# PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

## FACULTAD DE CIENCIAS E INGENIERÍA


# ANÁLISIS DE UN SERVICIO BANCARIO MÓVIL SEGURO UTILIZANDO UNA APLICACIÓN INSTALADA EN LA TARJETA SIM

Tesis para optar el Título de Ingeniero de las Telecomunicaciones, que presenta el bachiller:


**Jonathan Hendrick Narváez Moya**

**Asesor: Marco Antonio Mayorga Montoya**


Lima, abril del 2012

# RESUMEN

El presente trabajo de tesis presentará el análisis técnico y económico para un nuevo y seguro canal de bancarización ofrecido recientemente en nuestro país. Este canal se basa en el uso de una aplicación desarrollada por los proveedores de servicios móviles e instalada en la tarjeta SIM y que utiliza como medio de transporte la red móvil para conectarse a diversas plataformas bancarias y financieras, permitiendo a los usuarios efectuar operaciones como registro de bancos, almacenamiento de cuentas bancarias y tarjetas de débito/crédito, consulta de saldos, transferencias de fondos entre cuentas propias y/o terceras, pago de servicios asociados (luz, agua, etc), recargas prepago y consulta de ultimas transacciones.

En el primer capítulo de este trabajo se encontrarán las motivaciones, objetivos e hipótesis consideradas para la tesis. En el segundo capítulo se brindará la base teórica para el desarrollo de los servicios de valor agregado ofrecidos por un operador móvil usando como origen la tarjeta SIM, resaltando la importancia de estándares y especificaciones brindadas por diferentes organizaciones y que permiten la interoperabilidad necesaria para estos casos. En el tercer capítulo se presentará el análisis de la arquitectura del sistema, considerando tanto el lado del operador como el de la entidad bancaria. El cuarto capítulo mostrará los diferentes mecanismos de seguridad del servicio bancario a analizarse, con la finalidad de hacer frente a los diversos ataques sufridos por las entidades financieras. Finalmente, en el quinto capítulo se demostrará la factibilidad económica para sustentar la iniciativa de activar éste servicio en nuestro país.

El análisis a efectuarse tendrá como resultado ampliar el concepto de las bondades brindadas por un operador móvil más allá de la voz y la mensajería de texto, mediante los llamados servicios de valor agregado, para ser considerados como un partícipe importante del desarrollo de la tecnología móvil.

# DEDICATORIA

*A mi mamá Estela,*

*A mis padres, Chabu y Vicente,*

*A mis hermanos, Joseph y Ale.*

# AGRADECIMIENTOS

Agradezco a mi mamá Estela, por haberme dado todo su amor y por estar siempre a mi lado.

Agradezco a mi madre Chabu, que mediante su diario ejemplo se ha convertido en el principal motor para alcanzar mis objetivos. A mi padre, por las enseñanzas inculcadas y que me han servido para guiarme en mi vida.

Agradezco a mis hermanos, por su cariño brindado y la paciencia otorgada a pesar de las diferencias causadas por nuestras distantes edades.

Agradezco al Ingeniero Marco Mayorga por su continua preocupación y seguimiento para finalizar este trabajo de tesis, así como los conocimientos compartidos.

A mis compañeros de trabajo, sin cuyo valioso aporte no hubiera podido ser acabado esta monografía.

# ÍNDICE

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# ABREVIATURAS

*AES:* Advanced Encryption Standard.

*APDU:* Application Protocol Data Unit.

*ATR:* Answer to Reset.

*CMOS:* Complementary Metal Oxide Semiconductor.

*EMV:* Europay MasterCard VISA.

*HTTP:* Hypertext Transfer Protocol.

*ICCID:* Integrated Circuit Chip Identification.

*IMSI:* International Mobile Subscriber Identity

*MEL:* Maya Embedded Language.

*PCI DSS:* Payment Card Industry Data Security Standard.

*RSA:* Rivest, Shamir & Adleman.

*SMSC:* Short Message Service Center.

*SMPP:* Short Message Peer to Peer.

*SOAP:* Simple Object Access Protocol.

*SVA:* Servicio de Valor Agregado.

*USSD:* Unstructured Supplementary Services Data.

*VPN:* Virtual Private Network.

*WAP:* Wireless Application Protocol.

*WML:* Wireless Markup Language.

# GLOSARIO

*AES:* Elegido como el nuevo estándar de criptografía simétrica por ser inmune a ataques conocidos, tener un diseño simple y poder ser implementado en la mayoría de escenarios posibles desde dispositivos con recursos limitados (smart cards) hasta procesadores paralelos.

*APDU:* Es la unidad de transmisión de datos de las tarjetas inteligentes. Esta comunicación se realiza entre la tarjeta y el mundo exterior, como puede ser una lectora de tarjetas inteligentes. Existen dos clases de APDU: los comandos y las respuestas, cada uno con su formato definido por la ISO.

*CMOS:* Es el tipo de material con el que está basada la fabricación de un circuito especial llamado del mismo nombre *CMOS*, el cuál tiene la característica de consumir un nivel muy bajo de energía eléctrica cuando está en reposo.

*EMV:* Es un estándar global para las tarjetas de pago de crédito y débito basadas en la tecnología de smart cards.

*I-mode:* Es un conjunto de tecnologías y protocolos diseñados para poder navegar a través de mini páginas diseñadas específicamente para dispositivos móviles como teléfonos o PDA's. Para mostrar las páginas, utiliza un lenguaje muy parecido al HTML normal pero modificado para los teléfonos móviles.

*PCI DSS:* Es un estándar de seguridad que define el conjunto de requerimientos para gestionar la seguridad, definir políticas y procedimientos de seguridad, arquitectura de red, diseño de software y todo tipo de medidas de protección que intervienen en el tratamiento, procesado o almacenamiento de información de tarjetas de crédito.

*RSA:* Algoritmo asimétrico de encriptación, basado en la generación de un par de llaves diferentes conocidas como pública y privada, relacionadas entre sí. El emisor encripta el mensaje con la llave pública del receptor, quien utiliza su llave privada para desencriptar la data.

# INTRODUCCIÓN

Los teléfonos móviles se han convertido en una parte integral del panorama del siglo XXI con una penetración alrededor del mundo de 4,5 mil millones de suscriptores a finales del año 2011, según las cifras ofrecidas por la *Global Suppliers Association*[1] (GSA). Mientras que América del Norte y Europa tienen las tasas de penetración más alta, alcanzando el 100% en muchos países occidentales; en América del Sur y Asia representan los mercados móviles de mayor crecimiento. El teléfono móvil es el dispositivo que las personas llevan consigo en todo momento. Servicios más allá de voz y mensajes de texto están en auge en todo el mundo y los usuarios quieren los mismos servicios en su teléfono móvil que se puede obtener a través de una PC conectada a Internet.

Los teléfonos móviles representan una solución rentable para los usuarios de los bancos y servicios bancarios, las instituciones financieras y operadores, lo que les permite reducir la brecha digital en lugares donde la banca tradicional y los servicios de Internet son demasiado caros o simplemente no existen.

El espectacular aumento en el uso de teléfonos móviles ha sido seguido de cerca por el aumento del fraude móvil. Aunque deseosos de utilizar los servicios financieros móviles, muchos abonados se preocupan por el aspecto de la seguridad en la realización de transacciones financieras a través de la red móvil. De hecho, la falta de seguridad es vista como el mayor obstáculo en la adopción generalizada de los servicios financieros móviles. Las transacciones por Internet sufren el mismo problema, al igual que las transacciones de pago tradicionales. De esta manera, la prevención del fraude se ha convertido en un ingrediente esencial en el éxito de todos los modos diferentes de las transacciones financieras.

En el presente trabajo de investigación se presentará los conceptos de la tecnología móvil actual y como ésta puede ser utilizada para el diseño e implementación de una arquitectura sobre la cual se realicen transferencias bancarias seguras.

[1] *La GSA representa mundialmente a los proveedores móviles, dedicados a infraestructura, semiconductores, terminales, desarrollo de aplicaciones y servicios, así como soporte de servicios.*

# CAPÍTULO 1

# ASPECTOS GENERALES

## DEFINICIÓN DEL PROBLEMA

A través del tiempo, las entidades financieras han diversificado los canales bancarios para atender la gran cantidad de clientes que manejan, como se grafica en la Figura 1.1, donde se puede observar que cada canal ha sido implementado de acuerdo a la tendencia tecnológica. Hoy en día, el teléfono móvil se convierte en un elemento masivo y amigable que permite integrar los sistemas financieros a la vida cotidiana de los clientes. Sin embargo, lo más importante para estos fines es brindar un alto nivel de seguridad que ofrezca la confianza necesaria para realizar transacciones de este tipo.

Gran parte de las soluciones brindadas por las entidades bancarias es la extensión de sus páginas de Internet para los dispositivos móviles inteligentes o mejor

conocidos como *Smartphones*. Sin embargo, al finalizar el 2011 existe un 38% de suscriptores usando *Smartphones* a nivel mundial, tal como lo indica comScore; y al cierre del segundo trimestre del año 2011, solo el 12% de la población en Perú cuenta con este tipo de dispositivos, según lo informado por la versión digital del diario de negocios "*biznews*", dejando de lado un alto porcentaje de los usuarios de servicios móviles. Por ello, para llegar a todos los suscriptores móviles se debe considerar un elemento seguro, masivo y que además permita diseñar una aplicación estándar y de fácil manejo para el usuario.

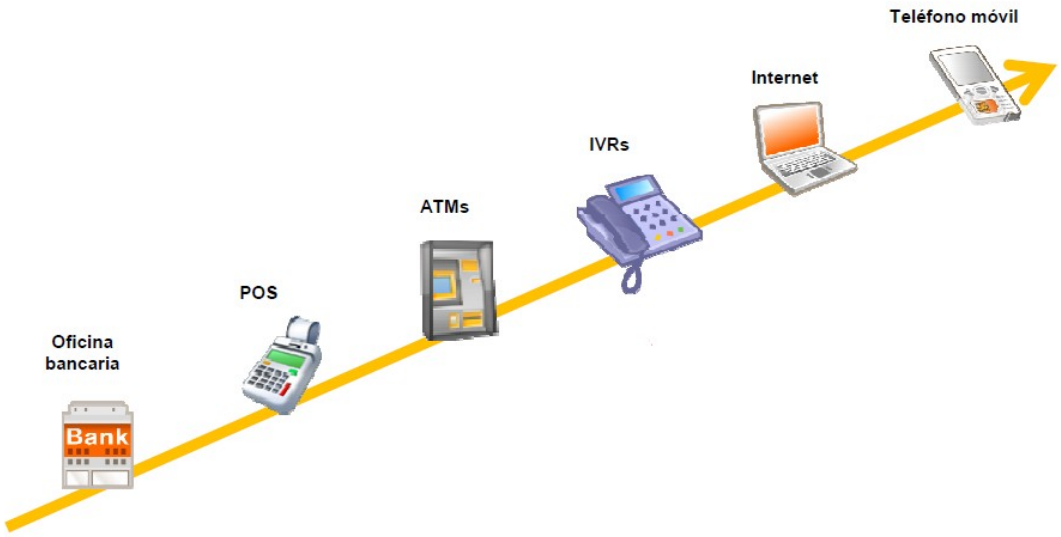


Figura 1.1. Evolución de canales bancarios a través del tiempo.

*Fuente: Edgar, Dunn & Company*

Además, existe una gran demanda para facilitar el acceso a los servicios financieros por dos motivos: los usuarios tienen acceso al crédito y pueden manejar su dinero de forma segura, mientras que las instituciones financieras amplían su base de usuarios y procesan más transacciones.

Por otro lado, desde el punto de vista de los operadores móviles el servicio tiene también un impacto positivo de cara a sus clientes, considerando el alto número de suscriptores. Según la GSM Association, los suscriptores móviles alrededor del

mundo llegan a tres billones hoy en día y se proyecta que para el año 2015 se tendrá alrededor de 5.4 billones. De esta manera, un canal bancario móvil se presenta como un servicio de valor agregado interesante que permita expandir el mercado tanto a usuarios bancariamente activos como a aquellos que no lo son.

Por ello, se identifica como el problema principal la implementación de un canal masivo y seguro de transacciones financieras que satisfaga las necesidades de actuales y potenciales clientes bancarios y que a la vez signifique un ahorro significativo para la entidad financiera. Para ello, se planteará y analizará una solución en el presente trabajo de investigación, tal como lo muestra de manera resumida en la siguiente gráfica.

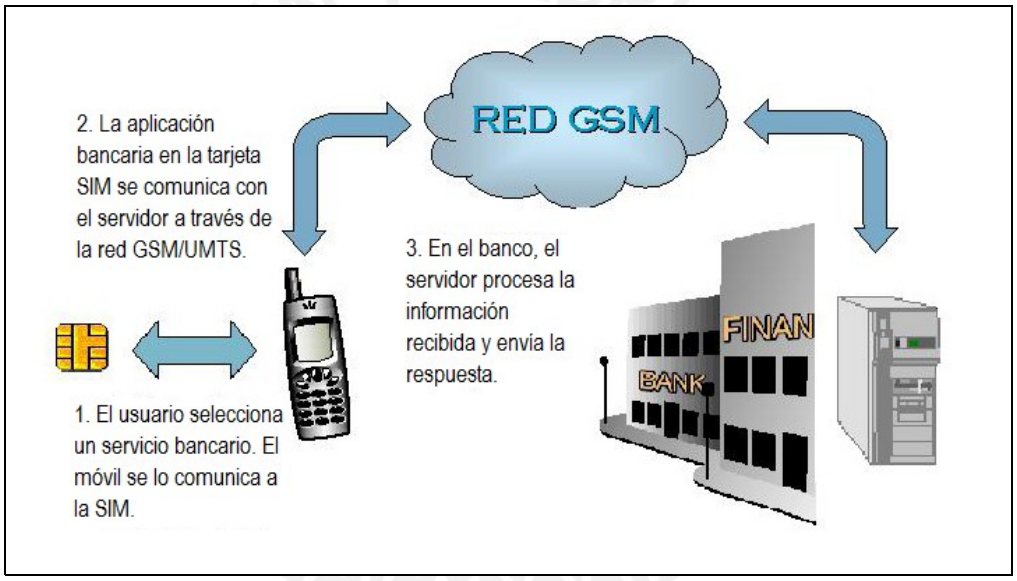


Figura 1.2. Servicio bancario utilizando la red del operador móvil.

*Elaboración propia*

## JUSTIFICACIÓN DEL PROYECTO

Luego de haber alcanzado la madurez en término de penetración y asentado el uso de la voz y los SMS, la industria móvil concentra esfuerzos en el desarrollo de Servicios de Valor Agregado (SVA) que permitan mantener su crecimiento.

El aumento de la competencia entre operadoras de redes móviles impone una mayor disputa por dichos servicios. La búsqueda incesante de diferenciales competitivos exige de las operadoras gran creatividad en el lanzamiento de servicios y en la simplicidad de relacionamientos con el cliente.

La tarjeta SIM/USIM es 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. Luego de autenticado el usuario, la tarjeta SIM/USIM se convierte en una plataforma para tener a disponibilidad los SVA al 100% de la base de usuarios del operador móvil.

En el entorno actual de las telecomunicaciones, los servicios innovadores no sólo deben ser lanzados en el menor plazo de tiempo, sino también con una mayor flexibilidad para futuras actualizaciones de servicios y fácil mantenimiento. Las actuales tecnologías móviles permiten implementar servicios con las características antes mencionadas, teniendo siempre como objetivo principal el crecimiento de la industria móvil. Es importante que los operadores móviles evangelicen a sus clientes sobre los diferentes servicios de valor agregado implementados por cada uno.

El servicio bancario móvil seguro propuesto en este proyecto es un ejemplo de la capacidad tecnológica brindada por los operadores móviles para el desarrollo y despliegue de los SVA.

## OBJETIVOS DEL PROYECTO

### Objetivo General

El objetivo general de este trabajo es presentar un análisis técnico-económico de un servicio de valor agregado brindado por el operador móvil y diseñado para efectuar transacciones bancarias seguras utilizando una aplicación instalada en la tarjeta SIM/USIM.

**Objetivos Específicos**

- Conocer los beneficios del desarrollo de aplicaciones en las tarjetas SIM/USIM para la implementación de servicios de valor agregado.
- Identificar los elementos desplegados sobre una red móvil que permiten la implementación de servicios de valor agregado.
- Identificar los elementos de la arquitectura del servicio bancario móvil seguro usando una aplicación en la tarjeta SIM/USIM.
- Resaltar las características de seguridad impuestas para un servicio de transacciones bancarias como el expuesto en el presente trabajo.
- Ampliar el concepto del uso de las redes móviles como medio de comunicación, resaltando los servicios de valor agregado desarrollados sobre estas redes, como por ejemplo el mostrado en el presente trabajo.

## HIPÓTESIS DEL PROYECTO

Mediante el presente trabajo de investigación se busca ampliar el concepto del uso de las redes móviles más allá de las comunicaciones de voz y mensajería personal, mediante el análisis de un servicio de valor agregado, como es el caso de un sistema bancario seguro utilizando una aplicación en la tarjeta SIM.

Se podrá comprobar que las tecnologías y plataformas actuales desplegadas en la red de un operador móvil permiten implementar servicios de valor agregado de fácil de uso, gran flexibilidad y un alto nivel de seguridad.

# CAPÍTULO 2

# MARCO TEÓRICO

## INTRODUCCIÓN

En este capítulo se presentarán los lineamientos teóricos para el diseño de una arquitectura en el mundo de la telefonía móvil que permita implementar una solución que satisfaga el escenario expuesto en la hipótesis.

Para ello recorreremos los conceptos relacionados a la smart card SIM/USIM, la herramienta de aplicaciones SIM Toolkit y el ambiente de programación Java Card. De igual manera, se explicarán las nociones de las plataformas de servicios como la OTA y el Gateway S@T, fundamentales para el desarrollo de las aplicaciones implementadas para ofrecer servicios de valor agregado, como el expuesto en esta tesis.

## SMART CARD[2]

Una smart card (tarjeta inteligente) es una tarjeta plástica con circuitos integrados que permiten la ejecución de cierta lógica programada.

Existen dos categorías de tarjetas, en función de sus capacidades:

- **Tarjetas de memoria:** Almacenan datos que pueden ser leídos *a posteriori*, posiblemente con cierto control de acceso o con mecanismos de memoria destructiva (sólo lectura). Toda la funcionalidad de estas tarjetas está en una memoria ROM (Read Only Memory), de forma que siempre responden de la misma forma a una instrucción: leyendo la dirección de memoria correspondiente.

- **Tarjetas con microprocesador:** Además de almacenar información, estas tarjetas incorporan un microprocesador para el tratamiento de dicha información mediante el software correspondiente. Se suele incluir dentro de este tipo a las **tarjetas criptográficas**, que además poseen un coprocesador criptográfico capaz de realizar cifrado utilizando por ejemplo algoritmos como RSA, DES o triple DES. Aunque la inclusión de este coprocesador suele aumentar el precio del chip.

Dentro de las tarjetas con microprocesador, a las que llamaremos smart card en este trabajo, podemos encontrar dos tipos diferentes:

- **Tarjetas con contactos:** Deben ser insertadas en un dispositivo de aceptación de tarjetas (CAD= Card Acceptance Device). Estas tarjetas se comunican con el exterior mediante el uso de una interfaz de comunicación serie consistente en ocho puntos de contacto. Este tipo de tarjetas se encuentran estandarizadas en la serie ISO/IEC 7816.

- **Tarjetas sin contactos:** Estas no necesitan ser colocadas en un CAD. Se comunican con el mundo exterior a través de una antena enroscada en la tarjeta. La energía se puede suministrar a través de una batería o la puede acumular la antena. El estándar de comunicación de tarjetas inteligentes sin contacto es el ISO/IEC 14443.

[2] *En base a las especificaciones [EUR2009a] y [GSM2000].*

Las smart cards, también conocidas como tarjetas de circuitos integrados (ICC= Integrated Circuit Card), presentan tres tipos de memoria como se puede ver en la Figura 2.1.

- **Memoria no volátil ROM (Read Only Memory):** Se usa para guardar los programas de la tarjeta. Aquí se encuentra el sistema operativo de la tarjeta que maneja el protocolo del sistema de entrada y salida (E/S), maneja el microprocesador, procesa comandos externos, maneja las memorias y efectúa los algoritmos de autenticación.

- **Memoria no volátil EEPROM (Electrically Erasable Programmable Read Only Memory):** El contenido de este tipo de memoria se puede modificar durante un uso normal de la tarjeta. Se usa para guardar datos (es el equivalente del disco duro de una PC). Almacena aplicaciones, la arquitectura de archivos específicos, información de datos, códigos opcionales, datos del sistema operativo. Los parámetros más importantes de una EEPROM son el número de ciclos de escritura en el tiempo de vida de una tarjeta, el periodo de retención de los datos y el tiempo de acceso a los datos.

- **Memoria volátil RAM (Random Access Memory):** Se usa como espacio temporal de trabajo para guardar y modificar datos. Como se sabe, la información de la RAM no se puede preservar cuando la fuente de alimentación se apaga. A diferencia de la memoria EEPROM, a la RAM se puede acceder un número ilimitado de veces.

Así también cuentan con otros elementos como:

- Un **componente de seguridad** que básicamente son detectores de condiciones anormales de exposición a la luz, temperatura, frecuencia del reloj, voltaje de alimentación, interferencias y ataques físicos. De igual manera, protege a la tarjeta contra ataques del tipo SPA (Simple Power Analysis) o DPA (Differential Power Analysis).

- Un **sistema de entrada y salida (I/O)** bidireccional del tipo serial half-duplex, a través del cual una smart card intercambia paquetes de datos APDU's (Application Protocol Data Units) con la aplicación del CAD.

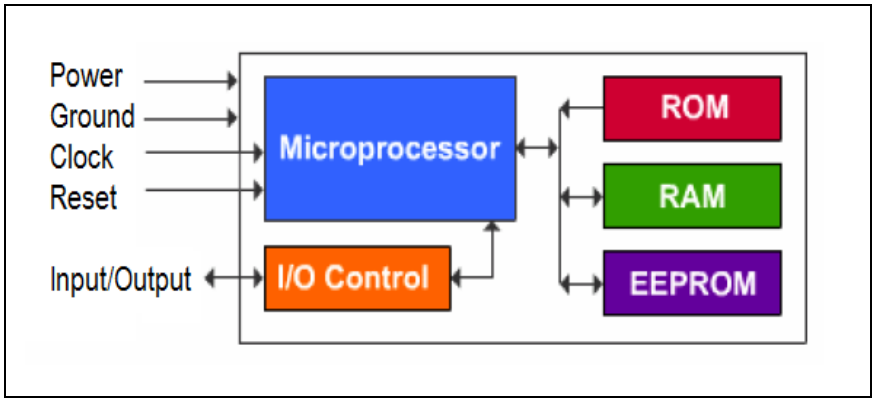


Figura 2.1. Componentes de una tarjeta inteligente con microprocesador.

*Fuente: Oberthur Technologies*

El interés en las smart cards se debe a las ventajas que aportan. Una ventaja es su potencial computacional. Otras son la seguridad, la portabilidad y la facilidad de uso. Para conseguir la información que contiene una smart card hace falta la posesión física de la tarjeta, conocimientos del hardware y software y equipamiento adicional. La seguridad se hace mayor con el uso de funciones criptográficas, es decir, que los datos guardados en la tarjeta se pueden codificar para salvaguardar la privacidad en la memoria física, y los datos intercambiados entre la tarjeta y el mundo exterior se pueden firmar y codificar. Además, el acceso a una smart card suele requerir la introducción de un PIN (número de identificación personal) que evita su uso por parte de personas no autorizadas. Otra ventaja es la portabilidad. Se puede llevar una smart card en la cartera de la misma forma que se lleva una tarjeta bancaria. Así mismo, las smart cards también son muy prácticas. Para comenzar una transacción, se inserta la tarjeta en el dispositivo, y se retira del mismo cuando el trabajo haya concluido.

Las aplicaciones prácticas de una smart card se pueden clasificar de forma general en tres categorías principales:

- **Identificación:** Las smart cards proveen unas medidas de seguridad para identificar el titular de la misma con el fin de permitirle o no el acceso.

- **Transporte de datos:** Las smart cards se usan como un dispositivo de almacenamiento de información practico, portátil y seguro.

- **Finanzas:** Las tarjetas pueden usarse en transacciones, remplazando por ejemplo a los cheques.

## TARJETA SIM/USIM[3]

De acuerdo a los estándares de telefonía móvil GSM y UMTS, el enlace de radio facilita la intrusión, de modo que usuarios no autorizados pueden usarlo de manera fraudulenta. Para impedirlo se adoptan varias medidas de seguridad, entre las que destacan el encriptado digital del enlace de radio (para asegurar la privacidad de la conversación) y la autenticación (que es la comprobación de la validez de un terminal). La consecución de estas dos medidas se basa en el empleo de una smart card de identificación de usuario SIM (Subscriber Identity Module) en GSM o USIM (Universal Suscriber Identity Module), para el mundo UMTS.

Todas las especificaciones concernientes a la SIM como a la USIM se encuentran en las normas GSM 11.11 y en TS 102 221. A continuación se presenta un resumen de las características físicas y lógicas mencionados en dichos documentos, con la finalidad de conocer las capacidades de este tipo de smart cards.

### Características Físicas y Eléctricas

Se especifican las siguientes particularidades de la tarjeta SIM/USIM, de acuerdo con la ISO 7816-1,2:

- **Formato y Diseño:** Cualquier SIM/USIM debe incluir en la parte exterior al menos el código ICCID, identificador exclusivo e irrepetible de cada tarjeta fabricada y emitida. Existen tres tipos o formatos físicos de SIM/USIM (ver Figura 2.2.):

- ID-1: Tarjeta que posee las dimensiones de una tarjeta de crédito (85.6 x 54 x 0.76 mm)

[3] *En base a las especificaciones [3RD2009a], [3RD2009b], [EUR2001], [EUR2005b] y [GSM1999].*

- Plug-in: O microtarjeta, con unas dimensiones de 25 x 15 x 0.76 mm.

- Mini: O más conocida como MicroSIM, tiene dimensiones de 15 x 12 x 0.76 mm.

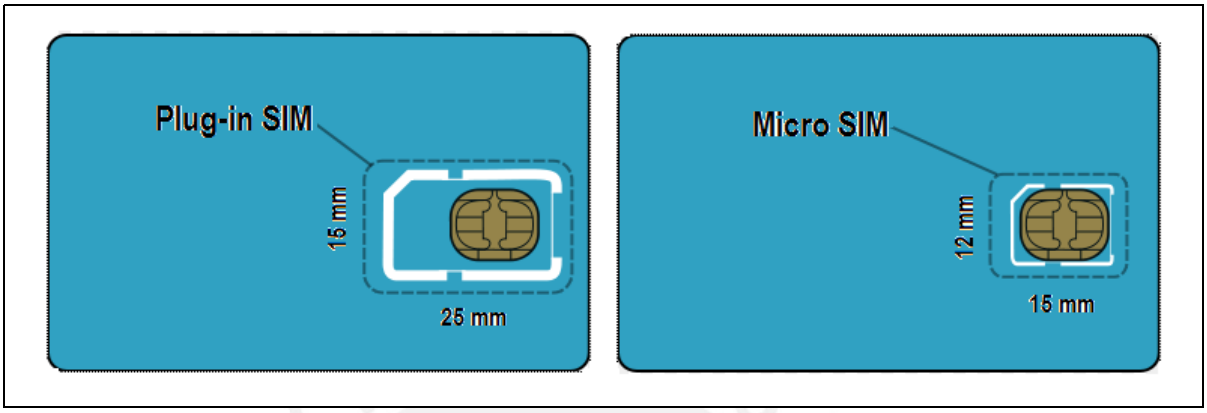


Figura 2.2. Formatos Plug-in y Micro de una tarjeta SIM/USIM.

*Fuente: Morpho*

- **Rango de Temperatura en operación:** El rango de la temperatura para un completo uso operacional debe estar entre -25°C y +70°C.

- **Contactos:** En este punto se definen la disposición, (des)activación y presión para los contactos eléctricos de la SIM/USIM.

- **Seguridad contra la estática:** Ya que la ICC es un dispositivo CMOS, el fabricante de ME's debe tomar las precauciones necesarias para salvaguardar siempre a la tarjeta, al ME y a la interface SIM/ME de las descargas estáticas, sobre todo cuando la tarjeta (U)SIM es insertada en el ME.

**Protocolo de comunicación**

De acuerdo al ISO 7816-3 los APDU's se transmiten gracias al protocolo de transporte TPDU. El protocolo T=0 está orientado a bytes o caracteres, mientras que el protocolo T=1 está orientado a bloques de datos.

El protocolo T=0 se utiliza tradicionalmente en GSM. Tanto para las tarjetas USIM como para los terminales UMTS, el protocolo T=0 es obligatorio, mientras que el protocolo T=1 es obligatorio para el terminal pero no para la tarjeta.

**Modelo Lógico**

La SIM/USIM tiene una estructura jerárquica de archivos organizados con condiciones de acceso asociados (ver Figura 2.3.). Un archivo puede ser del tipo aplicación o simplemente administrativo y en cualquier caso está compuesto de una cabecera y un cuerpo. La cabecera contiene la estructura y atributos del archivo fijados durante la fabricación de la tarjeta; y el cuerpo contiene la información del archivo. Para identificar a un archivo específico se utiliza un ID formado por dos bytes y codificados en notación hexadecimal. El primer byte identifica el tipo de archivo, y para la GSM/3GPP es:

- '3F': Master File
- '7F': Dedicated File
- '2F': Elementary File bajo el Master File
- '6F': Elementary File bajo un Dedicated File

Existen tres tipos de archivos en la SIM/USIM tal como se indica en la ISO 7816-4 (ver Figura 2.4):

- **Master File (MF):** El archivo raíz de la SIM card y por lo tanto de existencia obligatoria y es el único archivo de esta clase que tiene condiciones de acceso. Debajo de él se encuentran los Dedicated Files y los Elementary Files.

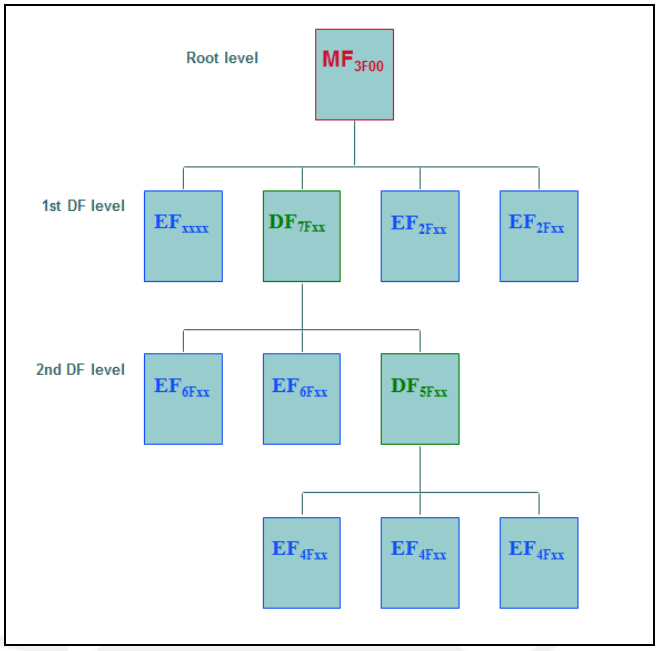


Figura 2.3. Modelo jerárquico de archivos en la SIM/USIM.

*Fuente: Oberthur Technologies*

- **Dedicated File (DF):** Es una agrupación funcional de archivos que contiene a sí mismo y a todos los archivos que lo tengan como progenitor. Los DF solo están formados por la cabecera. En las especificaciones se mencionan dos archivos DF: uno para almacenar la aplicación GSM/USIM y otro para las características de los servicios de telecomunicaciones brindadas por el operador.

- **Elementary File (EF):** Es un archivo formado por cabecera y cuerpo, es decir posee información. Los EF no contienen ningún archivo, son la última rama del árbol. Existen los siguientes tres tipos de estructura para un EF:

  - EF Transparente: Consiste en una secuencia de bytes sin ninguna estructura específica.

  - EF Lineal: Consiste en una secuencia de registros de la misma (fija) o diferente (variable) longitud.

- EF Cyclic: Usado para almacenar registros en orden cronológico. Cuando todos los registros hayan sido utilizados, el siguiente almacenamiento de información deberá sobrescribir el registro con la información más antigua.

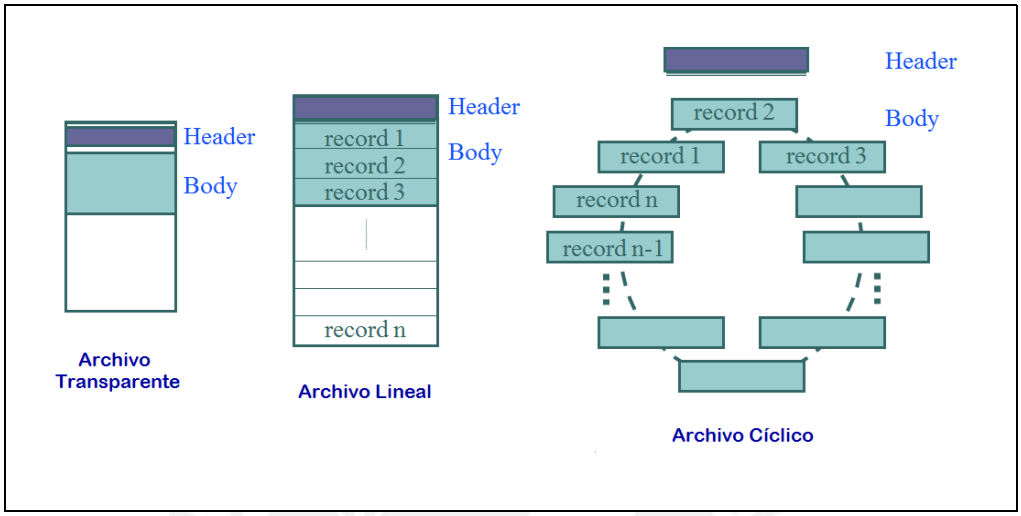


Figura 2.4. Tipos de estructura de un EF.

*Fuente: Oberthur Technologies*

Como se mencionó en el punto anterior, existen archivos administrativos y de aplicación en estas tarjetas. Para nuestro interés, lo más importante es la aplicación GSM o USIM (dependiendo del tipo de tecnología móvil) que ofrece un conjunto de servicios básicos tanto al terminal como a la red GSM o UMTS. En las tarjetas para redes UMTS, o llamadas UICC (Universal Integrated Circuit Card), también se puede definir una aplicación GSM que proporcionará compatibilidad hacia atrás si la tarjeta se emplea en redes 2G. Las normas GSM 11.11 y 3GPP TS 31.102 describen cada aplicación respectivamente. Podemos indicar que la aplicación USIM es un superconjunto de la tarjeta SIM en contenidos, funcionalidades y mecanismos de seguridad. Todos los elementos presentes en la USIM se pueden particularizar convenientemente para transformarla en una tarjeta SIM válida en una red GSM/GPRS (General Packet Radio Service).

## SIM APPLICATION TOOLKIT[4]

Al comienzo del estándar GSM, la SIM, al igual que cualquier smart card, estaba dotada de un microprocesador y de 8 Kbytes de memoria. A medida que ha ido pasando el tiempo, se ha incrementado la potencia del hardware (memorias RAM, ROM, Flash y EEPROM más rápidas, incremento de la capacidad de proceso con sistemas RISC de hasta 32 bits) como su capacidad para soportar servicios y funcionalidades avanzadas, incorporando tecnologías antes reservadas a sistemas de mayor capacidad (sistemas operativos multitarea como MultOS, lenguajes de alto nivel como Java o MEL, interoperabilidad, acceso remoto, etc.).

Por ello, en las denominadas tarjetas Fase 2+ aparece la noción de aplicación que se almacena y ejecuta dentro de la tarjeta y que utiliza el terminal como interfaz al mundo exterior a través del estándar SIM Application Toolkit, proporcionando al usuario nuevos servicios de valor añadido.

La especificación SIM Application Toolkit (STK) define los comandos y procedimientos necesarios para que las aplicaciones almacenadas en la SIM puedan interactuar y operar con cualquier ME que soporte esta capacidad. STK es una facilidad opcional que no debe influir en las funciones GSM de la tarjeta SIM. STK contiene comandos adicionales e independientes a los definidos en la GSM 11.11 (para el caso de redes GSM) para la comunicación entre el SIM y el ME. Esto facilita que las nuevas aplicaciones de las operadoras o de terceras partes puedan residir en el SIM con la aplicación GSM.

El modelo de comunicación con una tarjeta inteligente sigue un esquema maestro-esclavo en el que la tarjeta inteligente tiene un comportamiento pasivo (esclavo), esperando a recibir comandos APDU para ejecutarlos. Es el ME el que inicia la acción enviando una APDU, y la SIM se limita a ejecutar los comandos que le ordenan. Con los comandos proactivos de STK los papeles se invierten: la SIM se convierte en el maestro y puede enviar comandos al ME para que éste los ejecute. Entre los comandos proactivos STK tenemos:

- Mostrar un texto proveniente de la tarjeta en el ME.

[4] *En base a las especificaciones [3RD2004], [EUR2005a], [EUR2009b] y [EUR2004].*

- Enviar un mensaje corto o SMS (Short Message Service).

- Establecer una llamada de voz a un número guardado en la SIM.

- Establecer una llamada de datos a un número guardado en la SIM.

- Enviar un control de servicio suplementario o una cadena USSD (Unstructured Suplementary Service Data).

- Generar un tono en el auricular.

- Iniciar un diálogo con el usuario.

- Requerir la inicialización de la SIM y notificar cambios de los EF's

- Proporcionar información local desde el ME hacia la SIM.

Con la funcionalidad que le proporciona STK, la SIM puede realizar el control de las llamadas y de los mensajes cortos, por ejemplo:

- La SIM puede proporcionar un mensaje completo SMS al terminal para que éste lo envíe.

- Puede recibir directamente un mensaje SMS enviado desde la red. Este mensaje puede contener, por ejemplo, una nueva aplicación que se ejecutará en la SIM o datos/comandos para el STK.

- Puede realizar control de llamada inteligente. Los números de teléfono introducidos por el usuario pasarán a la aplicación SIM antes de ser marcados para que ésta pueda modificarlos convenientemente o incluso bloquearlos.

- Según la información local sobre identidad de celda, estado de llamada, estado de cobertura, etc. las aplicaciones residentes en la SIM pueden, si lo desean, modificar su comportamiento cuando la situación del móvil cambia.

Las aplicaciones STK suelen diseñarse siguiendo un modelo cliente-servidor. Con los comandos proactivos, la aplicación en la SIM puede establecer un canal de datos con el ME y, a través del ME, con un servidor remoto en la red. El ME permite entonces intercambiar datos entre la aplicación en la SIM y el servidor de forma transparente.

Actualmente las comunicaciones entre el cliente (la aplicación en la tarjeta SIM) y el servidor se realizan a través de SMS, USSD o GPRS.

La norma TS 03.48 define los métodos para proteger el contenido de los mensajes de aplicación, describiendo formato e implementación de los llamados *Paquetes seguros* para el servicio de mensajes cortos punto a punto (SMS-PP) y para el servicio de difusión de mensajes cortos (SMS-CB). La TS 03.48 no especifica el tipo de mecanismo de seguridad (cifrado simétrico o de clave pública, firma digital, etc.) ni los algoritmos criptográficos a utilizar, por lo que éstos dependerán de la implementación. La seguridad real del sistema estará en función de la robustez de las claves y algoritmos elegidos. El SIM puede encargarse de "almacenar" de forma segura los algoritmos criptográficos y las claves correspondientes en el lado del cliente.

Las aplicaciones STK interactúan con el usuario a través del sistema de menús del teléfono móvil (ver Figura 2.5.). Las aplicaciones pueden añadir una entrada al sistema de menús del móvil para que el usuario seleccione los nuevos servicios. Cuando el usuario selecciona un servicio STK en el menú de su teléfono, el ME comunica a la SIM la selección y la SIM activa la aplicación correspondiente. La aplicación seleccionada se comunica con el servidor remoto intercambiando la información necesaria para proporcionar el servicio. Si el servicio requiere la intervención del usuario, la aplicación STK puede ordenarle al ME que pida una entrada al usuario, que le permita elegir entre una lista de opciones o que muestre un texto por pantalla. El ME transmite la respuesta del usuario a la SIM para que la interprete.

Figura 2.5. Vista tipo de un menú STK.

*Elaboración propia*

## TECNOLOGÍA JAVA CARD

El desarrollo de aplicaciones para smart cards fue tradicionalmente un proceso largo y difícil. Aunque las tarjetas están estandarizadas en tamaño, forma y comunicación, los trabajos para desarrollar una aplicación dependían generalmente de un fabricante a otro. La mayoría de aplicaciones eran desarrolladas a bajo nivel, lo que supone un gran consumo de tiempo y ya que las aplicaciones estuvieron desarrolladas para ejecutarse en plataformas propietarias, aplicaciones de proveedores diferentes no podía coexistir y ejecutarse en una sola tarjeta.

La tecnología Java Card ofrece un camino para superar los obstáculos mencionados anteriormente. Esta tecnología permite a las ICC y otros dispositivos de memoria muy limitada ejecutar pequeñas aplicaciones, llamadas 'applets', usando la tecnología Java. Asimismo, proporciona a los fabricantes de ICC una plataforma de ejecución segura e interoperable que puede almacenar y actualizar múltiples aplicaciones en un único dispositivo.

Es importante señalar que si bien Java Card permite que programas escritos en lenguaje de programación Java puedan ejecutarse sobre una ICC, tales dispositivos pequeños están lejos de poder soportar la completa funcionalidad de la plataforma Java. Por ello, Java Card soporta solo un subconjunto de características de la plataforma Java, el cual fue elegido cuidadosamente, de tal forma que los desarrolladores disfruten de todas las ventajas de trabajar bajo el lenguaje de programación Java:

- La programación orientada a objetos proporciona una mayor modularidad y reutilización del código, dando lugar a mayor productividad de programación.

- Las funciones de protección, característicos del lenguaje de programación Java, se aplican a los applets de Java Card.

- Disponibilidad completa de poderosas herramientas de desarrollo.

De igual manera, Java Card define un entorno de ejecución adecuado para las características de las smart cards. Dicho entorno cumple con los actuales estándares ICC. La última versión concerniente a esta tecnología, la especificación Java Card Platform 2.2.2, incluye tres documentos que brindan la base de interoperabilidad entre las aplicaciones Java Card:

- **Especificación Java Card Virtual Machine (JCVM):** Define un subconjunto del lenguaje de programación Java y presenta una definición de la máquina virtual deseable para las aplicaciones smart card.

- **Especificación Java Card Runtime Environment (JCRE):** Describe con precisión el comportamiento del entorno Java Card, incluyendo la gestión de memoria, la gestión de applets y otras características de la ejecución.

- **Especificación Java Card Application Programming Interface (API):** Describe un conjunto del núcleo y extensión de los paquetes y clases de Java para programar las aplicaciones de las smart cards.

En consecuencia, estos documentos presentan la arquitectura de software de Java Card y sus principales componentes (ver Figura 2.6.):

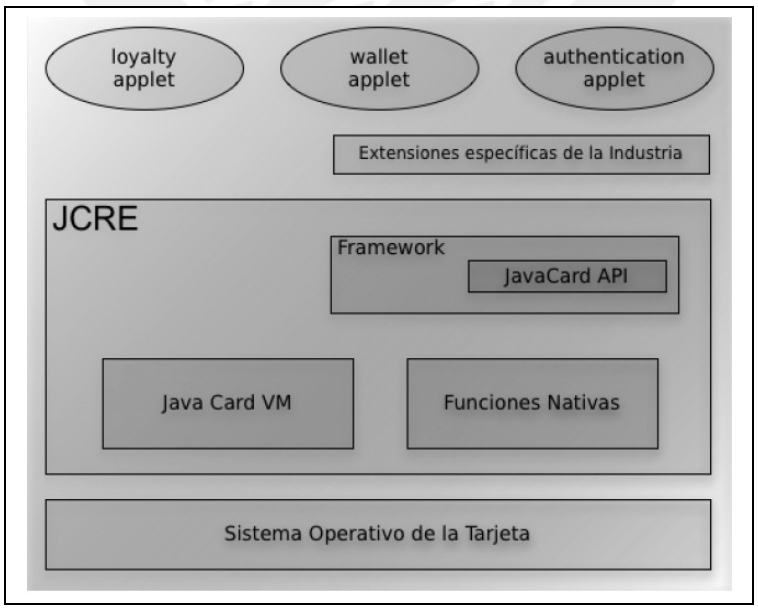

Figura 2.6. Arquitectura Java Card.

*Fuente: Oracle*

- La **Máquina Virtual Java Card** es un subconjunto de la Máquina Virtual de Java (JVM), ya que comparten similares componentes y procesos, de tal manera que sean soportados por el lenguaje Java Card.

- El **Entorno de Ejecución Java Card** consiste en una serie de componentes de un sistema Java Card y que se ejecutan en el interior de una smart card. El JCRE es responsable de la gestión de recursos, comunicación de red, ejecución de applets y de la seguridad del sistema, sirviendo básicamente de sistema operativo de la smart card.

- Las **API's de Java Card** consisten en un juego de clases personalizadas para programar aplicaciones de smart cards acordes al modelo ISO 7816. Estas clases son compactas y cortas, incluyendo clases adaptadas de la plataforma Java para proveer soporte al lenguaje Java y a los servicios de criptografía.

Java Card permite a los desarrolladores crear, probar y desplegar aplicaciones y servicios de manera rápida y segura. Este acelerado proceso reduce costos de desarrollo, aumenta la diferenciación de producto y mejora el valor para los clientes. En conclusión, la tecnología Java Card brinda los siguientes beneficios:

- **Interoperabilidad:** Applets desarrollados con Java Card podrán ser ejecutados sobre cualquier tarjeta inteligente que soporte la tecnología Java Card, independientemente del vendedor de la tarjeta y del hardware subyacente.

- **Seguridad:** La tecnología Java Card se basa en la seguridad inherente al lenguaje de programación Java para proporcionar un ambiente de ejecución seguro. Diseñado mediante un proceso abierto, despliegues probados de la plataforma y las evaluaciones de seguridad garantizarán que los emisores de tarjetas se benefician de la tecnología más capaz y segura disponible en la actualidad.

- **Capacidad para Multi-Aplicaciones:** La tecnología Java Card permite que múltiples aplicaciones convivan en la misma TCI.

- **Dinamismo:** Nuevas aplicaciones pueden ser instaladas de manera segura después que la tarjeta haya sido expedida, permitiendo a los emisores de tarjetas responder dinámicamente a los cambios de necesidades de sus clientes.

- **Compatibilidad:** La tecnología es compatible con los estándares internacionales para TCI como el ISO7816 (expuesta anteriormente) o el EMV.

## JAVA CARD EN LAS TARJETAS SIM/USIM

Los fabricantes de tarjetas SIM, que aportan valor añadido a un hardware tan desnudo, han optado desde el inicio por una arquitectura abierta, partiendo de sus desarrollos propietarios a nivel de sistema operativo. Para ocultar las diferencias entre fabricantes (sistemas operativos) se ha optado por el modelo de máquina virtual en torno a la tecnología Java. Todas las aplicaciones se ejecutan sobre un sistema estándar y genérico, y es tarea del fabricante de tarjetas SIM adaptar esa máquina virtual al sistema operativo y al hardware subyacente. Así el desarrollador no tiene que preocuparse por las peculiaridades del sistema operativo o del hardware del fabricante, a la hora de desarrollar una aplicación.

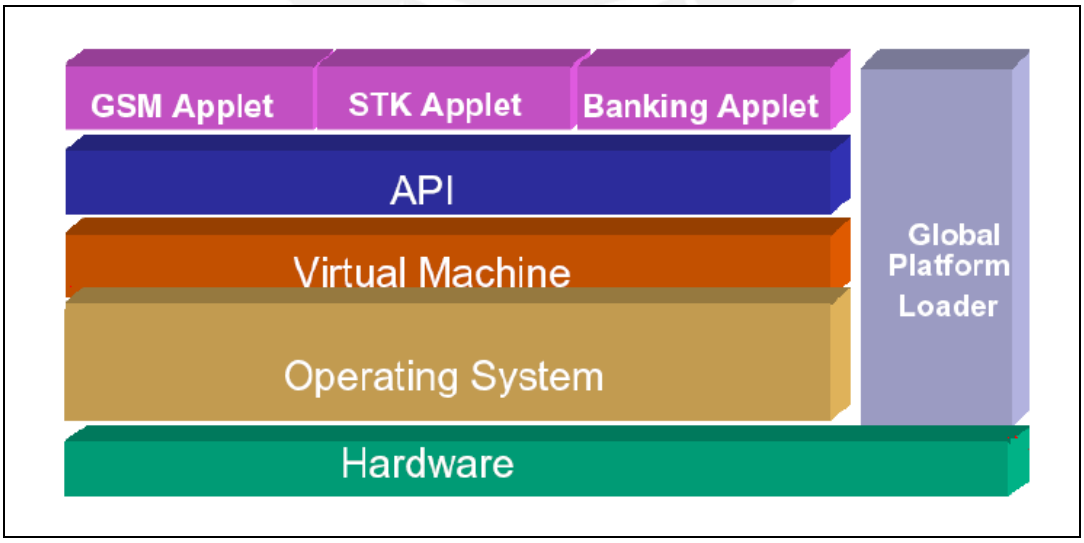


Figura 2.7. Estructura de una tarjeta SIM Java Card 2.1.

*Fuente: Gemalto*

La base para todos los sistemas operativos de tarjetas inteligentes con código ejecutable se encuentran en la especificación GSM 02.19. Aquí, se presenta una lista de todos los servicios básicos de un API independiente del lenguaje para el código ejecutable del programa en la tarjeta SIM. En el año 1999, el ETSI apostó por la tecnología Java, estandarizando el API para el desarrollo de aplicaciones para este lenguaje sobre la tarjeta SIM. De esta manera, en las especificaciones GSM 03.19 y TS 43.019 se encuentran la SIM API para la tecnología Java Card 2.1. Las especificaciones de la UICC API para UMTS se describen en la norma TS 31.111 y en la TS 102.241 se encuentra la UICC API para la versión 2.2 de Java Card.

## TECNOLOGÍA OVER THER AIR[5]

Para las tarjetas basadas en las especificaciones Java Card, la TS 03.48 define un conjunto de comandos usados en la gestión remota de applets; comandos basados en la especificación Open Platform 2.2 sobre gestión de applets. Over The Air o conocido también como OTA es una tecnología usada para los propósitos mencionados en la TS 03.48, respecto a la gestión de aplicaciones en la tarjeta SIM, sin la necesidad de estar conectados físicamente a ésta.

Cuando hablamos de gestión, se hace referencia a la carga, instalación y borrado de applets; convirtiéndose para los operadores en una poderosa herramienta para gestionar fácilmente las aplicaciones residentes en la tarjeta.

OTA se basa en una arquitectura cliente-servidor (ver Figura 2.8), formada en un extremo por un sistema back-end (servidor de aplicaciones, sistema de cobro, atención al cliente) y en el otro extremo, la tarjeta SIM. Como se ve en la Figura 2.8, el sistema back-end envía peticiones de servicios a una plataforma OTA, el cual transforma las peticiones a mensajes cortos o SMS's; los cuales se envían al Centro de Mensajes Cortos o conocido por sus siglas en inglés SMSC (Short Message Service Center) que los remite a la(s) tarjeta(s) SIM indicada(s) por el sistema back-

[5] *En base a la especificación [EUR2005a]*

end. La comunicación entre el SMSC y la plataforma OTA se realiza mediante el protocolo de comunicación SMPP (Short Message Peer to Peer).

El funcionamiento general de una plataforma OTA se puede describir de la siguiente manera:

- Recibir las peticiones de servicios a través de un API Gateway, que identificará la tarjeta SIM a ser modificada. Para esto, la plataforma OTA cuenta con una base de datos que indica para cada tarjeta SIM: el fabricante de la tarjeta, el ICCID, el IMSI y el MSISDN.

- Generar la estructura de los mensajes seguros para que sean entendibles por la tarjeta SIM. Para conseguir esto, la plataforma OTA tiene un arreglo de librerías, las cuales contienen el formato a utilizar para cada marca de fabricante de tarjetas SIM. De esta manera la plataforma OTA da formato a los mensajes independientemente de la tarjeta receptora.

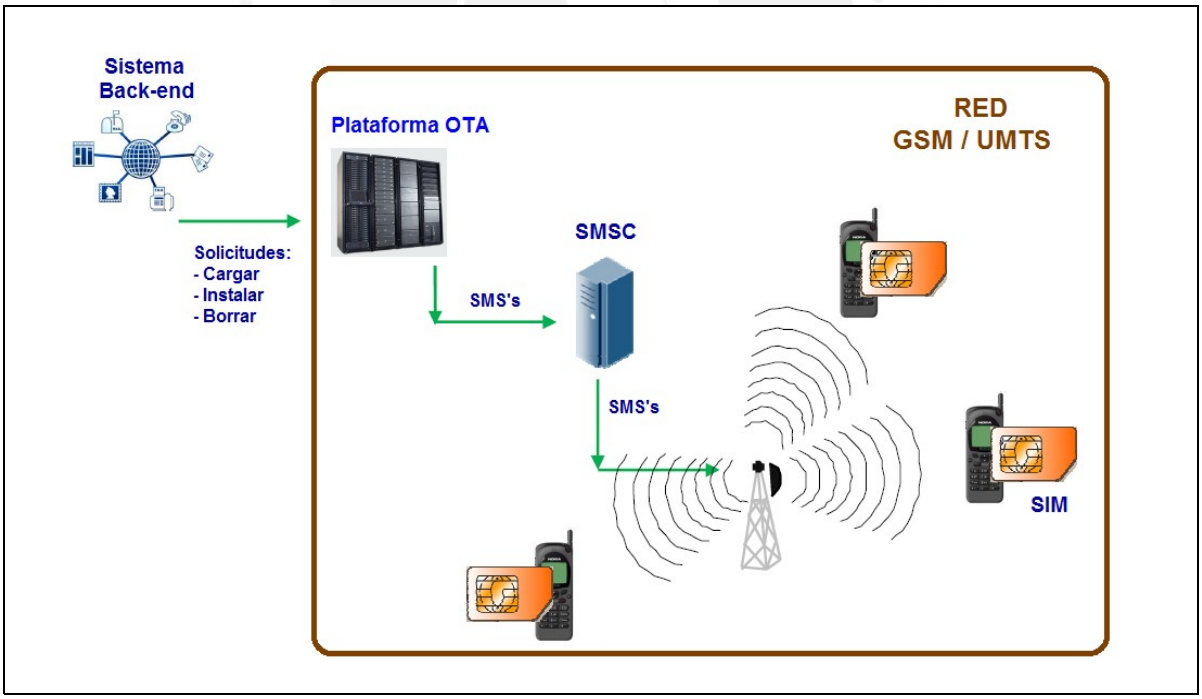


Figura 2.8. Arquitectura de la tecnología OTA.

*Fuente: Gemalto*

## SIMALLIANCE TOOLBOX[6]

Frente a la inminente explosión de Internet a finales del siglo pasado, la telefonía móvil empezó a dirigir su mirada a este "boom", lo que motivó la creación de lo que hoy se conoce como Internet móvil. Esto obligó a buscar protocolos y tecnologías que permitan universalizar la transferencia y visualización de datos y aplicaciones a través de un equipo móvil; apareciendo de esta manera, especificaciones como WAP, I-mode y S@T. Esta última se describirá brevemente en las siguientes líneas, ya que forma parte trascendente de la arquitectura final de este trabajo.

La SIMalliance es una organización sin fines de lucro establecida en 1999 por cuatro fabricantes líderes de SIM cards en el mundo (Gemplus, Giesecke & Devrient (G&D), ORGA Kartensysteme y Schlumberger) para obtener la convergencia entre el mundo móvil y el Internet, y promover un acceso estandarizado al contenido de Internet usando los recursos tecnológicos existentes: SIM, terminal móvil e infraestructura. Cabe indicar que la SIMalliance cuenta actualmente con doce miembros.

A mediados del año 2000, la SIMalliance publicó la primera versión completa de las especificaciones SIMalliance Toolbox (S@T). Las especificaciones S@T aseguran la interoperabilidad entre los fabricantes de tarjetas SIM y permite a los operadores y proveedores de servicios entregar fácilmente productos de Internet Móvil al mercado masivo. Asimismo, S@T permite a los operadores ofrecer servicios de Internet Móvil en todos los equipos celulares, inclusive aquellos que no tienen un navegador de Internet (celulares Fase 2+), considerada una de sus mayores ventajas frente al resto de tecnologías de acceso al Internet móvil. S@T está basado en los estándares STK y las especificaciones Java Card; considerados, en conjunto, como el óptimo ambiente en una SIM para el desarrollo de aplicaciones de valor agregado y que ya fueron sustentados en las secciones anteriores.

Para conseguir que los servicios ofrecidos al usuario tengan una característica dinámica; es decir, que las páginas S@TML sean transferidas desde un servidor que mantenga la información actualizada, SIMalliance detalla en sus diversas especificaciones, los siguientes tres elementos:

[6] *En base a las especificaciones [S@T2009a], [S@T2009b], [S@T2009c], [S@T2009d], [S@T2009e] y [S@T2009f].*

- **Bytecode S@T:** Interpretación técnica de una página S@TML residente en el árbol de aplicaciones STK o proporcionadas dinámicamente por el proveedor de contenidos.

- **Browser S@T:** Aplicación Java cargado en la tarjeta SIM donde se ejecuten los diferentes servicios de valor agregado definidos por el operador y las actualizaciones enviadas por el S@T gateway, así como el despliegue de un conjunto de menús dinámicos. Su propósito es ofrecer una herramienta genérica de navegación embebida en la SIM card.

- **Gateway S@T:** Plataforma albergada por el operador móvil que permite difundir los servicios ofrecidos. Ésta plataforma, atenderá las solicitudes enviadas por la tarjeta (bytecode S@T) permitiendo la conexión al proveedor de contenidos. La respuesta es una(s) página(s) S@TML que el gateway S@T deberá codificar en bytecode S@T para poder entregarlo al browser de la tarjeta.

En las especificaciones S@T, se define un lenguaje de programación estandarizado denominado S@TML (S@T Markup Language), un derivado del lenguaje WML utilizado en Internet por la especificación WAP, y que se usa para la creación de las páginas de navegación del browser S@T y que debe ser adoptado por los fabricantes de tarjetas SIM así como por los proveedores de contenido. Este lenguaje está formado por dos componentes:

- **Núcleo S@TML:** Que es propiamente un subconjunto del lenguaje WML y que facilita la definición de los servicios que son útiles para los usuarios móviles.

- **Extensiones S@TML:** Corresponden a extensiones WML específicas a la SIMalliance y permiten la migración de servicios existentes basados en los comandos proactivos del STK.

Como se ha indicado, S@TML utiliza conceptos del lenguaje WML, con la finalidad de asegurar compatibilidad al momento de interactuar entre ellos. Es así que se definen elementos básicos como:

- **Deck:** Es la unidad más pequeña que puede ser cargada en el browser S@T para su ejecución. Un deck contiene uno o más cards.

- **Card:** Es la unidad más pequeña de navegación para el browser S@T y contiene los comandos bytecode S@T.

Como se puede observar en la Figura 2.9, el gateway S@T recibe los bytecode S@T y entrega las páginas S@TML de respuesta a través del SMSC. La comunicación entre el SMSC y la interfaz del gateway S@T se realiza mediante el protocolo de comunicación SMPP. De igual manera, es importante indicar que al conectarse con los diferentes proveedores de contenidos a través de Internet, el gateway S@T debe soportar los protocolos de comunicación de esta tecnología en una de sus interfaces; como el caso del protocolo HTTP (HiperText Transfer Protocol) para la capa de servicios y aplicaciones.

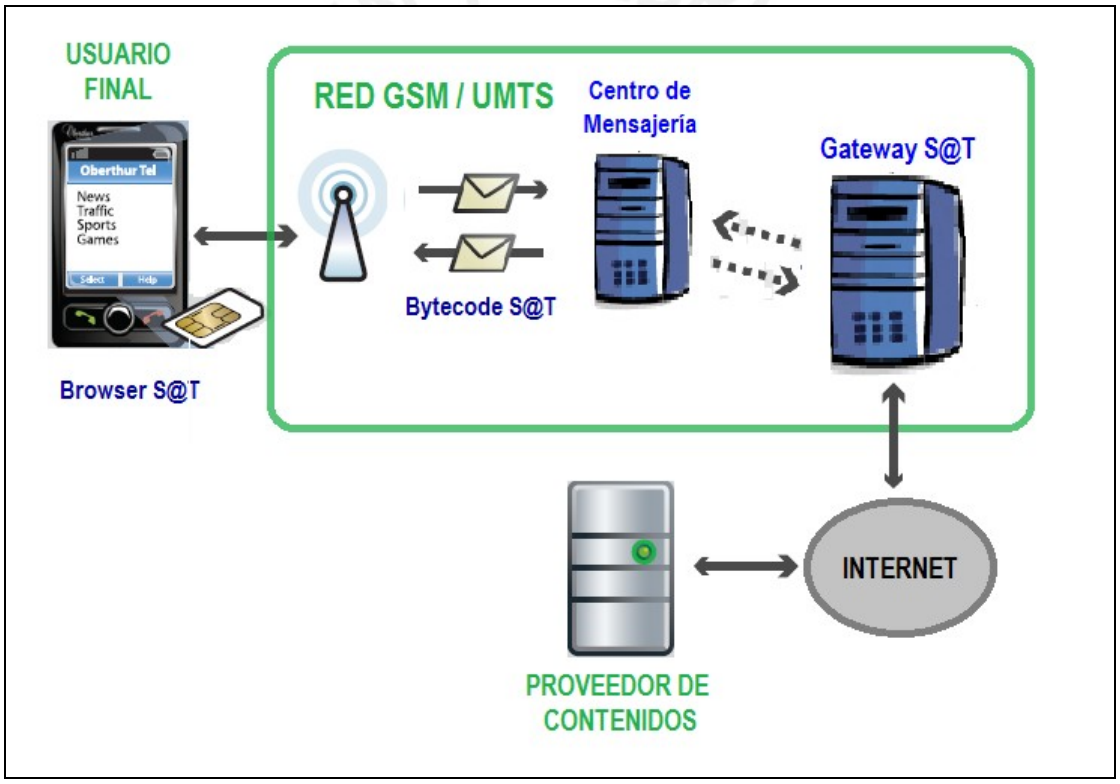


Figura 2.9. Arquitectura de la tecnología S@T.

*Fuente: Oberthur Technologies*

La implementación más conocida en el mundo móvil para la interconexión con los proveedores de contenidos, es que el gateway S@T contenga una tabla de

equivalencias o alias. En la programación de las páginas del browser S@T, éstas incluyen un campo de destino, que puede o no residir en la tarjeta SIM, y que también forma parte del bytecode S@T enviado. En el caso que se requiera efectuar una solicitud hacia un servidor externo, el gateway S@T relaciona el campo destino programado en las páginas S@T con la dirección IP del proveedor donde se debe enrutar la solicitud; para encaminarla hacia el destino correcto. El proveedor responderá a la solicitud a través de página(s) S@TML, que el gateway S@T deberá transformar en bytecode S@T para enviarlo al usuario final.

# CAPÍTULO 3

# ARQUITECTURA DEL SERVICIO BANCARIO MÓVIL SEGURO UTILIZANDO UNA APLICACIÓN EN LA TARJETA SIM

## INTRODUCCION

Los fundamentos teóricos expuestos anteriormente, brindarán el soporte para la solución a la hipótesis planteada al inicio de este trabajo. Un concepto amplio de la arquitectura a diseñar, es que brindará acceso a servicios personalizados por cada entidad financiera a través de la red desplegada por el operador móvil.

Como se verá más adelante, la arquitectura asegura la comunicación extremo a extremo, por lo cual se considera adecuado segmentarla de tal manera de analizar los componentes del lado del operador y los componentes del lado de la entidad

bancaria. Ambos segmentos estarán interconectados a través de un enlace dedicado de Internet o sobre una VPN (Virtual Private Network).

En este capítulo se detallará cada uno de los componentes y su integración para la arquitectura final del servicio.

## ARQUITECTURA DEL LADO DEL OPERADOR MÓVIL

Tal como lo muestra la Figura 3.1, existen dos elementos particulares de la arquitectura en este segmento:

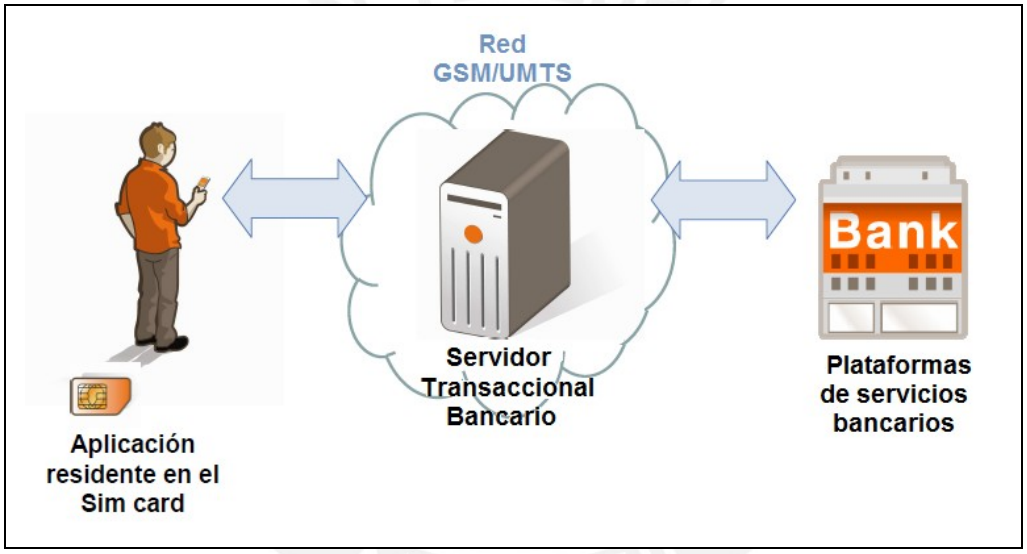


Figura 3.1 Esquema general del lado del operador móvil.

*Elaboración propia*

- La aplicación contenida en la tarjeta SIM que permite enviar las solicitudes a la entidad bancaria, así como recibir las respuestas a dichas solicitudes y mostrárselas al usuario. Denominaremos a dicha aplicación Banca Móvil, por razones de familiaridad del servicio hacia el usuario. Cabe mencionar que el alcance de esta tesis no abarca la programación de la aplicación.

- Un servidor, residente en la red del operador móvil, exclusivo para las transacciones bancarias (solicitudes y/o respuestas) cursadas extremo a extremo al que llamaremos Servidor Transaccional Bancario o STB.

**Aplicación Banca Móvil**

Banca Móvil es el nombre de la aplicación residente en la tarjeta SIM y dispuesta para este servicio. Esta aplicación debe ser implementada en dos partes:

a) **Browser S@T:** Desarrollada para permitir al usuario la navegación fácil y rápida de menús en su dispositivo móvil, de acuerdo a las especificaciones S@T mencionadas en el capítulo anterior. La aplicación tendrá como finalidad primordial brindar el acceso seguro a los diferentes servicios ofrecidos por una entidad bancaria, motivo por el cual, existirá un proceso de personalización de los menús de la aplicación de acuerdo al banco asociado.

b) **Applet Java:** Para manejo de archivos, encriptación y esquema de seguridad del servicio. Será desarrollado bajo los conceptos de la SIM Java Card 2.1 de acuerdo a las especificaciones mencionadas en el capítulo II.

Algunas pantallas de la navegación a través de la aplicación instalada en la tarjeta SIM se pueden observar en la Figura 3.2.

Mediante la especificación TS 03.48 contamos con la facilidad de poder gestionar las aplicaciones residentes en la tarjeta SIM, tal como lo es Banca Móvil. Un posible escenario es que la aplicación Banca Móvil no se encuentre visible en el menú de aplicaciones del browser S@T de las tarjetas emitidas al mercado. Luego, mediante un estudio de mercado se puede definir un *target* de suscriptores a los que se debe mostrar la aplicación, ya que éstos están familiarizados con los servicios bancarios. Es aquí, donde la plataforma OTA cobra relevancia para nuestro servicio. Por ello, es importante contar con su ella en la red del operador, de tal manera que gestione estos mensajes seguros hacia la tarjeta SIM.

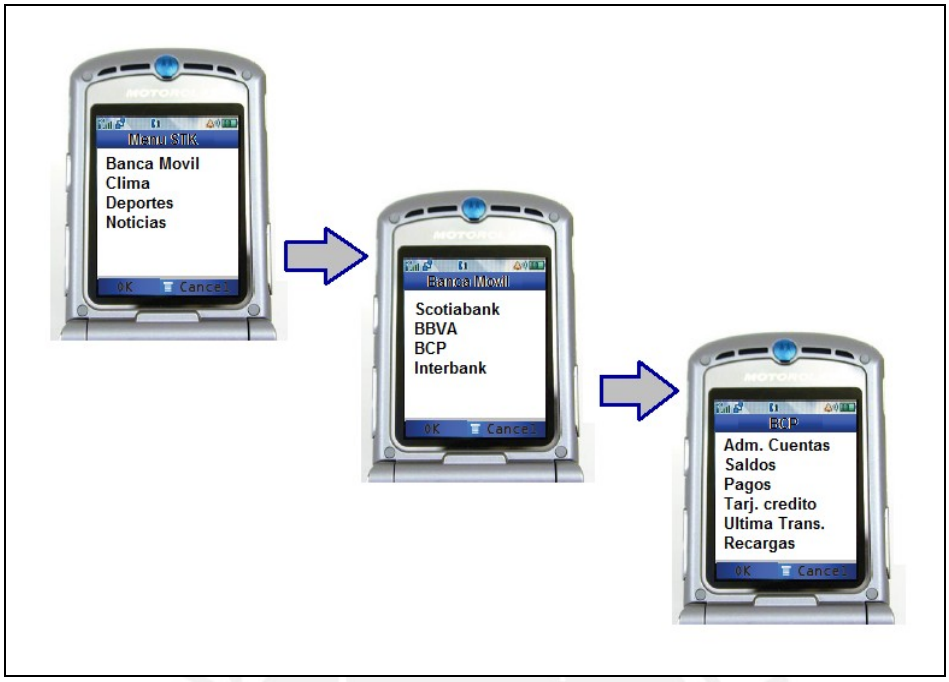


Figura 3.2. Ejemplo de un flujo de opciones de la aplicación Banca Móvil.

*Elaboración propia*

**Servidor de Transacciones Bancarias**

El Servidor de Transacciones Bancarias o STB recibe las peticiones enviadas por la aplicación y las enruta hacia las plataformas de la entidad bancaria correspondiente, convirtiéndose en la interfaz del operador móvil hacia el mundo bancario. Asimismo, se encarga de devolver las respuestas enviadas por las entidades bancarias.

Como se acotó, el STB enrutará la solicitud recibida hacia el banco correspondiente gracias al Banco_ID adjunto en cada solicitud; en tal sentido, el STB debe tener una tabla de equivalencias con los Banco_ID y su respectiva dirección IP, siendo así también un concentrador de bancos.

Como toda plataforma dentro de un sistema, en este caso la red del operador móvil; el STB debe estar comunicado con el servidor de gestión de alarmas del

operador, de tal manera que se mantenga un constante seguimiento del desempeño y funcionamiento del STB.

La arquitectura del servicio permitirá el intercambio de solicitudes y respuestas entre la aplicación Banca Móvil y las entidades bancarias. Para dicho escenario, usaremos las herramientas S@T mencionadas en el Capítulo II. Tal como se grafica en la Figura 3.3, Banca Móvil podrá comunicarse con las servidores ubicados en las entidades bancarias (proveedor de contenidos) cursando elementos desplegados sobre la red móvil. Cabe indicar que la arquitectura posee alta disponibilidad; es decir, presenta el respectivo hardware de redundancia que entrará en funcionamiento cuando el STB principal no funcione de manera adecuada.

De acuerdo a lo expuesto en el párrafo anterior, la función del gateway S@T es convertir las solicitudes enviadas por el SMSC (originadas por el browser S@T de la aplicación) a solicitudes HTTP hacia el STB, así como traducir las páginas S@TML con las respuestas de los bancos al bytecode S@T a ser interpretado por el browser S@T de la aplicación.

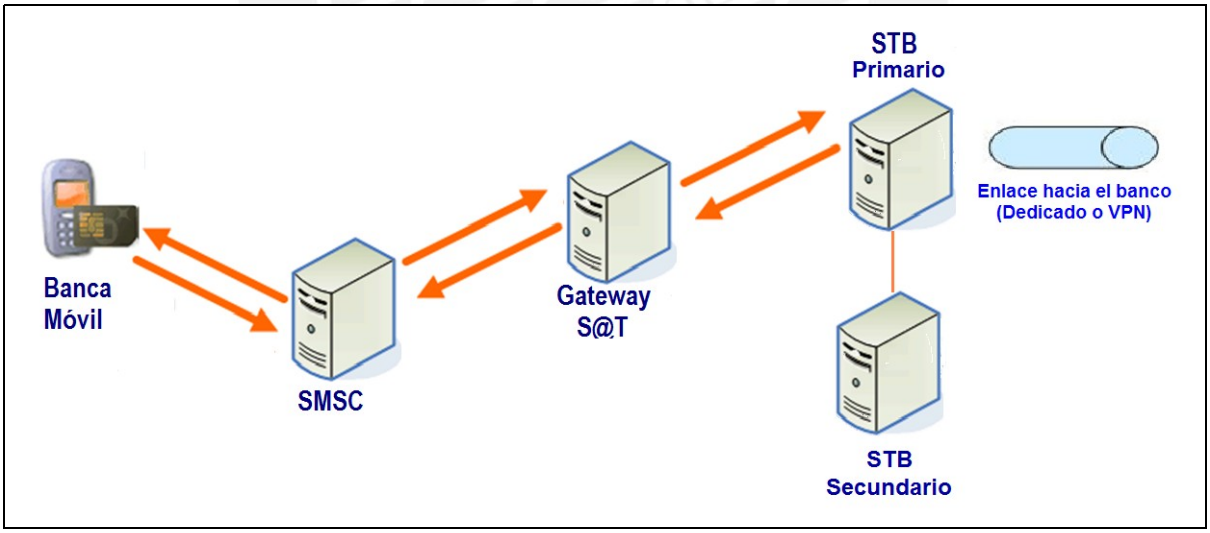


Figura 3.3. Arquitectura del servicio en el operador móvil.

*Elaboración propia*

## ARQUITECTURA DEL LADO DE LA ENTIDAD BANCARIA

Del lado de la entidad financiera, existe un desarrollo más particular del servicio, ya que como se indicó en el primer capítulo, se trata de un nuevo canal de transacciones, que antes no se había implementado. De este lado, se encuentran las diferentes plataformas que generarán las respuestas adecuadas a las solicitudes enviadas por el usuario. Cabe mencionar que el alcance de esta tesis abarca a aquellas plataformas del lado de la entidad bancaria que ofrezcan los niveles de seguridad exigidos por el diseño del servicio.

Los componentes de este segmento del servicio son:

- La Plataforma de Servidores Bancarios o PSB es un concentrador de las solicitudes enviadas por el STB y de las respuestas entregadas por las aplicaciones bancarias.
- El Módulo de Seguridad o HSM es un equipo para efectuar las operaciones criptográficas además de almacenar las llaves maestras.
- El servidor de aplicaciones: Aplicación web que recibe peticiones SOAP del PSB y las envía al sistema back-end de la entidad bancaria para el procesamiento de estas transacciones.
- El servidor Base de Datos: Almacena información de usuarios registrados, datos de estadísticas, y parámetros de seguridad.

### Hardware Security Module

El Hardware Security Module o HSM es un módulo de seguridad que ofrece funciones de cifrado para la seguridad de datos punto a punto. Actuando como un periférico a un equipo host, el HSM ofrece servicios criptográficos necesarios para implementar la gestión de claves, autenticación de mensajes y la encriptación del numero de identificación personal (PIN) para entornos de tiempo real. Además, el HSM es físicamente seguro gracias a las cerraduras, interruptores electrónicos y circuitos de detección de falsificaciones.

En la presente arquitectura, el HSM almacena las Llaves Maestras originadas por los fabricantes de tarjetas SIM y que sirven para efectuar las operaciones criptográficas y generación de las Llaves de Transacción.

**Plataforma de Servidores Bancarios**

La Plataforma de Servidores Bancarios o PSB es aquella plataforma que se encargará de analizar casa solicitud enviada por el STB, con la finalidad de enrutarla hacia el servidor bancario correspondiente. Para ello, la lógica del PSB se basa en una lista de transacciones previamente configuradas con un identificador, de tal manera que cada etiqueta se relacione a un servidor bancario específico. De igual manera, las respuestas brindadas por los mencionados servidores de la entidad bancaria, deberán ser recibidas por el PSB y entregadas al STB.

El PSB se conecta a los servidores de aplicaciones, a los servidores de bases de datos así como el HSM de la arquitectura, tal como se muestra en la Figura 3.4.

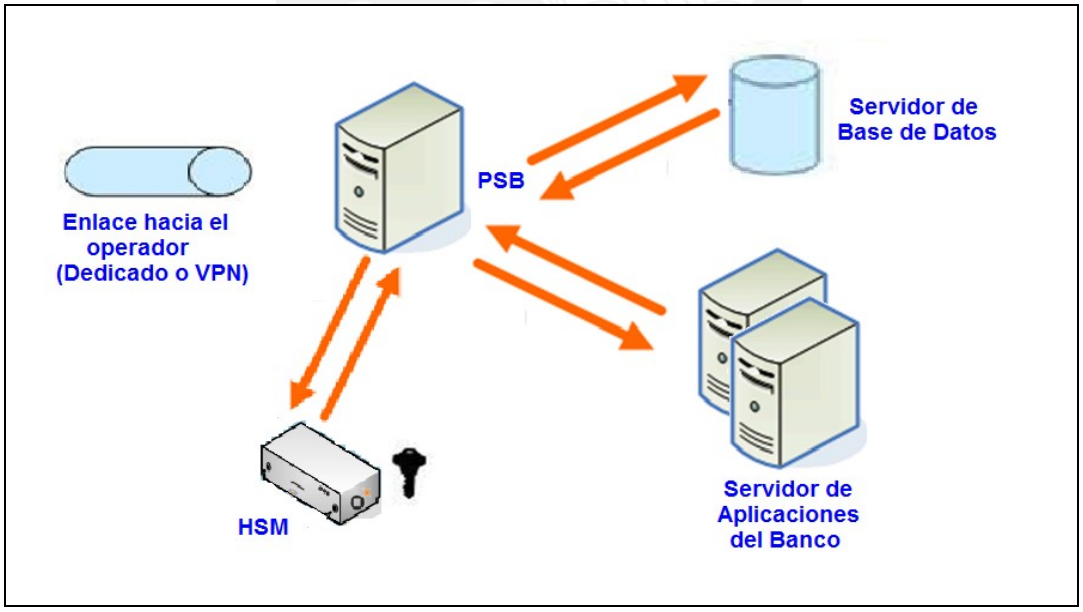


Figura 3.4. Arquitectura del servicio en la entidad bancaria.

*Elaboración propia*

# CAPITULO 4

# SEGURIDAD DEL SISTEMA BANCARIO MÓVIL UTILIZANDO UNA APLICACIÓN EN LA TARJETA SIM

## INTRODUCCIÓN

Este capítulo incluye cómo se ha diseñado la seguridad en el sistema bancario móvil, y cómo la seguridad se lleva a cabo en el ciclo de vida del mencionado servicio.

No debemos olvidar que el servicio bancario propuesto está orientado a transacciones seguras entre la aplicación instalada en la tarjeta SIM y el servidor. La seguridad que debe ofrecer este tipo de servicio implica:

- **Autenticación:** Verificar que la otra entidad en la comunicación es quien asegura ser. En la inicialización de la conexión, el servicio debe asegurar que las dos entidades son auténticas y, posteriormente, debe asegurar que una tercera parte no suplanta a ninguna de las dos partes legítimas.

- **Integridad:** Asegurar que los datos de una comunicación no se alteren, es decir, que los datos recibidos por el receptor coincidan con los transmitidos por el emisor. Y en caso de no ser así, detectar esta modificación.

- **Confidencialidad:** El intercambio de datos entre las dos partes de la comunicación debe permanecer secreto, de manera que ninguna persona no autorizada pueda acceder a esta información.

- **No repudio:** Prevenir que el emisor o el receptor nieguen un mensaje transmitido. Puede ser de dos tipos:

  - Con prueba de origen: el destinatario tiene garantía de quien es el emisor, de forma que puede probar ante una tercera parte que el mensaje fue enviado por éste.

  - Con prueba de entrega: el emisor tiene la prueba de que los datos han llegado íntegramente al destinatario correcto.

Asimismo, el servicio se ejecuta sobre un ambiente hostil, estando expuesto a diferentes clases de ataques, incluyendo pero no limitados a:

- **Hurto:** El acto de robar el dispositivo (tarjeta SIM) y efectuar transacciones en nombre de su dueño.

- **Sniffing:** El acto de espiar y robar información que atraviesa una red. Permite al hacker obtener acceso no autorizado a información y datos sensibles en una determinada red.

- **Spoofing:** Una aplicación exitosamente enmascarada se hace pasar por otra falsificando datos y así conseguir una ventaja ilegítima.

- **Falsificación:** Es el acto de enviar falsamente una solicitud al usuario final asegurando ser el proveedor de servicios financieros o bancarios, en un intento de estafa a que renuncien a la información privada que será luego robada.

- **Ataques de repetición:** Es el acto de repetir datos válidos de manera fraudulenta. El atacante intercepta los datos y los retransmite en nombre del remitente.

- **Ataques "Man in the Middle":** El acto de interceptar una comunicación entre dos entidades, modificándola y retransmitiéndola. Las dos entidades creen estar comunicándose entre ellas.

La seguridad es muy importante en este servicio bancario móvil, porque la aplicación tiene acceso a datos personales (números de cuenta, balances de cuentas, etc.) y permite realizar operaciones financieras con estas cuentas. Cualquier ataque exitoso tendrá un impacto gigante en los negocios.

Si los ataques de spoofing son posibles, el atacante podría realizar cualquier transacción financiera en nombre de individuos o instituciones y robar dinero. Esto conlleva una pérdida monetaria para el proveedor de servicios financieros o para el individuo/institución. Una débil seguridad cuando se transfiere datos sobre una red (por ejemplo la red móvil GSM/UMTS) permite a un atacante husmear información sensible, como números de cuenta o base de datos de tarjeta habientes. La pérdida de información propietaria o estratégica podría tener un gran impacto en el negocio del proveedor de servicios financieros, si por ejemplo, el atacante vende la información a un competidor.

El costo directo de los ataques incrementa el costo del soporte al usuario final. El proveedor de servicios financieros, tiene que contactar al usuario final para corregir el problema y responder a sus inquietudes. Otro impacto es la pérdida de confianza del usuario final, quien puede decidir mover sus negocios a la competencia. Los proveedores de servicios financieros tienen que gastar dinero en restablecer su reputación, pudiendo inclusive ser considerados responsables de los inconvenientes del usuario (perdida de dinero, perdida de información propietaria, etc.).

Para el cliente SIM, los problemas de seguridad tienen que ser tomados en cuenta temprano porque es imposible modificar la tarjeta SIM después de ser dispuestas en el mercado. A continuación se presentarán los principales conceptos implementados en el esquema de seguridad.

## DOS ELEMENTOS FUERTES DE AUTENTICACIÓN

Antes de acceder a los servicios bancarios, los usuarios deben autenticarse por sí mismos. Este paso se basa en dos elementos de autenticación, es decir, los usuarios

debe proporcionar su identidad mediantes dos métodos de autenticación. La elección de los dos métodos de autenticación puede efectuarse a partir de la siguiente lista de opciones:

- Algo que el usuario final conozca (PIN, contraseña, etc.)
- Algo que sólo el usuario final tenga (tarjeta SIM, token, etc.)
- Algo propio e individual del usuario final (huella digital, datos biométricos, etc.)
- Para el servicio bancario móvil implementado, los dos elementos de autenticación corresponden a:
- PIN (algo que el usuario conozca)
- Tarjeta SIM (algo que sólo el usuario tenga)

Para asegurar la seguridad apropiada, los dos elementos de autenticación deben ser requeridos para cada transacción. Esto significa que el usuario final debe brindar su PIN cada vez que quiera completar una transacción usando el servicio bancario móvil.

## ADMINISTRACIÓN DE LLAVES

Uno de los requerimientos del PCI DSS es brindar procedimientos sobre la gestión de llaves usadas para la encriptación de los datos. Para cumplir con este requisito, el esquema de seguridad proporciona un mecanismo para gestionar (instalar, borrar y actualizar) estas llaves “de transacción” usadas para encriptar la información.

Las llaves de transacción son usadas para asegurar los datos entre el cliente SIM y el PSB. Las llaves de transacción se cargan vía over-the-air durante el proceso de activación o durante el proceso de renovación de llaves. Para el esquema de seguridad usando el cliente SIM, se ha definido una infraestructura de administración de llaves que gestione las llaves maestras. Estas llaves maestras deben ser compartidas de manera segura entre el proveedor de llaves y la institución financiera.

## CLASIFICACIÓN DE DATOS

El esquema de seguridad permite clasificar los datos, donde cada tipo tiene restricciones de acceso y de operación. Para el sistema de seguridad usando el cliente SIM se definen cinco tipos de datos:

- **Datos en claro:** accesible para todos.
- **Datos o códigos PIN:** solo la institución financiera puede tener acceso a estos datos. Deben ser usados sólo para los códigos PIN. El formato para estos códigos deben obedecer el estándar ISO 9564-1.
- **Datos transaccionales encriptados:** el PSB puede tener acceso a estos datos y usarlos para realizar una transacción.
- **Datos sensibles:** solo la institución financiera puede acceder a ellos. Estos datos puede ser de formato libre.
- **Datos privados:** solo los usuarios finales pueden acceder a estos datos.

Esta política de clasificación incrementa la protección de los datos así como asegura que las inquietudes sean separadas apropiadamente. Además incrementa la seguridad en el PSB, garantizando que éste no acceda a información no debida.

## IDENTIFICADOR DE TRANSACCIÓN ÚNICA

Para evitar los ataques de repetición, un sistema de detección de anti-repetición basado en identificadores de transacción única se define en el esquema de seguridad. Un identificador de transacción única está asociado a cada solicitud. Esto garantiza que una determinada solicitud solo sea aceptada por el PSB por única vez. Si el PSB recibe la misma solicitud nuevamente, ésta será rechazada.

**ÚNICA LLAVE POR TRANSACCIÓN**

De acuerdo al estándar EMV y los usuales requerimientos regulatorios, una diferente llave es usada para asegurar datos en cada transacción. Con este mecanismo, es más complicado para un atacante encontrar las llaves que asegurar los datos. Por ejemplo, uno de los métodos clásico de criptoanálisis es encontrar patrones repetitivos (identificadores de cuenta). Este mecanismo evita los patrones repetitivos de varias transacciones, aun cuando contenga los mismos datos.

**HARDWARE SECURITY MODULE**

La seguridad del PSB se basa en un Hardware Security Module o HSM. Solo las operaciones criptográficas, como están definidas por el esquema de seguridad, están permitidas por el HSM. El HSM no contiene otras operaciones criptográficas, a fin de evitar huecos de seguridad. Por ejemplo, las operaciones criptográficas para encriptar y desencriptar el PIN no están definidas en este firmware.

Todos los datos de seguridad almacenados en la base de datos del PSB, están asegurados por las llaves maestras locales del HSM. Por las propiedades del HSM es imposible conseguir los valores en claro de los datos de seguridad.

**ESQUEMA DE SEGURIDAD DEL SERVICIO BANCARIO MÓVIL USANDO EL CLIENTE SIM**

Aquí se describe el esquema seguro establecido entre el cliente SIM y el PSB. Los principales actores en esta solución bancaria móvil son el cliente SIM y el PSB. Debido a las tecnologías usadas, ambos son suficientemente seguros para manejar datos sensibles. La seguridad de la aplicación se basa en la tecnología de la tarjeta SIM y la seguridad del PSB está basada en un HSM. El principal reto es intercambiar información entre los dos elementos sin poner en peligro la información sensible. La aplicación Banca Móvil y el PSB no se comunican a través de un enlace directo, y algunos elementos terceros inseguros (componentes de la red GSM/UMTS, el SMSC, etc.) están involucrados en la transmisión de la información sensible. El esquema de

seguridad ha sido definido para establecer un canal seguro end-to-end (extremo a extremo) entre el cliente SIM y el PSB.

El esquema de seguridad está basado en una infraestructura de llaves simétricas y se usa para:

- Configurar la seguridad end-to-end entre el cliente SIM y el PSB.
- Garantizar o asegurar los mensajes entre el cliente SIM y el PSB.

**Configuración de la seguridad end-to-end**

El cliente SIM y el PSB tienen las mismas llaves para la administración de llaves. El objetivo de la configuración de la seguridad end-to-end es la carga segura de las llaves de transacción en el cliente SIM. Una vez que se hayan cargado las llaves de transacción, el cliente SIM y el PSB compartirán las mismas llaves para intercambiar los datos de manera segura.

Para configurar la seguridad end-to-end, el PSB debe generar las llaves de transacción para una determinada tarjeta SIM. Luego, el PSB asegura las llaves de transacción generadas con la llave de administración de llaves pertenecientes a la tarjeta SIM dirigida, y las envía al cliente SIM. La aplicación obtiene los valores en claro de las llaves de transacción gracias a su llave de administración de llaves y la almacena de manera segura en la tarjeta SIM. Mientras tanto, el PSB almacena de manera segura las llaves de transacción generadas en su base de datos

La configuración de la seguridad end-to-end es el primer paso del proceso de activación. Luego de la activación, la seguridad end-to-end debe ser renovada cuando sea necesario o requerido; por ejemplo, expiración de la llaves.

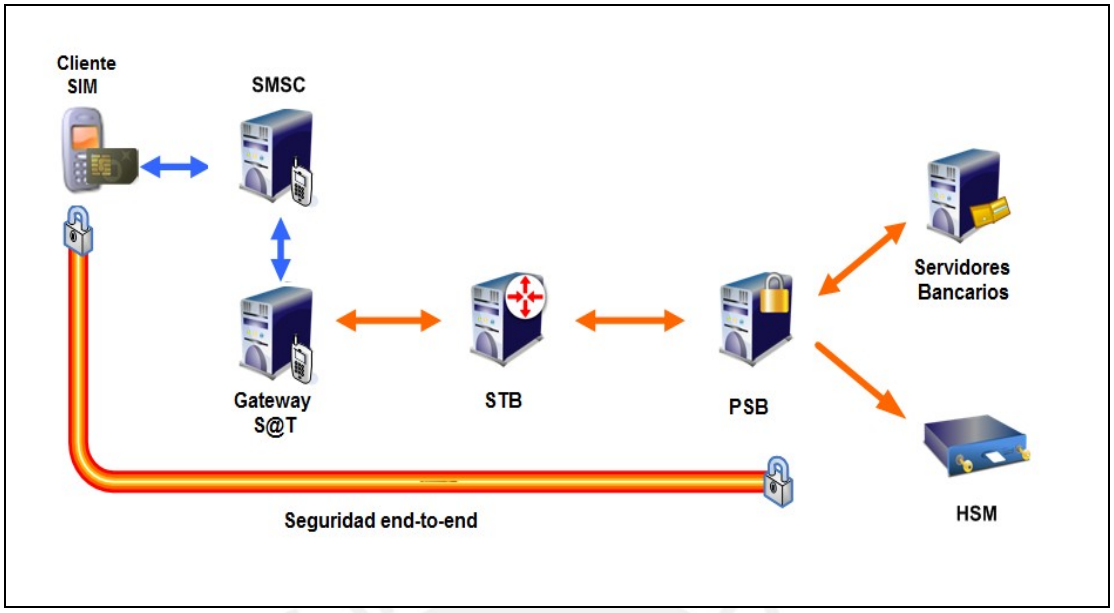


Figura 4.1. Seguridad end-to-end configurada

*Elaboración propia*

**Mensajes Seguros**

Una vez que la seguridad end-to-end ha sido configurada, el PSB y el cliente SIM pueden intercambiar datos de manera segura. Para enviar datos al PSB, el cliente SIM asegura la información usando una llave de transacción diversificada y la envía hacia el PSB. Gracias a que las llaves de transacción han sido almacenadas en la base de datos del PSB, éste pude tener acceso a la información.

## SEGURIDAD EN ACCIÓN

En la práctica, los conceptos descritos se usan en concreto en la solución del servicio bancario móvil. El ciclo de vida del cliente SIM puede ser dividido en cinco etapas, de la siguiente manera:

- **Personalización:** El fabricante de tarjetas elabora la tarjeta y el centro de personalización carga la aplicación Banca Móvil en la tarjeta. Durante el proceso de carga, las llaves de administración de llaves son generadas para cada tarjeta y almacenadas de manera segura en la tarjeta SIM.

- **Instalación:** En esta etapa, el servicio bancario usando la aplicación Banca Móvil ha sido desplegado y está listo para ser usado. Para que la solución esté completamente operable, el servidor debe ser instalado. Durante la instalación, las llaves maestras deben ser configuradas en el PSB. Las llaves maestras deben ser provistas por el fabricante. Cada fabricante de tarjetas debe entregar sus propias llaves maestras. Luego de esta etapa, la aplicación Banca Móvil y el PSB comparten las mismas llaves de administración de llaves y están listo para configurar el canal seguro end-to-end.

- **Activación:** Antes de poder realizar transacciones, el usuario final debe activar el cliente SIM. Desde un punto de vista de seguridad, la etapa de activación es clave, ya que crea una seguridad end-to-end y define como identificar al usuario final en la solución del servicio bancario móvil.

- **Transacciones:** El cliente SIM está activo y el usuario final puede efectuar transacciones financieras. Cada vez que el cliente SIM tiene que intercambiar información con el PSB, se aplica el proceso de “mensajes seguros” para asegurar la integridad, privacidad, autenticidad y no repudio de los datos.

- **Renovación de seguridad:** Es recomendable que después de un año, la seguridad end-to-end sea renovada. Esto significa que el proceso de configuración de la seguridad end-to-end debe ser efectuado nuevamente.

A continuación se explicará de manera detallada las primeras tres etapas del ciclo de vida de la seguridad del servicio, considerando un fabricante de tarjetas SIM y una entidad bancaria.

**Generación, Personalización e Instalación de Llaves**

El fabricante de tarjetas SIM y la entidad financiera deberán manejar HSM locales para poder realizar estas actividades. El fabricante o proveedor de

tarjetas SIM generará tres Llaves Maestras: MK1, MK2, MK3 identificadas por una etiqueta y que quedarán almacenadas en el HSM local del proveedor.

Luego, para cada tarjeta SIM, es decir, para cada ICCID, se genera una llave única conocida como “Llave de Registro” (cuya función se indicará después), utilizando un algoritmo que tenga como entradas la llave maestra MK1 y el ICCID de la tarjeta SIM. El siguiente paso es cargar la Llave de Registro en la aplicación Banca Móvil. Una vez terminado el proceso de personalización y generación de llaves, es el momento de enviarlas cuando el operador móvil y la entidad bancaria lo soliciten.

Para ello, el HSM del proveedor de tarjetas SIM debe generar una “Llave de Transporte” y dividirla en tres partes usando algoritmos específicos. Por otro lado; cada una de las partes, tanto la que enviará (fabricante) como recibirá (banco) las llaves, maneja tres custodios debidamente identificados para cada segmento de la Llave de Transporte. Cada custodio del fabricante anotará el componente asignado de la Llave de Transporte sin compartirlo con los otros. Después, cada custodio del fabricante enviará su componente a su similar del banco. Cuando los custodios del banco lo reciben, ingresarán por separado los componentes en el HSM local del banco. Una vez ingresados, se regenera la misma Llave de Transporte del fabricante en el HSM local del banco.

Ahora es el turno de las Llaves Maestras. Se utiliza el mismo concepto de tres custodios; sin embargo, en esta ocasión el contenido será encriptado con la Llave de Transporte por el HSM local del fabricante. Cada llave maestra es entregada al custodio correspondiente para ser enviadas hacia el banco. Los custodios del banco, ingresarán la información encriptada con la Llave de Transporte en el HSM local, el cual procederá a descifrar las Llaves Maestras MK1, MK2 y MK3 y almacenarlas para su debido uso.

Para generación de las llaves, se utilizará el algoritmo criptográfico de llaves asimétricas RSA y el proceso de encriptación se efectuará bajo otro algoritmo criptográfico, AES.

**Activación del servicio**

Previo al uso efectivo del servicio bancario móvil a través de la aplicación, el usuario debe registrarse adecuadamente en los sistemas de la entidad financiera, solicitando la activación del servicio. Como se mencionó al inicio de este capítulo, uno de los pilares de la seguridad del servicio consiste en el uso de dos elementos de autenticación. Uno de ellos es la tarjeta SIM y el otro es un código PIN, el cual debe ser entregado al cliente por el banco durante la solicitud de la activación del servicio. La entidad bancaria, por su lado debe almacenar en sus sistemas de seguridad y base de datos la información personal del cliente, incluyendo el código PIN del servicio bancario móvil.

Una vez confirmado que el banco tiene la información cargada en sus sistemas, el cliente puede realizar el registro del banco asociado mediante la aplicación Banca Móvil instalada en la tarjeta SIM.

Para conseguir esto, el usuario deberá navegar a través de las opciones del menú de la aplicación hasta aquella que permita el registro, como lo indica la Figura 4.2.

Al elegir esta opción, la aplicación enviará una solicitud hacia el STB para que informe sobre la lista de bancos asociados al operador móvil. Dicha lista entregada por el STB será desplegada en la pantalla del móvil, tal cual se muestra en la Figura 4.3.


Figura 4.2. Registro del servicio (i)

*Elaboración propia*

El usuario elegirá el banco al que previamente ha solicitado el registro del servicio. Al momento de elegirlo, la aplicación enviará hacia el STB la solicitud de conexión hacia el banco indicado. El STB, mediante su tabla de equivalencias asociará el Banco_ID con la dirección IP y enrutará el mensaje hacia el PSB del banco solicitado.

A partir de ahora, son las plataformas del servicio bancario móvil en la entidad financiera las que se encargarán de la solicitud. El PSB devolverá una respuesta al pedido de registro, requiriendo información del cliente de acuerdo a la configuración elegida por el banco, como pueden ser DNI y PIN (ver Figura 4.4).


Figura 4.3. Registro del servicio (ii)

*Elaboración propia*


Figura 4.4. Registro del servicio (iii)

*Elaboración propia*

Una vez ingresados los datos del cliente, la aplicación encripta esta data utilizando la Llave de Registro (instalada durante la etapa de personalización) e incluye el ICCID de la tarjeta SIM. Los datos viajan a través de la red del operador móvil hasta llegar al PSB. Éste al reconocer que se trata de una solicitud de registro, entregará la data encriptada y el ICCID al HSM local del banco.

El HSM utiliza la llave maestra MK1 y el ICCID para regenerar la Llave de Registro y descifrar la data. Si lo consigue, el HSM renvía la información a los sistemas del banco pero ahora encripta la data con la llave maestra MK2, que sólo los sistemas de seguridad del banco conocen.

Una vez que la información es desencriptada y aprobada por los sistema de seguridad y bases de datos del banco, el HSM genera la Llave de Transacción mediante un algoritmo que utiliza el MK3 y el ICCID de la tarjeta solicitante y lo entrega al PSB conjuntamente con el mensaje de confirmación de registro. Es importante señalar que la Llave de Transacción ha sido encriptada por el HSM con la Llave de Registro de la tarjeta solicitante.

La aplicación Banca Móvil recibe la respuesta satisfactoria del proceso de registro en el banco así como Llave de Transacción que usará a partir de ese momento para cualquier futura operación bancaria con dicho banco. La llave de Transacción también es almacenada en la base de datos del PSB, quedando configurada la seguridad end-to-end.

# CAPÍTULO 5

# FACTIBILIDAD ECONÓMICA DEL SERVICIO BANCARIO MÓVIL SEGURO

## ANÁLISIS DE ENTORNO

Para el presente análisis se han considerado dos perspectivas: económico-social y de mercado. A continuación desarrollaremos cada una de ellas.

### Entorno Económico-Social

Para analizar el panorama económico consideramos como indicadores importantes el PIB y su evolución en el tiempo (a nivel de la región A. Latina y Perú); así como, el grado de inversión, posicionando a Perú como país atractivo para la inversión en diversos sectores.

Además, dada la naturaleza de la presente investigación se presentará un breve análisis de la situación actual de bancarización en el Perú y su correspondiente posicionamiento en la región.

La economía peruana terminó el año 2011 con un crecimiento 6.9%, mostrando una leve caída, luego de la reciente crisis económica europea, respecto del crecimiento obtenido en el 2010 (ver Figura 5.1).

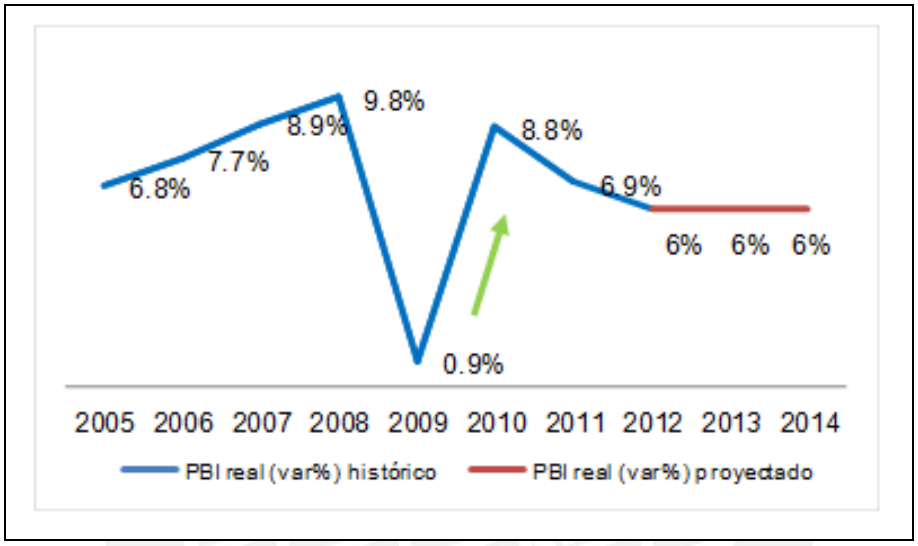


Figura 5.1. Variación anual de PBI, 2005-2011 (%)

*Fuente: Banco Central de Reserva del Perú*

Sin embargo, dicha tasa superó la de 4.6% que en promedio registraron los países de América Latina y El Caribe. Incluso estuvo por encima de los registrados por las principales economías de la región, tales como Chile (6.3%), México (3.9%) y Brasil (2.8%).

Asimismo, las proyecciones de crecimiento del PBI para los próximos 3 años, según el Marco Macroeconómico Multianual 2012-2014 del Ministerio de Economía y Finanzas indican que la economía tendrá comportamiento positivo de alrededor del 6%.

Por otro lado, el PBI nominal en el año 2011, ascendió a US$ 168 miles de millones. Según diversos análisis de entorno económico, el PBI de Lima Metropolitana es, aproximadamente, 36% del PBI total. Por tanto, se infiere que en el 2011, Lima Metropolitana registró, aproximadamente, US$ 60 miles de millones.

A continuación se muestra la evolución de PBI nominal, en los últimos 5 años:

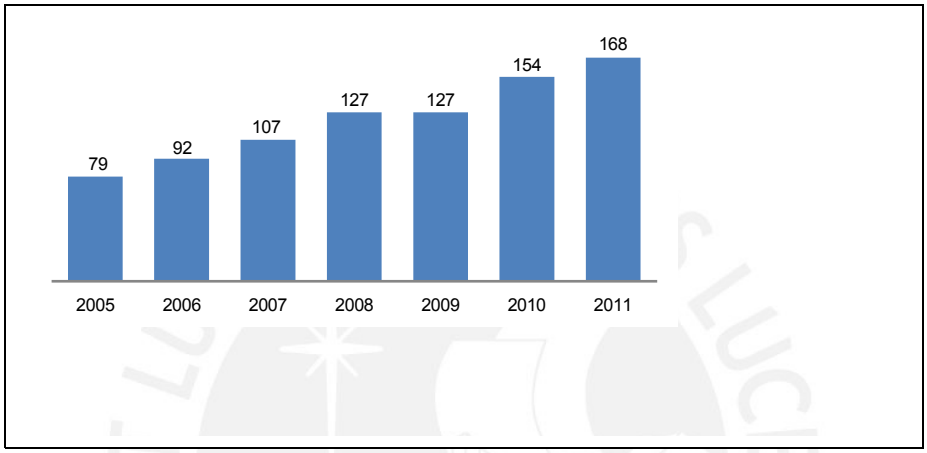


Figura 5.2. PBI nominal, 2005-2011 (miles m US$)

*Fuente: Estadísticas del Fondo Monetario Internacional*

Asimismo; las tres clasificadoras de riesgo económico-social como son Fitch Ratings, Standard & Poor's y Moody's ubican al Perú en la categoría de Grado de Inversión (ver Figura 5.3), es decir, un país considerado atractivo para invertir y por ende obtener ganancias.

Por otro lado, el proceso de bancarización en los últimos 10 años ha registrado una tendencia constante de crecimiento. El último ratio presentado por la Superintendencia de Banca, Seguros y AFP (SBS) alcanza niveles de 30%, como se indica en la Figura 5.4.

| Rango | S&P | Países | Rango | Fitch | Países | Rango | Moody's | Países |
|---|---|---|---|---|---|---|---|---|
| A | Desde AAA+ hasta A- | CHL | A | Desde AAA+ hasta A- | CHL | A | Desde Aaa1 hasta A3 | CHL |
| B | BBB+ | | B | BBB+ | | B | Baa1 | MEX |
| | BBB | MEX, BRA, PER | | BBB | MEX, BRA, PER | | Baa2 | BRA |
| | BBB- | COL | | BBB- | COL | | Baa3 | PER, COL |
| | BB+ | | | BB+ | | | Ba1 | |
| | BB | | | BB | | | Ba2 | |
| | BB- | | | BB- | | | Ba3 | |
| | B+ | BOL, VEN | | B+ | BOL, VEN | | B1 | BOL |
| | B | ARG | | B | ARG | | B2 | VEN |
| | B- | ECU | | B- | ECU | | B3 | ARG |
| C | Desde CCC+ hasta C- | | C | Desde CCC+ hasta C- | | C | Caa1 | |
| | | | | | | | Caa2 | ECU |
| | | | | | | | Caa3 | |
| | | | | | | | Ca | |
| D | D | | D | Desde DDD+ hasta D- | | | C | |
| Sin clasificación | n.a | | Sin clasificación | n.a | | Sin clasificación | n.a | |

Grado de inversión

Figura 5.3. Clasificación de Latinoamérica según las evaluadoras de riesgo

*Fuente: S&P, Fitch y Moody´s*

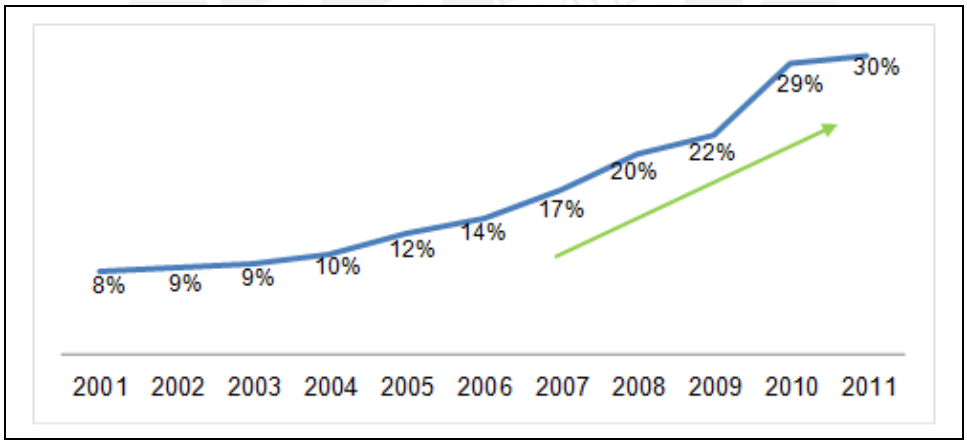


Figura 5.4. Ratio de bancarización durante el período 2001-2011 (%)

*Fuente: Banco Central de Reserva del Perú*

Durante los últimos 4 años la bancarización ha crecido alrededor de 7%, debido en gran parte a los depósitos impulsados principalmente por la actividad

generada en provincias (participación importante del sistema micro-financiero).Otro factor que ha impulsado este crecimiento es la cobertura de los servicios financieros, reflejada en el aumento de canales de atención al público. Este proceso es parte de la descentralización que se viene operando en los distintos sectores económicos en nuestro país.

**Entorno de Mercado**

En el presente proyecto, la tecnología móvil es la plataforma para su desarrollo. En este apartado se analizará la evolución del servicio móvil a nivel de ingresos, suscriptores y tecnología.

El mercado de telecomunicaciones en Perú ha mantenido un crecimiento constante en los últimos 5 años. La inversión en este sector también ha respondido al crecimiento del mismo, tal como se muestra en la Figura 5.5.

Tal como lo indica la Figura 5.6, en Perú el servicio móvil ha tomado mayor participación del total de ingresos del mercado de telecomunicaciones, aumentando desde un 37% en el año 2005 hasta un 64% en el año 2010.

En cuanto al número de suscriptores móviles, éste ha registrado una tasa de crecimiento de 30% en los últimos 5 años, desde 5 583 000 en el 2005 hasta 29 003 000 en el año 2010. Esta tendencia creciente del número de suscriptores se ve reflejada en el nivel de penetración del servicio, que alcanzó el 98% en el año 2010, como se grafica en la Figura 5.7.

El crecimiento sostenido del número de suscriptores ha venido evolucionando conjuntamente con las tecnologías móviles (desde GSM en 1990 hasta LTE 2010 en la actualidad) sobre las cuales se desarrollan los diversos dispositivos ofrecidos en el mercado y con los que pueden ser ofrecidos muchos servicios adicionales, tales como el desarrollado en la presente tesis. Este proceso no sólo está ocurriendo en Perú, sino también se refleja en toda la región latinoamericana, tal como lo muestra la Figura 5.8.

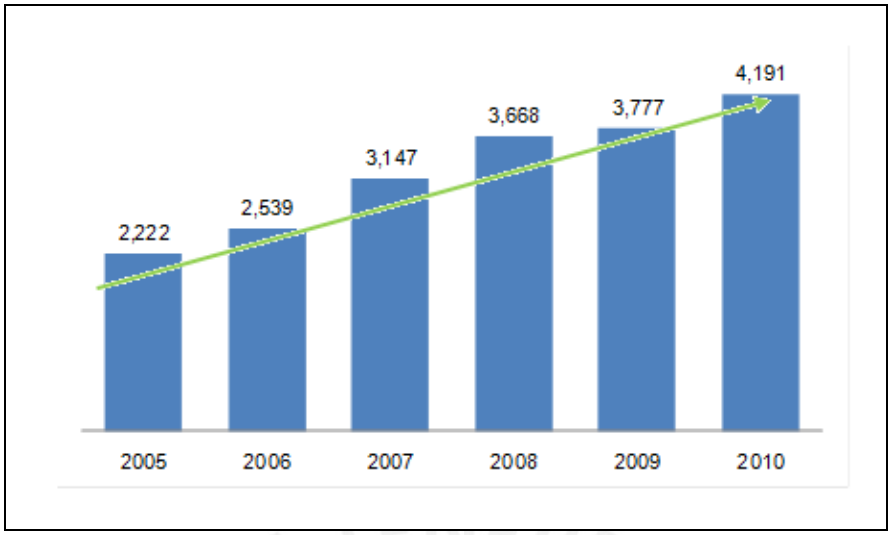


Figura 5.5. Ingresos del sector Telecomunicaciones (mil US$)

*Fuente: OSIPTEL*

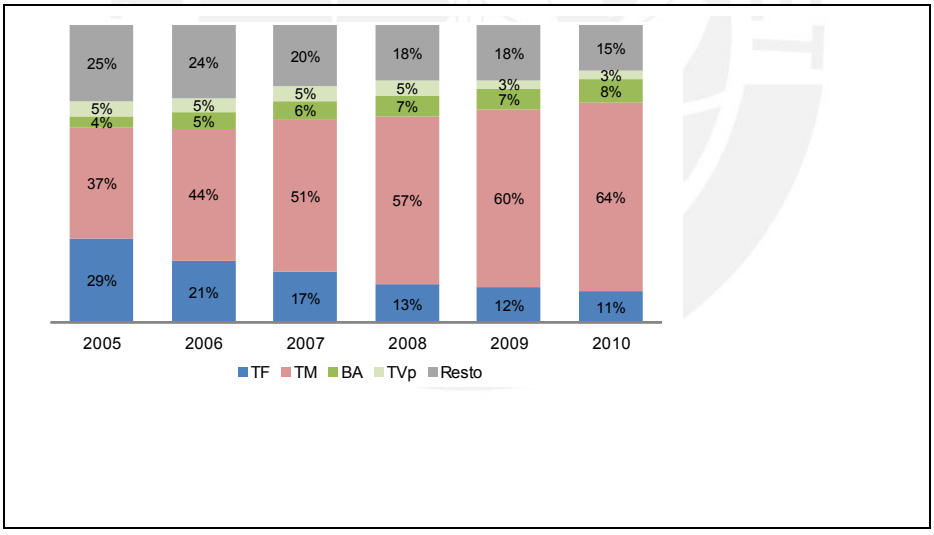


Figura 5.6. Participación del total de ingresos por servicio (%)

*Fuente: OSIPTEL*

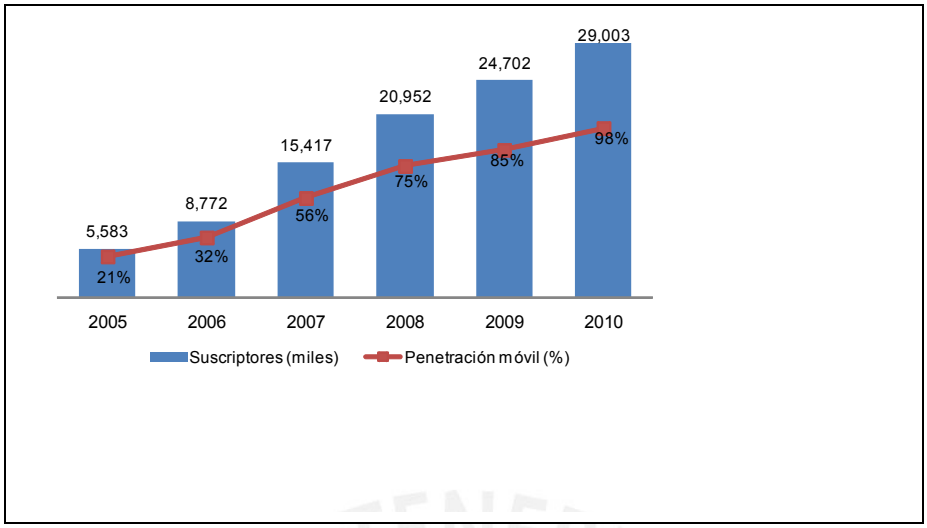


Figura 5.7. Suscriptores de móviles (miles) vs. Penetración (%)

*Fuente: OSIPTEL*

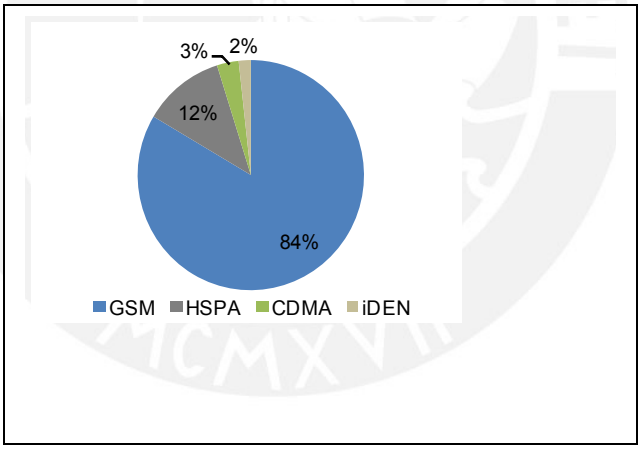


Figura 5.8. Cuotas de mercado de las tecnologías móviles en LATAM 2011.

*Fuente: 4Gamericas*

## ANÁLISIS DE MERCADO

Para esta sección, se tomará en cuenta la situación actual de la demanda (bancos) y la oferta (operadores) que envuelve al servicio en cuestión en nuestro país.

### Demanda

Como se indicó en el primer capítulo, existe una constante evolución de los canales de atención ofrecidos por las entidades bancarias. Esto se debe a dos motivos principales:

- Reducir el costo humano; es decir, disminuir la cantidad de personas que atienden a los clientes ya sea de manera presencial (oficinas) o remotamente (teléfono). Para cualquier empresa, el costo humano es mucho más alto a largo plazo, que la inversión en un nuevo canal tecnológico.

- El continuo progreso tecnológico ofrece día a día la posibilidad de marcar diferencias en relación a la competencia. Los usuarios de cualquier servicio consideran importante la facilidad con el que éste llega a sus manos.

Mediante la Tabla 1 se presenta un resumen de los diferentes canales ofrecidos actualmente por los principales bancos en nuestro país. Como se observa, el campo de canal  móvil, presenta dos ítems: SMS no seguro y SMS seguro.

El *SMS no seguro* refiere al canal por el cual el cliente envía un texto definido hacia un número corto también fijo para indicar a una aplicación ubicada en el banco la operación a realizarse. Lo definimos como un canal no seguro, porque el SMS generado por el usuario no ofrece método alguno para evitar los ataques de seguridad mencionados en el Capítulo 4. Por otro lado, el canal móvil *SMS seguro* es aquel que se ha analizado en esta tesis.

| CANAL / BANCO | Agencia | ATM | IVR | Internet | | Móvil | |
|---|---|---|---|---|---|---|---|
| | | | | WEB | WAP | SMS no seguro | SMS seguro |
| BCP | SI | SI | SI | SI | SI | SI | NO |
| BBVA | SI | SI | SI | SI | SI | SI | NO |
| Interbank | SI | SI | SI | SI | SI | SI | NO |
| Scotiabank | SI | SI | SI | SI | SI | SI | SI |
| Banco de la Nación | SI | SI | SI | SI | SI | NO | NO |

Tabla 1. Canales ofrecidos por los bancos en Perú.[7]

*Elaboración propia*

**Oferta**

Referente al canal móvil mediante una aplicación en la tarjeta SIM, en la actualidad sólo América Móvil Perú (Claro Perú) ofrece este servicio y presenta como único cliente al banco Scotiabank. Sin embargo, se espera que el resto de entidades bancarias opten por el servicio a partir del éxito que se busca tener mediante este nuevo método de acceso.

## EVALUACIÓN FINANCIERA DEL PROYECTO

### Sustento metodológico

Este proyecto consiste en la oferta de un servicio de valor agregado (SVA) en una plataforma móvil existente. En ese sentido, para su evaluación económica, se partirá de la premisa que dicho servicio será ofrecido por un operador móvil con una red de telecomunicaciones ya desplegada en el mercado, usando específicamente los valores de mercado de la empresa América Móvil Perú S.A.C.

[7] *De acuerdo a la información ofrecida en la página web de cada banco mencionado.*

Para nuestro análisis, el método a ser utilizado será el de flujos de caja incrementales; en el cual se registran sólo los ingresos y costos atribuibles a esta nueva iniciativa de negocio. La evaluación se hará por 5 años, periodo máximo trazado para la recuperación de la inversión realizada por el operador.

**Flujos Financieros**


Figura 5.9. Modelo de negocio.

*Elaboración propia*

Este análisis se hará bajo un modelo de negocio (ver Figura 5.9) en el que el banco es el cliente directo del operador. La mecánica de este modelo es que el banco va a pagar al operador un precio acordado por cada transacción que el usuario final (clientes del banco) realice.

a) **Ingresos:** Para la estimación de los ingresos (ver Tabla 2), se definen las siguientes premisas:

- El operador ingresará este servicio al mercado a través de un solo banco los primeros 2 años. A partir del año 3, el operador proyecta obtener un cliente (banco) adicional en su cartera.

- De acuerdo con contrato, el precio inicial por transacción se mantendrá por los 2 primeros años en un valor de US$ 0.11. A partir del tercero, el precio disminuirá a una tasa de 0,5%, considerando un incremento en el volumen transaccional.

- El número de transacciones registra un comportamiento creciente constante de 4% mensual.

El flujo correspondiente a la línea de ingresos incrementales resulta, al final del año 5, con una tasa de crecimiento anual compuesta (TACC) de 74%. Esto principalmente por la razón de crecimiento mensual de las transacciones (4%).

El número de transacciones anuales estimadas, al inicio del proyecto, son de 210 000, cifra promedio registrada en el mercado en el primer año de operación de este servicio.

Tal como lo indica la primera premisa, el operador trabajará con un solo banco los dos primeros años. Para el tercer año, el operador iniciará un contrato con un nuevo banco y la estimación de transacciones para éste será de 216 000.

| **Año** | **0** | **1** | **2** | **3** | **4** | **5** |
|---|---|---|---|---|---|---|
| Número de bancos | | 1 | 1 | 2 | 2 | 2 |
| Transacciones banco 1 | | 210 000 | 336 217 | 538 294 | 861 826 | 1 379 811 |
| Transacciones banco 2 | | | | 216 000 | 345 823 | 553 674 |
| Precio banco 1 (US$) | | 0.111 | 0.111 | 0.111 | 0.110 | 0.110 |
| Precio banco 2 (US$) | | | | 0.111 | 0.111 | 0.111 |
| **INGRESOS (US$)** | | **23 377** | **37 428** | **83 669** | **133 479** | **212 636** |

Tabla 2. Ingresos 1-5 años.

*Elaboración propia*

**b) <u>Costos Operativos (OPEX)</u>:** En cuanto a los costos operativos incrementales (ver Tabla 2), el único factor que se puede atribuir

directamente a la ejecución del nuevo negocio es el mantenimiento del Servidor de Transacciones Bancarias (STB).

De acuerdo con el análisis de mercado realizado, el mantenimiento correspondiente se genera luego de los dos primeros años y por un monto fijo de US$ 2 360 mensuales.

| Año | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| Mantenimiento (US$) | | | | -28 320 | -28 320 | -28 320 |
| **OPEX (US$)** | | | | **-28 320** | **-28 320** | **-28 320** |

Tabla 3. OPEX 1-5 años.

*Elaboración propia*

c) **Costos de Inversión (CAPEX):** Desde el punto de vista del operador, la inversión incremental (ver Tabla 3) que éste deberá realizar es la adquisición del STB. Esta inversión contempla la compra de dos servidores (considerando la redundancia del sistema para el caso de fallas), el software, y la completa instalación del sistema con el resto de equipos y plataformas de la red, así como la capacitación adecuada al personal operativo.

| Definición | Precio (US$) |
|---|---|
| STB | -11 800 |
| STB de redundancia | -11 800 |
| Licencia de software | -82 600 |
| Instalación + Capacitación | -29 500 |
| **CAPEX** | **-135 700** |

Tabla 4. CAPEX.

*Elaboración propia*

d) **Costo de Capital Promedio Ponderado (WACC):** El WACC es el costo que enfrenta el inversionista al comprometer sus recursos en determinada inversión, dejando de lado otras alternativas. La metodología utilizada es la siguiente:

$$WACC = r_E * \left(\frac{E}{E+D}\right) + r_D * (1 - t_e) * \left(\frac{D}{E+D}\right)$$

Para el desarrollo de la fórmula y sus respectivas variables, favor remitirse al Anexo. Luego del correspondiente análisis presentado en dicho anexo, se concluye que el valor del WACC es 9.94% para el servicio brindado por el operador en nuestro país. Es importante considerar este valor, para poder obtener el valor de retorno en el plazo establecido (cinco años).

e) **Resultados**

A continuación se presenta el resultado del análisis financiero mediante un cuadro que resume los valores calculados en los puntos anteriores y que nos servirán para obtener el beneficio (VAN) del servicio al quinto año de implementado, así como el tiempo en que se recuperará la inversión realizada.

| Año | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| Número de bancos | | 1 | 1 | 2 | 2 | 2 |
| Transacciones banco 1 | | 210 000 | 336 217 | 538 294 | 861 826 | 1 379 811 |
| Transacciones banco 2 | | | | 216 000 | 345 823 | 553 674 |
| Precio 1 | | 0.111 | 0.111 | 0.111 | 0.110 | 0.110 |
| Precio 2 | | | | 0.111 | 0.111 | 0.111 |
| **INGRESOS** | | **23 377** | **37 428** | **83 669** | **133 479** | **212 636** |
| | | | | | | |
| Mantenimiento | | | | -28 320 | -28 320 | -28 320 |
| **OPEX** | | | | **-28 320** | **-28 320** | **-28 320** |
| | | | | | | |
| **CAPEX** | **-135 700** | | | | | |
| | | | | | | |
| **Flujo de Caja Acumulado** | **-135 700** | **-112 323** | **-74 895** | **-19 546** | **85 614** | **269 930** |

Tabla 5. Flujo de caja incremental final.

*Elaboración propia*

| | |
|---|---|
| **Valor incremental del nuevo proyecto de Banca Móvil (VAN)** | **US$ 144 596** |
| **Periodo de recuperación de la inversión incremental** | **3 años** |

Tabla 6. Resultados de análisis financiero.

*Elaboración propia*

Finalmente, podemos concluir que la ganancia de este proyecto es de US$ 144 596 para un horizonte temporal de cinco años. Asimismo, la inversión será recuperada en un plazo aproximado de 3 (tres) años.

Desde el punto de vista comercial, esta inversión es válida pues representa el inicio de una estrategia que generará una nueva necesidad en los usuarios finales de los dispositivos móviles.

En esta evaluación se está tomando un escenario conservador ya que supone el incremento sólo de un banco como cliente. Sin embargo, la coyuntura en la región de América Latina sugiere que este tipo de servicios registrará relevancia en los próximos años y por tanto, la expectativa de obtener un número mayor de clientes es alta.

# CONCLUSIONES

- El marco teórico expuesto así como el caso práctico expuesto en esta tesis permiten resaltar características de los servicios de valor agregado desarrollados a partir de un applet, tales como:

  - STK permite desarrollar aplicaciones que residen en la tarjeta SIM y proporcionan al usuario servicios de valor añadido más allá del ámbito de los servicios de telefonía, aprovechando las ventajas en seguridad que proporcionan las tarjetas inteligentes: autenticación, confidencialidad e integridad de los datos (por ejemplo claves) o encriptación y firma digital con algoritmos criptográficos como AES y RSA.

  - Java Card se ha destacado por superar las dificultades de desarrollo de aplicaciones en las tarjetas inteligentes, como son el consumo de tiempo, así como la interoperabilidad entre proveedores. Java Card es tan importante, que la ETSI

estandarizó la interface para el desarrollo de aplicaciones para este lenguaje sobre la tarjeta (U)SIM.

- La gestión remota de applets brinda la capacidad de implantar servicios novedosos en poco tiempo y conseguir diferenciarse de la competencia para captar nuevos clientes atraídos por dichos servicios. A su vez, el manejo remoto de las aplicaciones permite llegar a diversos segmentos definidos por el mercado en diferentes períodos de tiempo.

- Acceder a servicios ubicados en Internet utilizando la tarjeta SIM como origen es factible gracias a las especificaciones S@T. Éstas además consideran el aspecto dinámico de la información almacenada en servidores y plataformas distantes, como es el caso del sistema bancario analizado en el presente trabajo.

- El servicio bancario móvil utilizando un applet en la tarjeta SIM permite demostrar que las tecnologías mencionadas en este trabajo de investigación sirven para la implementación de servicios de valor agregado que pueden cubrir la totalidad de la base de datos de los usuarios del operador móvil, si así se desea, convirtiéndose de esta manera en una herramienta masiva de penetración del servicio.

- Alojando la aplicación dentro de la tarjeta SIM se garantiza la seguridad del sistema. Como la tarjeta SIM es un dispositivo a prueba de fraude que también almacena llaves de cifrado, algoritmos y procesos de datos es esencialmente la misma tecnología que la utilizada en los chips de las tarjetas bancarias. Toda la información procesado en la tarjeta SIM está codificada antes de ser enviada a través de la red del operador de telefonía móvil y sólo se decodifica en la entrada de la arquitectura del sistema en la entidad financiera (en la plataforma PSB), donde se verifica la transacción. Por otro lado, el applet desarrollado para el servicio bancario móvil es amigable y flexible, de tal manera que permita la personalización deseada por cada entidad bancaria que se asocie al servicio.

- Por otro lado, el servicio bancario móvil analizado le ofrece al operador móvil impulsar una imagen innovadora hacia sus clientes, incrementando la lealtad de éstos y también servir como canal para adquirir nuevos usuarios. De igual manera, permite que el operador móvil expanda la oferta de servicios utilizando infraestructura existente para proveer SVA.

- A partir del análisis financiero, el servicio bancario móvil implementado es altamente atractivo para el operador, ya que éste obtiene flujos de caja positivos a partir del segundo año de implementado el servicio. Pero dejando por un momento los números fríos del cálculo realizado, es importante señalar que muchos estudios han coincidido en que se debe fomentar el desarrollo económico y social de un país a través de la implantación y extensión de las Tecnologías de Información y Comunicación (TIC). Es así que se espera una evolución importante de la bancarización móvil como ejemplo de una TIC para el desarrollo en nuestro país.

# BIBLIOGRAFIA


[3RD2004] 3RD GENERATION PARTNERSHIP PROJECT. "3GPP TS 09.02 V7.15.0: 3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile Application Part (MAP) specification (Release 1998)". Marzo de 2004.

[3RD2009a] 3RD GENERATION PARTNERSHIP PROJECT. "3GPP TS 31.101 V8.0.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; UICC-terminal interface; Physical and logical Characteristics (Release 8)". Enero de 2009.

[3RD2009b] 3RD GENERATION PARTNERSHIP PROJECT. "3GPP TS 31.102 V8.6.0: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) application (Release 8)". Marzo de 2009.

[3RD2001] 3RD GENERATION PARTNERSHIP PROJECT. "3GPP TS 31.110 V4.1.0: 3rd Generation Partnership Project; Technical Specification Group Terminals; Numbering system for telecommunication IC card applications (Release 4)". Diciembre de 2001.

[4GA2012] 4GAMERICAS. Mobile Market Shares – Americas. Estados Unidos. 2012.
URL: http://www.4gamericas.org/index.cfm?fuseaction=page&pageid=849
Última consulta: 22/03/2012

[AGG2011] AGGARWAL, Neeraj & BILODEAU, James. "Untapped Potencial: Mobile Banking for the Unbanked". BCG Perspectives. 23 de agosto de 2011.
URL:
https://www.bcgperspectives.com/content/articles/financial_institutions_telecommunications_untapped_potential_mobile_banking_for_unbanked/
Última consulta: 06/01/2012.

[AME2012] AMERICA MOVIL. "Informe anual". México. 2005-2011.
URL: http://www.americamovil.com/amx/es/search?query=informe%20anual&m=
Última consulta: 26/02/2012

[BAN2012] BANCO CENTRAL DE RESERVA DEL PERÚ. Estadísticas. Perú. 2012.
URL: http://www.bcrp.gob.pe/estadisticas.html
Última consulta: 18/03/2012

[BOY2007] BOYD, Caroline & JACOB, Katy. "Mobile Financial Services and the Underbanked: Opportunities and Challenges for Mbanking and Mpayments". The Center for Financial Services Innovation. Abril de 2007.

[DAM] DAMODARAN ON LINE. "The Cost of Capital". Estados Unidos. 2012.
URL: http://pages.stern.nyu.edu/~adamodar/
Última consulta: 18/03/2012

[EDG2008a] EDGAR, DUNN & COMPANY. Artículo. “Mobile Financial Services Study”. Abril de 2008.
URL: http://www.edgardunn.com/pointsOfView/issuesopportunities.cfm?xobj=100003&issueopportunityid=100012
Última consulta: 18/09/2011

[EDG2008b] EDGAR, DUNN & COMPANY. Artículo. “Outlook for Mobile Wallets and Mobile Financial Services”. Febrero de 2008.
URL: http://216.239.213.7/mmt/downloads/EDC-GSMA%20Report%208%20Feb%202008.pdf
Última consulta: 22/09/2011

[EMV2011] EMVCo. Artículo. “EMV Standard”.
URL: http://www.emvco.com/about_emv.aspx
Última consulta: 22/11/2011.

[EBE2001] EBERSPÄCHER, Jörg & VÖGEL, Hans-Jörg. “GSM Switching, Services and Protocols”. Weinheim, Alemania. 2001.

[EUR2000a] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. “ETSI TS 100 929 V8.0.0: Digital cellular telecommunications systems (Phase 2+); Security related network functions (GSM 02.30 version 8.0.0 Release 1999)”. Octubre de 2000.

[EUR2000b] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. “ETSI TS 100 940 V7.8.0: Digital cellular telecommunications systems (Phase 2+); Mobile radio interface layer 3 specification (GSM 04.80 version 7.8.0 Release 1998)”. Octubre de 2000.

[EUR2005a] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. “ETSI TS 101 181 V8.9.0: Digital cellular telecommunications systems (Phase 2+); Security mechanisms for SIM application toolkit; Stage 2 (3GPP TS 03.48 version 8.9.0 Release 1999)”. Junio de 2005.

[EUR2009a] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. “ETSI TS 102 221 V8.2.0: Smart Cards; UICC-terminal interface; Physical and Logic characteristics (Release 8)”. Junio de 2009.

[EUR2009b] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. “ETSI TS 102 223 V9.0.0: Smart Cards; Card Application Toolkit (CAT) (Release 9)”. Octubre de 2009.

[EUR2001] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. “ETSI TS 142 017 V4.0.0: Digital cellular telecommunications systems (Phase 2+); Subscriber Identity Modules (SIM); Functional characteristics (3GPP TS 42.017 version 4.0.0 Release 4)”. Marzo de 2001.

[EUR2005b] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. “ETSI TS 151 011 V4.14.0: Digital cellular telecommunications systems (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment

(SIM-ME) interface (3GPP TS 51.011 version 4.14.0 Release 4)". Marzo de 2005.

[EUR2004] EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE. "ETSI TS 151 014 V4.5.0: Digital cellular telecommunications systems (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.014 version 4.5.0 Release 4)". Diciembre de 2004.

[FON2012] FONDO MONETARIO INTERNACIONAL. 2012.
URL: http://www.imf.org/external/spanish/index.htm
Última consulta: 17/03/2012

[GEM2011] GEMALTO. "Mobile Financial Services". Canada. 2011
URL: http://www.gemalto.com/telecom/mfs/index.html
Última consulta: 01/04/2012

[GLO2011] GLOBALPLATFORM. GlobalPlatform Card Specifications v2.2.1. Enero de 2011.

[GSM1996] GLOBAL SYSTEMS FOR MOBILE COMMUNICATIONS. "GSM TS 01.02 V5.0.0: Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network (PLMN)". Marzo de 1996.

[GSM2000] GLOBAL SYSTEMS FOR MOBILE COMMUNICATIONS. "GSM TS 02.09 V6.1.0: Digital cellular telecommunications system (Phase 2+); Security aspects (GSM 02.09 version 6.1.0 Release 1997)". Febrero de 2000.

[GSM1999] GLOBAL SYSTEMS FOR MOBILE COMMUNICATIONS. "GSM TS 02.17 V8.0.0: Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM); Functional characteristics (GSM 02.17 version 8.0.0 Release 1999)". Noviembre de 1999.

[GSM1995] GLOBAL SYSTEMS FOR MOBILE COMMUNICATIONS. "GSM TS 11.11 V5.0.0: Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface (GSM 11.11)". Diciembre de 1995.

[GSM1996] GLOBAL SYSTEMS FOR MOBILE COMMUNICATIONS. "GSM TS 11.14 V5.2.0: Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface (GSM 11.14)". Diciembre de 1996.

[ITU2009] INTERNATIONAL TELECOMMUNICATION UNION. Artículo. "The World in 2009".
URL: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2009.pdf
Última consulta: 20/03/2012.

[ITU2010] INTERNATIONAL TELECOMMUNICATION UNION. Artículo. "The World in 2010".
URL: http://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2010.pdf
Última consulta: 20/03/2012.

[LAT2012] LATINIA INTELLIGENTIA. Artículo. "La Banca Móvil en Latinoamérica (4° Edición)". Febrero de 2012
URL: http://www.latinia.com/IF/Documentos/LatiniaIntell5.pdf
Última consulta: 01/04/2012

[MOR2011] MORPHO. "Native SIM cards for GSM Networks". Alemania. 2011.
URL: http://www.morpho.com/e-documents/telecoms/?lang=en
Última consulta: 16/10/2011

[OBE2012] OBERTHUR TECHNOLOGIES. "Mobile Money Brochure". 2012.
URL: http://www.oberthur.com/download.aspx
Última consulta: 28/03/2012

[ORG2009] ORGANIZACIÓN PARA LA COOPERACION Y DESARROLLO ECONOMICOS. "Telefonía móvil y desarrollo financiero en América Latina". España. 2009.
URL: http://www.oecd.org/dataoecd/47/39/42825577.pdf
Última consulta: 02/03/2011.

[OSI2012] ORGANISMO SUPERVISOR DE LA INVERSION PRIVADA EN TELECOMUNICACIONES. Información Estadística de Telecomunicaciones. Perú. 2012
URL:
http://www.osiptel.gob.pe/WebSiteAjax/WebFormGeneral/sector/VerInfoEstadistica.aspx
Última consulta: 17/03/2012

[RSA2003] RSA LABORATORIES. "Cryptographic Message Syntax Standard". Enero 2003.
URL: http://www.rsa.com/rsalabs/node.asp?id=2129
Última consulta: 17/12/2011.

[S@T2009a] SIM ALLIANCE TOOLBOX. "S@T TS 01.00 v4.0.0: S@T Bytecode (Release 2009)". 2009.

[S@T2009b] SIM ALLIANCE TOOLBOX. "S@T TS 01.10 v4.0.0: S@T Markup Language S@TML (Release 2009)". 2009.

[S@T2009c] SIM ALLIANCE TOOLBOX. "S@T TS 01.20 v4.0.0: S@T Session Protocol (Release 2009)". 2009.

[S@T2009d] SIM ALLIANCE TOOLBOX. "S@T TS 01.2 v4.0.0: S@T Operational Commands (Release 2009)". 2009.

[S@T2009e] SIM ALLIANCE TOOLBOX. “S@T TS 01.23 v4.0.0: S@T Push Commands (Release 2009)”. 2009.

[S@T2009f] SIM ALLIANCE TOOLBOX. “S@T TS 01.50 v4.0.0: S@T Browser Behavior Guidelines (Release 2009)”. 2009.

# ANEXO

En el anexo se presenta el desarrollo de la fórmula para obtener el Costo de Capital Promedio Ponderado (WACC), cuyo valor nos permite calcular los flujos de caja finales del análisis económico.