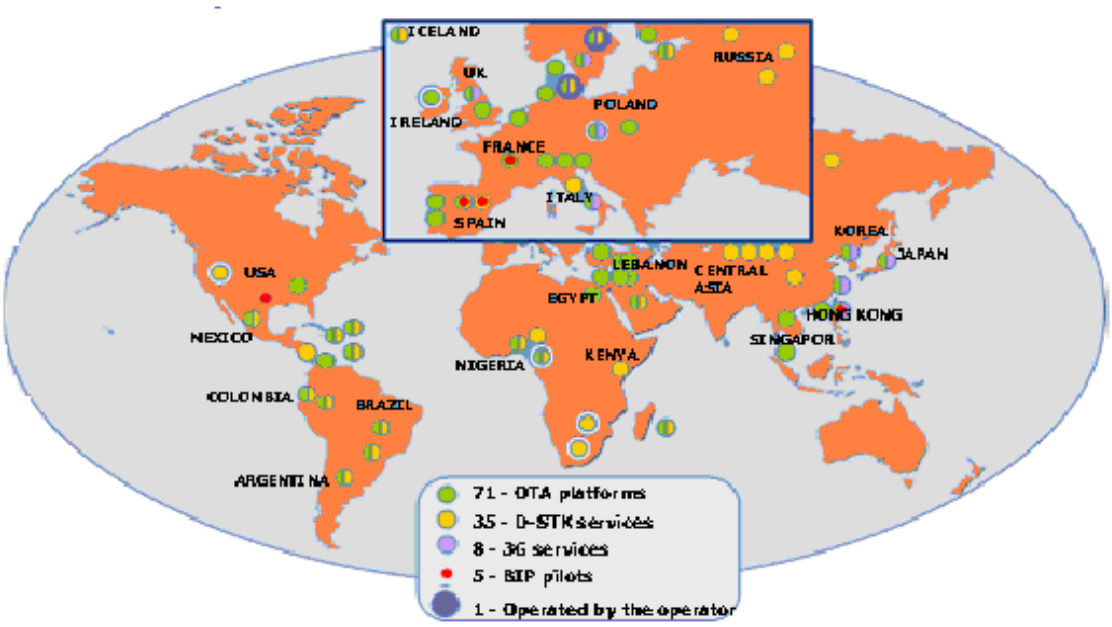


Figura 1.1 Soluciones OTA implementadas a nivel mundial

Debido al rápido crecimiento de las redes móviles, dentro de la región también se han realizado implementaciones de esta solución en más de 22 operadoras, tal como se indica en la figura 1.2:

Figura 1.2 Soluciones OTA implementadas a nivel mundial

1.2 Justificación E Importancia

La implementación de una plataforma que permita adicionar servicios de valor agregado, actualización de aplicaciones, descarga de *Applet*s entre otros a los terminales y tarjetas SIM de una manera transparente, rápida y fácil para los usuarios, implica sobre todo, su puesta en marcha, el desarrollo y avance tecnológico de la red celular, con un servicio confiable y de calidad para brindar servicios de valor agregado a todos los subscriptores.

La plataforma OTA proporciona servicios de gestión remota de las tarjetas SIM y terminales GSM. Específicamente realiza operaciones remotas de ficheros y aplicaciones, es decir, permite realizar la activación y carga de nuevos servicios y/o aplicaciones en las tarjetas SIM de los abonados, así como configuración de servicios en los terminales GSM en base a la capacidad de éstos.

OTA es la base para la mayoría de soluciones o aplicaciones de servicios de valor agregado basados en SIM, puesto que, a través de ésta plataforma se realizan las actualizaciones del cliente de las aplicaciones.

La gestión remota se la puede realizar a través de varios canales de comunicación con la red: SMSC (Short Message Service Center), señalización SS7, canales de datos GPRS y/o UMTS.

Inicialmente el diseño contempla la integración vía la plataforma SMSC, sin embargo cuando existe un gran número de abonados GSM que serán servidos o gestionados por la plataforma OTA y debido al alto costo de licencias de la plataforma SMSC, se deberá realizar un análisis costo-beneficio de la integración de OTA a través de SS7 o canales de datos.

Es importante considerar que en el perfil eléctrico de las tarjetas SIM del operador pueden definir servicios o aplicaciones ocultas, las cuales posteriormente podrán ser activadas únicamente a través de la plataforma OTA.

1.3 Consideraciones

Este proyecto considera lo siguiente:

a) La solución deberá garantizar un funcionamiento continuo con una confiabilidad del 99%.

b) Los accesos requeridos a la plataforma deben ser bien por una consola propia o vía comunicación serial. También deben permitir acceso remoto sobre una red IP.

c) La solución deberá tener seguridad de acceso, mediante usuarios y claves. Los perfiles deben ser configurables con diferentes niveles de acceso.

d) Deberá proveer interfaces de usuario y de administración gráficas tipo Web (GUI´s) para realizar configuraciones del sistema, actividades de operación y mantenimiento, gestión de servicio al cliente, y generación de reportes y estadísticas.

e) La solución deberá contar con herramientas (*hardware* y *software*) para respaldar la información, especialmente de las configuraciones y bases de datos; y con funciones de configuración de respaldos automáticos y administración de éstos.

f) La solución deberá permitir supervisión a través de un sistema de gestión.

g) La solución deberá permitir total integración y compatibilidad con otras plataformas o aplicaciones de servicios basadas en tarjetas SIM de cualquier proveedor, como por ejemplo: *Gateways* de Navegación, Respaldo de Agenda, Servicios basados en localización, etc.

CAPíTULO II

MARCO TEÓRICO

2.1 Tecnología De La Plataforma Ota

Esta plataforma permite al operador gestionar los contenidos de la tarjeta SIM de cada uno de sus suscriptores de manera remota y segura, basada en estándares de la norma GSM 03.40 [1] y 03.48 [2].

Con la plataforma el operador podrá realizar servicios de activación, actualización de aplicaciones STK (SIM Tool Kit), descarga de Applets,

[1] Realización técnica del servicio de SMS, Doc. No. MPM05:0037, 2006, Smartrust

[2] 3GPP TS 23.048: Mecanismos de seguridad para aplicaciones Toolkit de tarjetas (U) SIM.

actualización de parámetros y archivos GSM, entre otros servicios. Junto con las aplicaciones SIM TOOL KIT en lo que se refiere a tarjetas SIM.

Con respecto a terminales, la plataforma OTA permite a las operadoras configurar los parámetros de las terminales móviles tales como WAP, MMS y GPRS a través del envío de una SMS a las mismas, luego de la recepción de forma automática del IMEI (identificador de la marca y modelo del terminal) enviado por un Applet en la tarjeta SIM.

Hoy en día, la gran diversidad de los Terminales y de sus respectivas funcionalidades, vuelve más difícil la implementación de estrategias de mercadeo de los servicios avanzados de datos enfocadas y personalizadas, e inclusive la difusión masiva de dichos servicios.

La implementación de esta solución resulta en una serie de ventajas y beneficios para el Operador dentro de los cuales encontramos:

- Reducción de costos
- Optimización de recursos de red
- Preservación del ARPU de datos

- Incremento del ARPU de datos
- Reducción del CHURN
- Mejora de la Atención a los Clientes

El ARPU (acrónimo de Average Revenue Per User, ingresos medios por usuario) es la media o promedio de ingresos por usuario que obtiene, en un periodo de tiempo, una compañía de servicios con amplia base de usuarios. Se calcula dividiendo el total de ingresos obtenidos en el periodo de tiempo, por el total de usuarios activos de la empresa.

Pueden calcularse ARPU para diferentes periodos de tiempo y/o diferentes segmentos de mercado de la empresa, por ejemplo: ARPU prepago mensual, ARPU contrato empresa semanal.

Puede aplicarse a cualquier empresa de servicios, pero es particularmente usada en el sector de las telecomunicaciones, fundamentalmente en la telefonía móvil, puesto que ayuda a valorar la empresa teniendo en cuenta no sólo su número de usuarios totales, sino también la "calidad" de éstos: si aportan dinero a la compañía o no, y en qué cantidad lo hacen. Tengamos en cuenta que es común que las empresas de telefonía móvil tengan gran cantidad de usuarios que apenas aportan ingresos, puesto que sólo emplean sus teléfonos para recibir llamadas. Así, un ARPU alto indica gran cantidad de usuarios que realizan gasto, y viceversa.

CHURN determina el nivel de retención de clientes que el negocio puede soportar. Es la medida del número de usuarios que se mueven dentro o fuera de un número total de clientes en un periodo de tiempo específico.

La plataforma ofrece las siguientes características para la administración de los parámetros de los terminales móviles:

a) Servicio Automático de aprovisionamiento Over□The□Air de los parámetros de las Terminales Móviles.

b) Módulo de generación de Campañas de actualizaciones masivas de parámetros en los Terminales Móviles.

c) Aprovisionamiento remoto de parámetros tales como: WAP, MMS, SYNCML, e□Mail client, etc.

d) Soporte de los protocolos de actualización de Terminales Móviles más utilizados en la industria: Nokia Smart Messaging, Over The Air Settings, OpenWave, etc.

Todos los anteriores servicios pueden ser desplegados gracias a la arquitectura modular, integrada y escalable de la plataforma OTA. La plataforma OTA puede funcionar en equipos tales como; SUN, HP o LINUX.

La administración de terminales de un operador GSM debe tener en cuenta el aprovisionamiento de los servicios avanzados de datos (WAP, GPRS, MMS, etc.) y por lo tanto, los Terminales deben ser configurados con los parámetros propios del Operador para acceder dichos servicios.

La aplicación de la plataforma OTA permite aprovisionar remotamente vía OTA estos parámetros:

- Aprovisionamiento por Agente de *Customer Care*: En este caso, el Agente de *Customer Care* solicita, a través de su GUI (*Graphic User Interface*) la actualización de los parámetros de servicios de datos de una suscripción en particular y la plataforma OTA averigua en su base de datos el modelo de terminal usado por el suscriptor para seleccionar el protocolo y los parámetros a utilizar.

- Aprovisionamiento Automático, en donde el *Applet* que detecta el IMEI instalado en la SIM detecta un cambio de Terminal por el Suscriptor y notifica inmediatamente a la plataforma OTA, al recibir la notificación de nuevo terminal por parte del agente de la SIM, se actualiza la Base de datos y se solicita a la plataforma de aprovisionamiento de Terminales, parte de la plataforma OTA, la actualización de los parámetros, indicándole el protocolo a utilizar en función del modelo de Terminal detectado, es donde la solución de aprovisionamiento de Terminales da formato al mensaje de actualización basándose en el protocolo correspondiente y con el detalle de las características del modelo que está utilizando el suscriptor. Finalmente, la solución envía al nuevo Terminal la actualización de los parámetros, en forma automática y casi

inmediata, sin que haya sido necesaria la intervención del usuario final. En la figura 2.1, se indica el concepto:

Figura 2.1 Aprovisionamiento automático de terminales

En términos de aprovisionamiento de parámetros de terminales, la plataforma permite:

- Indicar al agente de Atención al Cliente el modelo del terminal para el cual se requiere la actualización de los parámetros para seleccionar en forma automática el protocolo y los parámetros adecuados.

- Solicitar en forma automática y transparente para el Suscriptor, la actualización de los parámetros de servicios de datos, en cuanto detecta que un suscriptor está haciendo uso de un nuevo terminal.
- Aprovisionar remotamente, vía OTA los parámetros de servicios de datos avanzados en todos los modelos de terminales que soporten alguno de los protocolos a actualización OTA del mercado.

Las ventajas que se obtienen a través del aprovisionamiento de parámetros de terminales son:

- Garantizar el acceso a todos los servicios de datos ofrecidos por el operador (incluyendo nuevos servicios como MMS) a la mayor cantidad de suscriptores, actualizando sus respectivos terminales con la mayor conveniencia para los suscriptores, es decir en forma transparente.
- Facilitar la labor de Centro de Atención a Clientes y por ende, reducir costos asociados.
- Mantener el ARPU de datos, al garantizar la continuidad del servicio mediante una actualización automática y casi inmediata de los parámetros, cuando se detecta que un suscriptor adquirió un nuevo terminal, no configurado.
- Identificar el IMEI que generó la última llamada para suspenderlo en la red y reportarlo como robado.

La plataforma OTA puede utilizar diversos canales para la actualización de tarjetas SIM, siendo el tradicional, el SMSC (usando el protocolo SMPP).

La plataforma es capaz de integrarse con la mayor parte de proveedores de SMSC en el mercado tales como: ASICION, CMG, NOKIA, SEMA, CONVERSE, etc.

Adicionalmente y con el objetivo de reducir la carga al SMSC también puede integrarse directamente a la red para configurar y/o modificar tanto terminales como tarjetas SIM con un alto nivel de efectividad y sin necesitad de utilizar la capacidad de la SMSC con mensajes no cobrables.

Todas estas alternativas están disponibles para el operador móvil dependiendo de los requerimientos de campañas OTA que se presenten.

La plataforma OTA se basa en lenguajes de programación y bases de datos más estándares del mercado tales como ORACLE y sistemas operativos como UNIX y LINUX.

Los módulos de la plataforma OTA tienen un sistema de jerarquía basado en programación orientada a objetos (OOP), con lo cual la escalabilidad y el desempeño de la plataforma se garantiza. El lenguaje generalmente utilizado es JAVA y el formato de los archivos generados es XML.

Todas las funcionalidades de la plataforma OTA son de fácil acceso y a través de una interfaz WEB, lo que permite que cualquier equipo conectado a la red pueda gestionar la plataforma a través de comunicación TCP/IP.

La plataforma maneja un completo esquema de perfiles, que permite acotar el rango de funcionalidad de cada uno de los usuarios activos en el sistema. Las interfaces WEB con las que cuenta la plataforma OTA son las siguientes:

- CUSTOMER CARE: En este caso el agente de servicio al cliente puede ejecutar un servicio OTA para satisfacer algún requerimiento del usuario final.

- SELF CARE: Aquí el usuario mismo puede ejecutar un servicio OTA determinado que altere los contenidos de su tarjeta SIM.

- ADMINISTRATOR: Con esta opción el operador puede ejecutar servicios OTA del tipo administrativos.

- CAMPAIGN MANAGER: Con esta herramienta se pueden ejecutar servicios OTA que generen mensajes cortos en forma masiva para un grupo de usuarios.

Cuando se gestiona configuraciones a terminales o tarjetas SIM de manera masiva, la plataforma OTA, al final de la misma, obtendrá un reporte de efectividad que permitirá al operador decidir, por ejemplo, que las tarjetas SIM que no hayan sido actualizadas entren a una nueva campaña (configuración de tarjetas SIM o terminales de manera masiva) para tener más tarjetas SIM o terminales actualizados

2.2 Usuarios De La Plataforma Ota

Los usuarios de la plataforma OTA pueden ser categorizados como se indica a continuación:

- Administradores
- Agentes de Servicio al Cliente
- Subscriptores

2.3 Implementación De Una Plataforma Ota

Para implementar una Plataforma de tecnología OTA se necesitan los siguientes componentes:

- Sistema de *back end* para envío de requerimientos
- Un *Gateway* OTA para procesar los requerimientos en un formato entendible para la tarjeta SIM y los Terminales.
- Un SMSC para envío de requerimientos a través de la red inalámbrica.
- Una portadora para transportar el requerimiento: actualmente se utiliza la portadora SMS
- Un terminal para recibir el requerimiento y transmitirlo hacia la tarjeta SIM.

- Una tarjeta SIM para recibir y ejecutar los requerimientos.

2.4 Sistema De Back End

El sistema de back end puede ser representado ya sea por el sistema de facturación de la operadora, un ejecutivo de atención al cliente, un proveedor de servicios, una interfaz web

El sistema de aprovisionamiento tiene que estar conectado a la red móvil (ya sea por LAN o por Internet). Los requerimientos de servicio contiene el servicio requerido (activar, desactivar, cargar, modificar…) el subscriptor, los datos para realizar el servicio. El sistema de back end entonces envía el servicio requerido hacia el Gateway OTA.

2.4.1 Gateway Ota

El *Gateway* OTA recibe los Requerimientos de Servicio que indicará la tarjeta que será modificada / actualizada / activada. De hecho, dentro del *Gateway* OTA existe una base de datos que indica para cada tarjeta, el fabricante de SIM (Schlumberger, Gemplus, DeLaRue…), el número de identificación, el IMSI y el MSISDN.

El segundo paso es dar formato al requerimiento de servicio en un mensaje que pueda ser entendido por la tarjeta SIM de destino. Para lograr esto, el Gateway OTA tiene un conjunto de librerías que contienen los formatos a utilizar para cada tipo de tarjeta SIM dependiendo del fabricante. El Gateway OTA da formato al mensaje de manera diferente en función de la tarjeta destino.

El tercer paso consiste en enviar el mensaje con el formato correspondiente al SMSC utilizando el correcto conjunto de parámetros tal como se encuentra descrito en el estándar 03.48. El Gateway OTA generará los SMS que sean necesarios para completar el Requerimiento de Servicio. En este punto el Gateway OTA también responsable por la integridad y seguridad del proceso.

2.4.2 Smsc

SMSC, que corresponde a las siglas en inglés de Short Message Service Center (central de servicio de mensajes cortos), es un elemento de la red de telefonía móvil cuya función es la de enviar/recibir mensajes SMS.

En el momento que un usuario envía un mensaje de texto (SMS) a otro usuario lo que sucede es que el terminal envía dicho mensaje a la SMSC correspondiente al operador del usuario remitente. La SMSC guarda el mensaje y lo entrega a su destinatario cuando este se encuentra en cobertura. Por lo general la SMSC, dentro de los cientos de parámetros configurables que se pueden modificar, dispone de un tiempo máximo durante el cual el mensaje es guardado, si en ese tiempo el destinatario no es localizado, el mensaje es eliminado para no causar encolamientos en la plataforma, cabe decir que también el usuario remitente puede especificar el tiempo máximo, pero siempre siendo el configurado en la SMSC el determinante.[3]

Un mensaje que consiste de un máximo de 160 caracteres alfanuméricos por página puede ser enviado desde o hacia un Terminal.

Para la transmisión y recepción de mensajes SMS, las SMSC utilizan interfaces de redes convencionales, así como algunos desarrollados específicamente para las comunicaciones sobre red móvil. Algunos de los protocolos más utilizados son los siguientes:

* SMPP (*Short message peer-to-pee*r)
    o Más extendido y no propietario.

[3] Short Message Service Center, http://es.wikipedia.org/wiki/Short_Message_Service_Center, 05/12/2008

* EMI/UCP (External *Machine Interface/Universal Computer Protocol*)
    o Protocolo propietario desarrollado por LogicaCMG.
* CIMD (*Computer Interface to Message Distribution*)
    o Propietario desarrollado por Nokia para sus SMSC Artuse.
* OIS (*Open Interface Specification*)
    o Propietario desarrollado por Sema Group (actualmente Airwide Solutions).

2.4.3 Canal SMS

La comunicación entre la tarjeta SIM y el Gateway OTA puede realizarse a través del intercambio de SMS y en este caso se lo denomina el canal SMS.

2.4.4 Terminal Móvil

El terminal móvil es un dispositivo inalámbrico electrónico que permite tener acceso a la red de telefonía celular o móvil. Su principal características es su portabilidad, que permite comunicarse desde casi cualquier lugar. Aunque su principal función es la comunicación de voz, su rápido desarrollo ha incorporado otras funciones como son cámara fotográfica, agenda, acceso a internet, bluetooth, infrarrojo e incluso GPS.

Los terminales tienen que ser phase 2 + según el estándar GSM.[4] los terminales móviles deberán tener todos los requerimientos para manejar una parte o todos los requerimientos de los estándares GSM. Con respecto a los servicios OTA, el terminal móvil deberá soportar y entender el lenguaje SIM TOOL KIT

2.4.5 Sim Tool Kit

Generalmente denominado STK, es un estándar del sistema GSM el cual habilita a la tarjeta SIM a iniciar acciones que pueden ser utilizadas para varios servicios de valor agregado.

El SIM TOOL KIT consiste en un conjunto de comandos programados en la tarjeta SIM los cuales definen como la SIM debe interactuar directamente con el mundo exterior e iniciar comandos independientemente del terminal y la red. Esto habilita a la tarjeta SIM a crear un intercambio interactivo entre la red de la aplicación y el usuario final y acceder o controlar el acceso a la red. La tarjeta SIM también envía comandos al terminal, tales como mostrar el menú al usuario.

---

[4] ETSI GSM 11.14 Sistema Celular Digital de Telecomunicaciones (fase 2+), especificación de las aplicaciones de la tarjeta SIM – Equipo móvil

SIM TOOL KIT está siendo utilizado por algunas operadoras alrededor del mundo para algunas aplicaciones, tales como BANCA MÓVIL, y browsing de contenido.

Una de las limitaciones que tuvo SIM TOOL KIT fue que una vez que se le entregaba la tarjeta SIM al usuario, se hacía muy difícil cambiar las aplicaciones y STK almacenados en la tarjeta SIM y para realizar esto, era necesario que el cliente retorne la tarjeta SIM a la operadora para que sea reemplazada por una nueva lo que representa un inconveniente económico, pero hoy en día, es posible modificar el menú STK para aplicaciones basadas en S@T (Sim Application Toolkit) de una manera rápida mediante la plataforma OTA, vía SMS.

Figura 2 2 Mecanismo de comunicación SIM ToolKit

SIM TOOL KIT se encuentra definido en el estándar GSM 11.14

2.4.6 Tarjeta SIM

Una tarjeta SIM es una tarjeta inteligente que puede proveer una autenticación segura para el usuario y es generalmente utilizada en el estándar GSM como un módulo de identificación del subscriptor. La tarjeta SIM es el componente más importante del mercado GSM ya que es el camino para los servicios de valor agregado. Las tarjetas SIM proveen de nuevos menús, números pregrabados para marcación rápida y la habilidad de enviar plantillas de SMS para preguntar a una base de datos o transacciones seguras.

La primera tarjeta SIM fue lanzada en 1985 por la operadora móvil celular alemana Netz C, la que fue simplemente una tarjeta magnética. La movilidad de la suscripción y el aumento de la seguridad a través de la remoción de la tarjeta fueron las principales ventajas de la introducción de la tarjeta. El número del teléfono y los otros datos necesarios al billing estaban relacionados a la tarjeta y no más al aparato celular.

También en 1985, algunos países europeos firmaron un acuerdo para el desarrollo del GSM y un nuevo padrón para uso de tecnología digital. En 1992, la primera red GSM fue lanzada.

En 1988 la tarjeta magnética fue sustituida por el smart card, siendo ésta la primera aplicación en smart card para comunicación móvil en el mundo.

Las especificaciones aplicables a las tarjetas SIM son:

GSM 11.11: Especificación de la interfaz SIM-ME (*Mobile equipment*)

GSM 11.14: Especificación de la tarjeta SIM *Application Toolkit* para la interfaz SIM-ME

La interface inteligente entre la tarjeta y el terminal, el nuevo nivel de seguridad a través del chequeo del PIN number (clave individual) y la autenticación en la red celular fueron las principales conquistas con la introducción del smart card.

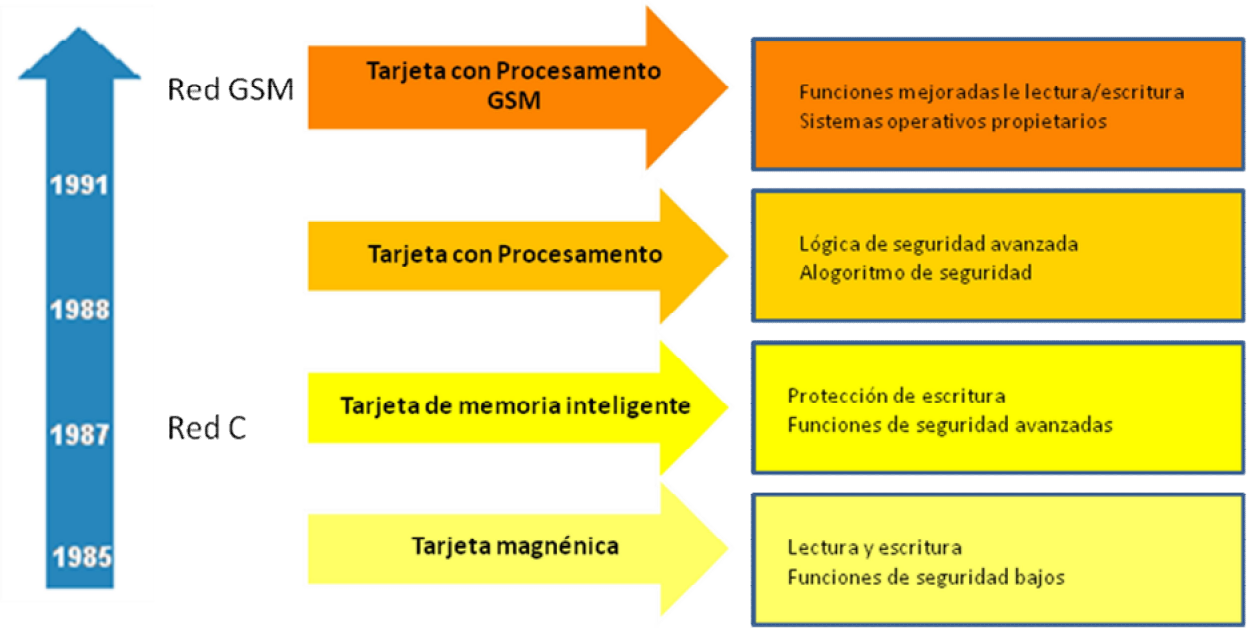


Figura 2.3 Cronología de la evolución de las tarjetas SIM

La tarjeta SIM en su versión “full size” posee 85 x 54 mm. Como los aparatos celulares se tornaron más compactos en los últimos años, el SIM Card ha sufrido una reducción en su tamaño a través del corte plug-in realizado alrededor del chip, y es utilizado en su versión plug-in en el tamaño 25 x 15 mm.

Las tarjetas SIM de bajo costo (sólo GSM 11.11) tienen poca memoria, de entre 2 a 3 kbytes según se describe en la especificación (directorio telefónico). Este espacio de almacenamiento es usado directamente por el terminal. El segmento de mercado de las tarjetas SIM de bajo costo está en constante declive.

Las tarjetas SIM con aplicaciones adicionales (GSM 11.14) están disponibles con muchas capacidades de almacenamiento diferente, siendo la mayor de 512 Mbytes. Tarjtes SIM de menor capacidad de memoria de 32 kbytes y 16 kbytes, son dominantes en zonas con redes GSM menos desarrolladas. También existen las tarjetas Large Memory SIM con capacidades del orden de 128 a 512 Mbytes de memoria EEPROM.

Con el lanzamiento de nuevas aplicaciones y servicios para los usuarios, una mayor memoria del SIM Card es requerida. De esta forma, operadoras nuevas ya están utilizando sus SIM Cards a partir de 32 Kbytes de memoria una vez que lanzan sus servicios desde el inicio con funciones de valor añadido o agregado, no se restringiendo sólo a servicios de voz y tienden a migrar rápidamente para

64 Kbytes, que ya se tornaron padrón para muchas operadoras, de modo a ampliar su oferta de servicios. En aproximadamente 2 años, debe ocurrir la migración para tarjetas de capacidad mayor.

Los sistemas operativos para tarjetas SIM son principalmente dos:

- Nativos: software propietario y específico del vendedor (correspondiendo típicamente con el segmento del mercado de bajo costo)
- Basados en Java: tienen la ventaja de ser independientes de hardware e interoperable.

Las tarjetas SIM disponibles actualmente son basados en máscaras (sistemas operativos) propietarias, o con “Virtual Machine Java” (simplemente denominados SIM Cards Java) y con “Micro-Browser implementado”, como por ejemplo el WIB Browser. Existen aun variaciones importantes como el Micro-Browser implementado sobre un SIM Card Java.

En el pasado era muy común la utilización de soluciones propietarias, lo que no refleja más la tendencia de mercado. Debido a las ventajas del Java y de los Micro-Browsers, las operadoras han adoptado estas soluciones en sus redes.

La mayor ventaja para las operadoras de telefonía móvil celular ofrecida por el Java es la interoperabilidad entre productos de diferentes proveedores, especialmente en lo que se refiere a las tarjetas SIM bien como la fácil y flexible administración, operación e implementación de nuevos servicios de valor agregado.

Las tarjetas SIM almacenan información específica de la red usada para autenticar e identificar a los suscriptores en ella, siendo la más importante el ICCID, el IMSI, la clave de autenticación (Ki) y la identificación de área local (LAI) .La tarjeta SIM también almacena otros datos específicos del operador como el número de SMSC (centro de servicio de mensajes cortos), el nombre del proveedor de servicio (SPN), los números de servicio de marcado (SDN) y las aplicaciones de servicios de valor agregado (VAS). Las correspondientes descripciones están disponibles en la especificación GSM 11.11 [6].

Un USIM (Universal Subscriber Identity Module) o Módulo de Identificación del Abonado es una aplicación para telefonía móvil UMTS que se ejecuta en una tarjeta inteligente UICC que está insertada en un teléfono móvil 3G. Almacena la información de abonado para su identificación en la red y otras informaciones como mensajes de texto. Su función y, en muchos casos, su aspecto son similares a los de una tarjeta SIM [6].

---

[5] GSM 11.11 Sistema Celular Digital de Telecomunicaciones (fase 2+), especificación de las aplicaciones de la tarjeta SIM

[6] USIM, http://es.wikipedia.org/wiki/USIM, 15/12/2008

Dentro de la tarjeta SIM existen parámetros vitales para la identificación de ésta dentro de la red, los cuales se describen brevemente a continuación:

- **ICCID**

Cada tarjeta SIM se identifica internacionalmente por su ICCID (International Circuit Card ID). Los ICCID se almacenan en las tarjetas SIM y también se graban o imprimen sobre el cuerpo de plástico de las mismas en un proceso de personalización. Se encuentra definido en la recomendación ITU-T E.118. Se encuentra compuesto por 18 dígitos más un dígito verificador calculado a través del algoritmo LUHN.

- **IMSI**

Las tarjetas SIM se identifican en sus redes móviles individuales mediante un IMSI (International Mobile Subscriber Identity, 'Identidad Internacional del Suscriptor Móvil') único. Los operadores de telefonía móvil conectan las llamadas a teléfonos móviles y se comunican con sus tarjetas SIM comercializadas usando su IMSI.

El IMSI se encuentra compuesto por tres componentes:

- *Mobile country code (MCC*
- *Mobile Network Code (MNC)*
- *Mobile Subscriber Identity Number (MSIN)*

- **MSISDN**

Es un número único identificador dentro de una red GSM o UMTS, hacen referencia a Mobile Station Integrated Services Digital Network (MSISDN), el cual hace referencia al número de suscripción RDSI del móvil, cuya longitud máxima es de 15 dígitos. El MSISDN suele ir formado por el código del país seguido, del número de abonado a la red del terminal.

- **Clave De Autenticación (Ki)**

La clave de autenticación (Ki, Authentication key) es un valor de 16 bytes usado para autenticar las tarjetas SIM en la red móvil. Cada tarjeta SIM tiene una Ki única asignada por el operador durante el proceso de personalización. La Ki también se almacena en una base de datos (conocida como HLR (Home Location Register) de la red del operador.

- **Proceso De Autenticación**

1. Cuando el teléfono se enciende envía su IMSI al operador de la red solicitando acceso y autenticación.

2. El operador de la red busca en su base de datos el IMSI y la clave de autenticación (Ki) relacionada.

3. El operador de la red genera un número aleatorio (RAND) y lo firma con la Ki de la SIM, generando así un número conocido como SERS_1 (*Signed Response* 1, 'Respuesta Firmada 1').

4. El móvil cliente de la red envía el RAND a la tarjeta SIM, que también lo firma con su Ki y envía el resultado (SRES_2) de vuelta al operador de la red.

5. El operador de la red compara su SRES_1 con el SRES_2 generado por la tarjeta SIM. Si los dos números coinciden, la SIM es autenticada y se le concede acceso a la red.

El algoritmo criptográfico usando en el estándar GSM para calcular el SRES_2 tiene un punto débil, permitiendo la extracción de la Ki de la tarjeta SIM y permitiendo elaborar duplicados (clones) de la misma.

El algoritmo de autenticación utilizado en los sistemas GSM es conocido como el algoritmo A3. La mayoría de operadores GSM utilizan una versión del algoritmo COMP128 como una implementación del algoritmo A3 [7].

El algoritmo A3 genera una respuesta de 32 bits utilizando el código de 128 bits generado por el HLR (Home Location Register) y el código de 128 bits que se encuentra en la tarjeta SIM denominado Ki (Subscriber Authentication Key). Que es una llave secreta compartida entre el terminal y el HLR.

- **Tarjetas *SIM JAVA***

La tarjeta SIM Java contempla funciones nuevas y especiales inherentes a la tecnología Java, lo que permite una mejor utilización de la memoria EEPROM de la tarjeta SIM. Algunos ejemplos pueden ser citados:

- *Garbage Collection:* después de la remoción de una aplicación (o *applet*), todos los componentes también son removidos, lo que deja a la memoria "limpia" y disponible para nuevo uso;

[7] Telecomunicaciones móviles, Marcombo, Eugenio Rey Veiga, Capítulo 19 "Seguridad en Sistemas de comunicaciones móviles"

- *Dynamic Memory Allocation:* bloques de memoria “limpia” y disponible para nuevos usos son vistas como único bloque de memoria disponible, no habiendo necesidad de bloque continuo de memoria disponible;
- *Memory De-fragmentation*: bloques de memoria son físicamente colocados en una secuencia (proceso similar al que ocurre en un PC). Reutilización de la memoria libre como bloque continuo de memoria disponible.

La tecnología Java ya ha sido comprobada en el mundo PC y aceptada por los institutos internacionales de estandarización como ETSI y 3GPP, ya habiendo especificaciones estandarizadas como Java 2.1.1 [8][7]

El Java también se encuentra aceptado como una solución interoperable para tarjetas SIM, que representa una solución para plataformas abiertas.

Las principales ventajas proporcionadas por la utilización de Java son mencionadas a continuación:

- Desarrollo único de aplicaciones => concepto *write once, run everywhere*;

[8] Media Formats , http://java.sun.com/javase/technologies/desktop/media/jmf/2.1.1/formats.html, 01/01/2009

- Existencia de muchos profesionales aptos para desarrollar aplicaciones en Java;
- Reutilización de programas;
- Mecanismo de carga de *applets* es estandarizado.

Para que las tarjetas SIM Java sean actualizadas vía OTA, éstas necesitan ser personalizadas con un “Perfil OTA” que habilita el UICC para obtener y ejecutar el comando OTA enviado por el Gateway OTA.

- **Tarjetas SIM Con *Micro Browser***

Las tarjetas con *Micro-Browser* permiten acceso a las informaciones y servicios basados en servidores que trabajan juntamente con un sistema OTA.

Mientras que las aplicaciones basadas en SMS:

- Utilizan comandos SIM *Toolkit;*
- Ejecutan y buscan informaciones específicas;
- Son enviadas para el terminal móvil celular vía SMS;

- Son visualizadas como Menús SIM *Toolkit* normales en el visor del terminal.

Las tarjetas SIM con Micro-Browser permiten aplicaciones dinámicas tales como:

- Las aplicaciones son almacenadas en un servidor;
- Las aplicaciones pueden ser alteradas cuantas veces sea necesario;
- No hay necesidad de sustituir tarjetas masivamente.

Algunas aplicaciones son residentes en la tarjeta y pueden ser actualizadas por el usuario, como homepages, bookmarks, etc.

- **Arquitectura De La Tarjeta Sim**

La memoria de la tarjeta SIM se la divide en memoria RAM, ROM y EEPROM, además de poseer CPU & ALU *Timer,* I/O Port, Seguridad y Lógica Fusa, de acuerdo a la figura 2.4.

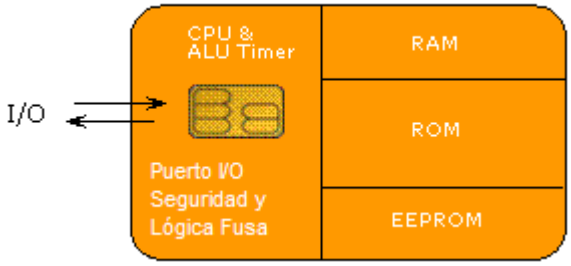


Figura 2.4 Segmentación de la memoria dentro de la tarjeta SIM

En la memoria EEPROM son ubicados los directorios y archivos inherentes a la configuración de la tarjeta SIM, comprendiendo el "Master File", los "Dedicated Files" y los "Elementary Files".

"Master File" (MF), "Dedicated Files" (DF) y "Elementary Files" (EF) son definidos de la siguiente forma según la norma GSM 11.11/ETS 300 045 [5]:

- *Master File* – Archivo único mandatorio. Contiene condiciones de acceso y, opcionalmente, DFs y EFs;
- *Dedicated File* – Archivo que contiene condiciones de acceso y, opcionalmente, EFs y otras DFs;
- *Elementary File* – Archivo que contiene condiciones de acceso y datos.

[5] GSM 11.11 Sistema Celular Digital de Telecomunicaciones (fase 2+), especificación de las aplicaciones de la tarjeta SIM

La configuración básica de la tarjeta SIM ocupa aproximadamente 8 kbytes de memoria EEPROM e incluye:

- Cabecera no–GSM ocupando aproximadamente 300 bytes;
- Master File ocupando aproximadamente 300 bytes;
    - PINs,PUKs, Kis, ADM keys, Tin, Layout, etc;
- Directorio GSM ocupando aproximadamente 750 bytes;
    - LP, IMSI, Key Kc & n, PLMN sel, HPLMN, ACM max, SST, ACM, GID 1 & 2, PUCT, CBMI, SPN, BCCH, ACC, FPLMN, LOCI, AD, Phase;
- Agenda de contactos ocupando aproximadamente 6600 bytes;
    - ADNs, FDNs, SMS,CCP, MSISDN, SMPS, SMSS, LND, Ext 1, Ext 2, Ext 3;
- OTA *Data Fields* ocupando aproximadamente 160 bytes;
    - SIM type, DL-Key, DL-Text, Seq-No, Orig. Address.

El espacio restante de memoria está destinado para las aplicaciones de valor agregado.

- **El Futuro De Las Tarjetas Sim**

El aumento de la competencia entre operadoras propietarias de redes GSM irá a imponer una mayor disputa por servicios de valor agregado y asistencia al cliente, demandando inversiones pesados en el control del churn y en la simplificación del uso del teléfono móvil celular como instrumento de conveniencia en la vida de las personas.

La busca incesante de diferenciales competitivos exigirá de las operadoras gran creatividad en el lanzamiento de servicios y en la simplicidad de relacionamientos con el cliente. La tarjeta SIM será pieza fundamental en la oferta de estos diferenciales a la medida de la evolución tecnológica rumbo a los procesadores más poderosos y veloces, mayor capacidad de memoria y lenguajes de programación que permitan el desarrollo e implementación de nuevas funcionalidades en plazos competitivos.

Con el aumento de la velocidad de transmisión de las redes móviles, aplicaciones direccionadas para la multimedia, Chat, m-commerce, etc, serán cada vez más los motores de la evolución de la tarjeta SIM, elemento fundamental en el desarrollo de soluciones de seguridad que viabilizan estos servicios.

El USIM fue proyectado con base en la experiencia de la estandarización de los SIM Cards GSM y ya nace estandarizando el mundo 3G para proveer funciones básicas de suscripciones y administración de red tales como la elección del idioma, preferencias cuando se está en roaming, seguridad y autenticación, además de permitir a los operadores, gran flexibilidad en el desarrollo de aplicaciones que de hecho consigan crear un diferencial competitivo.

La simplicidad de atención al cliente es parte de los nuevos retos que serán enfrentados por las operadoras internacionales, principales interesadas en la excelencia de la prestación de servicio en donde quiera que esté su cliente.

2.5 ETSI Ts 23 048 V5.9.0

El nombre completo del estándar es "DIGITAL CELLULAR TELECOMNUNICATIONS SYSTEM (PHASE 2 +) UNIVERSAL MOBILE TELECOMMUNICATIONES SYSTEM (UMTS) SECURITY MECHANISMS FOT THE (U)SIM APPLICATION TOOLKIT" El estándar especifica la estructura de los Paquetes Seguros en un formato general y su implementación utilizando Short Message Service Point to Point (SMS - PP) [9] y Short Message Service Cell Broadcast (SMS- CB) [10].

Adicionalmente, la codificación está especificada para un conjunto de comandos de aplicaciones dentro de los paquetes seguros Es un subconjunto de

los comandos especificados en el estándar 3GPP TS 51.011 y permite la administración remota de archivos en el UICC en conjunción con los SMS y los datos descargados al feature UICC.

Para UICC basados en el estándar 3GPP TS 43.019, el conjunto de comandos utilizado en la aplicación de administración remota está definido en éste estándar. Este documento se encuentra basado en una especificación de administración de tarjetas en Plataforma Abierta.

El estándar es aplicable para intercambio de paquetes seguros entre una entidad o PLMN GSM y una entidad en el UICC.

Los paquetes seguros contienen mensajes de aplicación a los cuales ciertos mecanismos en base al estándar 3GPP TS 22.048 que hayan sido aplicados.

9

10

[9] SMPP, http://en.wikipedia.org/wiki/Short_message_peer-to-peer_protocol, 27/02/2008

[9] SMPP, http://en.wikipedia.org/wiki/Short_message_peer-to-peer_protocol, 27/02/2008

2.5.1 Descripción Del Sistema De Seguridad De Comunicación Stk

Una descripción de una comunicación segura concerniente a (U) SIM Appication Toolkit junto con los mecanismos de seguridad descritos en el estándar 3GPP TS 22.048 se muestran en la figura a continuación:

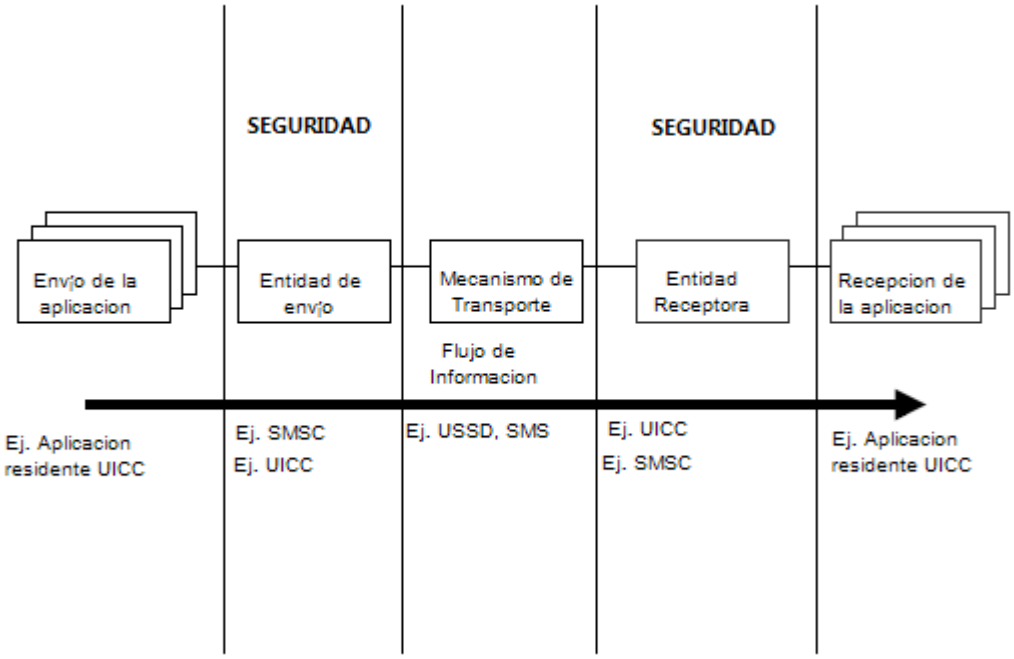


Figura 2.5 Descripción de un sistema de comunicación seguro

La aplicación remitente prepara un Mensaje de Aplicación y lo reenvía hacia la entidad de Envío, con la indicación del tipo de seguridad que será aplicado.

La entidad de envío adiciona un encabezado de seguridad al mensaje de Aplicación. Éste luego aplica el tipo de seguridad requerido a la parte de la cabecera de Comando y a todo el mensaje de Aplicación, incluyendo octetos de direccionamiento.

Bajo circunstancias normales, la entidad de Recepción recibe el Paquete de Comando, lo desempaqueta de acuerdo a los parámetros de seguridad indicados en la Cabecera de Comando. La entidad de Recepción subsecuentemente reenvía el mensaje de Aplicación hacia la Aplicación Receptora indicando el tipo de seguridad que se encuentra aplicado. La interfaz entre la aplicación Remitente y la entidad Remitente y la interfaz entre la entidad Receptora y la aplicación Receptora son propietarias y por lo tanto no se encuentran dentro del alcance de éste estándar.

Si está indicado en la cabecera del Comando, la entidad Receptora deberá crear un paquete de respuesta. El paquete de respuesta consiste en una cabecera de seguridad y opcionalmente, datos de una aplicación específica provista por la aplicación Receptora. Tanto la cabecera de Respuesta como los datos de una aplicación específica se encuentran seguros utilizando los mecanismos de seguridad indicados en el paquete de Comandos recibido. El paquete de respuesta será retornado a la entidad Remitente, en la capa de transporte.

A pesar de que no existe un acuse de recepción directo en un mensaje SMS-CB en el estándar 3 GPP TS 24.012, la aplicación Remitente puede requerir una respuesta. En este caso un paquete de Respuesta (seguro) podrá ser enviado utilizando diferentes portadores por la aplicación Receptora.

En algunas circunstancias un error relacionado con la seguridad puede ser detectado en la entidad Receptora. En ese caso la entidad Receptora deberá actuar de acuerdo a las siguientes reglas:

1. Nada deberá ser reenviado a la aplicación Receptora.
2. Si la entidad Remitente no requiere una respuesta, la entidad Receptora desecha el paquete de Comando y no tomará ninguna otra acción.
3. Si la entidad Remitente requiere una respuesta y la entidad Receptora puede ambiguamente determinar cual es la causa del error, la entidad Receptora deberá crear un paquete de Respuesta indicando la causa del error. Este paquete de Respuesta deberá tener seguridades de acuerdo al tipo de seguridad indicado en el paquete de Comando.
4. Si la entidad Remitente requiere una respuesta y la entidad Receptora no pueden determinar la causa del error, la entidad Receptora deberá enviar un paquete de respuesta indicando que un error no determinado ha sido detectado. Este paquete de Respuesta será enviado sin ningún tipo de seguridad.
5. Si la entidad Receptora recibe una cabecera de Comando no reconocible, el paquete de Comando será desechado y no tomará ninguna otra acción.

2.5.2 Estructura Generalizada De Un Paquete Seguro

Los paquetes de Comando y Respuesta tienen la misma estructura generalizada la cual consiste en una cabecera de seguridad de longitud variable

2.5.3 Estructura Del Paquete De Comando

La cabecera de Comando precede la los Datos de Seguridad en el paquete de Comando y es de longitud variable.

El paquete de comando será estructurado como se indica en la tabla 2.1:

Tabla 2.1: Estructura de un paquete de Comando

Elemento	Longitud	Comentario
Command Packet Identifier (CPI)	1 octeto	Identifica que el bloque de datos esta en un paquete de comandos seguro
Command Packet Length (CPL)	variable	Indica que el número de octetos incluyendo el identificador del comando de cabecera hasta el final del paquete seguro, incluye también octetos requeridos para cifrado
Command Header Identifier (CHI)	1 octeto	Identifica la cabecera del comando
Command Header Length (CHL)	variable	indica el número de octetos desde el SPI hasta el final de RC/CC/DS
Security Parameter Indicator (SPI)	2 octetos	--
Ciphering Key Identifier (Kic)	1 octeto	Identificador Llave y algoritmo para cifrado
Key Identifier (KID)	1 octeto	Identificador de llave y algoritmo para RC/CC/DS
Toolkit Application reference (TAR)	3 octetos	Aplicación dependiente de codificación
Counter (CNTR)	5 octetos	Contador de detección de respuesta e integridad de secuencia.
Padding Counter (PCNTR)	1 octeto	Indica el número de octetos utilizados para realizar el cifrado al final de los datos seguros
Redundancy Check (RC). Criptographic Checksum (CC) o Digital Signature	variable	La longitud depende del algoritmo. Un valor común es 8 octetos, pero puede llegar a se 48 octetos o más, el mínimo debería ser 4 octetos
Secured Data	variable	Contiene el mensaje de aplicación segura y los octetos usados en la criptografía.

Tabla 2.2: Representación lineal de un paquete de Comando

CPI	CPL	CHI	CHL	SPI	Kic	KID	TAR	CNTR	PCNTR	RC/CC/DS	Datos seguros
								Nota 1	Nota 1	Nota 1	Nota 1
	Nota 3		Nota 3	Nota 2	Nota 2	Nota 2	Nota 2	Nota 2	Nota 2		Nota 2

Nota 1: Estos campos son incluidos en los datos a ser cifrados, si el cifrado es indicado en la cabecera de seguridad
Nota 2: Estos campos son incluidos en el calculo del RC/CC/DS
Nota 3: Parte o todos los campos pueden ser también incluidos en el cálculo del RC/CC/DS, dependiendo en la implementación

Si se especifica cifrado, RC/CC/DS deberá ser calculado como se indica en la nota 2 primeramente y después se aplicará el cifrado como se indica en la nota 1

El SPI indica que un campo en específico no está siendo utilizado, la entidad Remitente configurará los contenidos de este campo en cero y la entidad Receptora ignorará su contenido.

Si el SPI indica que RC, CC o DS no se encuentra presente en la cabecera de Comando, el campo RC/CC/DS será de longitud cero.

Si el contador de direccionamiento es cero, esto indica que no existen octetos de direccionamiento, o que no es necesario el direccionamiento.

2.5.4 Codificación Del SPI

Primer Octeto:

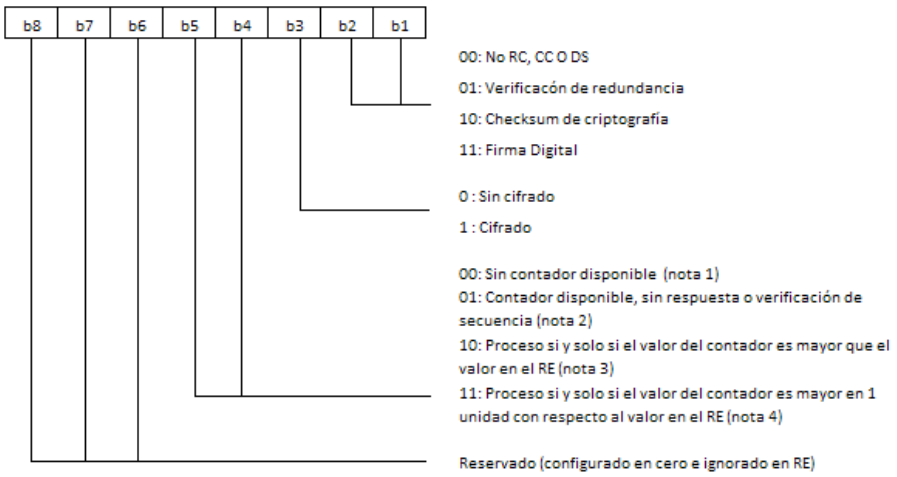


Figura 2.6 Descripción del primer octeto de la codificación del SPI

NOTA 1: En este caso el campo de contador se encuentra presente en el mensaje.

NOTA 2: En este caso el valor del contado es usado solamente para propósitos de información. Si el paquete Comando fue exitosamente desempaquetado, el valor del contador puede ser reenviado desde la entidad Receptora hacia la aplicación Receptora. Esto depende en implementaciones propietarias y sucede en una aplicación dependiente.

NOTA 3: El valor del contador es comparado con el valor del contador del último paquete Comando. Esto es tolerante a fallar en el nivel de transporte. Un escenario posible es una actualización global.

NOTA 4: Provee un control estricto además de la seguridad indicada en la nota 3.

Segundo Octeto:

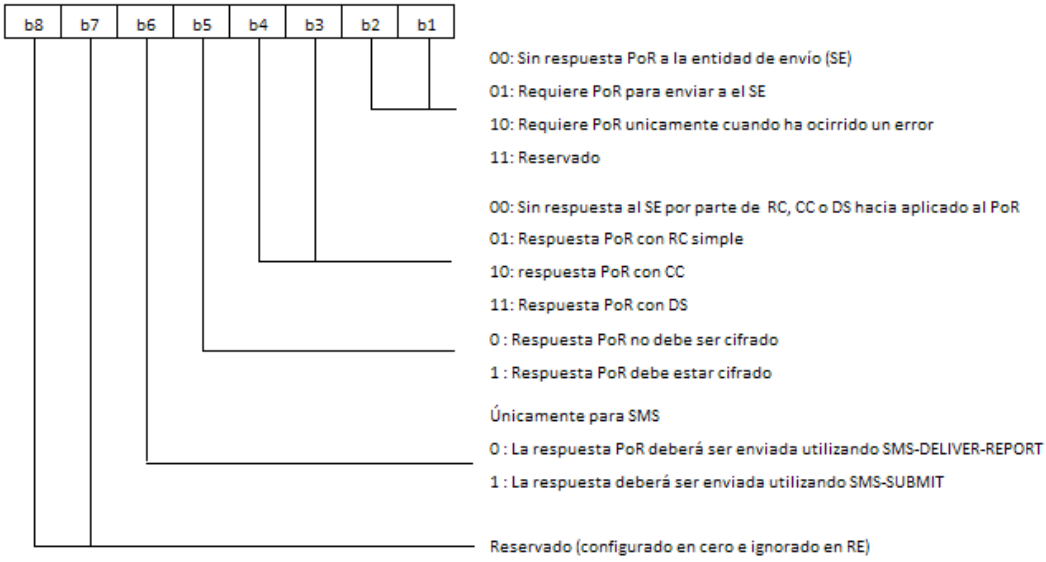


Figura 2.7 Descripción del segundo octeto de la codificación del SPI

2.5.5 Codificación Del KIC

El KIc se encuentra codificado como se indica a continuación

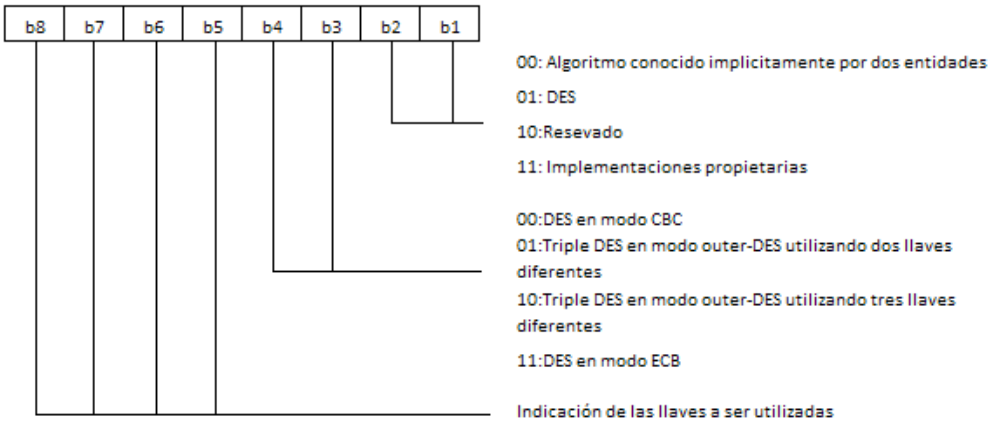


Figura 2.8 Descripción de la codificación del KIc

DES es el algoritmo especificado como DEA :en el estándar ISO 8731-1.

2.5.6 Codificación Del Kid

El KID se codifica como se indica a continuación:

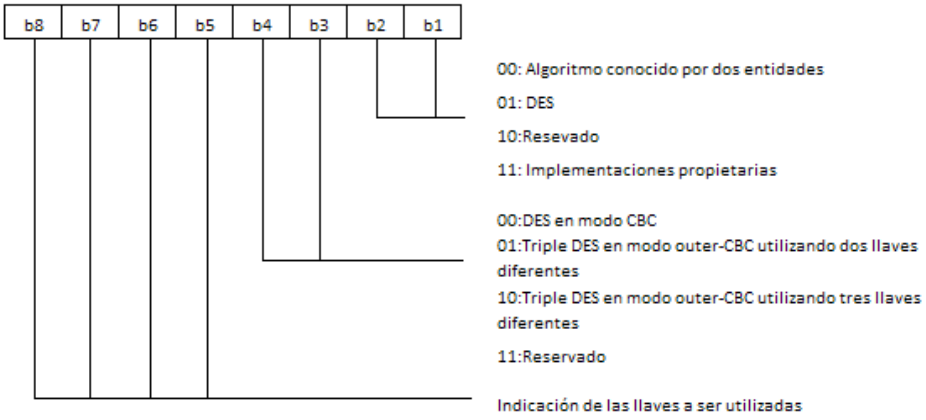


Figura 2.9 Descripción de la codificación del KID

2.5.7 Administración De Contadores

En el primer byte b4b5=00 del SPI, el campo del contador será ignorado por el RE y el RE no actualizará al contador.

Si b5 en el primer byte del SPI es igual a 1 entonces las siguientes reglas serán aplicadas al administrador de contadores con el objetivo de prevenir ataques de sincronización y contestación:

- El SE establece el valor del contador y no deberá se incrementado.
- El RE actualizará el contador en su próximo valor a partir de la recepción del paquete de Comando después de verificar que los controles de seguridad han pasado exitosamente.
- Cuando el valor del contador alcanza su máximo valor el contador se bloquea.

Si existe más de un SE, se tomará cuidado para asegurar que los valores del contador se mantengan sincronizados con lo que el RE espera del SE.

El nivel de seguridad está indicado a través de la interfaz propietaria entre la aplicación Remitente / Receptora y la entidad Remitente / Receptora. Los diseñadores de la aplicación deberán estar al tanto que si la aplicación Remitente requiere “No RC/CC/DS” o “Control de Redundancia” y “No contador disponible”, desde el SE, no se aplicará seguridad al mensaje de Aplicación y por lo tanto incrementa la amenaza de ataques maliciosos.

2.5.8 Estructura Del Paquete De Respuesta

Tabla 2.3: Estructura del paquete de respuesta

Elemento	Longitud	Comentario
Response Packet Identifier (RPI)	1 octeto	Identifica un paquete de respuesta
Response Packet Length (RPL)	variable	Indica el número de octetos incluyendo el RGI hacia el fin de los datos de respuesta adicional, incluyendo cualquier octeto requerido para el cifrado.
Response Header Identifier (RHI)	1 octeto	Identifica la cabecera de respuesta
Response Header Length (RHL)	variable	Indica el número de octetos incluyendo el TAR hacia el final del RC/CC/DS.
Toolkit Application Reference (TAR)	3 octetos	Tiene que ser una copia del contenido del TAR en el paquete de comando
Counter (CNTR)	5 octetos	Tiene que ser una copia del contenido del CNTR en el paquete de comando
Padding counter (PCNTR)	1 octeto	Indica el número de octetos usados para cifrar al final de los datos de respuesta adicional.
Response Status Code Octet	1 octeto	--
Redundancy Check (RC), Cryptographic Checksum (CC) or Digital Signature (DS)	variable	La longitud depende del algoritmo indicado en la cabecera de comando en el mensaje entrante. Un valor típico es de 4 a 8 octetos o cero, caso contrario se requiere RC/CC/DS
Additional Response Data	variable	Aplicación opcional de datos de respuesta específica, incluyendo los octetos.

Tabla 2.4: Representación lineal del paquete de respuesta

RPI	RPL	RHI	RHL	TAR	CNTR	PCNTR	Status Code	RC/CC/DS	Respuesta Adicional de Datos
					nota 1	nota 1	nota 1	nota 1	nota 1
	nota 3		nota 3	nota 2	nota 2	nota 2	nota 2		nota 2

NOTA 1: Si el cifrado es indicado en el paquete de comando SPI entonces estos campos deberán estar cifrados
NOTA 2: Estos capos deben estar incluidos en el calculo del RC/CC/DS
NOTA 3: Parte o todos los campos pueden estar incluidos en el calculo del RC/CC/DS, dependiendo en la implementación como SMS.

2.5.9 Comandos Estandarizados Para Administración Remota De Archivos

Existen dos elementos para la Administración Remota de Archivos en el UICC, el primero es el comportamiento del UICC residente en la Aplicación ToolKit, que es quien realiza la Administración Remota de Archivos y el segundo es la estructura del comando en el mensaje Data Download de la tarjeta SIM, el cual es especificado en el estándar 3GPP TS 31.111. Las condiciones de acceso para archivos GSM y 3G residentes en la aplicación no se encuentran estandarizados. Estos se encuentran bajo el control del diseñador, en cooperación con el Operador de la Red o el Proveedor de Servicios propietarios del UICC. Estas condiciones de acceso pueden ser dependientes a nivel de seguridad aplicada en el mensaje UICC Data Download.

2.5.10 Comportamiento De La Aplicación Para Administración Remota De Archivos

El o los parámetros en el mensaje Data Download hacia el UICC es o un solo comando, o una lista de comandos que deberán ser procesados secuencialmente.

La aplicación deberá tomar los parámetros desde el mensaje Data Download hacia el UICC y actuará a partir de los archivos GSM o 3G de acuerdo a estos parámetros.

Un comando “session” está definido como inicial a partir de la recepción de la lista de parámetros o comandos y termina cuando la lista de parámetros en el mensaje Data Download hacia el UICC se ha completado o cuando se ha detectado un error que pueda causar un retraso en el procesamiento de la lista de comandos.

Al inicio y al final del comando “session” el estado lógico (ej. Punteros del archivo) del UICC como se lo mira desde el ME no será cambiado a tal grado de para interrumpir el comportamiento del ME. Si existen cambios en el estado lógico de los cuales el ME tiene que estar advertido, la aplicación en el ME publicará un comando REFRESH de acuerdo al estándar 3GPP TS 31.111.

El siguiente directorio será implícitamente seleccionado y es el directorio que existirá al inicio del comando “session”:

El MF para el comando *“session”* enviado al sistema de archivos compartidos del ME

El ADF para el comando *“sesión”* enviado al sistema de archivos de la tarjeta USIM.

2.5.11 Codificación De Los Comandos

Una cadena de comandos podría contener un solo comando o una secuencia de comandos. Cada comando está codificado de acuerdo a la estructura generalizada definida a continuación, cada elemento con excepción del campo de Data es un solo octeto

Tabla 2.5: Representación estructura de comando

Clase de byte (CLA)	Código instr. (INS)	P1	P2	P3	Datos

Si el comando P3=’00’, entonces el UICC enviará de regreso todos los parámetros/datos disponibles de respuesta.

Los comandos administrativos aún no han sido definidos, por lo tanto se mantienen como propietarios los fabricantes del UICC.

2.5.12 Comandos De Entrada De La Tarjeta Sim

Los comandos estandarizados se enlistan en la Tabla 2.6. Los comandos se encuentran definidos en el estándar 3GPP TS 51.011, con excepción que el comando SELECT es extendido del comando especificado en el estándar 3GPP TS 51.011

Tabla 2.5: Representación estructura de comando

Comandos Operacionales
SELECT
UPDATE BINARY
UPDATE RECORD
SEEK
INCREASE
VERIFY CHV
CHANGE CHV
DISABLE CHV
ENABLE CHV
UNBLOCK CHV
INVALIDATE
REHABILITATE

Tabla 2.6. Comandos de entrada de las tarjetas SIM

2.5.13 Comandos De Salida De Las Tarjetas Sim

Los comandos enlistados en la Tabla 2.7 son definidos en el estándar 3GPP TS 51.011. Estos comandos solo ocurrirán en una cadena de comandos. Los datos de respuesta serán ubicados en un elemento Adicional de Datos de Respuesta del Paquete de Respuesta. Si se utiliza un SMS, esto resultará en la generación de un único SM por la UICC

Tabla 2.7. Comandos de salida de las tarjetas SIM

Comandos Operacionales
READ BINARY
READ RECORD
GET RESPONSE

2.5.14 Comportamiento De La Aplicación Para Administración De Applets Remotamente

- **Carga De Paquetes**

El proceso de carga de paquetes permite a los Operadores de la Red o Proveedores de Servicios cargar nuevos paquetes en el UICC. El Operador de Red o el Proveedor de Servicio administra la carga de los paquetes a través de una sesión de carga con la tarjeta.

Una sesión de carga en la tarjeta consiste en una secuencia de comandos como se describe en la Figura 2.11

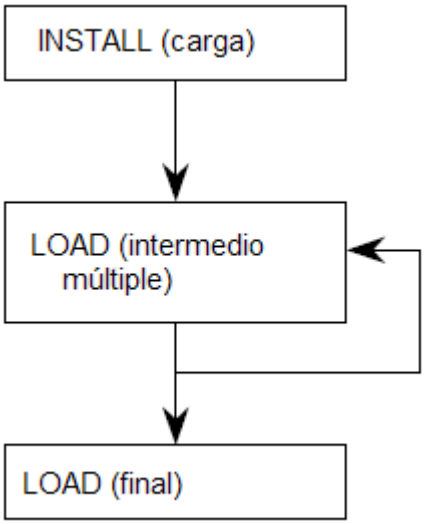


Figura 2.10. Secuencia de comandos de una sesión de carga

Dependiendo del tamaño del Applet, se utilizarán más de un SMS para la carga del paquete.

- **Instalacion Del Applet**

El proceso de instalación de Applets permite al Operador de Red o al Proveedor de Servicios instalar nuevas aplicaciones en el UICC. La instalación será realizada solamente si el paquete correspondiente ha sido cargado en la tarjeta.

- **Retiro Del Paquete**

El retiro del paquete se lo realiza a través del comando DELETE. El procedimiento de retiro será realizado por el UICC como se lo define a continuación:

1. Si se mantienen aplicaciones instaladas del paquete, la tarjeta rechazará el retiro con su correspondiente código de error.
2. Si el paquete está referido por otros paquetes, la tarjeta rechazará el retiro con su correspondiente código de error.

- **Retiro De Applets**

El proceso de retiro de Applets será realizado utilizando el comando DELETE. El UICC removerá los componentes que conforman el Applet.

- **Bloqueo / Desbloqueo De Applets**

El procedimiento de bloqueo y desbloqueo de Applets, permite al Operador de la Red o al Proveedor de Servicios a habilitar o deshabilitar una aplicación utilizando el comando SET STATUS como se encuentra descrito en el Anexo A del estándar. Cuando se bloquea una aplicación, no será posible ser accionado o seleccionado y todas la entradas del menú serán deshabilitadas.

- **Recupetación De Parámetros Del Applet**

El procedimiento de recuperación de parámetros del Applet permite al Operador de Red o al Proveedor de Servicios hacer una petición de los parámetros de un Applet remotamente. Este procedimiento se lo realiza utilizando el comando GET DATA como se encuentra definido en el Anexo A del estándar.

- **Codificación De Los Comandos**

Los comandos se encuentran codificados como un APDU para el procedimiento de Administración de Archivos Remotos.

Los mensajes para el Administrador de Tarjetas tendrán un valor TAR configurado en “000000” en hexadecimal.

- **Comandos De Entrada**

La siguiente Tabla indica los comandos de entrada de Administración de Applets:

Tabla 2.8. Comandos de Entrada de administración de Applet

COMANDO OPERACIONAL
DELETE
SET STATUS
INSTALL
LOAD
PUT KEY

- **Comandos De Salida**

La siguiente Tabla 2.9 indica los comandos de salida de Administración de Applets:

Tabla 2.9. Comandos de Salida de administración de Applet

COMANDO OPERACIONAL
GET STATUS
GET DATA

CAPÍTULO III

DISEÑO

3.1 INTRODUCCIÓN

Este capítulo tiene por intención proveer una comprensión general respecto de los productos y servicios propuestos con el fin de que la operadora pueda proveer los mejores servicios de gestión de terminales y tarjetas SIM para sus suscriptores.

A través de este estudio, se ofrece la siguiente solución:

Que la plataforma permita que la operadora móvil gestione varias tareas Over-The-Air (OTA) para tarjetas SIM GSM, UMTS. Esta plataforma abre las puertas a la operadora para proveer una combinación de beneficios a sus

negocios, incluyendo gerencia remota de archivos SIM (OTA SIM File Management y activación remota de suscriptores (OTA Subscriber Activation).

La plataforma para gestión de tarjetas SIM, provee una interfaz independiente de proveedor (U)SIM para la gerencia remota de tarjetas (U)SIM y utiliza el estándar Remote File Management (RFM). Protocolos OTA específicos (propietarios) para todos los más importantes proveedores de SIM, provee funciones para:

- Formatear mensajes OTA de acuerdo con el protocolo OTA adecuado.

- Mantener el contenido de archivos de la descarga OTA en almacenamiento temporario hasta que la descarga OTA sea concluida con éxito y actualizar la base de datos DP para reflejar los cambios.

- Colas / buffer configurables para garantizar carga continua en la SMS-C. El valor de la cola puede ser definido de acuerdo con la capacidad del canal para la SMS-C.

- Una Prueba-de-Recepción (PoR) puede ser solicitada para confirmación de ejecución de comandos (U)SIM.

- Cancelación de solicitaciones de descarga (caso soportada por el SMS-C).

- Carga remota (*Over-The-Air*) de datos de archivos contenidos en la tarjeta (U)SIM. (Solamente para tarjetas (U)SIM habilitadas para PoR)

- Envío de SMS de texto puro.

- Activación y desactivación de suscripciones. Descarga de parámetros de suscripción y alimentación de informaciones de suscriptores en la base de datos.

- Manejo transparente de *applets* para diferentes tarjetas por sus perfiles de tarjeta.

- Un repositorio completo de *applets.*

- Manejo flexible de definiciones de *applet* y parámetros de activación

- Actualizaciones de lotes de SIM

La plataforma para gestión de terminales es una solución de gestión de Configuraciones de Terminal (Terminal Settings Management) que se queda totalmente operacional con configuraciones y trabajos de integración mínimos, pero flexible y escalable para alcanzar las necesidades de operadoras a la medida que pasan a soluciones de Gerencia de Dispositivos Móviles (Mobile

Device Management) más avanzadas. La plataforma provee una solución completa de aprovisionamiento de configuraciones de terminal:

- Detección de Dispositivos para permitir un verdadero conocimiento de los dispositivos al encontrar, identificar y determinar el terminal de un usuario.

- Percepción de Eventos para permitir la recepción de señales generados por las varias situaciones que ocurren durante el ciclo de vida de un suscriptor, tales como cambio de terminal y falla de servicios, y para poseer la inteligencia sobre cuál Lógica de Negocios aplicar.

- Lógica de Negocios para decidir cuales acciones serán ejecutadas y cuales reglas aplicadas, así como la capacidad de utilizar las informaciones correctas basadas en el contexto de la situación.

- Informaciones actualizadas

- Conocimiento del histórico del terminal; si ha sido pre-configurado, recién utilizado por el mismo usuario y configurado

- Conocimiento sobre las capacidades del terminal; Informaciones correctas y actualizadas sobre todos los modelos, capacidades, protocolos y versiones OTA y conformidad con estándares

- Conocimiento de las características del suscriptor; suscriptor GPRS, prepago, pospago, corporativo, MVNO

- Mecanismo de descarga confiable que ofrece manejo de errores, generación de datos para tarifación, registros, alta capacidad e interconectividad.

3.2 PREMISAS

Para efectos de cálculo de licencias, el throughput necesario para una operadora, fue estimado en 30 SM/s en la hora punta.

- Para efectos de cálculo de licencias de gestión de terminales, fue considerado que la operadora no va a configurar envío automático de configuraciones para todos los cambios de terminales. En estas condiciones, fue estimado un total de 25.000 configuraciones por mes.

- La lógica del *applet* para la detección del IMEI de los terminales, ejecuta la evaluación de cambio de terminales en la tarjeta SIM y solamente envía eventos reales de cambio de terminal a la solución para gestión de terminales.

- Fue considerada integración con dos SMS-Cs. Conexión con más SMS-Cs es soportado por la plataforma pero no está incluido en este estudio.

- Para la utilización de la funcionalidad de trafico de OTA por GPRS, los terminales y tarjetas SIM deben soportar BIP.

- Este estudio considera que la operadora no tiene plataforma OTA, siendo necesaria apenas una carga de tarjetas y ninguna migración.

- La operadora ya tiene una plataforma de *SIM browsing* (para *dynamic browsing y service management* – gestión del menú estático).

-

3.3 DISEÑO

A continuación se indica un esquema general de la solución:

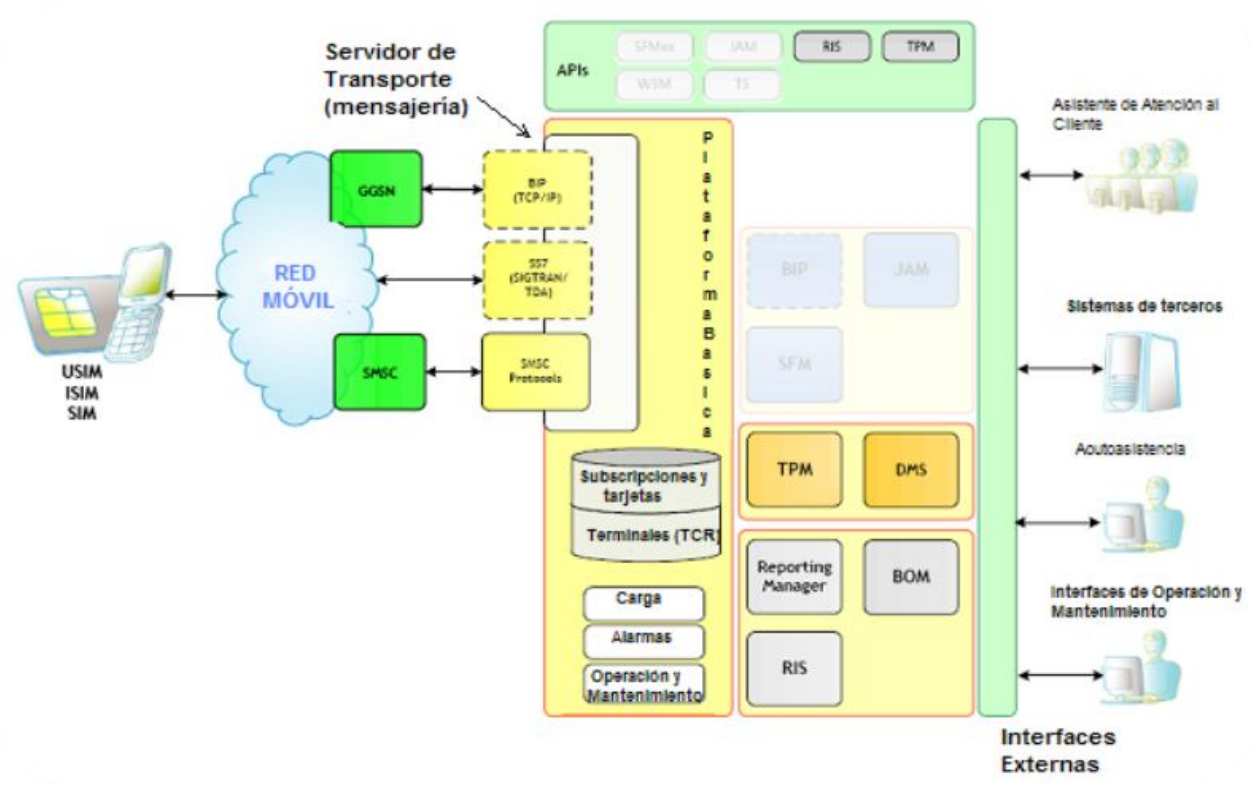


Figura 3.1.Visión general de la solución

3.4 DESCRIPCIÓN DETALLADA

3.4.1 Plataforma Básica: Delivery Platform Basic Framework

El DP Basic Framework es la base para las aplicaciones de las plataformas. El DP Basic Framework contiene funcionalidades genéricas para gestión de configuraciones, alarmas, registro y cobro de eventos, contadores estadísticos, mecanismos de transporte y la estructura de base de datos. [11]

[11] Recomendaciones de Hardware y Software DP, Doc. No. MPM02:0055, 2005, Smartrust.

El DP Basic Framework es diseñado para atender a los requisitos de las operadoras para mantenibilidad, disponibilidad, escalabilidad y desempeño.

DP Basic Framework (DPBF) provee un número de funciones básicas que pueden ser utilizadas por todos los módulos que ejecutan sobre el DPBF.

- Transporte de Mensajes
- Conexiones con las SMS-Cs
- Administración de usuarios con autenticación y control de acceso
- Funciones de operación y mantenimiento: gestión de configuraciones (*Configuration Management*), gestión de fallas (*Fault Management*), manejo de alarmas (*Alarm Handling*), manejo de eventos (*Event Handling*)
- Servicios para tarifación
- Protección de sobrecarga, distribución de carga de tráfico & control de flujo
- Base de datos

- ***Transporte de Mensajes***

DP Basic Framework provee la infraestructura de mensajería que es compartida por todos los módulos funcionales de DP.

DP Basic Framework soporta a un extenso conjunto de protocolos y suministradores de SMS-C y conexiones con varias SMS-Cs.

Opcionalmente la infraestructura de transporte de mensajes de DP se puede conectar al un módulo de High Speed Messaging (HSMP) que provee una conexión directa a la red SS7, dispensando el uso de la SMS-C.

La mensajería de DP puede ser transparente – cuando el sistema funciona como un gateway para la SMS-C – o puede proveer un completo mecanismo de almacenar-y-enviar (store-and-forward) incluyendo recuperación de transacciones.

Con el fin de mantener el status de cada mensaje enviado, DP Basic Framework continuamente recibe reportes de status de la SMS-C (confirmación de recepción por la SMS-C). Los reportes de status son tratados y si es necesario son enviados adelante a las aplicaciones.

Adicionalmente las aplicaciones pueden solicitar la prueba-de-recepción de la SIM (PoR), como se explicará más adelante, “Gestión Remota de Archivos (RFM): SFM Server”. Con el fin de soportar a una reiniciación del sistema, DP Basic Framework presenta la opción de almacenar y actualizar el status de todos los mensajes en la base de datos. La infraestructura de mensajería de DP Basic Framework tiene también una serie de funcionalidades para soportar a disturbios

en la SMS-C como reportes y confirmaciones perdidas o retrasadas. [11, sec 2.9]

]

- ***Estándares de Transporte de Mensajes Soportados***

El transporte de mensajes es completamente soportado de acuerdo con las especificaciones 3GPP TS 23.040 / GSM 03.40, incluyendo:

- Mensajes de texto 7-bit (GSM 03.38)
- Mensajes cortos binarios 8- y 16-bits (Unicode)
- Concatenación de mensajes cortos
- Mensajes del application toolkit 3GPP TS 23.048 / GSM 03.48

- ***Autenticación***

DP Basic Framework soporta autenticación y almacena las informaciones de cuentas de usuarios.

Las siguientes políticas de login son soportadas:

[11] Recomendaciones de Hardware y Software DP, Doc. No. MPM02:0055, 2005, Smartrust.

- Tamaños mínimo y máximo de contraseña flexibles
- Número máximo de reintentos
- Período de validad de contraseña

- ***Control de Acceso***

La DP Basic Framework soporta control de acceso en un nivel de perfil de usuario. Las siguientes políticas son soportadas:

- Grupos de suscripciones, tarjetas (U)SIM y terminales
- Aplicación (por ejemplo *Users, User Profiles, Cards* etc.)
- Archivo (U)SIM

Control de acceso es el mecanismo que verifica si un usuario tiene los derechos para realizar una tarea específica. Es usado para permitir diferentes papeles, delegación de tareas y delegación de derechos para subscripciones, Terminales, archivos (U)SIM y tarjetas (U)SIM. Derechos de acceso pueden ser definidos en un nivel de servicio. Los niveles usados son sólo de lectura (read-only) y completo. Los servicios típicos son User, User profiles, grupos de descripciones y aplicaciones de las tarjetas. Control de acceso es un servicio básico proveído por DP Basic Framework y compartido por todos los componentes de software

a) Control de acceso de suscripción

Control de acceso puede ser hecho en el nivel de subscripción. Esto es alcanzado cuando se utiliza el concepto de Subscription groups. Una subscripción puede pertenecer a varios grupos. Un usuario DP tiene acceso solamente a subscripciones que pertenecen a los grupos a los cuales el usuario tiene derechos de acceso. El concepto de Subscription groups puede también ser usado como base para soluciones corporativas o de hospedaje así como para agrupamiento de usuarios.

b) Control de acceso de tarjeta (U)SIM

Control de acceso puede también ser hecho en el nivel de SIM Card. Esto es alcanzado cuando se utiliza el concepto de (U)SIM groups. Una (U)SIM Card puede pertenecer a varios grupos. Un usuario DP tiene acceso solamente a (U)SIM Cards que pertenecen a los grupos a los cuales el usuario tiene derechos de acceso.

c) Control de acceso de envío de mensajes

La parte de mensajería también incluye funcionalidad de control de acceso. Control de acceso en la DP tiene que ver con el envío y recibimiento de mensajes, y el manejo de informaciones de status de mensajes. Se puede dirigir SMS-Cs tanto directamente como en un grupo. En este caso la carga es balanceada entre las SMS-Cs contenidas en el grupo a que se dirige.

- ***Registro de Rastros para Auditoría***

Cambios en el sistema de derechos de control de acceso son registrados en un archivo de rastros para auditoría (audit trail log). Esta funcionalidad asegura que intentos de quebrar la seguridad puedan ser detectados de forma fácil. En este archivo son registrados que persona (usuario DP) hizo cambios en atributos de usuario y parámetros de perfiles de usuarios. Estos cambios incluyen creación, actualización y remoción.

- ***Gestión de configuraciones***

Todos los datos de configuraciones de DP son almacenados en una base de datos y son manejados a través de una interfaz de usuario Java gráfica Para determinados parámetros, los cambios son aplicados inmediatamente. Conexiones SMS-C adicionales pueden ser configuradas y añadidas sin necesidad de reiniciar el sistema.

- ***Gestión de desempeño***

Los contadores son utilizados para proveer datos de los servidores para permitir presentar informaciones estadísticas, diagnósticas y de desempeño así como para depuración. Los valores de contadores pueden ser recuperados por

SNMP. Hay dos clases de contadores: contador e indicador. Contador es un contador incrementado continuamente, por ejemplo NrOfSentSM (Number of Sent Short Messages – número de mensajes cortas enviadas). Los Indicadores son un valor de status, por ejemplo NrOfSmWaitingForSend (Number of Short Messages Waiting for Send – número de mensajes cortas aguardando envío). Con un navegador SNMP, contadores pueden ser buscados para obtener los datos estadísticos deseados.[12]

- ***Gestión de fallas***

En el DP Basic Framework hay varias herramientas que pueden ser utilizadas para la gestión de fallas, por ejemplo: Registro de eventos (event logging) permite el acompañamiento de las requisiciones a través del sistema – de servidor a servidor. Requisiciones falladas serán registradas con la razón de la falla. Esto permite solución de problemas en un nivel de suscriptor. Ejemplos de otros eventos son iniciación del servidor, cambios de configuración y cambios de status de alarmas. Manejo de alarmas (alarm handling) permite el monitoreo de alarmas enviadas por componentes de la DP, así como la supervisión de los componentes de DP en ejecución. Contadores pueden ser utilizados para identificar comportamiento anormal en el sistema, por ejemplo para hacer la supervisión de tamaños de colas.

Alarmas y contadores en DP pueden ser accedidos por SNMP. Además, alarmas pueden ser monitoreadas con el DP Alarm Registro de rastros (trace

[12] Contadores y Calculadores DP Basic Framework, Doc. No. 10542-080, Revisión: B. 2005-11-14, Smartrust.

logging) permite un avanzada corrección de problemas. Los niveles de registro (log) pueden ser definidos dinámicamente en el servicio, módulo y clase[13]

3.4.1.1 Registro de eventos

Los datos de eventos de tráfico (Traffic Event) recibidos pueden ser exportados tanto en formato de archive como para la base de datos. Datos de eventos almacenados en la base de datos pueden ser utilizados por componentes opcionales como el Report Manager para juntar, por ejemplo, informaciones de histórico de descargas. La salida de datos de eventos (Event Data) puede ser filtrada – la selección puede ser hecha basada en cuales eventos y el resultado de cada evento (OK o Fallado). Múltiplos archivos (Multiple Files) pueden ser utilizados a través del uso de diferentes filtros. Esto también se aplica a los datos que deben ser almacenados en una base de datos de histórico de eventos.

- ***Servicios para tarifación***

El servicio para tarifación de DP Basic Framework recibe datos para tarifación de las aplicaciones de DP (DP Applications). DP Basic Framework almacena estos datos para tarifación y los escribe para un archivo para ser

[13] Tipos de Alarmas de la plataforma Basic Framework, Doc. No. 10542-078, Revisión: C. 2006-08-31, Smartrust.

colectado por transferencia de archivo. Registros para tarifación son almacenados en formato ASN.1 y pueden ser también producidos en formato ASCII.

Eventos para tarifación contienen datos que permiten la identificación del propio evento así como de la entidad o usuario cuya requisición de servicios disparó el evento. Además, los eventos para tarifación contienen informaciones de fecha y hora, identificación única del evento para tarifación y el MSISDN del suscriptor. [14]

- ***Protección de sobrecarga***

El modulo de transporte de mensajes (Messaging) es ajustado inicialmente para los limites de las SMS-Cs conectadas y de la configuración actual del sistema, y basado en esto la velocidad de la entrada de datos de los componentes de sistema conectados es ajustada. Esto es hecho en la entrada de todos componentes de sistema, tanto componentes de la DP como sistemas externos conectados por las API‟s de DP. El modulo de transporte de mensajes provee también la posibilidad de regular el caudal del sistema hasta un determinado límite superior (throttling).

- ***Repository Integration Server – RIS***

[14] Especificación de formato de CDR, 10542-086, Revisión: A. 2005-09-20, Smartrust.

Los repositorios de datos de la plataforma contienen un cantidad extensiva de datos de terminales, tarjetas (U)SIM, suscriptores y suscripciones. Los datos relacionados a estas entidades son proveídos a aplicaciones externas a través del servidor Repository Integration Server (RIS). El RIS provee un API para los extensivos datos almacenados en los repositorios de la DP. Con el uso de RIS, el aplicación conectada puede buscar, cambiar y remover datos en estos repositorios. RIS también provee datos históricos relativos a los eventos registrados por la plataforma básica.

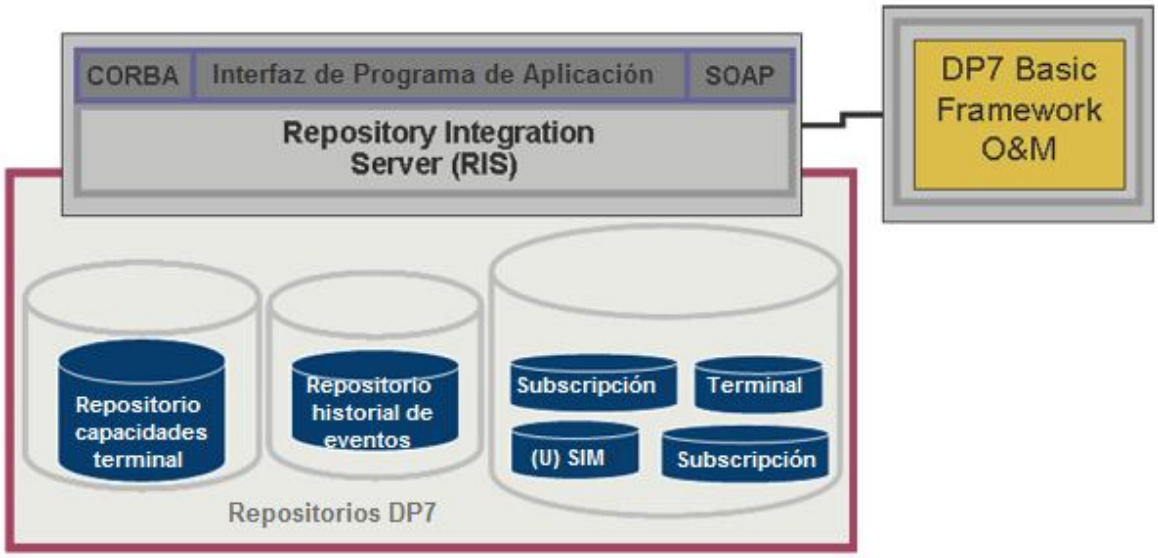


Figura 3.2. Visión general de la arquitectura RIS

- ***RIS API***

Los servicios de RIS son publicados a través de la RIS API. La RIS API consiste de una interfaz CORBA y una interfaz SOAP.

- Interfaz RIS CORBA – provee una interfaz basada en CORBA. La interfaz es definida en IDL y es implementada usando un JacORB que soporta al CORBA 2.3 Code set.

- Interfaz RIS SOAP interface - provee una interfaz Web *services* basada en SOAP 1.2. SOAP es un protocolo simple basado en XML que permite aplicaciones intercambiar informaciones sobre HTTP. El API SOAP es dividida en entidades lógicas descriptas en archivos WSDL (Web *Service Definition Language*).

- ***Repository Integration Server***

El RIS implementa los servicios proveídos por la RIS API y consiste de los siguientes módulos. [15]

- Módulo tarjeta - provee servicios para accede datos en el repositorio (U)SIM ((U)SIM *Repository*)

- Módulo terminal - provee servicios para acceder datos en el repositorio de terminales (*Terminal Repository*)

- Módulo suscriptor - provee servicios para acceder datos en el repositorio de suscriptores (*Subscriber Repository*)

- Módulo suscripción - provee servicios para acceder datos en el repositorio de suscripciones (*Subscription Repository*)

[15] Descripción plataforma Gestión de Dispositivos, Febrero 2005, Gemalto

- Módulo común – provee servicios para leer informaciones sobre las propiedades dinámicas asociadas a las entidades en los repositorios de la DP
- Módulo de histórico de eventos – provee servicios para leer datos de eventos en el repositorio de histórico de eventos *(Event History Repository*)
- Módulo TCR – un modulo opcional que provee servicios para accede los datos en el repositorio de capacidades de terminal (*Terminal Capabilities Repository)*
- Módulos personalizados – módulos opcionales que pueden proveer servicios personalizados para acceder a repositorios de la DP o repositorios de terceros

- ***Funciones de Importación y Actualización de Datos de Tarjetas (U)SIM y Suscriptores***

La plataforma básica incluye una avanzada función de importación y modificación de la base de datos que posibilita importar y/o modificar datos en la base de datos. Los datos de entrada para la función SimImport es escrita en archivos texto de acuerdo con un conjunto de especificaciones. Los archivos de entrada de importación de datos pueden ser divididos en dos partes, una conteniendo los datos del perfil de la tarjeta (U)SIM y otro conteniendo el lote de datos de las tarjetas. Estas dos partes pueden ser importadas separadamente. La función de actualización/modificación de datos provee a la operadora una manera de modificar y borrar datos en la base de datos utilizando archivos texto de importación. Actualización de datos incluye funciones para activar/desactivar SIM, asociar una tarjeta SIM a grupo de suscripción, cambiar la SIM de un suscriptor, y terminar con una SIM.

3.5 Gestión de Tarjetas SIM

La plataforma para gestión de tarjetas SIM tiene por componentes el SFM Server, responsable por la gestión de archivos en la tarjeta SIM y JAM Server, responsable por la gestión de applets Java.

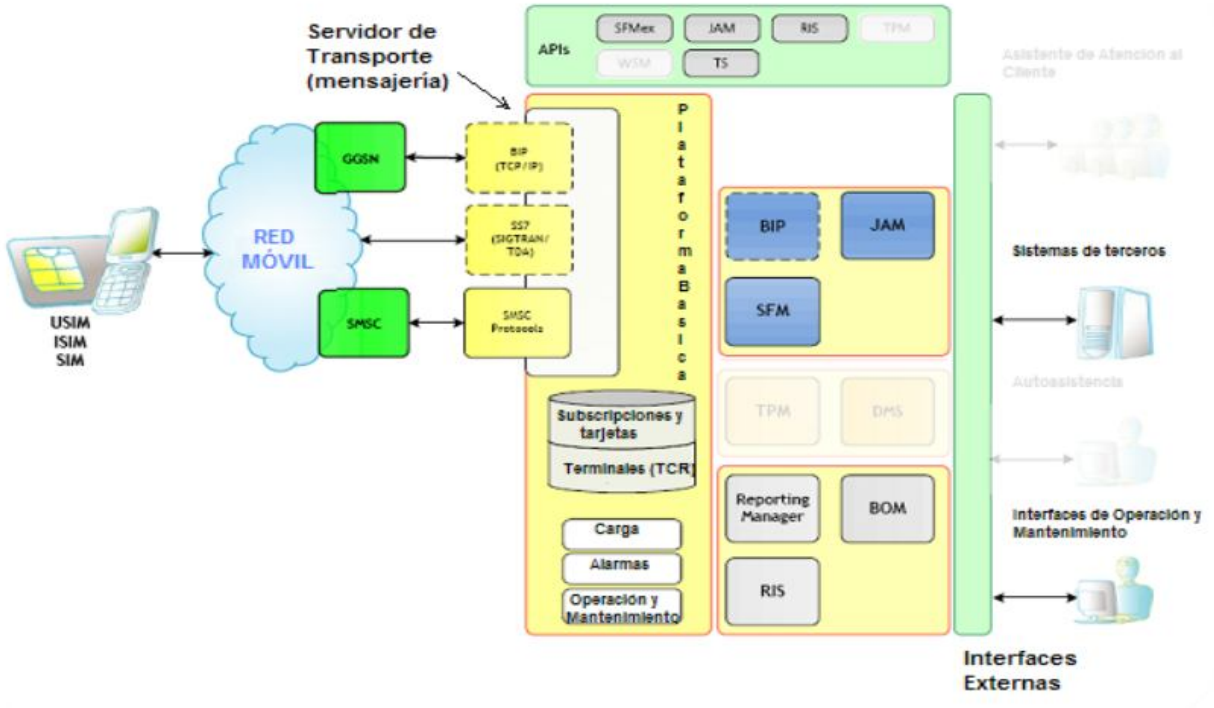


Figura 3.3. Arquitectura de la plataforma para gestión de tarjetas SIM, incluyendo componentes opcionales (rayados) y comunes

3.5.1 Gestión Remota de Archivos (RFM): SFM Server

El SIM File Management Server provee funciones para:

Formatear mensajes OTA de acuerdo con el protocolo OTA adecuado.

- Mantener el contenido de archivos de la descarga OTA en almacenamiento temporario hasta que la descarga OTA sea concluida con éxito y actualizar la base de datos DP para reflejar los cambios.
- Colas / buffer configurables para garantizar carga continua en el SMS-C. El valor de cola puede ser definido de acuerdo con la capacidad del canal SMS-C.
- Una Prueba-de-Recepción puede ser solicitada para recepciones de mandos de ejecución (U)SIM.
- Cancelación de solicitudes de descarga (en caso de que sea soportado por el SMS-C).
- Carga de datos en-el-aire (*Over-The-Air*) de archivos contenidos en la tarjeta (U)SIM. (Solamente para tarjetas (U)SIM habilitadas para PoR)
- Envío de SMs en *pure text* (texto puro).
- Activación y desactivación de suscripciones. Descarga de parámetros de suscripción y alimentación de informaciones de suscriptores en la base de datos.

El SFM Server recibe los pedidos de servicios OTA de los clientes. El SFM Server entonces verifica si los pedidos están correctos y transforma los pedidos de servicios OTA en mensajes cortos. La estructura de estos cortos mensajes es realizada de acuerdo con el estándar 3GPP TS 23.048 RFM o de acuerdo con el protocolo OTA específico del suministrador de SIM.

El SFM Server mantiene una imagen de las tarjetas (U)SIM en su base de datos.

La imagen es continuamente actualizada para reflejar todos los cambios que sean configurables por archivos en la (U)SIM.

La arquitectura del SFM Server permite un gran volumen de usuarios, ya que está basada en una plataforma comprobada para servicios de transacciones críticas.

El software del servidor puede ser configurado para manejar varios miles de clientes simultáneos.

El SFM Server utiliza los recursos de O&M centrales del DP Basic Framework para funciones tales como la emisión de registros de eventos para eventos importantes, alarmas, cuando ocurren errores, y generación de informaciones estadísticas. El SFM Server almacena varias imágenes de las tarjetas (U)SIM e informaciones de transacciones de descarga, incluyendo:

- El contenido de cada (U)SIM registrado durante la importación de datos de pre-personalización y pedidos OTA posteriores.
- El estado de los pedidos de servicios OTA. La información de estado es continuamente actualizada por notificaciones del SMS-C, de manera que clientes puedan pedir las informaciones de estado correctas.

La plataforma puede ser consultada cuanto a:

- Las actuales informaciones de imagen de la tarjeta (U)SIM.
- El histórico de pedidos del (U)SIM, para mantener un registro de cambios de estado.

Es posible consultar pedidos de servicios con varios criterios de búsqueda diferentes; tales como:

- Usuario (aplicación personalizada que envía el pedido de servicio).
- Tipo de pedido (descarga, carga y SM de *pure text).*
- Dirección del suscriptor (MSISDN, IMSI e ICCID).
- Pedir un identificador, como un ID único, o pedir intervalos de identificadores.
- Estado (continuo, expirado y suministrado).
- Informaciones detalladas del pedido, tales como estado de cadena y estado de SM, utilizando el identificador único de pedidos.

El SFM Server también puede ser utilizado para obtener informaciones estáticas sobre cada tarjeta (U)SIM, así como informaciones comunes de (U)SIM (perfil de tarjeta) y puede ser consultado cuanto a:

- Informaciones de tarjeta (U)SIM, tales como:
    - Dirección del suscriptor (MSISDN, IMSI y ICCID)
    - Nombre del perfil de la tarjeta que utiliza la dirección del suscriptor como identificador
- Informaciones sobre el perfil de la tarjeta, tales como:

- Máscara, chip, suministrador de SIM
- Protocolo SFM
- Descripción
- Tamaño de memoria
- Gap máximo de contador
- Lista de aplicaciones SIM que usan un nombre de perfil de tarjeta como identificador

- Informaciones de aplicaciones SIM de la lista de aplicaciones SIM del perfil de la tarjeta, tales como:
  - Tar, Pid, Dcs
  - Tipo de seguridad
  - AID
  - Lista de archivos SIM

Para que una aplicación SIM itere con la lista de aplicaciones SIM o busque la lista de aplicaciones SIM utilizando el nombre de la aplicación SIM como el identificador

- Informaciones de archivos SIM de la lista de aplicaciones SIM de los archivos de la tarjeta, tales como:
  - Tipo de archivo, ruta e id de archivo
  - Tamaño de registro, número de registros

- Imágenes guardadas

Para buscar un archivo itere por la lista de archivos SIM o consulte la lista de archivos SIM utilizando la ruta de archivo y el ID de archivo como identificador

3.5.2 API de integración (SFMex API)

El API SFMex provee funcionalidad para actualizar y leer los contenidos de un archivo OTA para todas las tarjetas almacenadas en SFM. Esto es alcanzado creándose una de las requisiciones disponibles (descarga de archivo, carga de archivo, descarga de comando etc.) y se envía la requisición para el servidor SFM. La interfaz también provee otras funcionalidades permitiendo otras clases de requisiciones como: cancelar una requisición OTA, buscar imagen de archivo, buscar información de tarjeta (U)SIM, buscar informaciones de perfil de tarjeta, consultar status de una requisición etc.

La aplicación que utiliza el API SFMex puede ser notificada cuando una requisición OTA cambia de status oyendo por eventos del API. Otros eventos están también disponibles con las funcionalidades de informar el estado del servidor SFM como conectado, desconectado, base de datos desconectada, congestionamiento etc. [16]

---

[16] Guía de programación API, Doc. No. 10542-123 Revisión: A. 2005-09-28,Smartrust

- ***Estándares Soportados***

- 3GPP TS 11.11 Especificación de la interfaz tarjeta SIM – Equipo Terminal (SIM –ME), versión 8.11.0
- 3GPP TS 51.011 de la interfaz tarjeta SIM – Equipo Terminal (SIM - ME) interface, versión 4.10.0
- GSM/ANSI-136 SIM especificación, *Phase 1*+, versión 5.1
- Especificación SIM para terminales duales PCS/AMPS/*Roaming* dentro de una misma red. V.3.4.
- Especificación PCN de terminal común versión 4.2 (CPHS *phase* 2). V4.2
- 3GPP TS 31.102 Especificación técnica de grupo de terminales, Característica de aplicaciones para, versión 4.11.0
- 3GPP TS 23.048 V5.8.0, Mecanismos de seguridad para aplicaciones *toolkit* (U)SIM
- 3GPP TS 11.14 versión 8.15.0, Especificación de las aplicaciones SIM *tool kit* – Terminal móvil (SIM - ME)
- International Standard ISO/IEC 9797, Mecanismo de integridad de datos utilizando una función de criptografía con un algoritmo de cifrado.
- ETSI TS 101 220 V5.0.0, ETSI Sistema de numeración para proveedores de aplicaciones de telecomunicaciones.
- ETSI TS 102 221 V6.3.0, interfaz de Terminal UICC; características físicas y lógicas.

- Especificación de tarjeta con plataforma, versión 2.0.1 (see http://www.globalplatform.org/)
- 3GPP TS 31.111 V6.0.0 Especificación técnica de grupo de terminales, USIM *Application Toolkit* (USAT)
- 3GPP TS 31.103 V6.6.0, Características de aplicaciones multimedia IP de SIM (ISIM)

- ***Especificaciones 3GPP***

- TS 11.11 v.8.11.0 – Especificaciones SIM.
- TS 51.011 v.4.10.0 – Especificaciones SIM con nombres cambiados, para seguir la nueva política de nomenclatura de 3GPP.
- TS 31.102 v6.4.0 – Especificaciones USIM.

- ***Archivos (U)SIM Soportados***

Tabla 3.1. Listado de archivos soportados por la plataforma de gestión de tarjetas SIM

Abreviación	Nombre de archivo	Ruta TS11.11-v.8.11.0	Ruta TS51.011-v4.10.0	Ruta TS31.102-v4.11.0
IMSI	International Mobile Subscriber Identity	3F007F206F07	3F007F206F07	7FFF6F07
OPL	The Operator PLMN List	N/A	3F007F206FC6	7FFF6FC6
PNN	PLMN Network Name	N/A	3F007F206FC5	7FFF6FC5
PLMNSEL	PLMN Selector	3F007F206F30	3F007F206F30	N/A
HPPLMN	Higher Prority PLMN Search Period	3F007F206F31	3F007F206F31	7FFF6F31
ACMMAX	ACM Maximum Value	3F007F206F37	3F007F206F37	7FFF6F37
SST	SIM Service Table	3F007F206F38	3F007F206F38	N/A
UST	USIM Service Table	N/A	N/A	7FFF6F38
ACM	Accumulated call meter	3F007F206F39	3F007F206F39	7FFF6F39
SPN	Service Provider Name	3F007F206F46	3F007F206F46	7FFF6F46
ACC	Access Control Class	3F007F206F78	3F007F206F78	7FFF6F78
FPLMN	Forbidden PLMNs	3F007F206F7B	3F007F206F7B	7FFF6F7B
EMLPP	Enhanced Multi Level Pre-emption and Prio	3F007F206FB5	3F007F206FB5	7FFF6FB5
BDN	Barred Dialling Numbers	3F007F106F4D	3F007F106F4D	7FFF6F4D
SDN	Service Dialling Number	3F007F106F49	3F007F106F49	7FFF6F49
SMSP	Short message service parameters	3F007F106F42	3F007F106F42	7FFF6F42
MSISDN	Subscriber Telephone Number for Mobile Subscription	3F007F106F40	3F007F106F40	7FFF6F40
FDN	Fixed Dialing Numbers	3F007F106F3B	3F007F106F3B	7FFF6F3B
ADN	Abbreviated Dialling Numbers	3F007F106F3A	3F007F106F3A	7FFF5F3A4F3A

Abreviación	Nombre de archivo	Ruta TS11.11-v.8.11.0	Ruta TS51.011-v.4.10.0	Ruta TS31.102- v4.11.0
CBMI	Cell Broadcast Message Identifier	3F007F206F45	3F007F206F45	7FFF6F45
CBMID	Cell Broadcast Message Identifier for Data Download	3F007F206F48	3F007F206F48	7FFF6F48
CBMIR	Cell Broadcast Message Identifier Range Selection	3F007F206F50	3F007F206F50	7FFF6F50
ECC	Emergency Call Codes	3F007F206FB7	3F007F206FB7	7FFF6FB7
MMSICP	MMS Issuer Connectivity Parameters	N/A	3F007F206FD0	7FFF6FD0
MMSUP	MMS User Preference	N/A	3F007F206FD1	7FFF6FD1
MMSUCP	MMS User Connectivity Parameters	N/A	3F007F206FD2	7FFF6FD2
MBI	Mailbox Identifier	N/A	3F007F206FC9	7FFF6FC9
MBDN	Mailbox Dialling Numbers	N/A	3F007F206FC7	7FFF6FC7
SPDI	Service Provider Display Information	N/A	3F007F206FCD	7FFF6FCD
PLMNwAct	User Controlled PLMN Selector With Access Technology	3F007F206F60	3F007F206F60	7FFF6F60
OPLMNwAct	Operator Controlled PLMN Selector With Access Technology	3F007F206F61	3F007F206F61	7FFF6F61
HPLMNwAct	HPLMN Selector With Access Technology	3F007F206F62	3F007F206F62	7FFF6F62

Es importante observar que cualquier otro tipo de archivo que no sea mencionado, puede ser actualizado (si tienen permiso para ser modificados a través de OTA) a través de una descarga genérica de APDU.

- ***Tarjetas (U)SIM Soportadas***

Las tarjetas compatibles con las especificaciones de 3GPP TS 03.48/3GPP TS 23.048 para RFM – Remote File Management – son totalmente soportadas por: [17]

Tabla 3.2. Listado de proveedores de tarjetas SIM que interactúan con la plataforma OTA

[17] GSM 03.40 Servicio de Mensajería Corta

Suministrador SIM	Especificaciones de protocolos OTA propietarios soportadas
Gemplus	ESMS Formatting Library Programming Guide Version 2.10 – January 1999 Valid for GemXplore (ESMS V1) and GemXplore98 (ESMS V2), and requires that the customer purchase the relevant library ESMS V1/2 from Gemplus.
Oberthur	SIM PHASE 2 With Data Download Functional Specification DOC: 190, 12NC: 4311 240 00901, Issue: AH
Giesecke & Devrient (G&D)	OTASS SIM Development Specification Step 2 Version 2.7 – 970320 OTASS/SIM Application Toolkit SIM Development Specification (v 3.5 1999-02-11). Is compatible with 2.7. (Refresh and Response commands is not supported via SFM)
ORGA	Data Download Specification for ORGA Phase 2 SIM Version 1.2.3 – 970709
Schlumberger	OTAC Library V1.8 User Manual Version 4.0 – 990520, Ref.: MRDMUT973023 OTAC LOW LEVEL Services User Guide Version 5.0 – 981117, Ref.: MSCPTH983336
Schlumberger SIMERA	SIMERA Technical Specification OTA Protocol Version 3.0 – 980817, Ref: MRDSTG983025
SETEC	GSM OTA Support, SMS messages, Technical description Version 1.5 – 980527
BULL	External functional specification of the GSM card v2.0 in utilization phase Version 2.0 – 980603, Drawing No.: 76 664 132 OtaV2.0
INCARD	Technical Specification for the OTA Application Feature of the Incard GSM card, Version 1.0 – 980703

Suministrador SIM	Especificaciones non-estándares de protocolos RFM 03.48/23.048 soportadas
DZ (XPonCard, Graphium)	DZSIM 3.0 Documentation Remote File Management Preliminary Draft, Version 00-03-10
XPon	DZSIM 3.0 Technical Handbook (Preliminary 1999-08-10). Normally the DZ library above should be used.
Giesecke & Devrient (G&D)	OTASS V 4.0 SIM Development Specification, Revision 1.0, 010718
Gemplus	(reference document not available, support implemented according to 03.48/23.048 standard)
Schlumberger	(reference document not available, support implemented according to 03.48/23.048 standard)
Logos	Remote File Management for the Logos SIM iMP Doc nb:LSC-IMP-ICD-002, Ver:1.3, 7 Maj 2001
Prism	SIM Technical Specification, Ref: PR-C1-Dat-9, ver. 1.6, September 2001
SAGEM	OTA SIM CARD EXTERNAL SPECIFICATION SIM V3, Doc ref. SCT U34 SIM SPF 022, version C, Date 24/09/01

3.5.3 Gestión Remota de Applets (RAM): JAM Server

Las funcionalidades implementadas por el JAM Server son suministradas mediante varias herramientas, tales como el manejo de órdenes de actualización de aplicaciones por batch, el asistente de servicio y el DP administrador.

Este servidor provee la capacidad de gestionar Java™ Card applets en la tarjeta (U)SIM.

Este JAM Server formatea los mandos RAM de acuerdo con las especificaciones RAM.

Debido a que existen aplicaciones propietarias de los más importantes suministradores de (U)SIM es importante indicar que el servidor soporta dichas aplicaciones.

El JAM Server maneja, de manera transparente, diferencias que puedan existir en implementaciones del ambiente de ejecución Java Card, así como los mandos de Remote Applet Management.

Java™ Card applets pueden ser applets independientes del kit de herramientas Java™ SIM o plug-ins Java utilizados. El JAM Server provee funciones para la gerencia de Java Card applets, tales como:

- Descargas en-el-aire (OTA) de mandos RAM formateados de acuerdo con el estándar adecuado.
- Cancelación de solicitaciones de descarga (caso soportada por el SMS-C).
- Carga de estados de tarjeta, datos de *applets* y memoria disponible del contenido de la tarjeta (U)SIM en-el-aire (OTA).

El servidor JAM recibe los pedidos de servicios de descarga de los clientes utilizando el JAM API. El servidor JAM verifica si los pedidos están correctos y crea mandos RAM de acuerdo con el estándar configurado.

El Servidor JAM mantiene una imagen de las tarjetas (U)SIM en su repositorio (U)SIM. El imagen es continuamente actualizado para reflejar todos los cambios a la (U)SIM. El servidor JAM utiliza los recursos O&M centrales del DP Basic Framework para funciones tales como la emisión de registros de eventos para eventos importantes, alarmas, cuando ocurren errores, y generación de informaciones estadísticas. El servidor JAM almacena varias imágenes de (U)SIM e informaciones de transacciones de descarga, incluyendo:

- El contenido de cada (U)SIM registrado durante la importación de datos de pre-personalización y pedidos OTA posteriores.
- El estado de los pedidos de servicios OTA. La información de estado es continuamente actualizada por notificaciones del SMS-C, de manera que clientes puedan pedir las informaciones de estado correctas.

La plataforma puede ser consultada cuanto a:

- Informaciones actuales de imágenes (U)SIM, tales como definiciones disponibles de *applets* y EEPROM.
- El histórico de pedidos del (U)SIM, para mantener un registro de cambios de estado.
- Informaciones sobre *applets* y paquetes de *applets* disponibles para descarga para una tarjeta específica, tales como un identificador de aplicación, el tamaño de *applets* y parámetros de instalación.
- Utilización [18]

[18] JAM Description, Doc No. MPM06:0031, 2006, Smartrust

3.5.4 Comandos RAM

El servidor JAM soporta las siguientes funcionalidades RAM. Para informaciones detalladas sobre comandos RAM específicos, consulte el estándar adecuado.

- Paquete de descarga con Java *applets* (INSTALL para carga + LOAD)
- Eliminación del paquete con Java *applets* (DELETE)
- Activación del Java *applet* en la tarjeta después de la descarga del paquete (INSTALL para instalación + INSTALL para poner disponibles)
- Instalación del Java *applet* en la tarjeta (INSTALL para instalación)
- Desactivar Java *applet* (DELETE)
- Bloqueo/desbloqueo de Java *applets* (SET STATUS)
- Recuperación de parámetros de *applets* (GET DATA)
- Recuperación de estados de tarjeta (GET STATUS)

3.5.5 Gestión Transparente de Distintos Java™ Cards

A pesar de la afirmación “escriba-una vez y ejecute en cualquier lugar” (write-once run-anywhere‟) existente en medio de la Java Card, no todas implementaciones de tarjeta en Java son totalmente interoperables.

Tarjetas de diferentes proveedores pueden portarse de maneras diferentes y poseer diferentes capacidades y funciones. Esto resulta, desafortunadamente, en el hecho de que un Java applet específico no pueda ser compilado una sola vez y ejecutado en cualquier tarjeta sin modificaciones.

El servidor JAM soluciona este problema al definir paquetes de applets en un nivel lógico.

Estos paquetes lógicos pueden contener una o más implementaciones físicas de los Java applets conectados a uno o más perfiles de tarjeta. El servidor JAM selecciona la implementación correcta, de acuerdo con el perfil de la tarjeta que está realizando la descarga.

3.5.6 API de integración: JAM API

Los servicios implementados por el servidor JAM son proveídos a aplicaciones clientes a través de la JAM API. La interfaz de comunicación entre la JAM API y el servidor JAM es basada en CORBA.

La interfaz CORBA es implementada usando JacORB que soporta al code set CORBA 2.3.

La seguridad del canal de comunicación es garantizada por el uso de un soporte embebido a IIOP sobre SSL en JacORB.

La autenticación usada para llamar al servidor es basada en parámetros de username/password para el usuario creado en DP Administrator.

El servidor JAM dispone de un mecanismo embebido para control de flujo para protegerse de recibir una sobrecarga e asegurar disponibilidad. La JAM API señaliza a las aplicaciones clientes para reducir la carga cuando necesario.[18]

- ***Estándares Soportados***

El mecanismo de RAM (Remote Applet Management) soportado por la plataforma está especificado en:

- ETSI SCP TS 102 226
- 3GPP TS 31.116

[18] JAM Description, Doc No. MPM06:0031, 2006, Smartrust

- 3GPP TS 23.048
- 3GPP TS 03.48

La API SIM de las tarjetas que soportan a JavaTM está especificada en 3GPP TS 43.019 Stage 2 (antigua 3GPP TS 03.19). Estas especificaciones se refieren a las especificaciones SUN JavaTM Card.

- ***Tarjetas (U)SIM Soportadas***

Las tarjetas SIM soportadas incluyen, pero no están limitadas, a:

- Gemplus GemXplore Xpresso v3.2 64k JAVA OS
- Oberthur SIMphonIC v3 64k
- Incard Mokard 64k
- Axalto Simera v3.3 64k
- G&D STARSIM JAVA 64k

El listado de tarjetas SIM soportadas incluye tarjetas de los proveedores Axalto, Bantry Technologies, Gemalto, Gemplus, G&D, Incard, I'M technologies, Logos Smart Card, Microeletrônica, Net-1 Prism, Oberthur, Sagem Orga y Watchdata Systems.

3.5.7 Gestión de Campañas: BOM

La gestión para actualización de aplicaciones por batch “Batch Order Manager” (BOM) es una aplicación de la Plataforma que permite actualizaciones en lotes flexibles y eficaces de tarjetas SIM y USIM.

El BOM fue proyectado para atender las demandas cada vez mayores de desempeño de actualizaciones remotas de grandes series de tarjetas (U)SIM, utilizando la Plataforma de Gestión de Terminales. El producto BOM posee la capacidad de ejecutar descargas en-el-aire (OTA) a un subconjunto fácilmente definido de suscriptores, utilizando las funcionalidades del servidor DP SIM File Management (SFM).

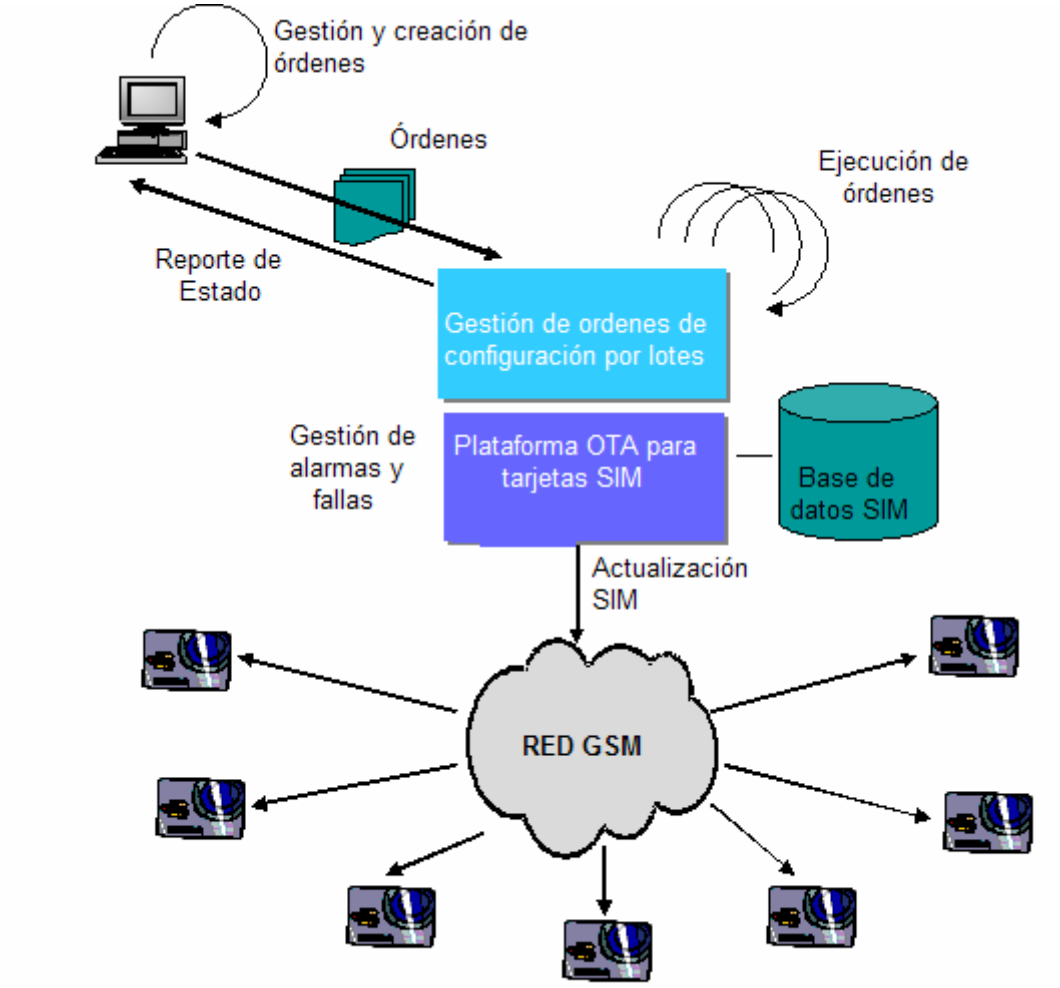


Figura 3.4. Visión general de BOM

El BOM utiliza archivos para obtener entradas y producir salidas para sistemas externos. La interfaz de archivos es utilizada para iniciar pedidos de trabajo en lotes y obtener informaciones sobre descargas. Una interfaz web que provee funcionalidades de supervisión y configuración. Esta interfaz web también puede ser utilizada para crear pedidos de trabajo para gerencia de roaming. BOM tiene funcionalidades para soportar largas actualizaciones para toda la base de usuarios en una operación, sin cualquier limitación o restricción. La base de datos de BOM puede también ser integrada a bases de datos externas con

informaciones de suscriptores para una selección más eficiente de suscriptores a ser actualizados. Los casos de uso incluidos en este producto son: [19]

- Actualización de archivos
    - BOM puede ser usado para actualizar cualquier archivo remotamente actualizable en la tarjeta (U)SIM para cambiar algún servicio.
    - Ejemplos:
        - Actualización de números de agenda para servicio de atención al cliente, correo de voz etc
        - Actualización del nombre de proveedor de servicios (SPN – *Service Provider Name)* mostrado en la pantalla del terminal
        - Actualización de una lista de redes preferidas
- Gestión de *applets*
    - BOM tiene una extensión opcional para gestión de *applets* Java que está incluida en esta propuesta.
    - Más informaciones en la sub-sección “Un asistente básico que crea un lote, paso a paso, utilizando descripciones anteriores de cambios en archivos.
    - BOM para gestión de *applets* Java”
- Envío de configuraciones de terminales

[19] Descripción BOM - Opción JAM , Doc No. MPM06:0010, 2006, Smartrust

- BOM tiene una extensión opcional para envío de configuraciones de terminales que está incluida en esta propuesta.

- ***Selección de suscriptores***

La selección del (U)SIM puede ser realizada de varias maneras:

- Un archivo de texto con una lista de MSISDN, ICCID o IMSI para actualización.
- Gama de MSISDN, ICCID o IMSI.
- Selección por búsqueda SQL, por ejemplo, grupos de SIM o suscriptores o perfiles de SIM.

- ***Lista de exclusión***

Una lista de exclusión (blacklist) puede ser definida en el Batch Order Manager. Los suscriptores en esta lista no recibirán descargas en lotes.

- ***Acción de actualización***

Las siguientes acciones pueden ser incluidas en una actualización:

- Actualización de cualquier archivo actualizable OTA en el SIM o USIM.
- Envío de un SM de texto
- Ejecución de un mando de base de datos (SQL *Command*)

Varias actualizaciones para diferentes archivos en el (U)SIM pueden ser ejecutadas en la misma acción de actualización.

- ***“Ping” SM***

Este recurso permite el envío de un "ping" a un suscriptor antes de la creación de las demás SM's para descarga - SM's que expirarían o fallarían.

El recurso es principalmente direccionado a grandes descargas, tales como 5-50 SM/descarga y aumentará significativamente el desempeño.

El recurso “ping” introduce un punto de verificación en la descarga, el cual no será pasado hasta que un estado de entrega sea recibido.

Si el estado recibido ha fallado o expirado, las demás SM's no serán enviadas al suscriptor. El “ping” SM puede, por lo tanto, ser utilizado para carga útil.

- ***Acciones dependientes de resultados***

De acuerdo con el resultado de mando de descarga (Éxito, Falla o Expirado), mandos específicos de base de datos y transmisiones de texto SM pueden ser especificados.

- ***Refresh***

El trabajo en lotes puede especificar que tipo de refresh va a ser realizado después de una descarga exitosa. Los siguientes tipos de refresh, como especificado en el 11.14, son posibles:

- Inicialización del SIM
- Inicialización del SIM y Notificación Completa de Cambio de Archivo
- Reset del SIM

Note que la funcionalidad depende del soporte a la tarjeta (U)SIM y el terminal.

- ***Ruteamiento de SMS-C***

El canal SMS-C de destino puede ser especificado en la descarga. Esto posibilita seleccionar un SMS-C específico para una descarga específica.

- ***Planificación Avanzada***

Los mecanismos de planificación incluyen la retransmisión de actualizaciones expiradas. Varias iteraciones pueden ser especificadas con diferentes periodos de vigencia, prioridades y umbrales de éxito. Las iteraciones serán ejecutadas hasta que el umbral sea alcanzado o hasta que la última iteración sea ejecutada.

Ejemplo: La creación de un trabajo que intentará enviar descargas a un grupo específico de suscriptores, una vez al día, con un periodo de validez de 1 hora, durante 2 semanas o hasta que 95% de los suscriptores hayan sido actualizados con éxito. El concepto de iteración vacía las colas SMS-C / HSMP y provee un mejor desempeño total. Varias iteraciones con pequeños periodos de validez pueden ser enviadas en lugar de una iteración con un largo periodo de validez.

- ***Control de flujo***

Para controlar la velocidad de descarga del BOM, existe disponible un mecanismo avanzado de control de flujo. Este mecanismo posibilita la configuración de las velocidades de descarga. Esquemas de límite de velocidad definen la velocidad de salida para cada hora del día. Además, el esquema de límite de velocidad puede ser configurado de manera diferente, de acuerdo con el día de la semana o con fechas específicas. Esto posibilita la optimización de los recursos de descarga de sms/SMS-C.

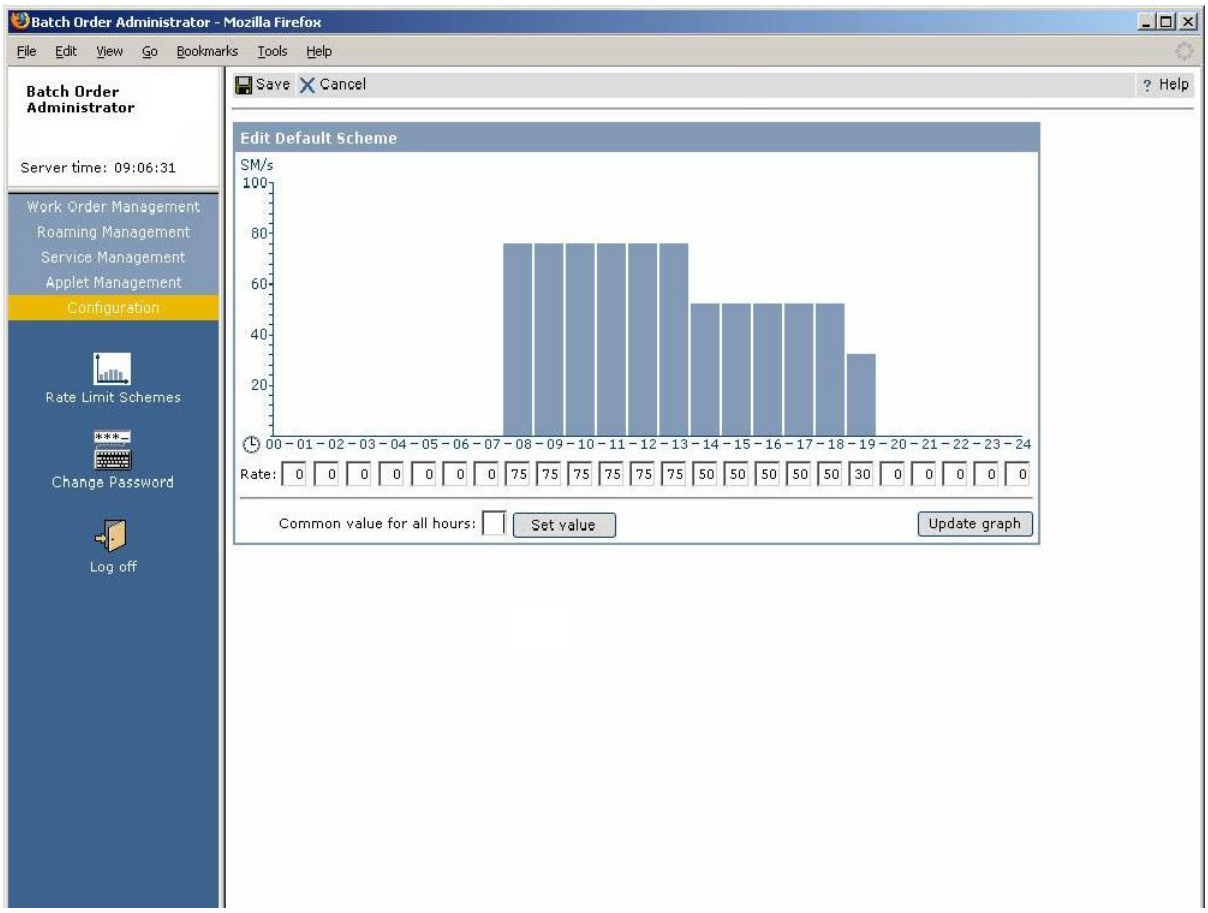


Figura 3.5. Ejemplo de un control de flujo mostrado en el Batch Order Administrator

La tasa puede ser definida como nivel total de sistema. Trabajos individuales pueden tener prioridades diferentes.

- ***Descargas múltiples***

El BOM soporta la ejecución simultánea de múltiplos trabajos en lote. El sistema puede también ser configurado para soportar trabajos continuos, en los cuales las selecciones son redefinidas a cada iteración.

- ***Prioridad***

El BOM soporta tres tipos de niveles de prioridad diferentes para trabajos en lote continuos, son los niveles bajo, medio y alto. La velocidad de envío es calculada automáticamente a partir de esas prioridades. La prioridad puede ser alterada para trabajos continuos.

- ***Estadísticas***

Para cada descarga de archivo especificada, se estima el número de SM's. Esta estimación es utilizada como la base para las estadísticas. Estadísticas de entrega en tiempo real están disponibles para cada lote en ejecución. Varias estadísticas son agregadas en un archivo de estadísticas, para cada lote ejecutado. Los datos estadísticos son generados en un archivo de texto.

- ***Notificación automática***

Al final de cada trabajo en lote, se envía un correo de notificación. Este correo incluye informaciones estadísticas.

- ***Recuperación***

Un procedimiento de recuperación en tiempo de ejecución es aplicado para proteger las funcionalidades BOM contra fallos de servidor o descarte impropio. En la recuperación, solamente serán enviadas las descargas anteriores incompletas.

- ***Asistente Básico***

Un asistente básico que crea un lote, paso a paso, utilizando descripciones anteriores de cambios en archivos.

3.5.8 BOM para gestión de applets Java

La opción JAM para BOM tiene funcionalidades para creación de tareas para actualización remota (OTA) de Java applets. Los siguientes casos de uso son soportados:

- Descarga de paquetes conteniendo *applets* Java
- Instalación de *applet* descargado
- Gestión de *applets* instalados (*status settings*)

- Borrado de paquetes con *applets* Java

Descargas pueden ser especificadas en una descripción de cambio de archivo (File Change Description) o utilizando el asistente de tarea en lote (Batch Job Wizard).[19]

Las siguientes acciones son soportadas:

Tabla 3.3: Acciones soportadas por BOM

Carga de paquetes	Descarga de *applets* Java hacia la tarjeta SIM
Instalación de *applets* **Activación de *applets***	Instalación de una *applet* descargado
Remoción de paquetes *lapplets*	Remoción
Cambiar *applet*	Cambiar el status para un *applet* instalado

3.6 Gestión de Terminales GSM

Es una solución integrada que trata de la diversidad actual de terminales y suscriptores. Esta plataforma aprovecha módulos y comunes para posibilitar una rápida implementación.

[19] Descripción BOM - Opción JAM , Doc No. MPM06:0010, 2006, Smartrust

Figura 3.6. Ejemplo Visión general de la gestión de terminales

La zona oscura en la figura 3.7 anterior ilustra tres estructuras de la plataforma para gestión de terminales. La Delivery Platform Layer es la plataforma que provee protocolo, conectividad y funciones operacionales. Estos incluyen conectividad SMS-C, Autenticación, Control de Acceso, funciones de Mantenimiento, Gerencia de Configuraciones, Gerencia de Fallos, Manejo de Alarmas, Servicios para Tarifación, compartición de carga de tráfico y control de flujo, los módulos de los extremos de la figura representan por un lado, el ambiente del usuario final para quién las configuraciones se realizarán con un mínimo de interacción y por otro lado está el módulo del ambiente del operador en donde se gestionarán las campañas de actualización de terminales vía interfaz aire..

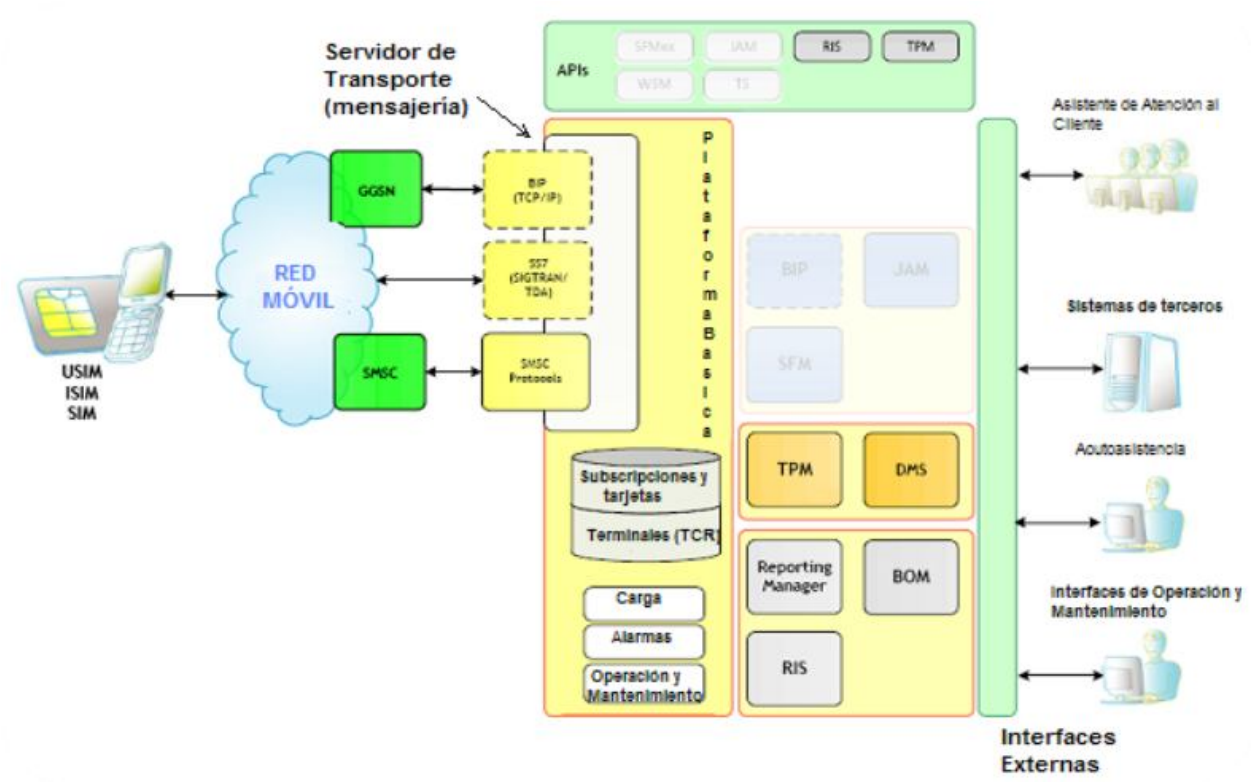


Figura 3.7. Arquitectura de la integración de la plataforma de gestión de terminales con componentes opcionales

Esta arquitectura contiene los siguientes componentes principales:

- El DM Server (DMS) provee una interfaz común para una gestión totalmente automatizada de dispositivos móviles. Puede ser utilizado para detectar automáticamente nuevos terminales o cambios de terminales suministrados por emulación de instancias EIR o clientes SIM. Inicia la ejecución del aprovisionamiento de configuraciones basado en condiciones tales como grupo de suscriptores, tipo de suscriptor y tipo de dispositivo.

- El *Terminal Provisioning Manager* (TPM) provee la gestión de configuraciones de terminal independientemente del suministrador del terminal y de estándares de aprovisionamiento de los suministradores de terminales más importantes.

Un Terminal Capabilities Repository (TCR) que mantiene informaciones sobre las capacidades del terminal, sobre como identificar el terminal (tanto para configuraciones automáticas como para específicas), y un protocolo pertinente para el aprovisionamiento OTA de configuraciones de dispositivos.

La plataforma para gestión de terminales ofrece varias maneras de aprovisionar el terminal de un suscriptor. Existen cuatro tipos de aprovisionamiento:

- Aprovisionamiento automatizado, en el cuál configuraciones son enviadas después de recibida una señal del TSD;
- Aprovisionamiento de auto mantenimiento, en el cuál los suscriptores piden configuraciones por diferentes interfaces;
- Aprovisionamiento asistido por la ayuda al cliente, en el cuál el centro de ayuda al cliente inicia el aprovisionamiento del terminal del suscriptor;
- Aprovisionamiento en lotes, el en cuál la operadora inicia el aprovisionamiento de los terminales de un grupo específico.

Para soportar esta diversidad de métodos de aprovisionamiento, la plataforma incorpora el proceso donde el flujo de MDM, posee un sistema de Detección de Eventos, Evaluación de Eventos, Aplicación de Lógica de Negocios y Ejecución de Acciones de Gerencia soportadas en todas las etapas por los repositorios centrales, es utilizada en todas las aplicaciones MDM implementadas. También ofrece una interfaz administrativa avanzada por la cual la operadora puede mantener la plataforma, personalizar perfiles de terminales, personalizar informaciones de usuarios, revisar reportes y estadísticas, etc.[20]

[20] OTAP-1100-FD, 2001, LOGICA Mobile Networks Limited

3.6.1 Servidor para Gestión de Terminales (DMS)

El servidor para gestión de terminales se encuentra diseñado para obtener alto desempeño y podrá manejar hasta 35 pedidos de aprovisionamiento por segundo, dependiendo de los casos de aprovisionamiento automático. El componente contiene cuatro áreas lógicas de funcionalidad, cada una con su objetivo principal, optimizadas para las características específicas de la responsabilidad funcional.

Figura 3.8. Arquitectura Rubros funcionales del Device Management Server. El componente rayado es opcional.

3.6.2 La función Automatic Device Configuration (ADC)

La ADC soporta métodos diferentes e independientes para la detección automática de nuevos terminales. Cuando el DM Server recibe un evento, el mismo provee una función de filtro para la detección de cambio de terminal. El filtro procesa las informaciones recibidas del terminal como eventos, y determina si el terminal es conocido y actualmente utilizado en esta suscripción. Para este propósito, la función de filtro utiliza informaciones de identidad de terminal y suscripción almacenadas en la base de datos.

También soporta la función de filtro para eventos recibidos, que puede ser aplicada para eliminar eventos recibidos del procesamiento. El propósito de este filtro es asegurar que solamente los eventos correctos y deseados disparen suministros.

3.6.3 La función "Pre-processing"

Cuando se detecta un cambio de terminales, se realiza la validación de la suscripción y del dispositivo. Una validación común sirve para asegurar que el dispositivo no esté en la lista negra y que la cota de suministro no haya sido excedida. Este es un paso importante de seguridad, y permite que la operadora controle el número de aprovisionamientos automáticos ejecutados por el suscriptor.

3.6.4 La función "Send Settings"

La configuración de terminales es ejecutada por medio del Terminal Provisioning Manager (TPM). Cuando se llega a esta etapa, las configuraciones son enviadas al terminal. Terminal Provisioning Manager (TPM) provee gestión de configuraciones de terminales (Device Configuration) independiente del proveedor del terminal, con soporte a estándares del mercado (OMA, WAP) así como protocolos de aprovisionamiento específicos de proveedor para soportar terminales de todos los suministradores de terminal. TPM provee: gestión de datos de aprovisionamiento en un formato independiente del protocolo; generación en tiempo de ejecución de mensajes de aprovisionamiento de acuerdo con el protocolo de aprovisionamiento OTA apropiado para un terminal específico; histórico de aprovisionamiento de terminales para mantener un registro de los

cambios dirigidos hacia cada terminal; APIs para uso en personalizaciones de TPM.

3.6.5 La función "Post-processing"

El paso "post-processing" (pos-procesamiento) controla las acciones finales que pueden ser realizadas después de la entrega de las configuraciones al dispositivo. Las acciones pueden ser actualizar o activar servicios externos o informar el progreso del aprovisionamiento.

3.6.6 Descripción de las Configuraciones de Terminales Soportadas

La solución para Gestión de Terminales soporta los protocolos de aprovisionamiento OTA más utilizados, posibilitando la implementación de configuraciones en una amplia gama de terminales. La solución contiene una lógica que determina, basada en varias entradas y otras informaciones, cómo y con cuales configuraciones el terminal debe ser aprovisionado, y también gestiona el proceso.

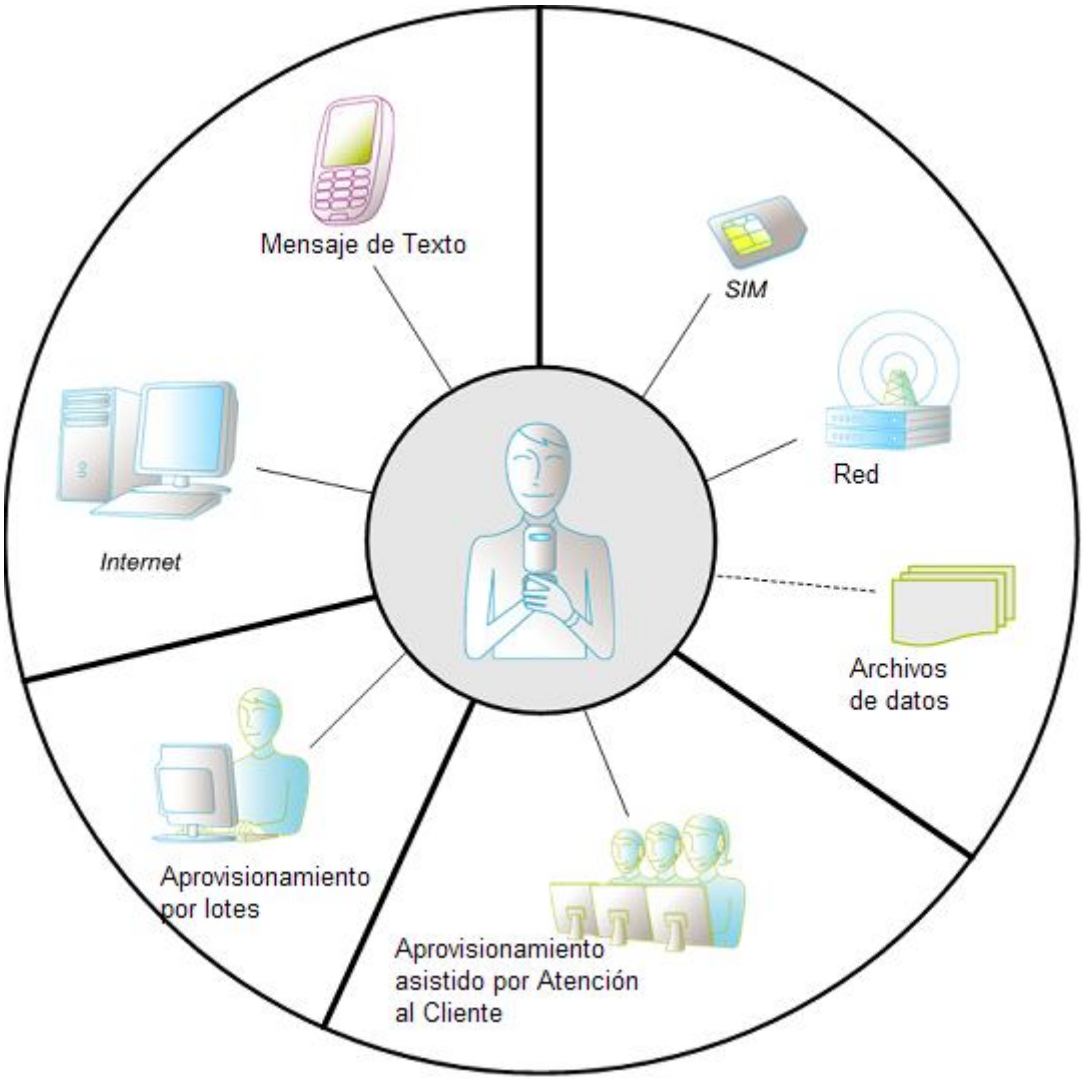


Figura 3.9. Visión general de la funcionalidad de aprovisionamiento de respaldos de terminales soportados.

El diseño utiliza el TPM para ejecutar el aprovisionamiento de configuraciones de terminal, basada en datos del terminal (capacidades, protocolos). Soporta el aprovisionamiento de configuraciones de terminales para una amplia gama de servicios. Las configuraciones incluidas son:

- WAP – Las configuraciones básicas para establecer una conexión con un proxy WAP para navegación o para aprovisionamientos adicionales

- MMS – Configuraciones básicas para establecer una conexión con el MMSC
- WAP *bookmarks* – WAP *bookmarks* específicos incluidos en las configuraciones WAP
- Internet – Las configuraciones básicas de conectividad necesarias para una sesión de internet
- Streaming – Configuraciones necesarias para la conexión a un servidor RFTP streaming

  SyncML DM – Configuraciones necesarias para definir una sesión de gerencia de dispositivos SyncML con un servidor
- SyncML DS – Configuraciones necesarias para establecer una conexión con un servidor de Sincronización/SyncML DS
- E-mail – Configuraciones de servidor de e-mail y de cuenta
- Push to talk over Cellular (PoC) – Las configuraciones básicas necesarias para una sesión “Push to talk over Cellular” (Pulsa y Habla por Móvil)
- Las configuraciones opcionales disponibles son:
- Wireless Village – Las configuraciones básicas necesarias para Mensajes Instantáneas y Presencia, como definidas en las especificaciones de Wireless Village
- WiFi – Configuraciones básicas para accesar una red inalámbrica con el terminal
- SIP – Configuraciones SIP para el cliente SIP del terminal
- ActiveSync – Configuraciones necesarias para definir una sesión de gerencia de dispositivos ActiveSync con un servidor
- Estas configuraciones son suministradas a partir de los siguientes protocolos de aprovisionamiento OTA:
- Nokia/Ericsson Over The Air Settings Specification (OTASS versiones 6.0, 6.5, 6.6, 7.0 y 7.1)
- Openwave Primary Provisioning 2.0
- Smart Messaging 3.0.0

- WAP 2.0 Client Provisioning
- OMA Client Provisioning Versión 1.1
- SyncML Device Management Bootstrap versión 1.1.2
- Software Windows Mobile 2003 y 2003 2a edición para Smartphone y Edición Pocket PC Phone
- Software Windows Mobile 5.0 para Smartphone y Edición Pocket PC Phone
- Software Windows Mobile 6,0 para Smartphone y Edición Pocket PC Phone

3.6.7 Configuración Automática de Terminal a través del Applet de detección de IMEI en la tarjeta SIM

En este caso, un suscriptor cambia a otro terminal y el cambio de terminal es detectado localmente en el SIM por el applet de detección de IMEI. La lógica de este applet ejecuta la evaluación de cambio de terminales en la tarjeta SIM y solamente envía eventos reales de cambio de terminal. Después de detectar un nuevo terminal, el applet enviará un pedido al DP con el IMEI y el MSISDN del suscriptor. Estos serán luego enviados al Gestor de Terminales, que iniciará la lógica de negocios adecuada. La solución enviará las nuevas configuraciones al terminal, si es necesario.

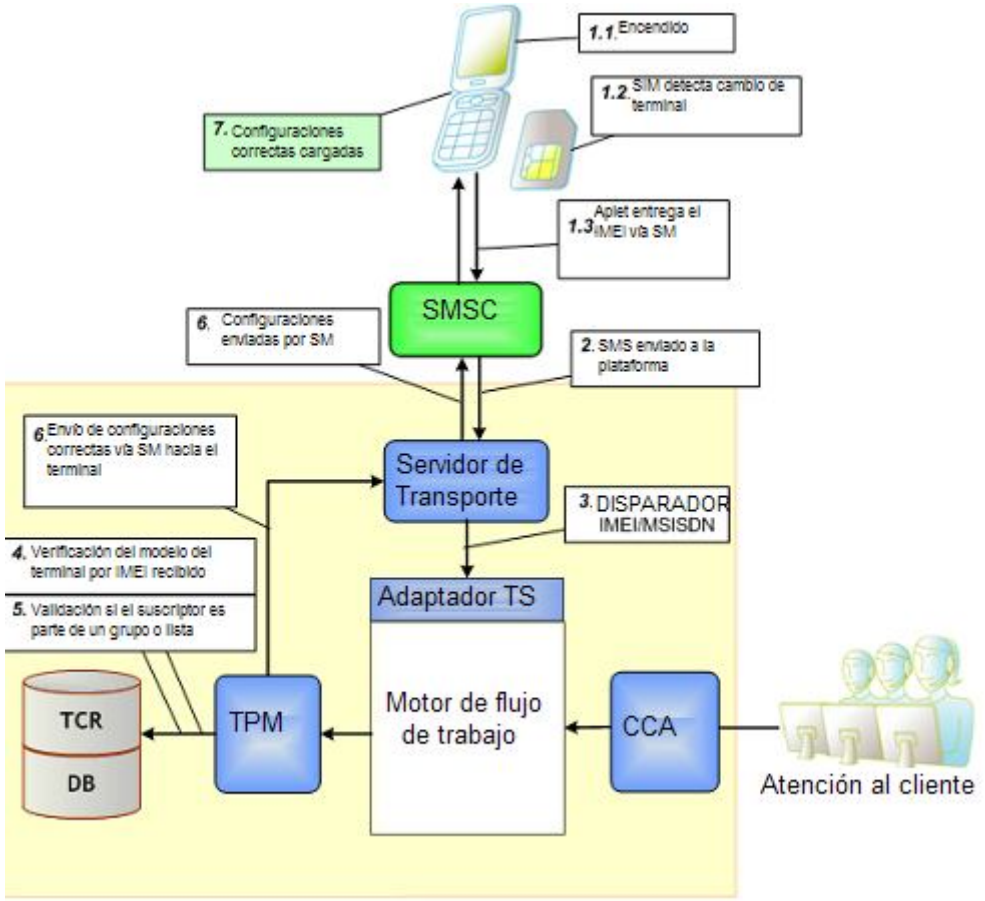


Figura 3.10. Configuración automática de terminales disparada por el applet de detección de IMEI

1. En la inicialización del dispositivo, al identificar que la tarjeta SIM está insertada en un nuevo terminal, el *applet* envía una SM de 8-bit con el MSISDN del suscriptor y el IMEI del terminal actual para la plataforma de gestión de terminales.

2. La plataforma de gestión de terminales recibe la señal SM del SMS-C en una conexión SMPP específica y, a través de un adaptador en su Agente de Mensajes, obtiene el IMEI, el MSISDN y el IMSI a partir de la SM, que serán utilizados para identificar el suscriptor y el terminal a ser configurado. Si el *applet* existente envía el SM como un SM de datos de 8 bit con encabezamiento 23.048, esta mensaje va a ser desempaquetada por el

Transport Server utilizando las llaves de seguridad en la base de datos de DP.

3. El IMEI y el MSISDN son enviados al DMS, que acciona la ejecución del flujo de trabajo ADC en el Mecanismo de Flujo de Trabajo. Este flujo de trabajo coordinará todas las actividades relacionadas al proceso de aprovisionamiento del cliente.

4. Inicialmente, el Mecanismo de Flujo de Trabajo solicita que TPM identifique el dispositivo a través del IMEI recibido. TPM pregunta al TCR el modelo del dispositivo y sus capacidades. Una vez que los datos son recuperados, ellos son enviados al Mecanismo de Flujo de Trabajo.

5. TPM también verifica si el suscriptor pertenece a un grupo de suscripción específico o si es parte de una lista de control de acceso (blanca o negra). Si el grupo o lista al cual el suscriptor pertenece requiere configuraciones especiales, TPM lo considerará.

6. Con todas las informaciones de dispositivo y suscripción disponibles, el Mecanismo de Flujo de Trabajo solicita que TPM configure el terminal. TPM formatea y envía las configuraciones de dispositivo en una SM, de acuerdo con el protocolo de aprovisionamiento al cliente OTA, soportado por el terminal.

7. Las configuraciones llegan al teléfono y, después que el suscriptor las acepta, el nuevo dispositivo está configurado correctamente para utilizar los servicios de datos disponibles.

3.6.8 Configuración de Terminales Disparada por WEB Self-Care

La Internet provee un método económico para permitir el auto mantenimiento de las configuraciones de terminales. La interfaz del Asistente para Self - Care (SCA) soporta suscriptores en el aprovisionamiento manual de configuraciones de terminal. Los suscriptores seleccionan el suministrador de su terminal y luego el nombre del modelo de su teléfono a partir de una extensa biblioteca de terminales. Los suscriptores obtienen asistencia visual a través de la imagen del terminal seleccionado. Alternativamente, los suscriptores pueden digitar su IMEI para que la plataforma de gestión de terminales identifique su terminal automáticamente. La siguiente figura muestra el SCA. Los colores, fuentes y gráficos pueden ser personalizados para la operadora, como estándar.

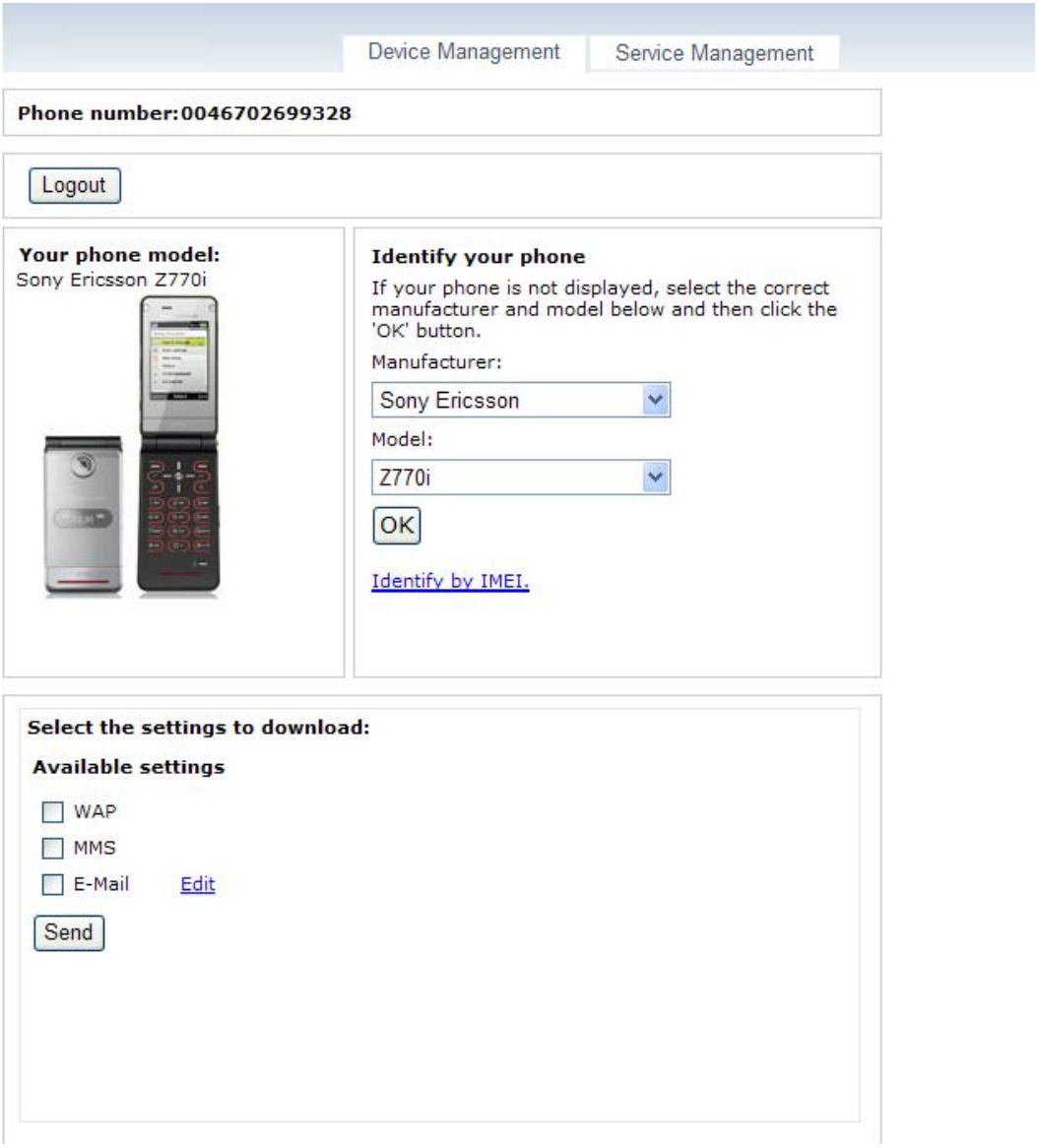


Figura 3.11. Configuración Ejemplo de interfaz SCA para aprovisionamiento de configuraciones de terminales por el suscriptor

SCA ofrece las siguientes funcionalidades:

- Cuando la suscripción es conocida en el sistema por una identidad de terminal (IMEI), el modelo del terminal es automáticamente pre-seleccionado.

- Cuando el terminal o suscripción no es conocido, el modelo del teléfono puede ser seleccionado de una lista *drop-down*.
- Definiciones de configuración del terminal, tales como MMS, WAP, GPRS y E-mail
- Son ofrecidas funciones administrativas, tales como:
- Soporte a varios idiomas - permitiendo la traducción del GUI a idiomas diferentes del inglés
- Manejo de alarmas basado en las funcionalidades del *DP Basic Framework*
- Generación de eventos basada en la generación de eventos del TPM

El SCA puede ser personalizado para el visual y aspecto del cliente a través de la edición de los modelos de interfaz de usuario del módulo. el web designer de la operadora o el administrador. también pueden proveer soporte adicional para personalización de acuerdo con la necesidad. El SCA crea registros de eventos del TPM para operaciones exitosas y falladas de descarga de configuraciones de dispositivos, por MSISDN, de manera que reportes pueden ser creados con base en estos registros. Más informaciones respecto de SCA pueden ser encontradas en el anexo [20].

3.6.9 Aprovisionamiento de Terminales Asistido por Customer Care

Las operadoras deben estar preparadas, en todos casos, para soportar el equipo de ayuda al cliente en sus contactos con suscriptores. Independientemente de los otros métodos implantados de aprovisionamiento, los suscriptores muchas veces necesitarán de soporte para las configuraciones de

[20] OTAP-1100-FD, 2001, LOGICA Mobile Networks Limited

sus terminales. Normalmente, llamadas de ayuda al cliente relacionadas a servicios de datos y configuraciones de terminales toman mucho tiempo. No es inhabitual que una llamada tome más de 20 minutos y, para "smart phones", más todavía. Por lo tanto, es vital que el equipo de ayuda al cliente tenga la capacidad de gestionar configuraciones de terminales de suscriptores. Con el sistema para gestión de terminales, agentes de ayuda al cliente y otros equipos de la operadora tienen la oportunidad de aprovisionar configuraciones de terminal manualmente, para los suscriptores. El Customer Care Assistant (CCA) utilizado por el sistema de gestión de terminales presenta informaciones detalladas sobre el terminal del suscriptor y su histórico. Es una aplicación basada en web que permite acceso simplificado a todo el equipo de ayuda al cliente.

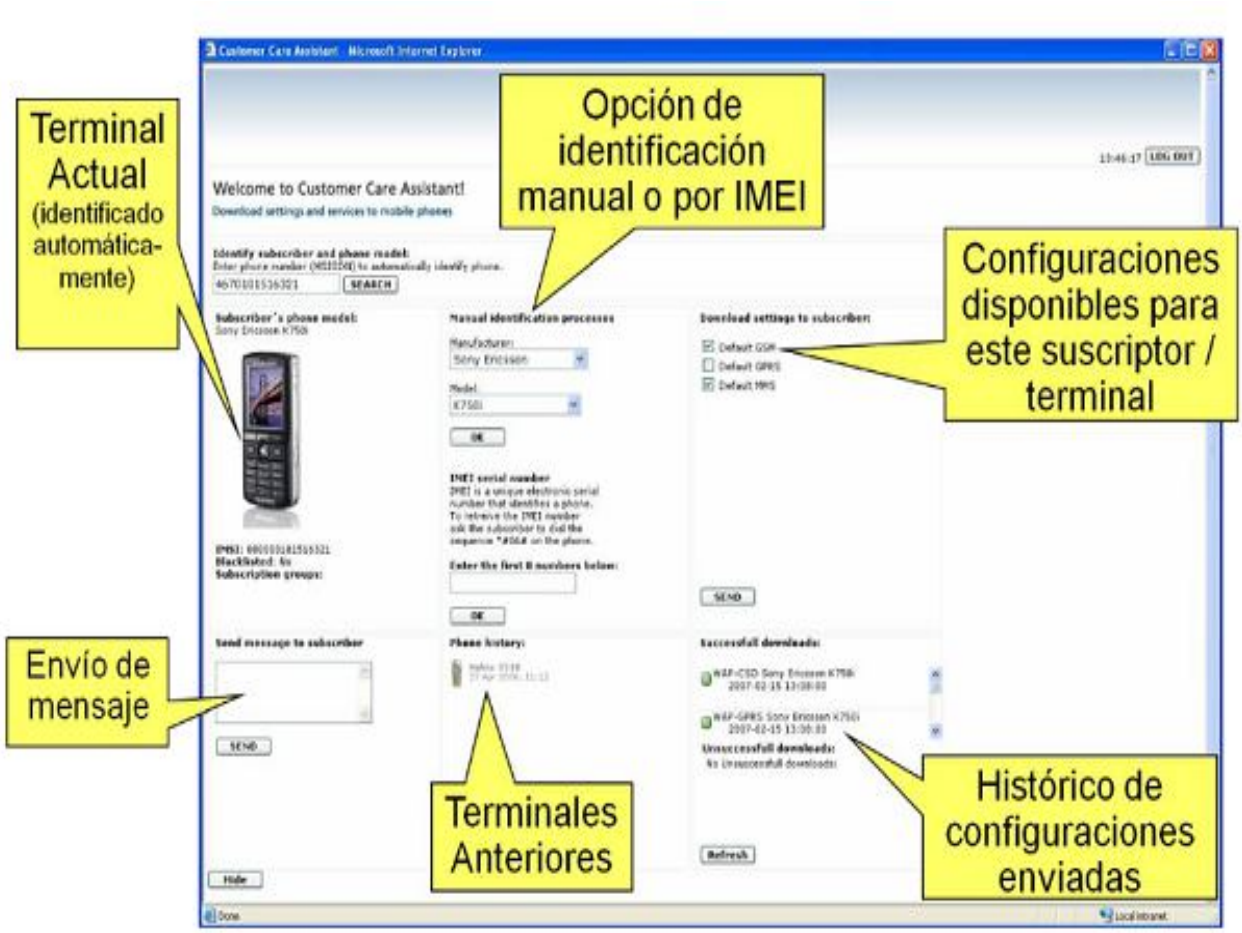


Figura 3.12. Ejemplo de la interfaz CCA para configuración de terminales asistida por Customer Care

Ejecutivos de ayuda al cliente pueden realizar descargas de configuraciones para terminales de suscriptores. Las informaciones del repositorio sobre capacidades de terminal, tipo de suscripción, histórico de la suscripción y del terminal son presentadas a los ejecutivos de ayuda al cliente en un formato fácil de leer. Al digitar el MSISDN del suscriptor, el ejecutivo de ayuda al cliente obtiene un panorama de los datos de suscripción (tales como IMSI y tipo de suscripción), terminal que utiliza el cliente actualmente o último terminal aprovisionado y el histórico de descarga de configuraciones. El CCA GUI soporta la identificación del terminal a partir del IMEI y a partir del nombre del suministrador y del modelo. Adicionalmente, el CCA tiene las siguientes funcionalidades:

- Visualización automática del último teléfono conocido
- Cuando el terminal o suscripción no es conocido, el modelo del teléfono puede ser seleccionado de una lista *drop-down*.
- Presentación del terminal e informaciones de suscripción
- Definición de configuraciones del terminal, incluyendo MMS, WAP, GPRS y E-mail
- Visualización del histórico de descargas para un MSISDN específico – tanto exitosas como fallidas - exhibiendo el terminal asociado con el nombre del proveedor y modelo
- Un SMS de texto puede ser directamente enviado al suscriptor seleccionado
- Para algunos terminales disponibles en el TCR, que soporta MMS y WAP, pero no soporta descargas OTA, por ejemplo, el CCA exhibirá instrucciones manuales para guiar el agente de ayuda al cliente en el proceso de configuración manual del terminal.

Son ofrecidas funciones administrativas, tales como:

- Soporte básico a idiomas - permitiendo idiomas diferentes del inglés
- Manejo de alarmas basado en las funcionalidades del DP Basic Framework
- Tarifación de generación de datos basada en registros de eventos creados por el servidor TPM

El CCA crea registros de eventos del TPM para operaciones exitosas y falladas de descarga de configuraciones de dispositivos, por MSISDN, de manera que reportes pueden ser creados con base en estos registros. [21]

3.6.10 Configuración de Terminales en Lotes

La opción Batch (Lotes) de la plataforma de gestión de terminales permite que las operadoras distribuyan configuraciones a grupos específicos de suscriptores. Las razones comunes para hacerlo son lanzamientos de nuevos servicios de datos, campañas orientadas de marketing y envío de informaciones actualizadas de configuración debido a cambios en la red. Un pedido de trabajo en lote es preparado a través del Campaign Manager del Sistema de Gestión de Configuración por lotes (BOM). El pedido de trabajo es ejecutado y se envía un SMS a cada uno de los suscriptores definidos en el pedido de trabajo. El mensaje puede ser configurado por la operadora y generalmente pedirá que el suscriptor la responda caso desee recibir configuraciones actualizadas. El suscriptor deberá leer el corto mensaje recibido y responderlo. La respuesta es enviada al sistema y la plataforma de aprovisionamiento inicia el proceso de configuración del terminal.

[21] 3GPP TS 51.011 (versión 4.x.x): "Especificación de la interfaz tarjeta SIM con Terminal móvil

Esta funcionalidad requiere que el BOM y el SFM sean implantados como parte de la implementación.

- ***Textos Informativos***

La información suministrada para guiar e informar el suscriptor durante el proceso de configuración del terminal es una parte importante de la experiencia del suscriptor. En todas las ejecuciones de configuración de terminal, una sucesión de mensajes es aprovisionada al suscriptor, informando sobre acciones de configuración a ejecutar e informando sobre la conclusión de la configuración. Estos mensajes mejoran la experiencia del suscriptor y lo ayudan a comprender la razón para la gestión de su terminal. El texto es generado por la combinación de textos estáticos con textos dinámicos para informaciones como marcas específicas (Ej. nombre del tipo de suscripción), código PIN a ser utilizado (si necesario) y configuraciones entregadas. La Tabla 3.4 provee ejemplos de estos mensajes informativos que son personalizados para la operadora.

Tabla 3.4: Lista de textos informativos que pueden ser personalizados

ID del Mensaje	Descripción	Ejemplo
AutoProvisioningWelcome	Marcada, informa al suscriptor que el terminal será configurado. Generada por el aprovisionamiento automático de configuraciones de terminal. Incluye instrucciones de PIN automáticamente, si necesario.	Percibimos que necesitas de nuevas configuraciones de teléfono para accesar algunos de nuestros servicios. Estamos preparando para enviarlas. Utilice el código PIN 1234 cuando solicitado. Saludos, Operadora
HandsetPreconfigured	Marcado, informa al suscriptor que su terminal está pre-configurado y que las configuraciones pedidas no pueden ser descargadas.	Su terminal está configurado de fábrica y sus configuraciones no pueden ser modificadas. Contacte la Ayuda al Cliente digitando 222 en su portable, caso desees asistencia adicional. Saludos, Operadora
AutoProvisioningFinal	Informa al suscriptor que la configuración fue concluida (todas las configuraciones aplicables fueron descargadas al terminal). Generada por el aprovisionamiento automático de configuraciones.	Ahora puedes aprovechar su portable al máximo. Has recibido las configuraciones para MMS y Streaming. Contacte la Ayuda al Cliente digitando 222 en su portable, caso desees asistencia adicional. Saludos, Operadora

3.6.11 Gestión de Informaciones de Terminales

Informaciones actualizadas sobre terminales de los suscriptores son esenciales para una configuración remota efectiva del terminal. La plataforma para gestión de terminales permite que las operadoras incluyan terminales específicos en una “blacklist” ("lista negra", bloqueo para recepción de

configuraciones). Esto puede ser necesario para terminales configurados de fábrica o terminales sujetos a cambios frecuentes de SIM. Las informaciones principales de terminales incluyen:

- Importación de lotes de terminales pre-configurados – la importación de informaciones sobre terminales pre-configurados al repositorio. Estos terminales son marcados como bloqueados para impedir el aprovisionamiento de configuraciones.

- Actualización de terminal para el bloqueo de aprovisionamiento automático – el bloqueo del recibimiento automático de configuraciones para un terminal específico.

3.6.12 Gestión de Informaciones de Capacidades de los Terminales

El Terminal Capabilities Repository (TCR) contiene informaciones sobre modelos de terminales y capacidades asociadas. Contiene las informaciones necesarias para enviar configuraciones al terminal con éxito. Permite que la plataforma de gestión de terminales realice lo siguiente:

a) Identifique el terminal a partir del *Type Allocation Code* (TAC) (más frecuentemente utilizado para descargas automáticas de configuraciones de terminales) o a partir del apareamiento entre nombre del suministrador – nombre del modelo (más común para auto mantenimiento y ayuda al cliente).

b) Seleccione el protocolo de aprovisionamiento a ser utilizado y las configuraciones que pueden ser aprovisionadas.

Las informaciones del TCR son actualizadas regularmente a través del Terminal Update Program para el servicio del TCR. Este servicio garantiza que las operadoras posean las informaciones más actualizadas del mercado de terminales, en rápida evolución. Las siguientes ilustraciones muestran la interfaz de usuario para el TCR Administrator:

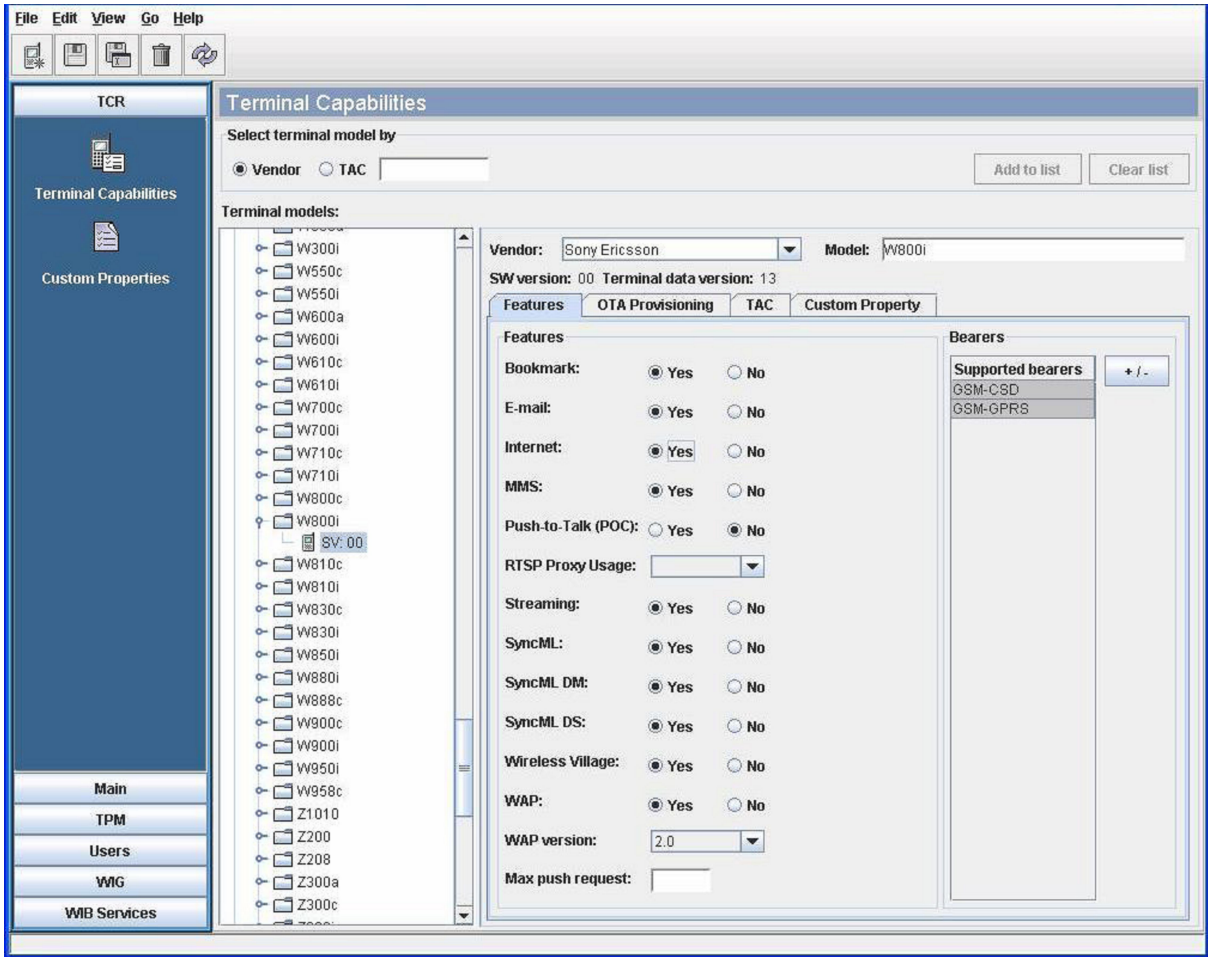


Figura 3.13. Ejemplo Interfaz de administración de TCR – capacidades de terminales

Además de las actualizaciones estándares aprovisionadas por la plataforma, las operadoras pueden definir sus propias propiedades personalizadas utilizando las herramientas de administración del TCR. La siguiente ilustración muestra la interfaz de usuario para la definición de propiedades personalizadas de terminal.[22]

[22] Descripción de Repositorio de Capacidades del Terminal, Doc. No. MPM07:0006, 2006, Smartrust

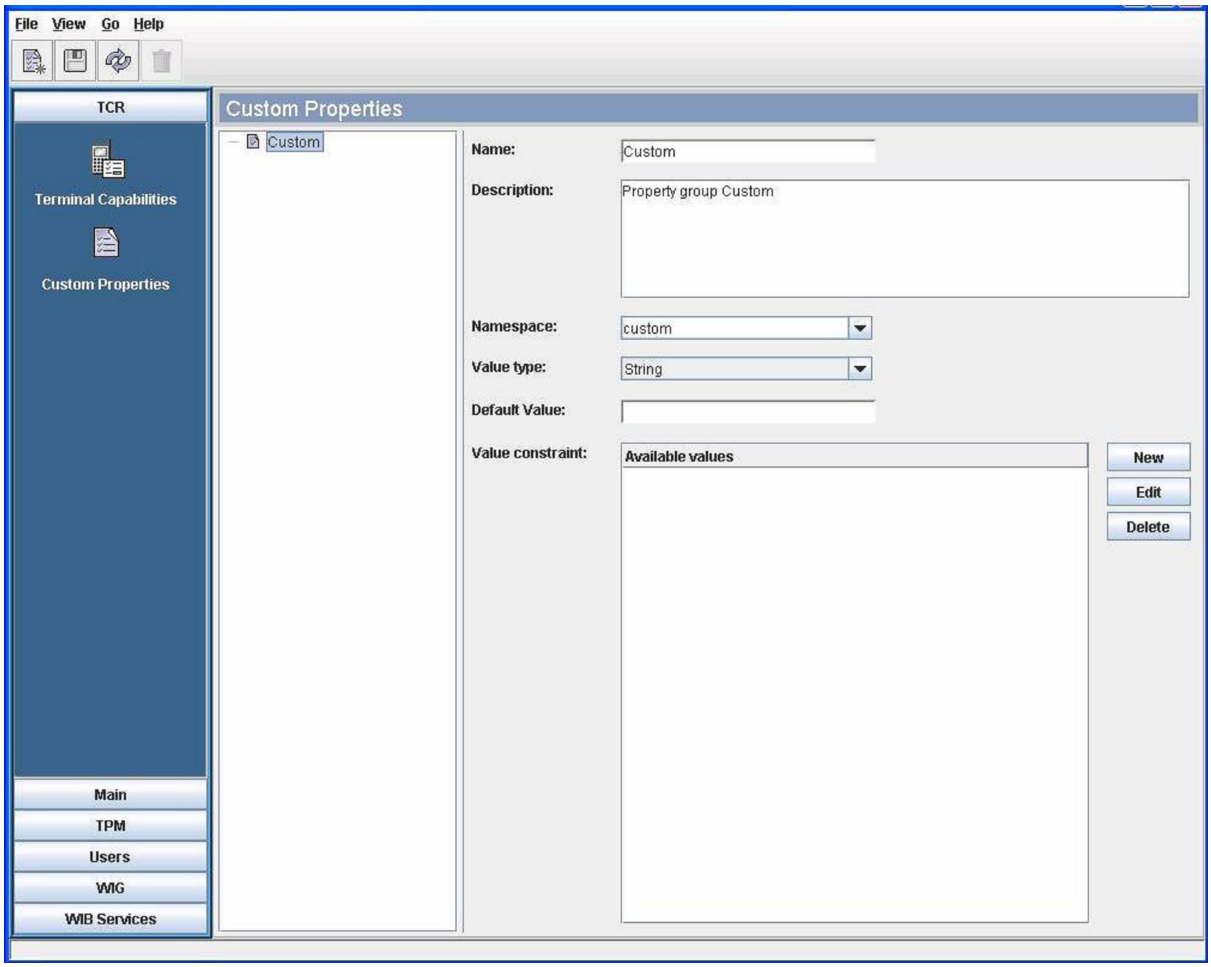


Figura 3.14. Ejemplo Interfaz de administración de TCR – propiedades customizadas

3.6.13 TUP – Terminal Update Program

El TUP es un servicio (adquirido anualmente) en el cual el sistema adquirido de Gestión de Terminales es frecuentemente actualizado con informaciones sobre los terminales más recientes en el mercado, garantizando la identificación y configuración de los mismos, como también la disponibilidad de informaciones detalladas sobre los terminales. Los gráficos abajo describen la evolución del número de códigos TAC y el número de terminales incluidos en releases TCR desde enero/2006. Como mostrado abajo, en promedio, el

Programa de Actualización de Terminal agrega casi 100 nuevos terminales al mes al TCR.[23]

Tabla 3.5 Número de códigos TAC por release

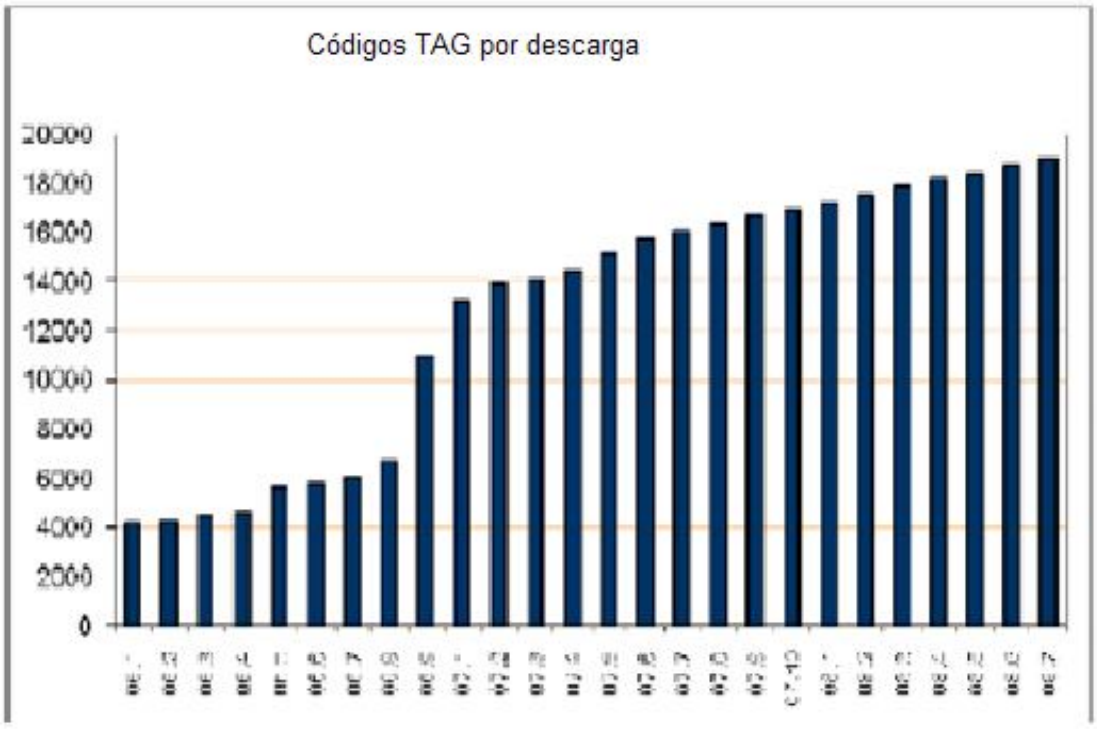


Tabla 3.6: Número total de terminales por release

[23] Revisión Técnica plataforma OTA, No. Doc. 108932ª0, Junio 06 2003,Gemplus

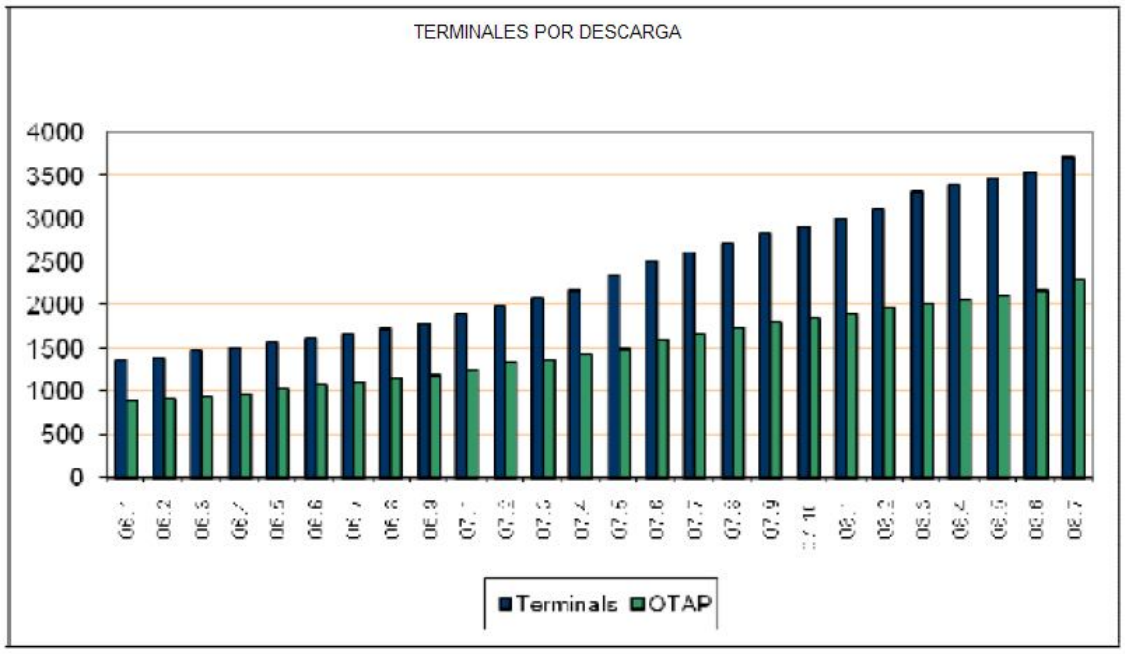
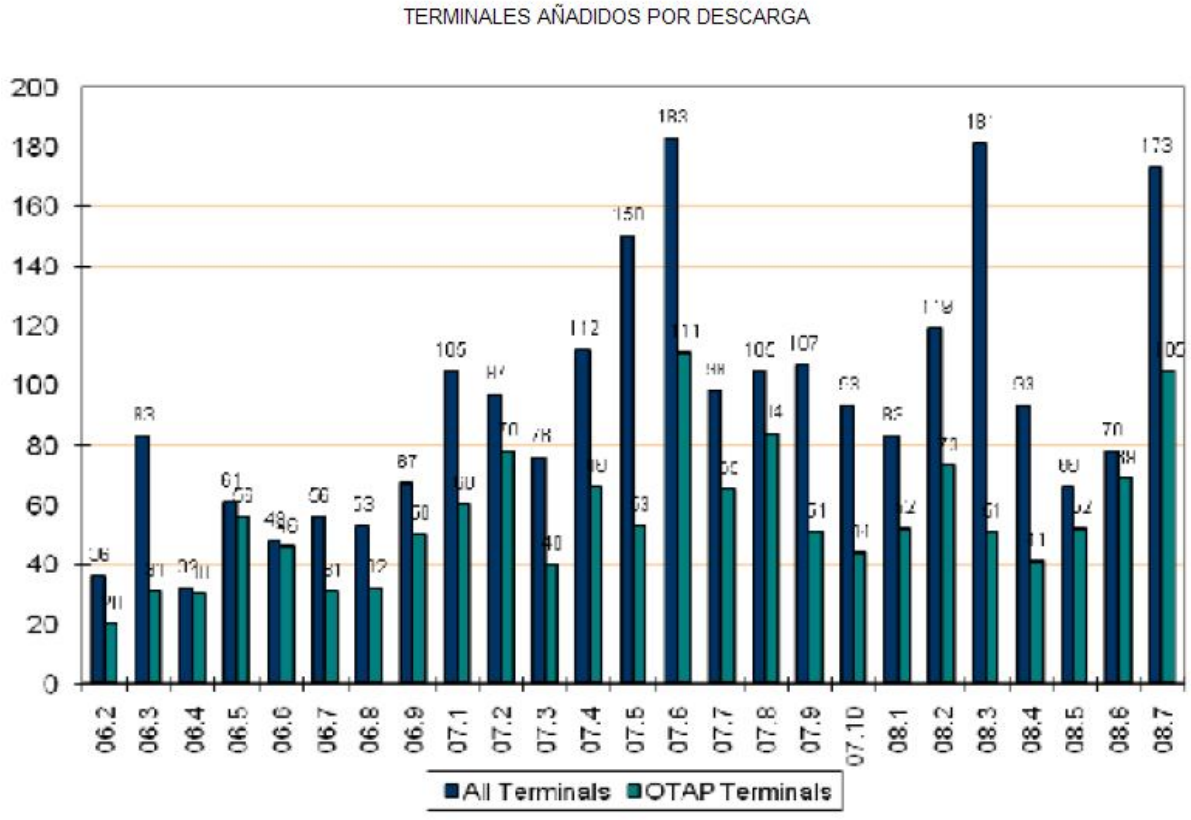


Tabla 3.7: Número de terminales añadidos por release



3.6.14 Terminales Soportados

El número TAC (Type Allocation Code) es un número de ocho dígitos que identifica el modelo de un terminal móvil. El TAC corresponde a los primeros ocho dígitos del IMEI (International Mobile Equipment Identity). Un mismo modelo de terminal puede tener asociados más de un rango de TACs. Para una óptima tasa de identificación de terminales un repositorio necesita tener el más grande número de TACs posible y al mismo tiempo el más grande número de modelos de terminales únicos (no se puede contar un mismo modelo dos veces). La siguiente tabla muestra cuantos TACs y modelos únicos tiene el repositorio de (TCR) actualmente: [24]

Tabla 3.8: Listado de TACs y modelos únicos tiene el repositorio de la plataforma de Gestión de Terminales

TACs	19009
Unique models	3708
Unique models with OTAP support	2284
Unique models for TAC recognition	189

3.6.15 Terminales solicitados por el cliente

[24] Terminales Soportados en el repositorio de capacidades del Terminal 2008-7, Smartrust

La plataforma para gestión de terminales tiene un módulo específico para administración del repositorio de terminales (TCR). A través de esta interfaz es posible manualmente crear y remover modelos de terminal, consultar y editar capacidades de terminal, crear y editar propiedades personalizadas de terminales . [25] Es muy importante observar que terminales de disponibilidad general probablemente ya estarán disponibles en el repositorio cuando fueren lanzados por la operadora. Con el fin de que los terminales exclusivos sean soportados es necesario que la operadora provea las siguientes informaciones del terminal:

- Requerimientos para terminales OTAP (*OTA-provisionable*)
    - Código TAC
    - Nombre e imagen del modelo
    - Estándar de protocolo de client provisioning utilizado por el modelo y, si aplicable, informaciones respecto de cualesquier desvíos de los estándares publicados (OTASS, Nokia Smart Messaging, Openwave, WAP provisioning, SyncML DM, OMA CP).
    - Informaciones respecto de todas las aplicaciones aprovisionadas vía OTA, por ejemplo CSD, GPRS, MMS, Bookmarks, Email, PoS, Wireless Village, capacidad de internet, capacidad de i-mode y streaming.
    - Ejemplo de documento de aprovisionamiento, instrucciones de desarrollo o documentación similar incluyendo las especificaciones de implementación.
    - Informaciones de capacidades y características soportadas por el terminal, User Agent profile (UA Prof.) y user agent string, versión de WAP.
    - Persona de contacto en el suministrador del terminal
    - Terminal para testes (unidad de producción, no prototipo)
- Requerimientos para terminales non-OTAP:
    - Código TAC

[25] Administrador de repositorio de capacidades del Terminal, No. Doc 846762-107, 2007-02-06, Smartrust

- Nombre e imagen del modelo
- Informaciones de capacidades y características soportadas por el terminal, User Agent profile (UA Prof.) y user agent string, versión de WAP.
- Instrucciones para configuración manual
- Persona de contacto en el suministrador del terminal

3.6.16 API de integración: TPM API

El API para el servidor TPM es construida usando tecnología CORBA 2.3.1. La TPM API consiste de estos objetos principales:

- DeviceConfiguration
- TerminalQuery

El objeto DeviceConfiguration maneja el envío de comandos de configuración así como permite consultar cuales comandos de configuración que resultarían de la ejecución de una configuración particular hacia un determinado suscriptor.

El objeto TerminalQuery soporta consultas sobre que clases de terminal son soportadas por el sistema y también cual terminal un determinado suscriptor tiene, si esto es sabido por el sistema.

3.7 Estadísticas y Reportes: Reporting Manager

La intención del sistema de gestión de reportes es proveer los reportes correctos para cada necesidad de usuario. Un conjunto de reportes predefinidos está incluido en el producto, los cuales pueden ser utilizados desde el primer día, si los prerrequisitos son correctamente cumplidos. El sistema de generación de reportes también puede ser extendido con reportes personalizados adicionales. Como esta herramienta puede ser utilizada para exportar datos del sistema principal, es importante llevar en cuenta que un archivo con todos MSISDN disponibles y varios campos de datos relacionados utilizará un enorme espacio en disco. El producto de reportes utilizado está compuesto por los siguientes recursos de alto nivel:

3.7.1 Óptimo diseño para reportes

Los autores de reportes pueden utilizar el diseñador visual de reportes (con un conjunto completo de controles de layout y diseño) para diseñar reportes altamente formateados, interactivos y profesionales.

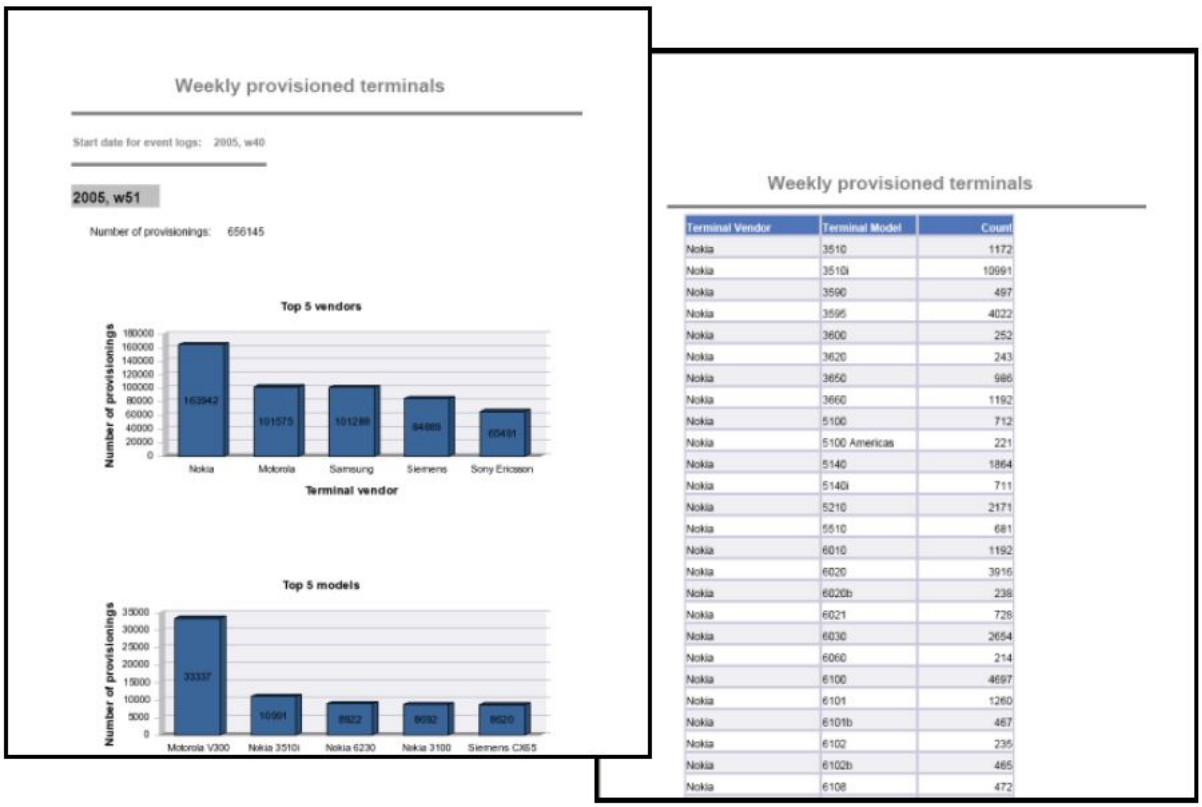


Figura 3.15. Ejemplo de reportes del Sistema de Generación de Reportes

3.7.2 Generación y entrega de reportes

Los reportes son publicados en la web, para mejores decisiones de negocios en todos los niveles de la organización. Los reportes pueden ser exportados y redireccionados a los formatos electrónicos utilizados por la mayoría de los usuarios finales (por ejemplo PDF, Excel y CSV). El área de IT puede centralizar la generación de reportes operacionales mientras distribuye la función de autoría a las líneas de negocios.

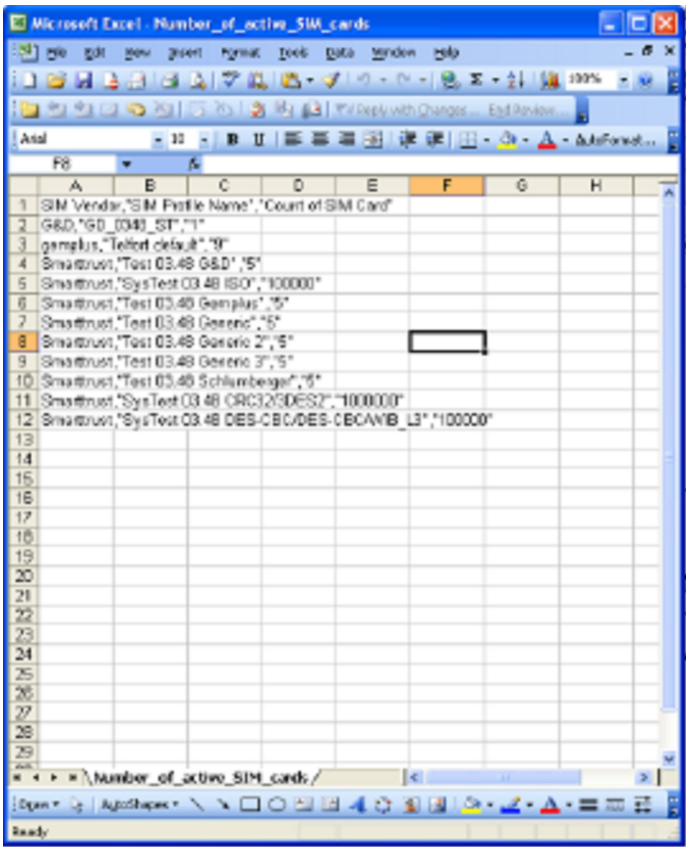


Figura 3.16. Ejemplo de formato de salida de los reportes

3.7.3 Planificación

La planificación de creación de reportes puede ser realizada diariamente, semanalmente o mensualmente, así como para fechas y horas específicas, etc.

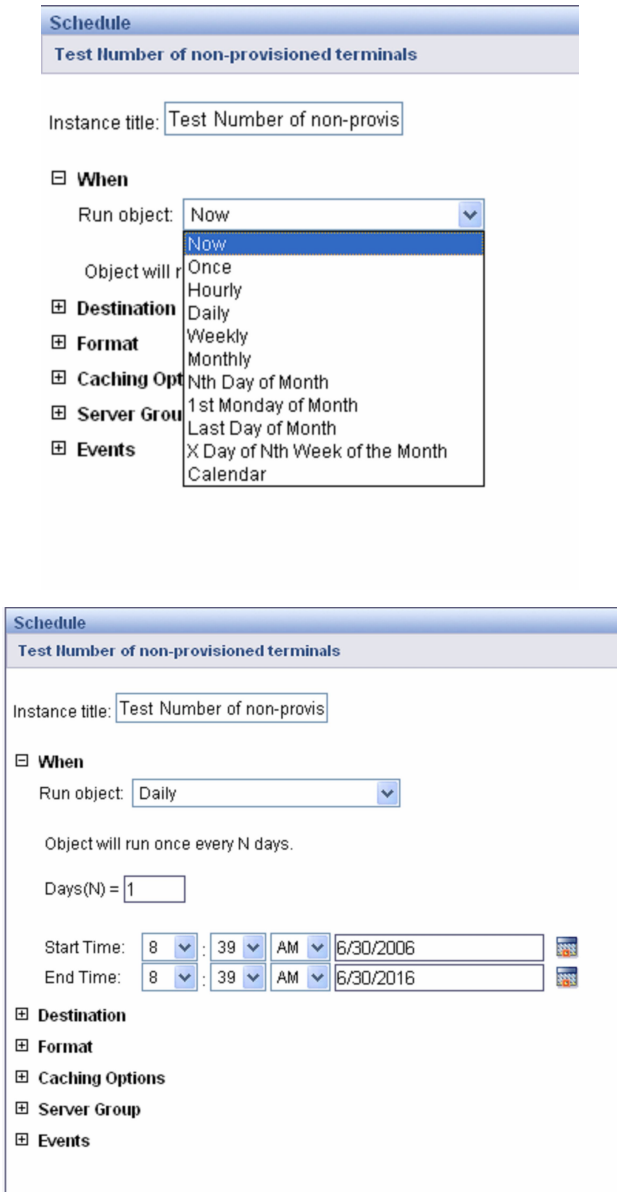


Figura 3.17. Planificación de Reportes

Se recomienda la planificación de generación de reportes para la noche (fuera de las horas pico). La utilización fuera de las recomendaciones influye negativamente el desempeño de producción del sistema, pues consume mucha capacidad de CPU. Además, es importante llevar en cuenta el formato preciso de exportación, Excel, PDF y CSV, para el caso de uso adecuado.

3.7.4 Detalle (drilling) de reportes

El Generador de Reportes ofrece un análisis adicional a algunos de los reportes creados, al analizar el reporte de manera más detallada. El detalle de reportes permite que el usuario analice mejor los datos para descubrir detalles detrás de resultados mostrados en una tabla, gráfico o sección. Por ejemplo, un reporte específico puede ser detallado por fecha, significando que el resultado puede ser analizado anualmente, mensualmente y diariamente, a través del modo de detalle.

3.7.5 Reportes Estándares y Personalizados

Como estándar, estos reportes estándares son suministrados como parte del sistema de Gestión de Reportes. [26]

Tabla 3.9 Tipos de reportes estándar generados

[26] 3GPP TSG SA WG3 Security – S3#30, Octubre 2003, Gemalto, Oberthur, Schumberger

Terminales aprovisionados semanalmente	El reporte cuenta el número de terminales aprovisionados con éxito, por semana, separados por suministrador y modelo de terminal. También muestra los 5 suministradores y modelos dominantes por semana (Event History y
Tipos de configuraciones aprovisionadas, por semana	El reporte muestra el número de terminales aprovisionados (con o sin éxito), separados por semana y tipo de aprovisionamiento. También muestra las 5 configuraciones aprovisionadas dominantes y la distribución por porcentaje de todas las configuraciones aprovisionadas por semana. (Terminal Provisioning Manager y DP7 Basic Framework)

Lista de MSISDN y perfiles SIM	El reporte muestra las suscripciones (MSISDN) y sus perfiles de SIM, tamaño de memoria y suministrador de SIM correspondientes. (DP7 Basic Framework y SFM)
Número de tarjetas SIM activas	Este reporte cuenta el número de tarjetas SIM activas, separadas por suministrador de SIM y perfil de SIM. (DP7 Basic Framework y SFM)
Número de terminales con capacidad MMS	El reporte cuenta el número de terminales con capacidad MMS, separados por suministrador y modelo de terminal. (DP7 Basic Framework y Terminal Capability Repository)
Número de terminales no aprovisionados	El reporte cuenta el número de terminales no aprovisionados, separados por suministrador y modelo de terminal. (Terminal Provisioning Manager, Terminal Capability Repository y DP7 Basic Framework)
Número de suscripciones aprovisionadas	El reporte cuenta el número de suscripciones aprovisionadas por grupo de suscripciones, perfil de SIM y modelo de terminal. (Terminal Provisioning Manager y DP7 Basic Framework)
Número de terminales aprovisionados	El reporte cuenta el número de terminales aprovisionados, separados por suministrador y modelo de terminal. (Terminal Provisioning Manager y Terminal Capabiliy Repository)
Número de terminales utilizados por múltiplas suscripciones	El reporte cuenta el número de terminales que han sido utilizados por más de una suscripción, separados por modelo de terminal. (Terminal Provisioning Manager y DP7 Basic Framework)
Terminales aprovisionados con MMS semanalmente	Reporta sobre el número de terminales que han sido aprovisionados con éxito con configuraciones MMS, semanalmente, por suministrador y modelo de terminal. Muestra los 5 suministradores y los 5 modelos dominantes para cada semana (Terminal Provisioning Manager, Event History y Terminal Capabiliy Repository)

3.7.6 Interfaz de usuario

Una gran parte de las tareas de operaciones y mantenimiento puede ser realizada por operaciones de línea de comando. Para este fin la plataforma puede ser accedida localmente vía comunicación serial, así como puede ser accedida por SSH a través de una red IP. Para la mayor parte de las operaciones es posible utilizar interfaces gráficas accedidas vía navegador Web por una red IP. Las interfaces más importantes están listadas en las próximas secciones. La plataforma DP tiene un portal por lo cual se puede acceder a mayoría de las interfaces de usuario de DP.

3.7.7 Administrador DP

El Administrador DP es un cliente para DP y es diseñado para:

- Permitir de manera facilitada intervenciones en base de datos de DP
- Administrar usuarios y sus privilegios a recursos de sistema, aplicaciones clientes y archivos de tarjetas
- Manejar contraseñas
- Manejar tarjetas SIM y USIM
- Administrar applets en las tarjetas
- Administrar parámetros de seguridad de las tarjetas
- Administrar llaves de autenticación y encriptación de las tarjetas
- Administrar vínculos de archivos de las tarjetas

El cliente Administrador DP tiene una estructura modular. Solamente las partes que el usuario registrado tiene derecho de uso son cargadas. Esta carga flexible es alcanzada en un nivel de grupo. Los grupos disponibles son:

- Users – Administración de usuarios de DP y sus privilegios
- Cards – Tarjetas (SIM/USIM), grupos de tarjetas y perfiles de tarjetas
- Gestión de applets Java
- Gestión de configuraciones de terminales (TPM)

El administrador de la plataforma de gestión de terminales es accedido a través de cualquier navegador Web, utilizando Java™ Web Start.

Figura 3.18 Pantalla de login del administrador DP

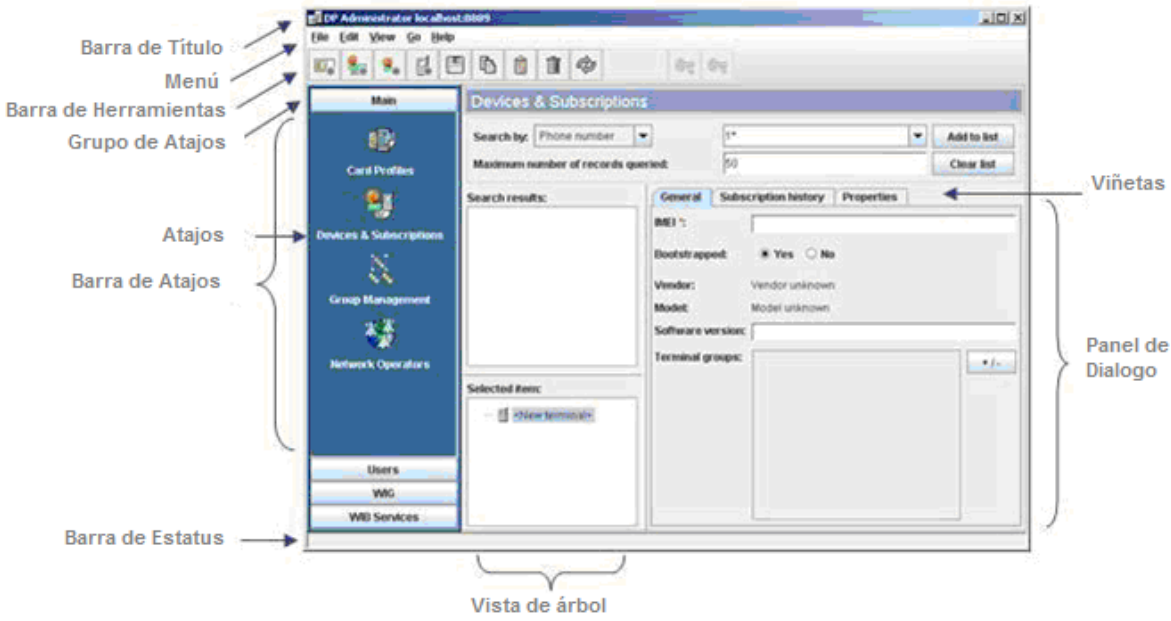


Figura 3.19 Pantalla principal del administrador DP

- ***Administrador DP – Módulo Java***

Todos los controles necesarios para administración de *applets* Java son realizados a través de la interfaz intuitiva y amigable de DP *Administrator*. Los paquetes y *applets* son definidos y/o importados en la base de datos de JAM con esta herramienta. Todos los parámetros requeridos pertenecientes a *applets* o paquetes Java son definidos por esta interfaz. [27]

- ***Administrador DP – Módulo TPM***

TPM es el componente central de la solución de gestión de configuraciones de terminales. TPM provee operaciones de gestión de terminales. El módulo TPM de Administrador DP es el módulo que permite ejecutar operaciones administrativas como crear, manejar y asociar clases de aprovisionamiento (*provisioning types*),

[27] Desarrollo de Aplicaciones Java para tarjetas SIM, January 2001,Sun Developer Network

perfiles de aprovisionamiento (*provisioning profiles*) y documentos de aprovisionamiento (*provisioning documents*).[28][32]

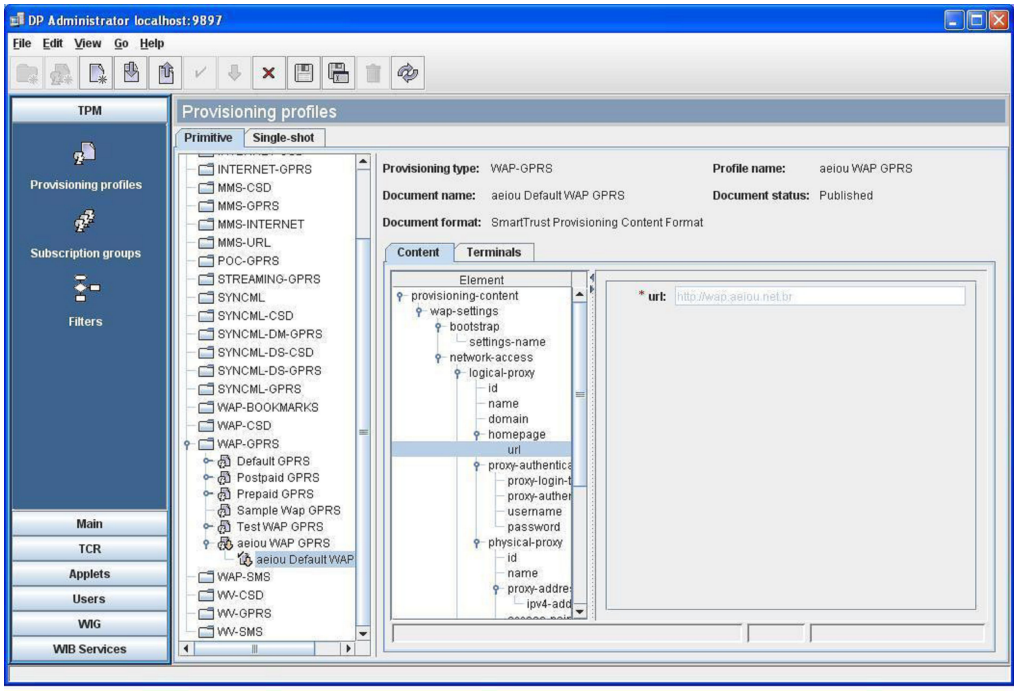


Figura 3.20 Gestión de configuraciones de terminales en la interfaz Administrador DP

3.7.8 Gestión de Alarmas (AM)

El sistema de generación de alarmas es una interfaz cliente para el servidor A&C (alarm & configuration) de DP Basic Framework. Alarm Manager es un cliente que es ejecutado en Windows. [29]

[28] Solutions Smartrust, http://www.smarttrust.com/mobile_solutions/mobile_solutions_certified_program.asp

[29] Manual de usuario para gestión de alarmas, Doc. No. 10542-081, 2005-09-30, Smart Trust

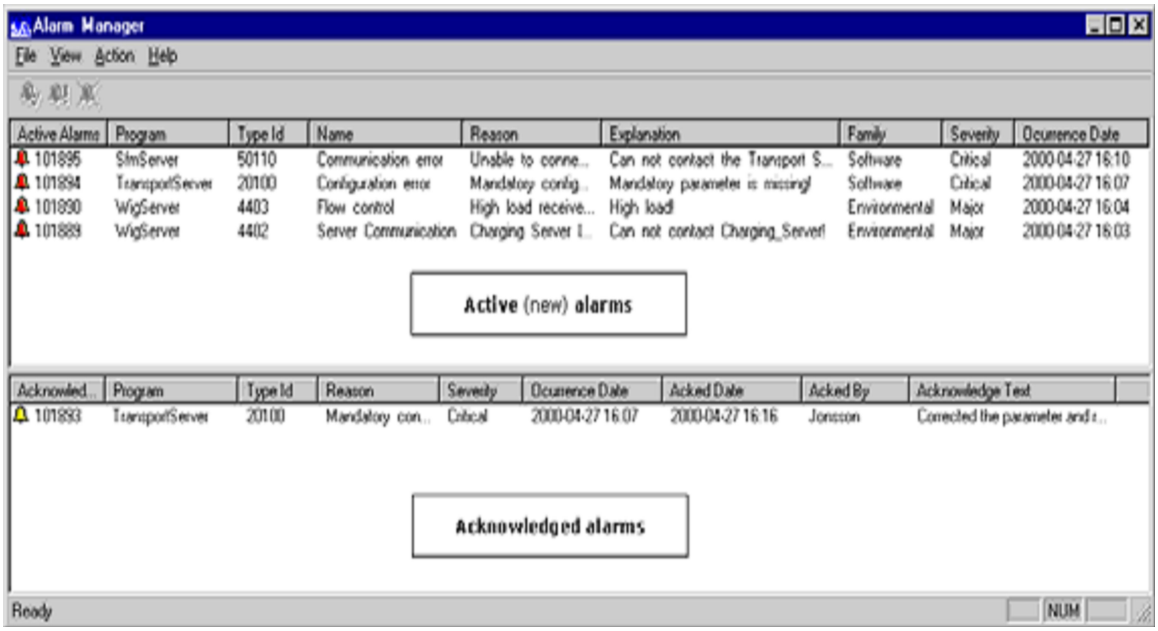


Figura 3.21 Ventana principal de la interfaz del sistema de gestión de alarmas

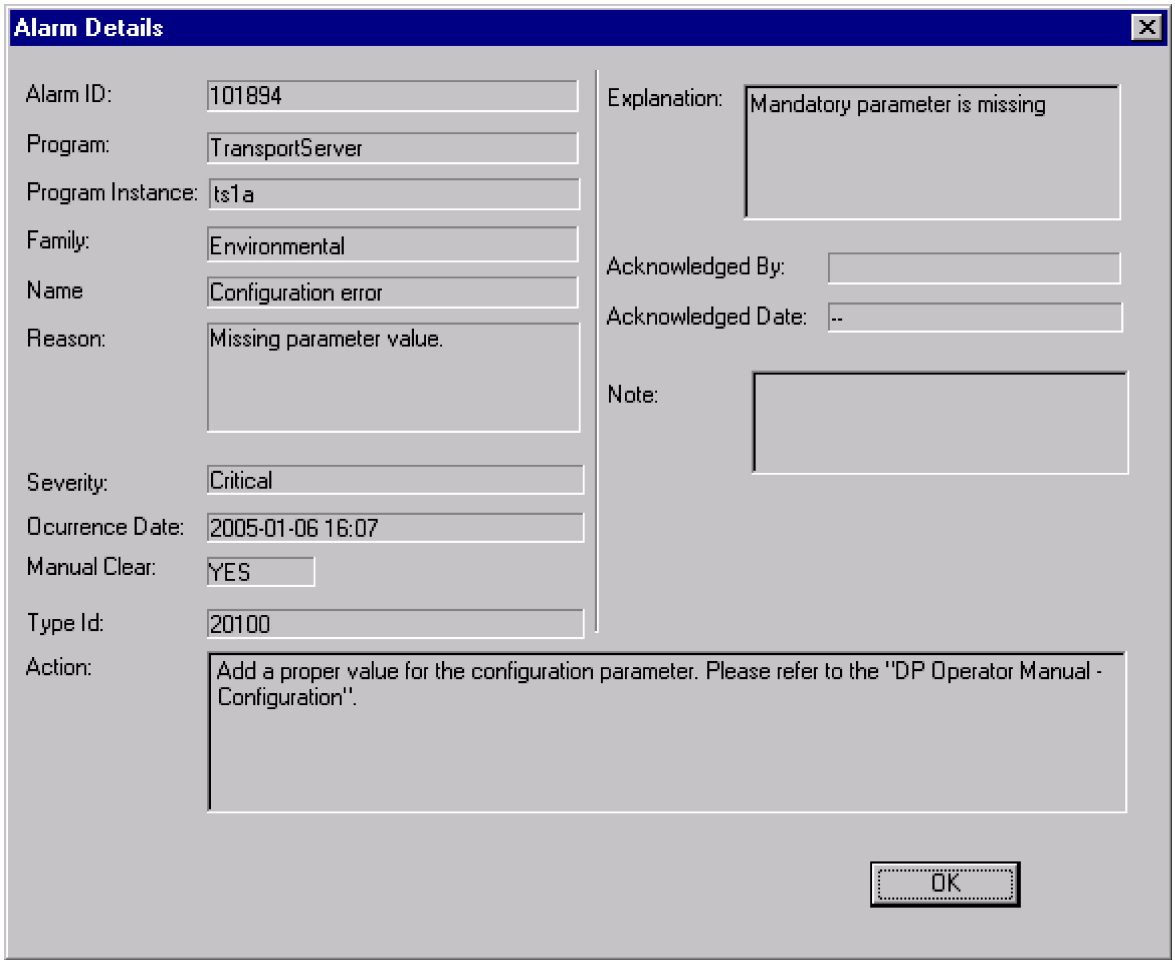


Figura 3.22 Detalles de la alarma

3.7.9 Sysview

Es una herramienta de presentación estadística. Sysview presenta las estadísticas más importantes de DP, de la base de datos y del hardware donde DP es ejecutada. Las estadísticas son presentadas en gráficos en un navegador Web. [30]

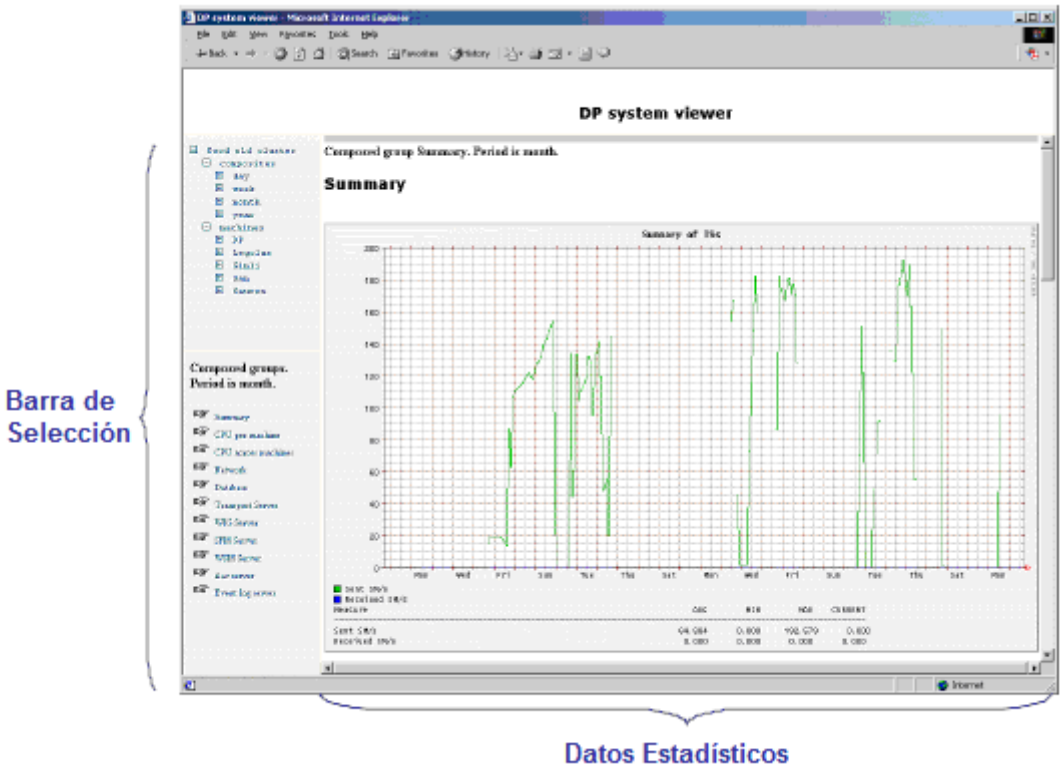


Figura 3.23 Pantalla principal de Sysview

3.7.10 Configuration Manager

[30] Guía de usuario SysView, Doc. No. PS 05:0016, Agosto 2005, Smartrust

Configuration Manager es una aplicación cliente desarrollada en Java y usada para crear, mirar y editar parámetros de configuración en DP. Configuration Manager es compatible para Sun™ Solaris™ y Microsoft® Windows®.

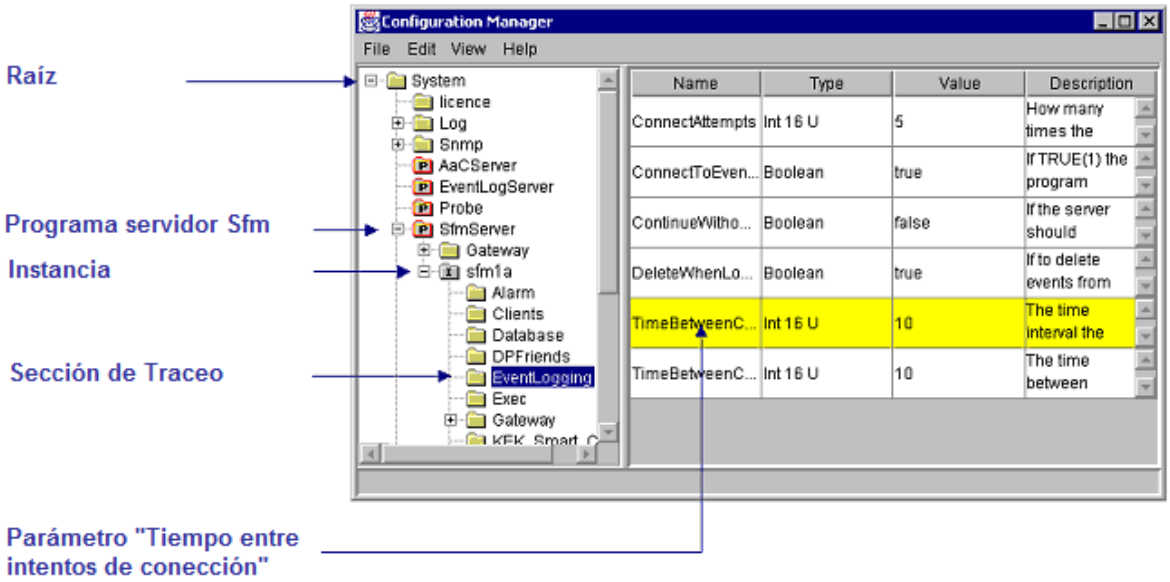


Figura 3.24 Pantalla principal de la interfaz Sysview

3.7.11 Service Assistant

Service Assistant es una aplicación cliente que ejecuta en plataforma Windows® y que tiene por objetivo a la operadora, proveedores de servicio y otros terceros autorizados. Service Assistant es utilizado para facilitar el mantenimiento de archivos, datos y otros parámetros almacenados en la SIM. El objetivo de este mantenimiento puede ser testear y verificar una nueva clase de tarjeta o ser utilizado en el soporte al uso de servicios por el suscriptor, incluyendo el manejo de tarjetas defectuosas. Service Assistant provee una aplicación Windows® que soporta un rango de operaciones de mantenimiento, como por ejemplo:

- Actualización de MSISDN(s) almacenados en la tarjeta
- Acrecentar, borrar o cambiar ADNs (*Abbreviated Dialing Numbers*)
- Redefinir y recargar una tarjeta defectuosa

- Cambiar un registro en un archivo específico en una selección de tarjetas
- Informar al usuario sobre las operaciones por mensajes
- Acompañar el status de requisiciones OTA
- Enviar comandos SIM toolkit

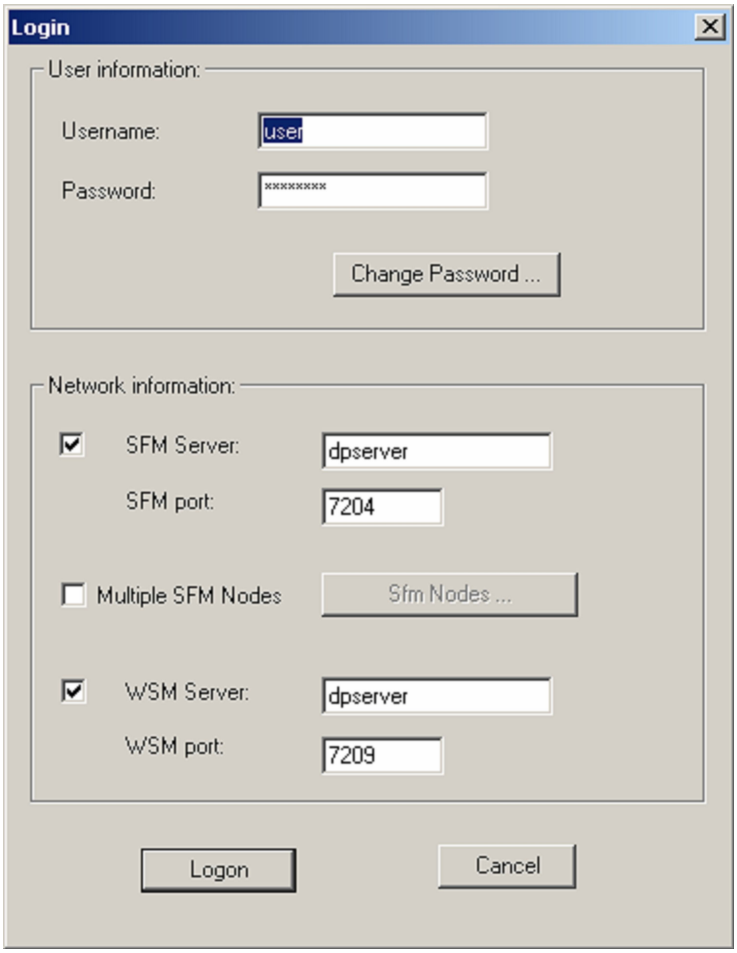


Figura 3.25 Pantalla de login de Service Assistant

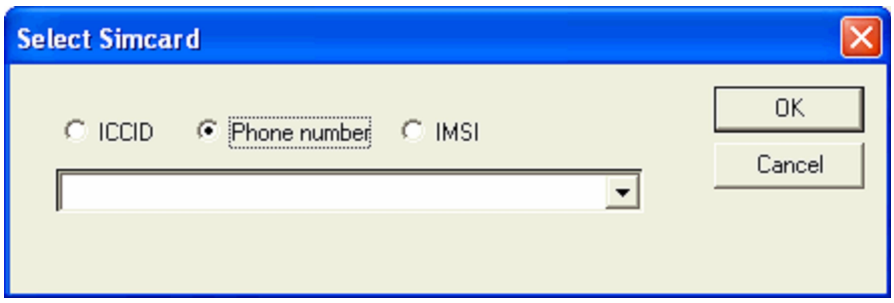


Figura 3.26 Pantalla de selección de tarjeta SIM en Service Assistant

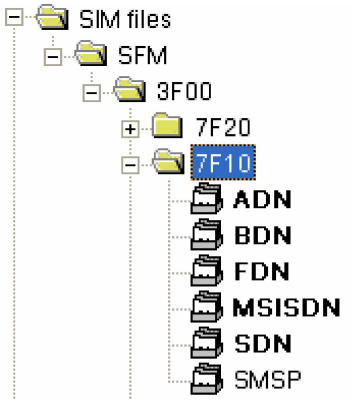


Figura 3.27 Hoja de selección de archivos en Service Assistant

3.7.11.1 Service Assistant – Módulo Java

El modulo JAM de Service Assistant provee al administrador de la plataforma la posibilidad de descargar, activar y remover applets Java.[31]

[31] 3GPP TS 11.11 v8.11.0 and ETSI TS 102 221 v5.0.0

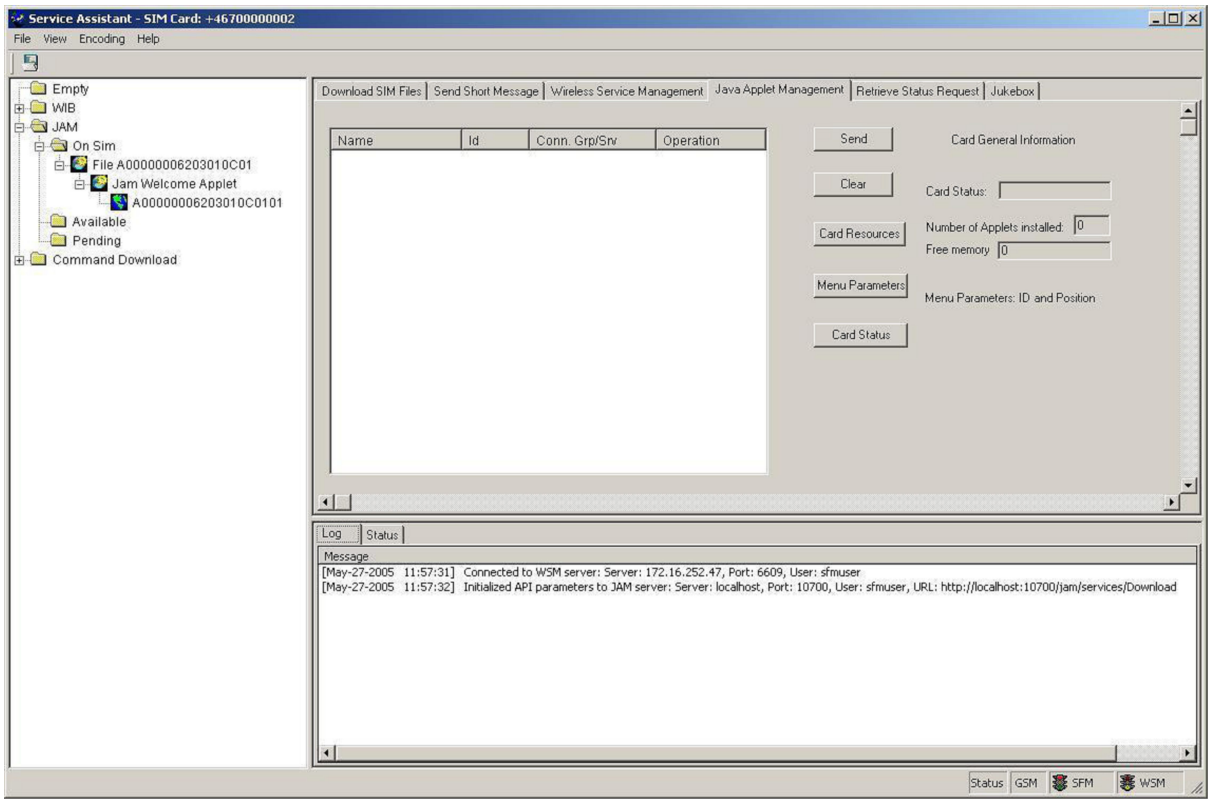


Figura 3.28 Gestión de paquetes y applets en la interfaz Service Assistant

3.7.12 Administrador de órdenes por lotes (BOA)

El administrador de órdenes por lotes es un cliente web usado para operar y hacer la supervisión y configuración de órdenes de trabajo (Work Orders). La funcionalidad suministrada por el Administrador de órdenes por lotes es dividida en los siguientes grupos. [32]

- Gestión de órdenes de trabajo *(Work Order Management)*
    - Creación de órdenes de trabajo *(Work Orders)*
    - Listar órdenes de trabajo y sus status.

[32] Manual de Operación BOM, Doc. No. 10543-125 Revisión: B. 2006-10-13., Smartrust

- Mirar detalles de una orden de trabajo.
- Iniciar, parar, pausar y reiniciar órdenes de trabajo.
- Cambiar prioridades de una orden de trabajo.
- Listar FCDs y SLDs y sus status.
- Mirar detalles de FCD y SLD.
- Borrar órdenes de trabajo y FCDs y SLDs no usados.

- Gestión de applets (Applet Management)
  - Crear órdenes de trabajo (*Work Orders*) para Java™ *Applet Management*.
- Configuración
  - Manejar esquemas de limitación
  - Cambiar contraseña.

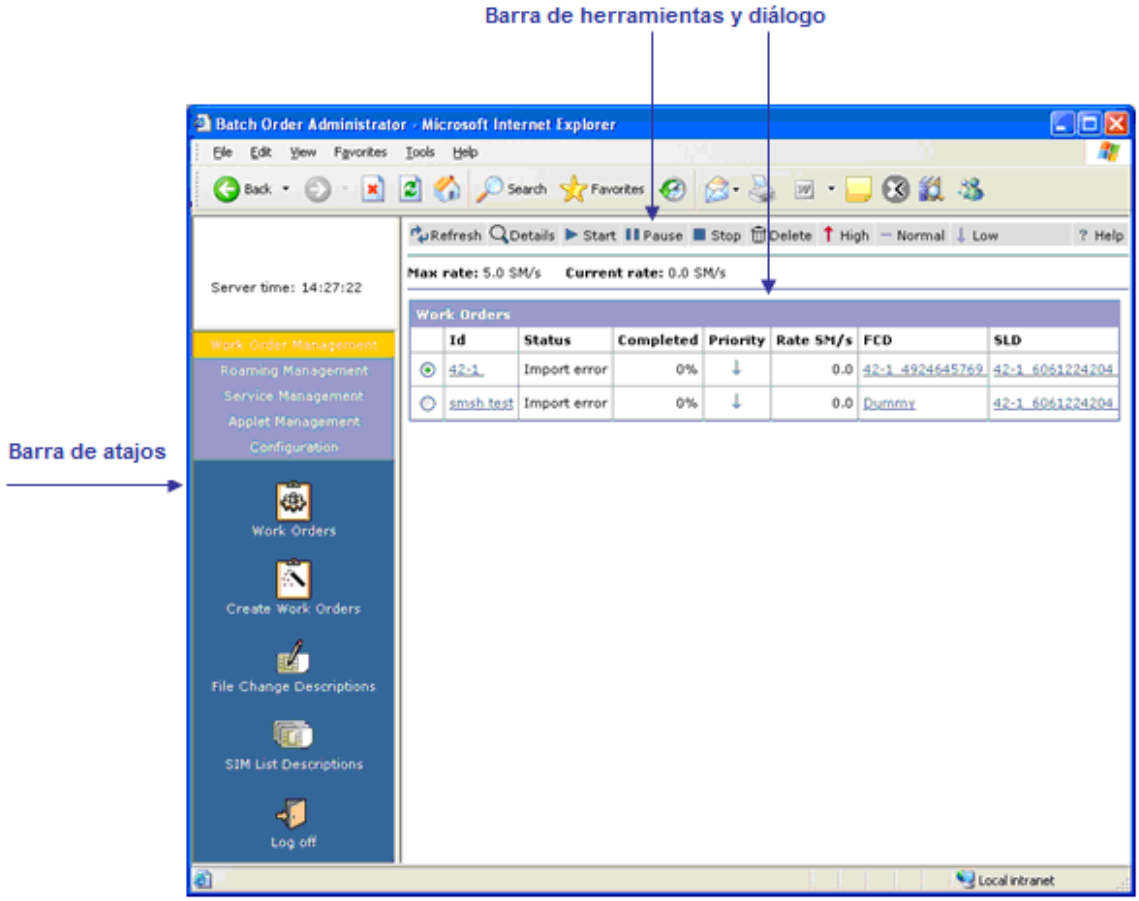


Figura 3.29 Pantalla principal de la interfaz de administrador de envío de órdenes por lote

3.7.13 Asistente para Customer Care (CCA)

El Asistente para Customer Care (CCA) es una herramienta basada en web que permite que el equipo de soporte al cliente realice descargas de configuraciones en-el-aire (OTA) para terminales de suscriptores. Al proveer este soporte avanzado al cliente, el nivel de servicio percibido por los suscriptores es más eficiente. Permite que el ejecutivo de soporte al cliente configure el terminal del suscriptor al descargar nuevos datos de configuración (como configuraciones MMS y GPRS) en-el-aire (OTA) y de manera transparente para el usuario.

3.7.14 Asistente para Self-Care (SCA)

El Asistente para Self-Care (SCA) es una herramienta basada en web que permite al propio suscriptor realizar descargas de configuraciones en-el-aire (OTA) para su terminal. Al proveer este soporte avanzado al cliente, el nivel de servicio percibido por los suscriptores es mucho mejor. Permite que el suscriptor configure su terminal al descargar nuevos datos de configuración (como configuraciones MMS y GPRS) mediante interfaz-aire (OTA).

3.7.15 Gestión de Reportes (RM)

El sistema de gestión de reportes es construido sobre la plataforma de inteligencia de negocios. Esta plataforma tiene dos interfaces:

- *Central Management Console*
- *InfoView*

Las interfaces del sistema de gestión de reportes están disponibles a través de cualquier clase de navegador Web. A partir de la página principal hay un fácil acceso a los clientes, herramientas administrativas, y documentación online. La página principal es accesada a través de la página principal de la DP haciendo clic en el hyperlink “Reporting Manager”.

3.7.16 Consola Central de Gestión

A través de la consola central de gestión los administradores del sistema pueden:

- Organizar usuarios, servidores, carpetas con contenidos, reportes y universos.
- Definir calendario y eventos
- Manejar parámetros y autenticación

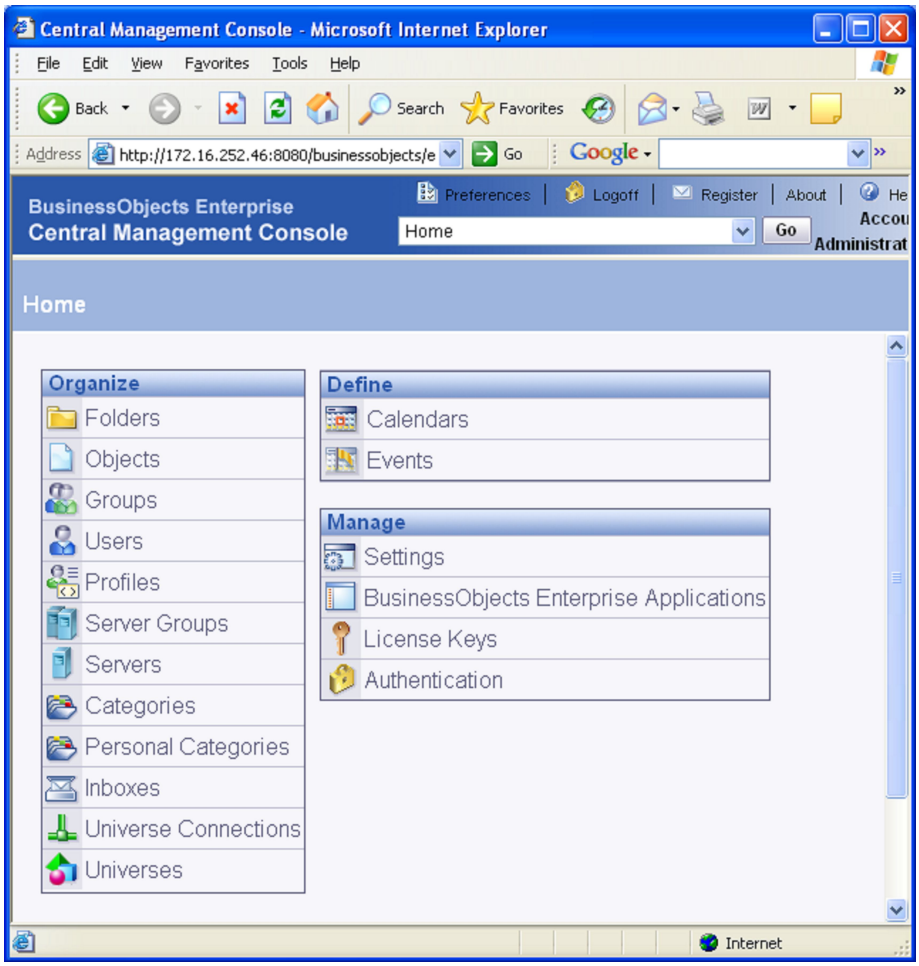


Figura 3.30 Pantalla Interfaz de Reporting Manager: Central Management Console de Business Objects

3.7.17 InfoView

Con InfoView, usuarios pueden:

- Crear, modificar, mirar y ejecutar reportes

3.8 Integraciones y Personalizaciones

3.8.1 SMS-C

Se define un protocolo SMS-C como la implementación específica de un protocolo SMS-C por un suministrador. Esto significa que cada implementación de protocolo SMS-C de suministrador es considerada como un protocolo SMS-C exclusivo. El diseño contempla conexiones por SMPP con dos SMS-Cs instalados en la operadora. Los siguientes protocolos son soportados por la solución.[33]

3.8.2 SMPP – Short Message Peer To Peer

Tabla 3.10 Short Message Peer to Peer

Suministrador de la SMS-C	Versión de Protocolo
Aldiscon-Logica	Version: 3.3, 3.4, 5.0
Comverse	Version: 3.3, 3.4, 5.0
Huawei, China	Version: 3.3, 3.4
Huges Software Systems, HSS	Version: 3.4
Openwave, Homisco	Version 3.4
UniSys	Version: 3.3

3.8.3 UCP – Universal Computer Protocol

Tabla 3.11 Universal Computer Protocol

[33] Protocolo de ejecución independiente (BIP) ,© Giesecke & Devrient ,GmbH, 2006

Suministrador de la SMS-C	Versión de Protocolo
CMG Telecommunication	Version: 3.1.2, 3.1.4, 3.5, 4.0
SEMA Group	Version: 1,2 (supports parts of CMG 3.1.2)

3.8.4 OIS – Open Interface Specification

Tabla 3.12 Open Interface Specification

Suministrador de la SMS-C	Versión de Protocolo
SEMA	Version: 5.0, 6.0, 7.4

3.8.5 NOKIA Cimd2 – Computer Interface to Message Distribution

Tabla .3.13 Computer interface to message distribution

Suministrador de la SMS-C	Versión de Protocolo
China Mobile Communications corporation	Version: 2.0, 3.0

3.8.6 Sistema de Gestión de Red (NMS)

Contadores de desempeño y alarmas en DP Basic Framework están disponibles por SNMP (Simple Network Management Protocol). Con un navegador SNMP, los contadores pueden ser pos-procesados para obtener una

presentación adecuada de las estadísticas y alarmas que pueden ser monitoreadas con un mínimo de mantenimiento manual

3.8.7 Applet de detección de IMEI en tarjetas SIM

Con el fin de realizar la detección automática de dispositivo (ADD – Automatic Device Detection) la solución necesita de un sistema de detección de IMEI Tracking que deberán estar instalados en las tarjetas SIM para detectar los cambios de terminales y emitir descargas de configuraciones para estos dispositivos. Opcionalmente, existe un sistema de detección de dispositivos basada en la red SS7. En este caso, el applet existente debe ser responsable de verificar cambios de terminal a través de comparaciones de IMEI y, al detectar un cambio, enviar un SM de 8-bit con IMEI a la plataforma de aprovisionamiento para identificar el modelo del terminal y sus capacidades, y enviará las configuraciones adecuadas al terminal. Este applet es configurado para enviar el SM a una dirección de destino específica asociada a la plataforma de gestión de terminales. La operadora deberá configurar las conexiones SMS-C y/o de red para redireccionar estos mensajes a la plataforma de gestión y aprovisionamiento de terminales.

3.8.8 Integración Opcional a la Red SS7: HSMP

El sistema de entrega de paquetes de alta velocidad (HSMP) permite manejar de manera flexible y eficiente grandes cantidades de SMS de una red GSM/3G, sin la necesidad de involucrar la SMS-C.

El HSMP ofrece un canal de entrega de SMS mejorado para los servicios de gestión de tarjetas SIM, applets Java y terminales. El producto atiende la demanda creciente de administrar y gestionar tarjetas SIM over-the-air. Campañas de actualizaciones de tarjetas SIM son ejemplos de actividades que pueden ser beneficiadas significativamente por un aumento del throughput y por un costo reducido por unidad de throughput. Además de aumentar la capacidad de SMS para la operadora y al mismo tiempo reducir los costos, el HSMP también mejora la experiencia al usuario por reducir el tiempo de entrega de las mensajes y por hacer que el tiempo de entrega sea más fiable que cuando se utiliza la SMS-C. También se puede citar otros beneficios:

- La funcionalidad de almacenar y enviar (store and forward) para el tráfico interactivo se encuentra ahora en la plataforma y no en la SMS-C. Un componente de la red de entrega de SMS es removido. Con eso tenemos un resultado de mejor disponibilidad, control y tiempos de respuestas más rápidos;

- Los reportes de estatus no son más necesarios. Ya no hay necesidad de esperar por este tipo de reportes generados en la SMS-C;

- Los tiempos de respuestas son más rápidos ya que ésta tecnología reduce el tiempo total en 1.5 segundos para el primer mensaje de respuesta.

- Otra tecnología única también patentada para reducir el tiempo total para un contexto de dos direcciones es relacionada en ejecutar algunos comandos de la SMS-C a la HLR en paralelo al contrario de la actual manera secuencial.

- La funcionalidad de horarios de re-tentativa (*retry*) fue hecha especialmente para el tráfico SFM, configurado por tipo de tráfico en tiempo real. Las SMS-Cs tienen un perfil de re-tentativas que trabajan con mensajes comunes, con el objetivo único de llegar a su destino, sin focalizar en el

tiempo total de entrega. Una SMS-C conectada al servidor trabajando con su mejor configuración, con varias re-tentativas, entrega el mensaje en 30 segundos como mejor tiempo.

- Con HSMP una SMS-C común no se carga por completo con el tráfico de OTA. Eso permite que la SMS-C, con sus licencias y capacidad, focalice los mensajes peer-to-peer de los usuarios.

- Al disminuir la carga de la SMS-C permite reducir la necesidad de comprar más licencias de tráfico pico para la SMS-C;

- Interfaces múltiples entre el HSMP y la red SS7 tienen como resultado una redundancia y/o aumento de optimización de capacidad/tráfico;

- La señalización del tráfico en la red SS7 optimiza y hay una minimización del impacto de performance en el HLR, pues el HSMP puede hacer *cache* de los datos relacionados a los suscriptores;
- Si la operadora prefiere, la SMS-C puede ser configurable como una solución de *backup* para el HSMP para que puedan ser hechos los mantenimientos y se puedan mantener las capacidades de entrega;
- El HSMP usa una pila de SS7. El software implementa todas las camadas SS7 del *Message Transfer Part* (MTP) nivel 3, hasta el *Mobile Application Part* (MAP).
- Usando la interfaz de señalización MAP es posible tener diálogos de señalización apropiados con el *Mobile Switching Centre, Visitor Location Register* (MSC/VLR), Home Location Center (HLR) así como otros nodos en la red GSM/3G.

Algunas de las funcionalidades ofrecidas por la solución son:

- Tratamiento de re-tentativas (*Retry Handling*)

- Tratamiento de alertas del HLR para caso de suscriptor ausente (*HLR Alert Handling – Absent Subscriber*) Para la situación en que el HLR ha registrado que el suscriptor no está activo, la plataforma espera por la alerta enviada por el HLR para intentar nuevamente entregar los mensajes.
- Esquemas de re-tentativa flexibles para caso de error temporario (*Flexible Retry Schemes – Temporary Error*) Cuando la red reporta problemas temporarios que impiden la entrega (como sobrecarga o fallas en la red) es aplicado un esquema flexible de re-tentativas, con posibilidad de diferentes perfiles dependiendo de la aplicación que envía (SFM, JAM, TPM etc.)
- Tratamiento de códigos de errores del *handset* (*Error Code Handling*) HSMP trata los errores originados del terminal mapeando para los errores típicos (temporario, permanente etc.).
- Utilización del *flag* "*More Messages to Send*" Cuando se utiliza este *flag*, la estación radio-base intenta mantener el canal de radio abierto esperando por más mensajes, ahorrando recursos de red y permitiendo menor tiempo de entrega.
- Tratamiento de dirección de suscriptor (*Subscriber Address Handling*) A través de utilización de un cache con la información de la última MSC para un determinado IMSI es posible reducir la cantidad de consultas en el HLR y también el tiempo de entrega.
- Tratamiento de versión MAP (*MAP Version Handling*)
- La configuración es hecha utilizando las mismas herramientas de la plataforma DP.

El tratamiento de alarmas se lo realiza utilizando las mismas herramientas de la plataforma DP, simplificando la integración por aprovechar la integración existente.

3.8.9 Integración Opcional a la Red de Datos: BIP

Como el tamaño de la memoria de las tarjetas SIM y USIM está siempre aumentando, más datos y aplicaciones más grandes están siendo almacenados en las tarjetas. Para manejar eficientemente el crecimiento de los datos y aplicaciones, es necesario un canal de datos con mucho más capacidad para la (U)SIM que los canales de SMS que son históricamente usados. Para solucionar esto, se ha introducido la solución BIP (Bearer Independent Protocol) que permite la descarga de datos para las tarjetas SIM y USIM a través de los servicios de datos TCP/IP como GPRS, EDGE y 3G. Servicios de RFM (Remote File Management) y RAM (Remote Application Management) si tornarán significativamente más veloces a través de BIP. A causa de esto la tecnología es ideal para manejar las tarjetas SIM con servicios como descargas de aplicativos Java, respaldo de agenda y activación over-the-air. El BIP es implementado como una función integral en todos los componentes de la plataforma asegurándose que manejar las tarjetas SIM puede ser transparentemente hecho con BIP en lugar de SMS. El BIP fue hecho para soportar todos los tipos de casos de uso de SIM OTA, por ejemplo el aprovisionamiento automático de los SIM o actualización de millones de tarjetas SIM al mismo tiempo usando el BOM. A continuación se indican algunos beneficios comerciales de BIP: [33

- Permite el uso eficiente de RAM (*Remote Application Management*) para corregir problemas o actualizar las tarjetas con nuevos *applets* Java, reduciendo la necesidad de cambiar tarjetas con errores o para servicios de alta capacidad como respaldo de agenda, así reduce el tiempo de penetración en el mercado;
- Alta capacidad de manejar los datos de los subscriptores, como descarga del listado de *roaming* o respaldo de SIM;

- Ahorro de SMS-C, SS7 y capacidad de radio y costos, por el uso del canal TCP/IP y GPRS en lugar de SMS, para entregar las descargas.

El BIP Server es un plug-in para el servidor de transporte y a causa de esto provee un ambiente muy fácil para una aplicación enviar datos para la SIM. La aplicación envía los datos (APDUs) de la misma manera que envía normalmente, el servidor BIP verifica si la SIM y el terminal soportan BIP, y el tipo de BIP que es soportado por la SIM. Si todas las condiciones para uso de BIP son satisfechas, el canal BIP es utilizado, caso contrario los datos son enviados por SMS, de forma transparente para el aplicación.

El BIP Server es un plug-in para el Transport Server y a causa de esto provee un ambiente muy fácil para una aplicación enviar datos para la SIM. La aplicación envía los datos (APDUs) de la misma manera que envía normalmente, el servidor BIP verifica si la SIM y el terminal soportan BIP, y el tipo de BIP que es soportado por la SIM (CAT-TP o SBC). Si todas las condiciones para uso de BIP son satisfechas, el canal BIP es utilizado, en otro caso los datos son enviados por SMS, de forma transparente para el aplicación.

3.9 Implantación de la Solución

3.9.1 Visión General del Arquitectura Técnica

De acuerdo con el objetivo propuesto en este estudio, se propone una arquitectura de un nodo, con redundancia interna de todos los elementos. Además de la redundancia interna de todos los elementos – que incluye también

los procesadores (la maquina principal tendría 8 cores) –, también se considera un disk array extra y una placa extra de conexión del servidor con el disk array.

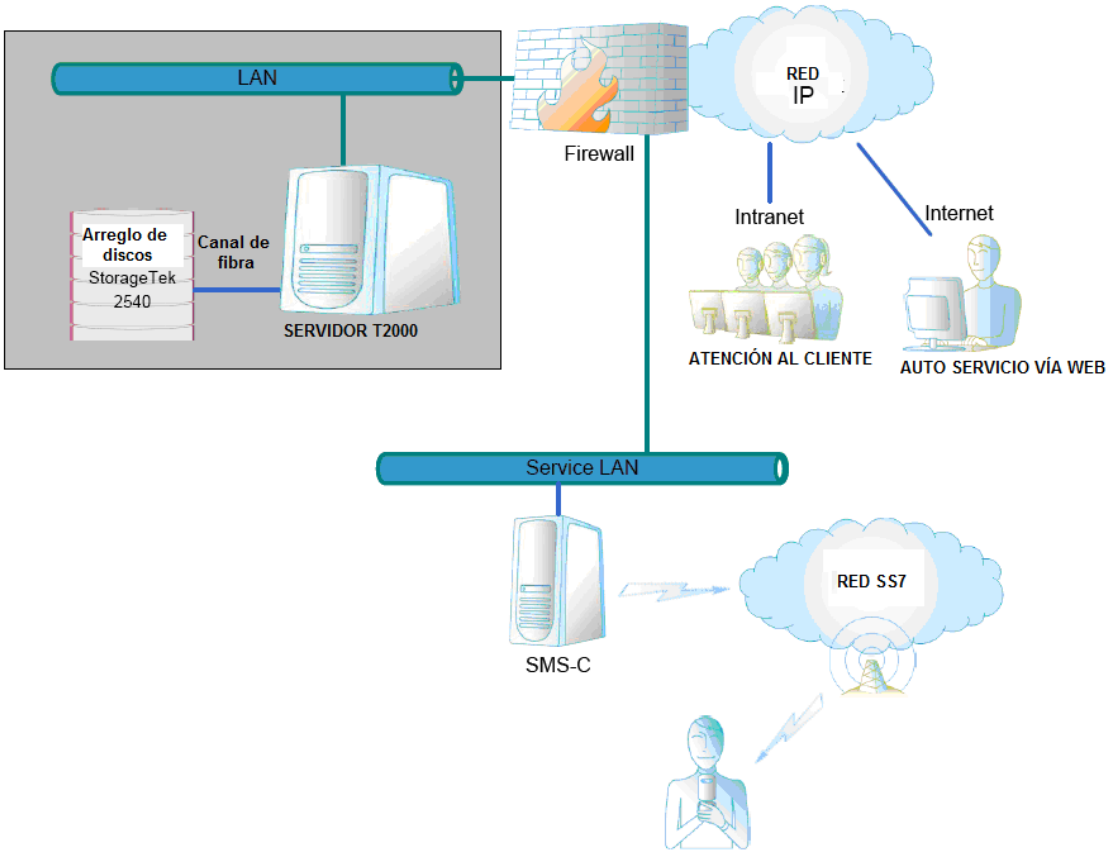


Figura 3.31. Visión general del arquitectura técnica

Para garantizar la escalabilidad futura, en caso de que el operador lo requiera, es importante mencionar que la solución podría ser reconfigurada para una arquitectura altamente disponible, con balance de carga. La opción Basic Framework Multi Node tiene una solución escalable, altamente redundante y económica. Esto es debido a la escalabilidad horizontal, por ejemplo, distribuyendo los procesos DP en varios nodos de hardware, con una cantidad de nodos flexible.

3.9.2 Dimensionamiento

Hay dos criterios básicos para dimensionamiento de la solución. Uno de ellos es la capacidad de almacenamiento del disk array, que está directamente ligada a la cantidad de tarjetas SIM aprovisionadas en la solución.

La cantidad de tarjetas SIM aprovisionadas es normalmente 40% hasta 100% mayor que la cantidad de suscriptores de la operadora, a causa de que las tarjetas SIM deben estar cargadas/aprovisionadas antes de que sean asociadas a un suscriptor (tarjetas pre activadas). El número de tarjetas SIM aprovisionadas es entonces cerca de la suma de las tarjetas que están en producción, con un número MSISDN asociado (tarjetas en las manos de suscriptores mas las tarjetas de “kits prepago”, con número MSISDN pre-asociado) y las tarjetas almacenadas para venta, sin un numero MSISDN asociado. El diseño en estudio presenta un disk array de 1752 GB de capacidad, con redundancia interna, que es estimada de ser suficiente para 10 millones de suscriptores, este cálculo se lo ha realizado haciendo una estimativa en base a la capacidad de espacio en el disco por usuario. Otro criterio y complemento para el dimensionamiento de la solución es la capacidad computacional (capacidad de procesamiento) de la solución, que está directamente ligada al número de mensajes (SMS) que pueden ser procesadas por segundo. En esta arquitectura, la escalabilidad es horizontal, que significa que más capacidad es añadida por la adición de nuevos servidores idénticos al servidor existente. Un servidor SunFire T2000 en una configuración de un nodo como la presentada en esta solución puede llegar hasta 100 SMS por segunto de throughput, considerando al throughput como la capacidad de procesamiento de un SMS por segundo, que es estimado de ser suficiente para 10 millones de suscriptores para los servicios contemplados en este análisis. Todavía se debe observar que esta estimativa de throughput es extremamente dependiente de los servicios instalados y de la manera como la operadora los

utiliza, siendo en último análisis la capacidad de throughput que debe ser observada para crecimiento de la capacidad de la solución.

En la tabla debajo se puede encontrar un resumen de las capacidades máximas estimadas de la plataforma que suplirían a las necesidades de una operadora:

Tabla 3.14 Resumen de las capacidades máximas de la solución

	Capacidad máxima de la solución
Cantidad de suscriptores	5.000.000
Cantidad de tarjetas aprovisionadas	10.000.000
Throughput en la hora pico	100 SM/s

3.9.3 Software

Los siguientes tipos de software de están incluidos en este estudio, en su versión más reciente:

- *Delivery Platform Basic Framework (DP)*
  - *Batch Order Manager (BOM) with JAM option*
  - *Repository Integration Server (RIS)*
  - *Reporting Manager (RM*)
- Sistema de Gestión de tarjetas SIM
  - *SIM File Manager (SFM) Server*
  - *Java Applet Manager (JAM) Server*

- Sistema de Aprovisionamiento

- Servidor para gestión de terminales (DMS)
  - *Terminal Provisioning Manager (TPM)*
  - *Terminal Capabilities Repository (TCR*
  - *Customer Care Assistant (CCA)*
  - *Self-Care Assistant (SCA)*

Los siguientes software adicionales a la plataforma OTA están incluidos en este estudio:

- Sun Solaris 10
- Oracle 10

3.9.4 Hardware

En la tabla 3.15 se puede encontrar el listado de hardware incluido en este estudio:

Tabla 3.15 Listado de hardware

Solución para un nodo		
1	T20Z108B-16GA2G	Servidor Sun SPARC Enterprise T2000, 8 procesadores core 1.2 GHz UltraSPARC T1, memoria 16 GB DDR2 (16*1 GB DIMMs), discos duros de 2*73GB 2.5" 10K rpm SAS , 1 DVD-RO/CD-RW , 2 (N+1) respaldo de alimentación, 4 puertos ethernet 10/100/1000, 1 puerto serial, 3 puertos PCI-E, 2 puertos PCI-X, Java Enterprise System pre instalado con compilador RoHS-5
2	X311L	Cable de potencia localizado Asiatico o Americano, Hazard Class Y, compilador RoHS-5
1	SOLZ9-10DC9A7M	Media Solaris 10 1/06
2	SG-XPCI1FG-QF4	Adaptador Host Bus Sun Storagetek PCI-X empresarial de 4 Gb, compilador RoHS 6
Arreglo de Disco Externo		

2	XTA2540R01QA1E730	Arreglo Sun StorageTek™ 2540 FC, Bandeja Rack, 1752GB, controladores12*146GB 15Krpm SAS, cache FC HW 2*512MB,controladores RAID, 2 fuentes de energía redundante, 2* ventiladores de enfriamiento redundantes, 4* SFPs de onda corta, software para gestión de arreglos comunes y 2* dominios de almacenaje utilizando software Sun Storage Tek(TM), RoHS-5
2	XTA-2500-2URK-19U	Rack universal Sun StorEdge™ con riel deslizante, RoHS-5
4	X311L	Cable de potencia localizado Asiatico o Americano, Hazard Class Y, compilador RoHS-5
2	SG-XPCI1FG-QF4	Cable óptico RoHS-6 compilante de 2M LC a LC FC
Rack		
1	SR2-2938-XPDS	Rack Sun 900-38 con puerta delantera y PDS instalado.
1	X6828A	Cable de potencia No. Amer., Sun Rack PDS
Laptops		
2	E6500	Dell Latitude E6500 (250GB HD, 2GB RAM)

3.9.5 Respaldos Automáticos

Las plataformas incluyen respaldo automático basado en disco. El disk array, dependiendo de la cantidad de suscriptores en la plataforma de la operadora, puede ser dividido durante la configuración del mismo. El propósito de utilizar un respaldo basado en disco es ganar velocidad en la recuperación de los datos. Además se recomienda que la operadora utilice un respaldo con un servidor de tape para que ningún dato sea perdido durante una situación de desastre.

Se recomienda el respaldo diario de tres ítems: el directorio de aplicaciones, el directorio de logs y la base de datos de usuarios. Las modificaciones que ocurren durante el día en la base de datos pueden ser recuperadas, en caso de desastre, través de logs. El respaldo debe ocurrir de manera online, y debe ser realizado en periodo de bajo tráfico, generalmente en

torno de 2 AM. Las rutinas de respaldo no deben causar interrupción, suspensión o deterioración en la plataforma, servicios relacionados a ella o plataformas externamente conectadas.

CAPíULO IV

PRESUPUESTO REFERENCIAL

4.1.1 Introducción

En este capítulo consta un análisis del costo global de las plataformas descritas en este estudio, esto incluye la plataforma de gestión de terminales y la plataforma para gestión de tarjetas SIM, licenciamiento, soporte y mantenimiento y hardware. Este estudio está dividido en los costos licenciamiento de software de las plataformas, hardware, opciones de BIP y HSMP.

Se debe considerar que para efectos de cálculo de licencias de gestión de terminales, fue considerado que la operadora no va a configurar envío automático de configuraciones para todos los cambios de terminales. En estas condiciones, fue estimado un total de 25.000 configuraciones por mes.

4.1.2 Plataformas de Gestión de terminales, tarjetas SIM, Software y Licenciamiento

Se ha considerado los rubros necesarios para la integración de las plataformas con el software necesario para el total funcionamiento descrito en este estudio, tanto para la gestión de terminales como para la gestión de tarjetas SIM.

Tabla 4.1 Costo de plataformas de gestión de terminales y tarjetas SIM

Producto	**Cantidad**	**Descripcion**	**Precio USD INCOTERM 2000 DDU**
Software Licencias			
DP Basic Framework (DP) Plataforma Básica	1	Plataforma OTA	
Repository Integration Server *Servidor de Repositorio de Integración*	1		
Reporting Manager (RM) *Gestión de Reportes*	4 usuarios		
Batch Order Management (BOM) *Gestión de órdenes de lotes*	1		
BOM JAM Option *Opción JAM*	1		
TCR Update Service *Servicios de Axtualización TCR*	1 año	Programa TCR por 1 año	
Gestión de Tarjetas SIM	900.000 subscriptores		

SIM File Management (SFM) *Gestión de archivos SIM*			
JAVA Applet Management (JAM) Server *Servidor para Gestión de Aplicaciones JAVA*			
Gestión de Terminales	900.000 subscriptores		
Device Manager Server (DMS) *Servidor de gestión de terminales*			
Terminal Capabilities Repository (TCR) *Repositorio de capacidades del terminal*			
Terminal Provisioning Manager (TPM) *Gestión de aprovisionamiento de terminales*			
Customer Care Assistant (CCA) *Asistente de Atención al cliente*			
Self Care Assistant (SCA) *Autoasistencia*			
Total Licencias de Software			700,000

Tabla 4.2 Costo soporte y mantenimiento

Producto	Cantidad	Descripcion	Precio USD INCOTERM 2000 DDU
Soporte y Mantenimiento	1 año	Primer año de soporte y mantenimiento	100,000

4.1.3 Hardware

Para el costo del hardware necesario para la integración de las plataformas en un solo nodo se ha considerado los costos de un solo proveedor.

Tabla 4.3 Costo de hardware

1	T20Z108B-16GA2G	Servidor Sun SPARC Enterprise T2000, 8 core procesador 1.2GHz UltraSPARC T1, memoria 16GB DDR2 (16 * 1GB DIMMs), disco duro 2 * 73GB 2.5" 10K rpm SAS, 1 DVD-RO/CD-RW slimline drive, 2 (N+1) generador de potencia, 4 puerots ethernet 10/100/1000, 1 puertos serial, 3 PCI-E slots, 2 PCI-X slots, Solaris 10 and Java Enterprise System software pre-instalado. RoHS-5 compliant
2	X311L	Cable de potencia localizado Asiatico o Americano, Hazard Class Y, compilador RoHS-5
1	SOLZ9-10DC9A7M	Media Solaris 10 1/06
2	SG-XPCI1FC-QF4	Adaptador Host Bus Sun Storagetek PCI-X empresarial de 4 Gb, compilador RoHS 6
External Disk Array		
2	XTA2540R01A1E730	Arreglo Sun StorageTek™ 2540 FC, Bandeja Rack, 1752GB, controladores12*146GB 15Krpm SAS, cache FC HW 2*512MB,controladores RAID, 2 fuentes de energía redundante, 2* ventiladores de enfriamiento redundantes, 4* SFPs de onda corta, software para gestión de arreglos comunes y 2* dominios de almacenaje utilizando software Sun Storage Tek(TM), RoHS-5
2	XTA-2500-2URK-19U	Rack universal Sun StorEdge™ con riel deslizante, RoHS-5
4	X311L	Cable de potencia localizado Asiatico o Americano, Hazard Class Y, compilador RoHS-5
2	X9732A-Z	Cable óptico RoHS-6 compilante de 2M LC a LC FC
Rack		
1	SR2-2938-XPDS	Rack Sun 900-38 con puerta delantera y PDS instalado.
1	X6828A	Cable de potencia No. Amer., Sun Rack PDS
Laptops		
2	E6500	Dell Latitude E6500 (250GB HD, 2GB RAM)
	TOTALES HARDWARE	**INCOTERM 2000 DDU** **USD 70.000**

4.1.4 Opción BIP

Debido a que la opción BIP no es un software indispensable para el funcionamiento de las plataformas, se lo ha considerado como un rubro adicional e incluyendo licenciamiento, soporte y mantenimiento del mismo:

Tabla 4.4 Costo de opción BIP

OPCION BIP			INCOTERM 2000 DDU
BIP Licencia	1	900.000 subscriptores	USD 90,000
Support & Maintenance	1 año		USD 15,000
Opción BIP	1		USD 25,000

4.1.5 Opción HSMP

Debido a que la opción HSMP no es un software indispensable para el funcionamiento de las plataformas, se lo ha considerado como un rubro adicional e incluyendo licenciamiento, soporte y mantenimiento del mismo:

Tabla 4.5 Costo de opción HSMP

OPCION HIGH SPEED MSG			INCOTERM 2000 DDU
Licencia HSMP	1		USD 60,000
Soporte y Mantenimiento	1 year		USD 10,000
Opción de Entrega de Servicios HSMP	1		USD 70,000

4.1.6 Costo Total

El costo total del proyecto de gestión de terminales y tarjetas SIM, es la suma de todas las cantidades descritas anteriormente. La Tabla 4.6 indica un resumen de todos los rubros sin considerar las opciones de BIP y HSMP.

Tabla 4.6 Costo total de las plataformas incluido soporte

Producto	Precio USD INCOTERM 2000 DDU
Licencias de Software	USD 700,000
Soporte y Mantenimiento	USD 100,000
Hardware	USD 70,000
TOTAL	**USD 870,000**

La Tabla 4.7 indica el resumen de los rubros totales considerando las opciones de BIP y HSMP.

Tabla 4.7 Costo total de las plataformas incluido opciones BIP y HSMP

Producto	Precio USD INCOTERM 2000 DDU
Total Licencias de Software	USD 700,000
Soporte y Mantenimiento	USD 100,000
Hardware	USD 70,000
LICENCIA BIP	USD 90,000
Soporte y Mantenimiento	USD 15,000
BIP OPTION	USD 25,000
LICENCIA HSMP	USD 60,000
Soporte y Mantenimiento	USD 10,000
Opción HSMP	USD 70,000
TOTAL	**USD 1,140,000**

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

La diversidad de dispositivos móviles (terminal y SIM) es solamente alcanzada por la diversidad de suscriptores de hoy. Esta es la razón de que la provisión de una plataforma que sea completamente operacional con una cantidad mínima de esfuerzo de configuración e integración, flexible y escalable lo suficiente para atender a las necesidades de las operadoras en la medida que ellas avanzan a soluciones más sofisticadas.

En este estudio se ha previsto un punto de control único para gestión OTA (Over-The-Air) de tarjetas SIM y terminales. La plataforma dirigida a eventos permite el automatización de procesos de negocio necesario para una amplia gestión del dispositivo móvil (terminal + SIM) que utiliza inteligencia sobre tres elementos – el suscriptor, la SIM y el terminal – para permitir a las operadoras manejar exitosamente los dispositivos de sus suscriptores.

Del estudio realizado, se ha llegado a la conclusión que la solución tiene los siguientes beneficios:

- Un empaquetamiento estandarizado que permite rápido soporte y una rápida implementación y puesta en marcha de las plataformas de gestión de terminales y tarjetas SIM

- Repositorios de terminales, SIM y suscriptores abiertos y unificados (permitiendo una gestión más relevante, con toma de decisiones basada en datos actuales e históricos), este repositorio permitirá asi mismo, la verificación de la utilización de gamas de los terminales de los usuarios, siendo un dato estratégico en la planificación comercial de la operadora.

- La plataforma OTA para gestión de tarjetas SIM y terminales brinda una amplia gama de posibilidades de integración a redes y sistemas abiertos y simplificados par la operadora, debido a que las plataformas se rigen a estándares, haciéndolas compatibles con diferentes fabricantes de plataformas de SMSC, terminales, tarjetas SIM.

- La utilización de las plataformas dentro de la red celular representa una solución completa que atiende a los requerimientos de gestión de tarjetas SIM, gestión de *applets* Java, detección de terminales, configuración de terminales, gestión de datos e implementación de reglas de negocio.

- La implementación de esta plataforma permite a la operadora maximizar sus ingresos de servicios de datos y minimizar sus costos de llamadas de *Customer Care* relativos a gestión de terminales y SIM.

- Repositorio de capacidades de Terminal (TCR) permitiendo una altísima tasa de reconocimiento de terminales (más de 99%), de diferentes fabricantes alrededor del mundo con detalles de las capacidades de terminales tal es como servicio de MMS, WAP, WEB *browser*, definición de la resolución de la pantalla, etc, su soporte a OTA y sus protocolos, y que es actualizado aproximadamente cada mes.

- La plataforma para gestión de tarjetas SIM también brinda soporte nativo a 3G (USIM, ISIM) y dual IMSI, esto significa en caso de existir cambios en parámetros del perfil eléctrico de la SIM, o en sus aplicaciones, la operadora no tendrá que reemplazar las tarjetas SIM a sus usuarios, nada más tendrá que enviar la actualización de los parámetros vía interfaz aire, representando un significativo ahorro para la empresa y una alta efectividad de alcance a los usuarios.

REFERENCIAS BIBLIOGRÁFICAS

[1] Realización técnica del servicio de SMS, Doc. No. MPM05:0037, 2006, Smartrust

[2] 3GPP TS 23.048: Mecanismos de seguridad para aplicaciones Toolkit de tarjetas (U) SIM.

[3] Short Message Service Center, http://es.wikipedia.org/wiki/Short_Message_Service_Center, 05/12/2008

[4] ETSI GSM 11.14 Sistema Celular Digital de Telecomunicaciones (fase 2+), especificación de las aplicaciones de la tarjeta SIM – Equipo móvil

[5] GSM 11.11 Sistema Celular Digital de Telecomunicaciones (fase 2+), especificación de las aplicaciones de la tarjeta SIM

[6] USIM, http://es.wikipedia.org/wiki/USIM, 15/12/2008

[7] Telecomunicaciones móviles, Marcombo, Eugenio Rey Veiga, Capítulo 19 “Seguridad en Sistemas de comunicaciones móviles”

[8] Media Formats , http://java.sun.com/javase/technologies/desktop/media/jmf/2.1.1/formats.html, 01/01/2009

[9] SMPP, http://en.wikipedia.org/wiki/Short_message_peer-to-peer_protocol, 27/02/2008

[10] 3GPP TS 23.041: “Realización Técnica del envío de mensajes cortos en broadcast (SMSCB)”

[11] Recomendaciones de Hardware y Software DP, Doc. No. MPM02:0055, 2005, Smartrust.

[12] Contadores y Calculadores DP Basic Framework, Doc. No. 10542-080, Revisión: B. 2005-11-14, Smartrust.

[13] Tipos de Alarmas de la plataforma Basic Framework, Doc. No. 10542-078, Revisión: C. 2006-08-31, Smartrust.

[14] Especificación de formato de CDR, 10542-086, Revisión: A. 2005-09-20, Smartrust.

[15] Descripción plataforma Gestión de Dispositivos, Febrero 2005, Gemalto

[16] Guía de programación API, Doc. No. 10542-123 Revisión: A. 2005-09-28,Smartrust

[17] GSM 03.40 Servicio de Mensajería Corta

[18] JAM Description, Doc No. MPM06:0031, 2006, Smartrust

[19] Descripción BOM - Opción JAM , Doc No. MPM06:0010, 2006, Smartrust

[20] OTAP-1100-FD, 2001, LOGICA Mobile Networks Limited

[21] 3GPP TS 51.011 (versión 4.x.x): "Especificación de la interfaz tarjeta SIM con Terminal móvil

[22] Descripción de Repositorio de Capacidades del Terminal, Doc. No. MPM07:0006, 2006, Smartrust

[23] Revisión Técnica plataforma OTA, No. Doc. 108932ª0, Junio 06 2003,Gemplus

[24] Terminales Soportados en el repositorio de capacidades del Terminal 2008-7, Smartrust

[25] Administrador de repositorio de capacidades del Terminal, No. Doc 846762-107, 2007-02-06, Smartrust

[26] 3GPP TSG SA WG3 Security – S3#30, Octubre 2003, Gemalto, Oberthur, Schumberger

[27] Desarrollo de Aplicaciones Java para tarjetas SIM, January 2001,Sun Developer Network

[28] Solutions Smartrust, http://www.smarttrust.com/mobile_solutions/mobile_solutions_certified_program.asp, 10/01/2009

[29] Manual de usuario para gestión de alarmas, Doc. No. 10542-081, 2005-09-30, Smart Trust

[30] Guía de usuario SysView, Doc. No. PS 05:0016, Agosto 2005, Smartrust

[31] 3GPP TS 11.11 v8.11.0 and ETSI TS 102 221 v5.0.0

[32] Manual de Operación BOM, Doc. No. 10543-125 Revisión: B. 2006-10-13., Smartrust

[33] Protocolo de ejecución independiente (BIP) ,© Giesecke & Devrient ,GmbH, 2006