COMERCIO MÓVIL, (M-COMMERCE). IMPLEMENTACIÓN DE UN SERVICIO DE APLICACIÓN MÓVIL PARA FUERZA DE VENTA, "I-PEDIDOS V1.0"

María Alejandra Dulcey Morán
Fernando Alanso Mejía Londoño

Director:
Ing. Javier Alexander Hurtado Guaca

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICAIONES
POPAYÁN
2002

TABLA DE CONTENIDO

TABLA DE FIGURAS

LISTA DE TABLAS

1. INTRODUCCIÓN

El comercio electrónico móvil (m-commerce), se podría definir, simplemente, como la extensión inalámbrica del ecommerce, es decir como el uso de dispositivos móviles para interactuar y realizar transacciones mediante una conexión a Internet; sin embargo es importante notar que detrás de esto existen muchas implicaciones tecnológicas, económicas e incluso sociales que de la misma forma como lo hizo el Internet convencional, ya se están haciendo notar.

Son claras las limitaciones que actualmente presentan los dispositivos que soportan el Internet móvil, empezando por el tamaño de las pantallas, hasta su poca capacidad de procesamiento. Es casi obvio que estas limitaciones impiden que la aceptación del Internet móvil sea masiva y es más difícil aún si todos están acostumbrados a un Internet relativamente rápido, con un atractivo visual bastante impresionante y con niveles de seguridad aceptables.

En busca de satisfacer las nuevas expectativas de los usuarios de telefonía móvil y de la gran acogida que han tenido los sistemas inalámbricos, se ha empezado una nueva etapa en creación de redes alta velocidad, que serán capaces de llegar al usuario de forma ágil, segura y eficiente; y con un gran valor agregado: la nueva forma de prestación de servicios, en el cual el usuario es el centro del sistema, ya que todo lo que se le ofrece esta moldeado de acuerdo a su perfil.

Esta nueva generación de tecnología, trae consigo la preocupación tanto a las empresas como a los clientes acerca del costo y financiación de los servicios de m-Commerce. Por el lado de las empresas es necesario pensar en el capital necesario

para el despliegue de infraestructuras de estas tecnologías, (obtención de licencias, marketing y comercialización); ya que no solamente basta con diseñar servicios innovadores y atractivos, es fundamental saber comunicarlo e identificar los segmentos cubiertos por cada servicio.

Los clientes, por su parte, deberán preocuparse por el costo que este nuevo servicio significa para ellos. Así, una política de precios debe estar orientada a obtener un incremento en el consumo de servicios y una mayor retención en los clientes, teniendo en cuenta que la base y razón de ser de este tipo de tecnología son los clientes.

En esta monografía se estudia el m-commerce considerando aspectos como definición, seguridad en los sistemas inalámbricos desde el punto de vista de las transacciones, sistemas basados en localización y el modelado de una aplicación que evidencia la posibilidad de implementar algunos de estos conceptos utilizando la tecnología disponible en nuestro país en una solución eficiente y con un nivel de seguridad aceptable. A continuación se describen por capítulos los tópicos tratados en esta monografía.

- *CAPITULO 2 "m-commerce"*

  Aquí se muestra que es m-commerce, cual es su filosofía, las ventajas y desventajas que tiene, sus barreras y cuales son las tecnologías que le apuestan a esta nueva forma de negocios.

- *CAPITULO 3 "TRANSACCIONES Y SEGURIDAD EN m-commerce"*

  En este capitulo se describen las necesidades de un sistema de transmisión de datos móvil seguro, según las especificaciones del MeT, (Mobile electronic Transactions), el cual define un conjunto de estándares para que además de mostrar al usuario un sistema confiable, también sea coherente, a pesar de las diferencias entre dispositivos utilizados como agentes de usuario.

- *CAPITULO 4 "Sistemas De Localización En Sistemas Móviles"*

  En este capítulo se abordan de forma general los conceptos más relevantes de los sistemas de localización más utilizados y que puede ser adoptados en las nuevas redes de tercera generación.

- *CAPITULO 5 " Modelado Sistema i-Pedidos"*

  Se presenta el análisis del dominio del sistema desarrollado, identificando los aspectos más relevantes del problema planteado como, actores del sistema, casos de uso y modelo de negocios.

1.1. I-PEDIDOS V1.0

I-pedidos es una nueva alternativa para agilizar los procesos de despacho y venta de los pedidos realizados por un usuario.

Las ventas de productos son el corazón y sustento de la empresa, y su inicio es la captación de los pedidos de venta de los clientes, distribuidores, mayoristas, etc. Que siguen un largo y costoso camino hasta que llegan a su destino final. Este proceso está plagado de demoras, malos entendidos, equivocaciones y alta inversión en horas hombre, lo cual implica una suma de costos y el deterioro en la relación con el cliente.

I-pedidos resuelve en gran parte esta problemática a través del desarrollo de una solución Wap y Web a la que pueden acceder todos los integrantes de la cadena de pedidos y registrar o consultar sus órdenes de compra.

A través de nuestra solución se pueden manejar los catálogos de varios productos, lista de precios, lista de empresas, y los clientes que están registrados en el sistema, tendrían su perfil, el cual le agilizara aun mas la compras a través del dispositivo móvil.

Además de estar disponible desde cualquier lugar y las 24 horas, evitar errores y agilizar la comunicación, el sistema tendrá un valor agregado muy poderoso, y es el

servicio basado en la localización, es así como el cliente que realiza el pedido; logra una movilidad total.

I-pedidos aparece entonces como el efectivo inicio del inevitable proceso de modernización y eficiencia del circuito de ventas de cualquier empresa por medio de la utilización del Internet móvil.

2. M-COMMERCE

Nos encontramos en un momento en el que la mayoría dispone de un teléfono móvil, incluyendo los grupos que en principio no fueron considerados como potenciales usuarios de este tipo de dispositivos, es decir, es evidente la adopción y aceptación de las tecnologías inalámbricas, por el público en general. Ahora bien, es importante pensar en las ventajas, innovaciones y oportunidades que representa la convergencia de los dos fenómenos tecnológicos de mayor crecimiento de los últimos años: Telefonía móvil e Internet. Esta convergencia anuncia el nacimiento y evolución del comercio electrónico móvil, "m-commerce", como una nueva forma de hacer negocios. La Figura 2-1 muestra la evolución de las tecnologías de información que actualmente mueven el mundo, empezando por el servicio de Internet fijo hasta llegar a la progresión de la aceptación y evolución del Internet móvil.

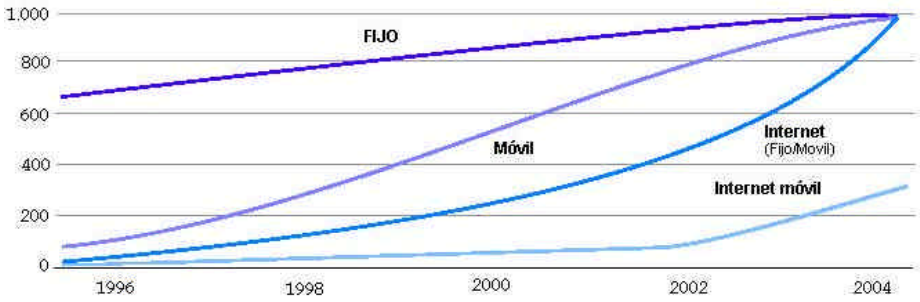

Figura 2-1. Evolución del número de usuario de Internet en el mundo (MM)[1]

[1] Fuente: Ericsson, http://www.ericsson.com/

Es necesario, sin embargo que las tecnologías que soportan el Internet móvil evolucionen lo suficiente para presentarlo al usuario como un generador de servicios potentes, seguros, confiables y asequibles que permitan demostrar las ventajas de la comunicación sin cables.

Así el m-commerce muestra claramente una posibilidad para mostrar al usuario servicios de valor agregado, aprovechando las capacidades del Internet y las tecnologías inalámbricas. Su principal ventaja es la posibilidad de con solamente un teléfono acceder a información, realizar compras, ubicar sitios, etc. y para las empresas lograr un contacto más estrecho con el usuario/cliente, que el que actualmente se obtiene con Internet.

Muchos expertos creen que el m-commerce llegará a ser la “aplicación crucial” que impulsará el crecimiento del sector móvil una vez que el mercado de llamadas de voz convencionales se sature, un fenómeno que probablemente ocurrirá dentro de unos años en los países desarrollados.

El m-commerce se está desarrollando más rápidamente en Europa y en Asia, donde los servicios móviles están relativamente más avanzados que en Estados Unidos, país donde la telefonía móvil está empezando a despegar. Sin embargo, con la llegada de los servicios de nueva generación, esta diferencia probablemente desaparecerá dentro de unos pocos años.

La tecnología WAP es simplemente instrumental, se constituye en una serie de normas para trasformar la información de Internet de manera que ésta pueda aparecer en la pequeña pantalla de un teléfono móvil o algún otro dispositivo portátil. Por ahora es la clave de la información móvil, el comercio móvil y una amplia gama de servicios de Internet que se pueden distribuir y enviar por las ondas. Es el vínculo esencial entre Internet en el PC y las crecientes funciones de los teléfonos móviles, las agendas personales y otros dispositivos inalámbricos. Con la aparición en los próximos años de los teléfonos celulares de nueva generación como los de tecnología UMTS (*Universal Mobile Telephone Service*), que permitirán la transmisión de imágenes de vídeo en total movimiento y de sonido de alta fidelidad por redes de móviles, la importancia técnica del WAP puede disminuir. Sin

embargo, la importancia del comercio móvil y otras formas de interacción con Internet seguirán creciendo.

I-mode, el servicio de comunicaciones de datos inalámbricos de Japón, creado por NTT DoCoMo, crece rápidamente, fue lanzado en 1999 como una nueva plataforma para comunicaciones con teléfonos móviles y actualmente cuenta con 28 millones de suscriptores[2]. Este crecimiento fue alimentado por una implacable conducción que le permitió extenderse más allá de las fronteras del mercado actual de las telecomunicaciones. El progreso ha sido dramático, con i-mode, DoCoMo proporcionó teléfonos móviles con las mismas capacidades para transmisión de datos que de voz; hoy en día DoCoMo, esta desarrollando dispositivos basándose en tres puntos cruciales: Manejo de multimedia, aplicaciones que expandan el rango de las comunicaciones móviles y la extensión del área de negocios. Así, Japón parece más preparado para el desarrollo y expansión del m-commerce.

2.1. QUE ES EL M-COMMERCE

El comercio electrónico móvil, o m-commerce, es una extensión lógica del comercio electrónico, mediante el uso de dispositivos inalámbricos para comunicar, interactuar y realizar la ejecución de negocios en redes móviles, utilizando total o parcialmente redes existentes (Internet, redes corporativas). De esta forma los usuarios podrían utilizar estos dispositivos para tener acceso a servicios como: acceso a cuentas bancarias, pago de facturas, transacciones de compra-venta, recepción de promociones, etc.

De esta forma y así como lo hicieron, primero la televisión y luego Internet, los teléfonos móviles han cambiado definitivamente nuestra cultura, en los tres casos el cambio ha supuesto modificaciones sustanciales, al menos, en los modelos de comunicación entre las personas y en los de comunicación y relación entre las personas y las empresas.

[2] Informe anual 2001 de NTT DoCoMo, “NTT DoCoMo, Annual report 2001”

2.1.1. Participantes (Cadena de Valor)

- **Los principales contendores**

  El mercado de Internet móvil tiene un enorme potencial y aunque es un sector embrionario, la estructura está empezando a tomar forma. En la base están los vendedores de hardware y/o de tecnología y las compañías que suministran la infraestructura física para las redes de móviles que han desarrollado tecnologías instrumentales como WAP. Entre éstas compañías están Nokia, Motorola y Ericsson.

- **Los suministradores**

  En medio están los suministradores de software que están desarrollando sistemas operativos de comunicaciones inalámbricas y que operarán en la próxima generación de dispositivos de bolsillo. Entre ellos están la asociación Symbian, a la cual pertenecen Psion, Nokia, Ericsson, Motorola, Matsushita y Sony con el sistema operativo Epoc, y Microsoft con el Windows CE.

  En la siguiente capa hay un grupo de compañías de software, entre las que están Palm Computing, AvantGo, Symbian, Microsoft y Openwave (Phone.com), el líder del mercado de micronavegadores. Estas firmas han empezado a ofrecer aplicaciones de software como correo electrónico y navegadores web.

- **Los operadores de redes**

  En la cima de la estructura están los operadores de redes de teléfonos móviles, que se prevé ofrecerán contenidos y servicios de valor añadido como noticias, cotizaciones de bolsa, horarios e información meteorológica a dispositivos móviles que utilicen WAP. Este grupo es quizás el menos definido, ya que podría incluir a los propios operadores de redes, a los suministradores de contenidos como Pearson, Reuters y Bertelsmann y a otras compañías de los sectores de distribución y servicios financieros. En

principio, el servicio de Internet móvil más popular probablemente será el correo electrónico.

- **Los fabricantes de equipos**

  Aún no está claro cuántas compañías del Internet móvil ganarán dinero en este mercado emergente. Por ejemplo, si el mercado de móviles sigue el mismo camino que el de tecnología de la información para PCs, el hardware se convertirá en un artículo de consumo de precio bajo en el que la clave del éxito será la producción de grandes cantidades de unidades a bajo coste por tan sólo unas pocas multinacionales. Katrina Bond, coautora del informe "*Mobile Ecommerce"*, de Analysys[3], señala: "Se prevé que en el 2003 haya 1.000 millones de abonados móviles, lo que representa una de cada seis personas de la población mundial".

La cantidad de información o las cosas que se pueden comprar por Internet con un móvil son todavía bastante limitadas, pero los investigadores de mercado dicen que su futuro es prometedor. Datamonitor[4] prevé que en el 2005 se gastarán 16.600 millones de dólares sólo en el m-commerce de artículos de consumo.

Karl Hicks, autor del informe, "Paradigmas cambiantes en el mundo de la estrategia del comercio móvil", (*Shifting Paradigms in the World of Mobile Commerce)*, afirma que "el verdadero potencial del m-commerce no se hará realidad hasta al menos dentro de tres años"[5]. Las causas son la carencia de teléfonos WAP y de contenidos de Internet que se puedan visualizar en un teléfono WAP. Además, hay algunos temas de facilidad de uso por solucionar. Andy Mullholland, director técnico de la compañía de servicios informáticos europea Cap Gemini[6], señala: "Hay limitaciones e inconvenientes que se deben resolver. Por ejemplo, la diminuta pantalla de texto de un teléfono implica que la información que aparezca debe ser sucinta y sencilla. No tiene las ventajas de una pantalla a color de un PC en la que se pueden ver imágenes complejas y navegar por todas partes". Y añade: "Una cosa esencial es

[3] http://www.analysys.com
[4] http://www.datamonitor.com
[5] http://www.venturedome.com
[6] http://www.cgey.com/

que los distribuidores reconozcan al teléfono como un canal más, ya que más de un millón de estos teléfonos entrarán en circulación este año, y dentro de tres años el 50% de todos los teléfonos móviles tendrán acceso a Internet".

El desarrollo de nuevas aplicaciones para el mercado de la telefonía móvil depende de una combinación acertada de factores, (incorporación de sistemas de posicionamiento, conocimiento del cliente, cobertura de los operadores móviles, individualización de servicios mediante el manejo de perfiles de usuarios, comodidad y facilidad de uso de los dispositivos móviles), que llevan a las empresas a dar un paso adelante y marcar la diferencia, es decir, el comercio móvil puede llegar a convertirse en una fuente de ventaja competitiva.

Las propiedades particulares del m-commerce, junto con las del comercio electrónico en sí, permiten inferir el modelo de desarrollo del m-commerce de la Figura 2-2, donde la generación de nuevos servicios móviles de datos está provocando desplazamientos en la cadena de valor y la aparición de nuevos agentes.

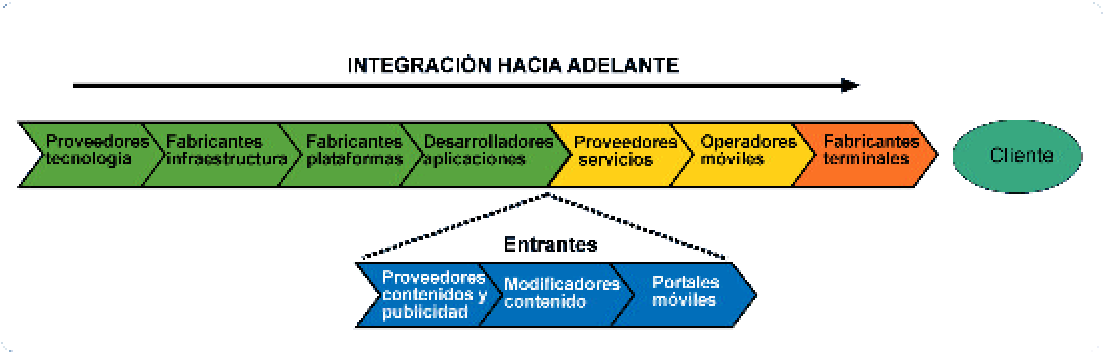

Figura 2-2. Cadena de valor del m-commerce

2.2. SERVICIOS DISPONIBLES

La gama de servicios ofrecidos, actualmente, por los operadores de telefonía móvil se puede considerar amplia pero limitada por la tecnología disponible. En los inicios de la telefonía móvil el servicio tradicional era el de voz (mediante tecnología analógica o digital con la aparición de GSM); con el tiempo se incorporaron servicios de valor agregado, tales como, buzón de voz, limitación de consumo, etc; sin

embargo estos servicios son solamente anexos al de voz, mediante la explotación de las posibilidades ofrecidas por la red.

La aparición de WAP, (Wireless Access Protocol), ha permitido la comercialización de otro tipo de servicios dando paso a una nueva generación, enfrentándose a las limitaciones de la tecnología GSM, (Global System for Mobile communication), las cuales han supuesto, equivocadamente, el fracaso de WAP y de los servicios de acceso a Internet móvil.

Se espera que las nuevas tecnologías, (GPRS y más adelante UMTS), junto con las perspectivas de penetración de Internet y sus respectivas regulaciones, permitirán redefinir la gama de productos y servicios capaces de ofrecerse al usuario por una operadora de red.

Así, lo que está claro es que la aparición de nuevos servicios exige diversas necesidades de ancho de banda sujetas a la disponibilidad de las tecnologías necesarias para soportarlas. La Figura 2-3, muestra las necesidades de ancho de banda de estos servicios, relacionadas con la aparición e implantación de dichas tecnologías.

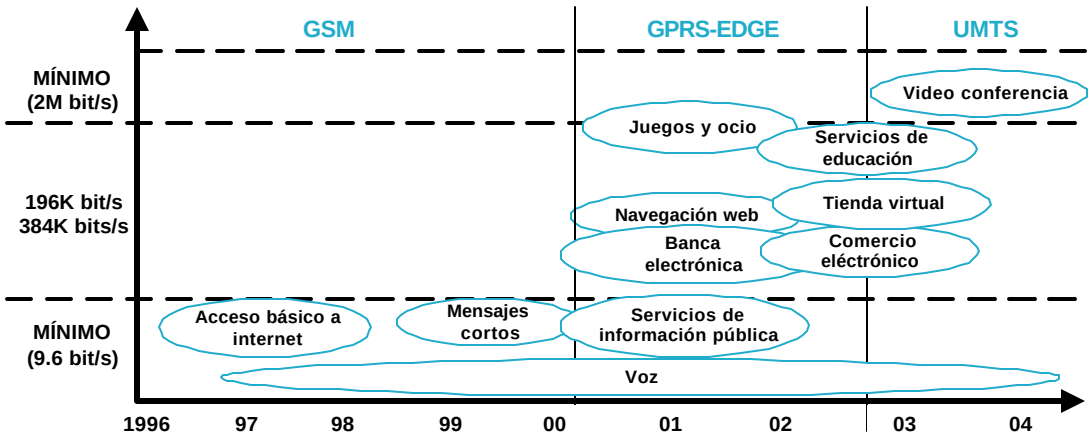

Figura 2-3. Servicios de m-commerce [7]

[7] Fuente: ArthurAndersen: http://www.arthurandersen.com

Datamonitor prevé que el campo de los servicios financieros móviles será uno de los que más se beneficiará del mercado del m-commerce. En concreto, considera la compraventa de acciones móvil como una "aplicación crucial". También prevé que "las aplicaciones que más se utilizarán serán aquellas que ayuden a los usuarios a tomar decisiones acertadas mientras se desplazan o están viajando".

Estos servicios se pueden dividir en tres categorías según su aplicación:

- Entretenimiento (Juegos sencillos, compra de loterías, etc.)
- Informativos (Noticias, Información de interés, etc.)
- Transaccionales (Operaciones bancarias, realización de pagos, pedidos de productos y servicios)
- Este último tipo de servicios, son los que más valor agregado proporcionan a los usuarios.

Las aplicaciones para el Internet inalámbrico y el comercio móvil serán distintas para cada uno de los usuarios, tanto individualmente como por país. Por ejemplo, existirán usuarios que en vez de querer pesados vídeos y aplicaciones de multimedia que requieren un amplio ancho de banda y poder de procesamiento, preferirán aplicaciones más ligeras y personalizadas, como por ejemplo noticias de interés o información sensitiva al tiempo, como el precio de las acciones o e-mail de prioridad.

Asimismo, resulta difícil que los consumidores utilicen sus teléfonos celulares para realizar transacciones complejas. Por el contrario, lo más probable es que realicen compras bastante simples como la adquisición de acciones, pasajes, entradas para el cine o transferencia de fondos. También se perfila como un servicio bastante popular la localización de personas, productos o servicios en un radio determinado. Sin embargo, aplicaciones mucho más pesadas como los vídeo juegos también tienen un mercado potencial. Por ejemplo, en Japón esta clase de servicios cuenta con gran expectativa. Asimismo, existen negocios que necesitan que sus trabajadores compartan cantidades importantes de información o ingresen al Intranet de la empresa mientras se están movilizando.

Ya que el m-commerce se trata de una forma más de comercio electrónico y como tal, los aspectos críticos del éxito del servicio son: el atractivo, la utilidad de los contenidos y el nivel de seguridad ofrecido al usuario. Es de aplicación tanto al modelo B2C (Business to Consumer) como al modelo B2B (Business to Business). De este modo, se tienen que adecuar los modelos de negocio tradicionales en las empresas a las condiciones particulares del acceso móvil al servicio.

2.3. VENTAJAS Y DESVENTAJAS

Las principales ventajas que presenta este nuevo paradigma del comercio están implícitas en su naturaleza, la movilidad, el hecho de no tener que llevar dinero o tener que hacer colas, además de tener disponibles en la palma de la mano el acceso a diferentes servicios personalizables, hacen del m-commerce una tecnología lo suficientemente atractiva para ir ganando mayor número de seguidores día a día.

A pesar de las atractivas ventajas que presenta el comercio móvil existen ciertos obstáculos que sortear, para que los servicios de Internet inalámbrico y por ende de comercio móvil puedan, finalmente, despegar. Actualmente, en el mundo occidental, el comercio móvil necesita de una plataforma basada en tecnología WAP (*Wireless Application Protocol*); la cual, todavía no ha penetrado lo suficiente en los mercados y aunque ya se utiliza en Europa, no obstante dista mucho de la amplitud de banda, flexibilidad y capacidad de procesamiento, propios de los computadores.

Para los fabricantes de dispositivos móviles, su gran reto es la variedad de sistemas de comunicación desarrollados. Entre ellos, el sistema GSM (*Global System for Mobile Communications*) es un estándar muy aceptado en Europa, pero con una capacidad muy limitada de transmisión de datos (9.6 kbits/sg), que no permite descargar archivos ni realizar tareas complejas a excepción de leer el correo electrónico. Frente a este sistema, el GPRS (*General Packet Radio Standard*) ya presenta una velocidad de transferencia de 115 kbits/sg, y permite a las operadoras cobrar en función de los datos transmitidos y no del tiempo de conexión.

La solución más avanzada llegará con la denominada tercera generación (*3G*). En Europa será el sistema UMTS (*Universal Mobile Telecommunications Systems*),

disponible en este año (2002), que permitirá velocidades de transferencia de hasta 2Mbits/sg (estimaciones más realistas cifran 200Kbps). Una vez implantado el UMTS, el m-commerce podría despegar definitivamente

El mejor aporte de la migración de tecnología es el aumento en el ancho de banda, lo que permitirá desarrollar nuevas y mejores aplicaciones (aplicaciones en tiempo real, video, mp3, etc.), mejorar la seguridad del comercio móvil, lo cual incrementará la confianza de los usuarios.

La siguiente gráfica muestra la migración de la infraestructura Wireless a través de las generaciones de tecnología.

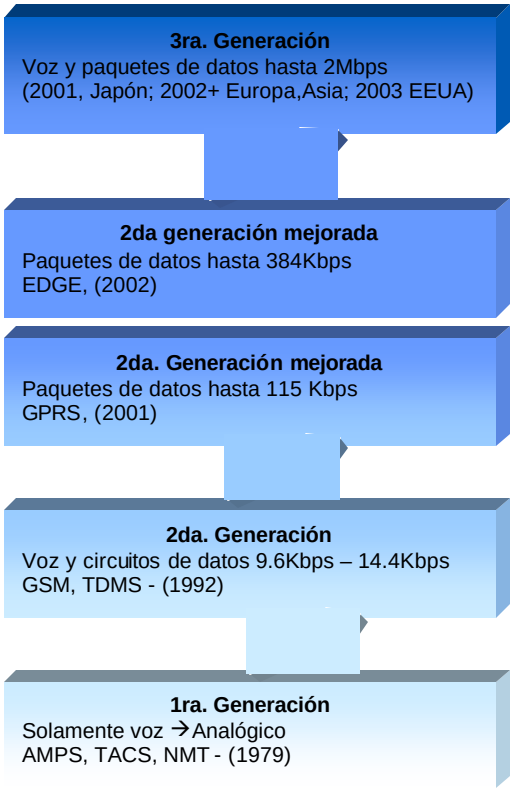

Figura 2-4. Migración de la infraestructura wireless

Estos factores combinados con los altos requerimientos de seguridad que imponen los sistemas inalámbricos y la información a transmitir, hacen que el camino por recorrer hacia el desarrollo de sistemas de comercio móvil altamente efectivos tenga muchos retos aún por superar.

2.3.1. Barreras tecnológicas, económicas y legales

Obtener ganancias a través de m- commerce será complicado ya que todo el mundo está acostumbrado a que toda la información sea gratuita, al ser este el modelo que se parece más al modelo de la web. Se espera que los ingresos por WAP sean menos del 2% de los ingresos de las operadoras en los primeros 18 meses y que luego crezcan lenta pero establemente en el futuro. Sin embargo el potencial del m-commerce no empezará a materializarse hasta dentro de tres años. Ahora hay muchas limitaciones y el móvil debe ser simplemente un canal más.

A continuación se señalan algunas de las barreras o limitaciones a las que se enfrenta Internet móvil.

2.3.1.1. Barreras tecnológicas

- Memoria de los dispositivos: algo tan aparentemente sencillo como otorgar capacidades de email a usuarios móviles se traduce por ejemplo en vigilar que no se llene el mini- buzón e ignorar por completo la información adjunta a estos e-mail (attachment), porque con la memoria llena, los mensajes nunca podrán llegar al destinatario
- Capacidad de las baterías: las actuales no sirven para ofrecer servicios tales como video, y MMS, (*Multimedia Messaging Service*) en general.
- Capacidades de presentación gráfica los dispositivos.
- Velocidad y definición de estándares transmisión de la información (los actuales 9.6 Kbps por conmutación de circuitos no dan para mucho)
- Seguridad en las transacciones económicas (Mastercard, Securenet y otros colaboradores trabajan para desarrollar un sistema de identificación digital para la compra a través de los dispositivos móviles).

2.3.1.2. Barreras económicas

- Costo de los dispositivos y accesorios (los teléfonos WAP son todavía un poco prohibitivos para la mayoría del público)

- Adaptación de los negocios online a las características de estos dispositivos móviles (de momento en un estado poco maduro, los contenidos son básicos para el desarrollo del mCommerce)
- Costo de los servicios ofrecidos para el usuario final (no todos serán gratuitos, ya tenemos los primeros ejemplos con el acuerdo Bertlessman-Napster).

2.3.1.3. Barreras legales

- Localización por posicionamiento, (un dispositivo móvil puede estar siempre localizado sin necesidad de reclamar servicios de la red, por el mero hecho de estar encendido y bajo el área de cobertura de unas celdas), ya que puede vulnerar el derecho a la intimidad.

2.4. SEGURIDAD

El modelo de seguridad del m-commerce consta de dos fases, las cuales se ilustran en la siguiente figura:

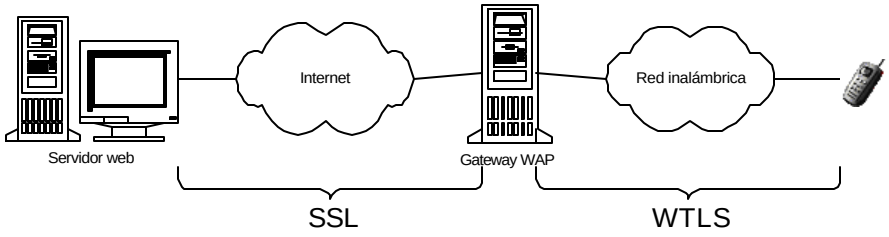

Figura 2-5. Modelo de seguridad WAP

En la primera fase se utiliza SSL para la comunicación entre la gateway y los servidores Web, el cual asegura, integridad, autenticidad y confidencialidad. La Gateway WAP toma los datos que le llegan por SSL y los adapta a un formato para los terminales móviles, utilizando WTLS, (*Wireless Transport Layer Security*) del protocolo WAP, por lo tanto la Gateway WAP sirve de puente entre el SSL y WTLS, las dos fases de seguridad en el modelo del m-commerce.

Mientras que el SSL esta diseñado para dispositivos y máquinas de una elevada potencia de procesamiento, WTLS, esta diseñado para que funcione en dispositivos móviles, los cuales tienen fuertes restricciones de procesamiento y de memoria.

El mayor problema que trae consigo esta estructura, es que por un momento, los datos están totalmente descubiertos, (sin protección alguna), ya que se deben desencriptar del protocolo SSL para pasarlos al protocolo WTLS. Este es el principal problema de seguridad del m-commerce y de la tecnología WAP en general.

Aunque probablemente la versión de WAP2.0 de una posible solución al problema, la verdadera solución no se establecerá hasta que se elimine la gateway WAP, de esta forma, se podría tener una conexión segura entre el terminal y el servidor ya que no sería necesario el proceso de desencriptación-encriptación.

Uno de los factores claves para la aceptación e implantación del m-commerce es la seguridad brindada en las transacciones, por esto, este tema es uno de nuestros casos de estudio y por lo tanto se le ha dedicado un capitulo en esta monografía, en el cual se describe en detalle, la estructura y el modelo necesario para brindar un sistema seguro al usuario.

2.5. FACTORES CLAVES PARA UN M-COMMERCE EXITOSO

El m-commerce será la próxima gran ola de arrastre de esta década, similar al impacto que tuvo el e-commerce durante la década de 1990 (la era de Internet). A continuación se proporcionan detalles de los factores claves para el desarrollo de aplicaciones de m-commerce:

2.5.1. Minimizar el número de operaciones con el teclado

Para evitar que los usuarios se pierdan mientras navegan por la Internet, las aplicaciones y navegadores inalámbricos deberán diseñarse de tal modo que el consumidor pueda completar una transacción con un número mínimo de operaciones con el teclado. Por ejemplo, un consumidor podrá llegar a la página de destino final para reservar un vuelo en un número mínimo de pasos.

El menú debe estar organizado de tal manera que permita a los consumidores tener acceso a la página final, pasando por alto el mayor número de páginas intermedias posible. Dicho de otra manera, las aplicaciones organizarán el contenido con jerarquías planas que expongan las áreas de uso más frecuente o las más populares. Este mejor método permitirá a los usuarios recuperar información fácil y al instante.

2.5.2. Promover la facilidad de uso de las aplicaciones inalámbricas

En general, la mayoría de los dispositivos móviles tienen características de entrada limitadas y pantallas pequeñas, tales limitaciones impiden al usuario tener acceso a la información y procesarla con facilidad. Como la mayoría de los teléfonos portátiles tienen minipantallas y teclados pequeños, las aplicaciones inalámbricas deben ajustar pantallas pequeñas. Los títulos de mensajes de alerta y notificaciones deben ser relativamente cortos, de menos de 10 caracteres. Además, como el ingreso de números y especialmente de texto es difícil, las aplicaciones deben tener la "inteligencia" para identificar la cadena de letras de una palabra con base en los primeros caracteres ingresados. En resumen, las aplicaciones inalámbricas deben tener un diseño que ofrezca una navegación fácil de seguir, coherente e intuitiva.

2.5.3. Personalizar el contenido con base en el perfil del usuario

Los consumidores de dispositivos inalámbricas desearán recibir contenido personalizado, clasificado por prioridad y filtrado de acuerdo con sus preferencias. En lugar de navegar para tener acceso a la información, los consumidores obtendrán una personalización inteligente para recuperar contenido y servicios altamente personalizados. Por ejemplo, los usuarios podrán recibir alertas personalizadas por correo electrónico, con contenido personalizado para negociar con acciones, reservar boletos o hacer ofertas por producto.

2.5.4. Proporcionar mensajes de alerta y notificaciones

Es probable que los servicios de mensajes cortos (SMS) sean una aplicación clave, "*Killer application*", para el m-commerce. SMS desempeña un papel decisivo en el m-commerce porque permite a los usuarios suscribirse a cierto contenido y servicios

que serán enviados automáticamente a sus dispositivos inalámbricos. Por ejemplo, los usuarios pueden programar sus dispositivos inalámbricos para recibir mensajes de alerta sobre promociones especiales, demoras o cancelaciones de vuelos, y nuevas ofertas.

En el futuro cercano, los consumidores podrán responder a los mensajes de alerta de SMS enviando una solicitud de compra-venta de acciones o autorizando pagos de facturas de cuentas atrasadas. Asimismo, SMS puede ofrecer compatibilidad con tecnología de flujo de trabajo y permitir a clientes de una compañía recibir y reenviar mensajes a una cadena de personas en toda la organización (y fuera de ésta si es necesario).

WAP, además, cuenta con especificaciones para el manejo de tecnología PUSH y MMS, (*Multimedia Messaging Service*). La tecnología PUSH, al contrario de una aplicación cliente/servidor convencional, permite enviar mensajes al cliente si necesidad de que el cliente realice una petición, por otra parte MMS, es un sistema de aplicación por medio del cual se habilita a un cliente WAP, proporcionándole operaciones de envío de mensajes utilizando varios tipos de medios. Estos servicios permiten a los desarrolladores de aplicaciones ofrecer una amplia gama de utilidades, las cuales se presentan al usuario como servicios con un alto valor agregado.

Además con la introducción de estándares para el manejo de estas tecnologías, (PUSH, MMS y SMS) permiten a usuario y proveedores ser testigos de implementaciones de estos servicios de forma segura confiable y eficiente.

Sin embargo, no se debe exagerar en el uso de alertas o notificaciones automáticas. Las aplicaciones inalámbricas deben permitir a los usuarios activar o desactivar mensajes de alerta o bien cambiar la configuración de los sonidos de aviso para evitar quedar inundados con mensajes de este tipo.

2.5.5. Permitir a los usuarios responder con un proceso eficaz

Los usuarios móviles podrán recibir contenido personalizado automáticamente y responder a las noticias de manera inmediata y eficiente. Por ejemplo, los

consumidores podrán tener acceso a sus cuentas bancarias y pagar facturas con sólo pulsar unas cuantas teclas. Los inversionistas podrán recibir alertas de cotizaciones de acciones que alcancen un valor umbral predefinido y vender o comprar con sólo pulsar un botón de su dispositivo inalámbrico. También hemos visto que los clientes pueden comprar productos sin tener que visitar más que un lugar.

Los usuarios podrán responder seleccionando una dirección URL para procesar de manera eficaz una transacción. Como se dijo antes, se deben minimizar el número de operaciones con el teclado y la cantidad de datos ingresados. En cuanto el usuario reciba un mensaje de alerta, una dirección URL estará disponible para que el usuario tenga acceso a ella y responda de conformidad.

2.5.6. Minimizar el costo del tiempo al aire

La mayoría de los servicios cobran a los usuarios cada minuto de acceso a datos. Cuando la tecnología de paquetes esté disponible ampliamente, es posible que se cobre a los usuarios por paquete (la cantidad de datos) o una cuota fija.

Hasta que esta estructura de tarifas se convierta en una oferta estándar en el mercado, las aplicaciones deberán estar diseñadas para minimizar el número de viajes de ida y vuelta al servidor del sitio.

2.6. PERSPECTIVAS FUTURAS

Algunos analistas prevén una gran oportunidad para el comercio móvil. No obstante, es incierto el tamaño de las ganancias que el comercio móvil pueda generar. Tal como el e-commerce, el m-commerce crecerá tan rápido como la infraestructura que utiliza como soporte se lo permita, según revela un estudio de Mori, agencia británica de investigación de mercados, el comercio a través del móvil multiplicará nada menos que por ocho el número de usuarios del comercio electrónico, se pronostica que el valor anual de los bienes y servicios consumidos a través de las redes móviles alcanzarán los US$ 13,000 millones en el año 2003, llevando esto a que los cálculos para el mercado mundial de m-commerce en el 2005 dicen que estará entre 6.4 billones y 210 billones de dólares. En la medida en que los

servicios de transmisión inalámbricos se desarrollen y que el número de usuarios de Internet móvil sobrepase a los usuarios que utilicen PC, se espera que este porcentaje pueda crecer de manera rápida y sostenida.

Puesto que Europa le lleva la delantera a Estados Unidos en el mercado de la telefonía móvil, se espera que el comercio electrónico móvil se desarrolle más rápidamente en los mercados europeos. Los países nórdicos, con su elevada penetración de Internet y la alta proporción de teléfonos celulares marcharán a la cabeza; sin embargo, EEUU debería equipararseles en unos cuantos años. De igual manera, los consumidores japoneses están muy interesados en las posibilidades del comercio móvil, de hecho ya están a la delantera con los desarrollos y aplicaciones en este campo.

Esta rápida expansión del mercado móvil hará que los operadores de las redes móviles, así como los portales de Internet, los proveedores de contenido y las firmas que ofrecen servicios en línea sentirán presión para adaptarse. Para que los portales móviles alcancen el éxito atrayendo el mayor número de usuarios, 'tendrán no sólo que agregar más valor, sino que deberán tener una marca propia poderosa y demostrar que atraen una gama de servicios de parte de comerciantes con marcas fuertes.

A la postre las distinciones entre red, comercio electrónico y comercio móvil se harán más difusas conforme las personas se acostumbren a tener acceso a cualquier información.

3. TRANSACCIONES Y SEGURIDAD EN COMERCIO ELECTRÓNICO MÓVIL

El crecimiento del mercado en la tecnología inalámbrica esta conducido principalmente por la necesidad de mejorar la productividad y reducir de costos en las transacciones. Últimamente la tecnología inalámbrica facilita la convergencia, en dispositivos, de funcionalidad y propósitos múltiples.

Tradicionalmente, los teléfonos móviles proporcionan servicios basados en voz, mientras que los computadores portátiles y asistentes digitales personales, (PDA, *Personal Digital Asisstant*), ofrecen acceso a datos, para dar así un incremento a la fuerza de trabajo móvil. Sin embargo, las limitaciones físicas de cada tipo de dispositivo han creado restricciones que se traducen en una experiencia de usuario inconsistente: tamaños de pantalla variables, capacidades de procesamiento y memoria limitadas, y plataformas operativas diversas; las cuales son una barrera para que el usuario tenga una experiencia similar entre dispositivos y redes inalámbricas. Además, los problemas de seguridad y los inadecuados procesos de pago, han impedido su adopción masiva.

Para promover la adopción de soluciones inalámbricas, empresarios y operadores inalámbricos necesitan ofrecer a empleados y clientes acceso fácil a transacciones e información de alto nivel, en el momento y lugar indicados para realizar sus negocios. Esto requiere una experiencia de usuario funcional y consistente comparada con la experiencia de usuario en el PC, más la seguridad de aplicaciones y transacciones confiables y entrega de servicios orientados a las necesidades de usuarios móviles.El crecimiento en la adopción de aplicaciones y servicios basados en dispositivos móviles será posible solamente cuando la experiencia de usuario tenga altos niveles de confiabilidad, conveniencia y valor

agregado, tal como el usuario lo percibe en los servicios fijos actuales. La introducción de una infraestructura inalámbrica confiable que pueda hacer disponibles en cualquier momento y lugar, información y transacciones, para los operadores inalámbricos, puede atraer nuevos usuarios, incrementar suscriptores y crear nuevos canales de ingresos; mientras que para las empresas puede reducir costos en las operaciones, incrementar ingresos y proporcionar mejores servicios a sus clientes.

La extensa adopción de aplicaciones y servicios inalámbricos requiere que se optimice:

- **Confiabilidad:** Los servicios digitales confiables deben ser construidos en infraestructuras y aplicaciones inalámbricas que sean altamente disponibles, transparentes y sin importar sobre que tipo de dispositivo funcione.
- **Seguridad:** Los servicios basados en autenticación de certificados digitales, autorización, encriptación y no-repudiación ayudan a asegurar la entrega de información y contenido de alto valor tal como se recibe por medio de la Internet fija o en una red privada virtual.
- **Experiencia de usuario:** Acceder a una URL debe ser fácil de tal forma que el Web inalámbrico sea conveniente y efectivo. Los usuarios deben ser capaces de acceder a contenido con el mismo nivel de confiabilidad que obtienen en Internet o en una red privada virtual.
- **Entrega de contenido:** La entrega y despliegue de contenido debe similar a la experiencia proporcionada por el PC, y conservarse con la introducción de nuevos dispositivos. Los usuarios deben percibir como valor agregado la habilidad para acceder fácilmente al contenido Web, la ejecución segura de transacciones y pagos y aprovechar el aumento en la productividad con aplicaciones móviles empresariales.
- **Comercio:** Los servicios inalámbricos deben incluir metodologías de pago y transacciones seguras que se acomoden a la experiencia y expectativas del usuario, es decir, los usuarios necesitan una forma fácil de pagar por el contenido móvil, tal como se realiza con los productos y servicios tradicionales.

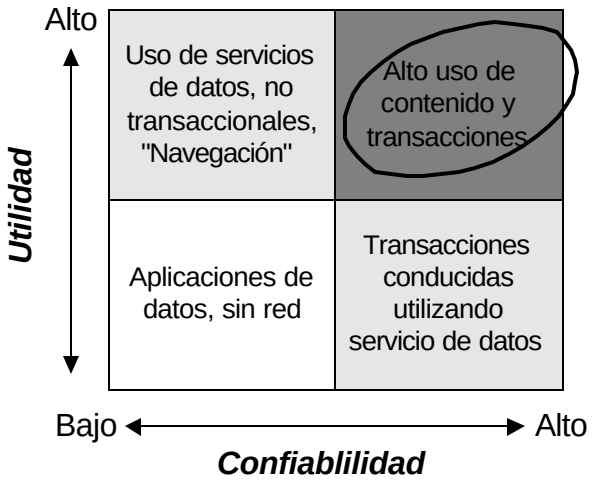

Figura 3-1. Relación de utilidad y nivel de confiabilidad de servicios inalámbricos[1]

El teléfono móvil rápidamente se esta envolviendo en mucho más que una teléfono sin cables; se esta transformando en un dispositivo personal confiable, (PTD, *Personal Trusted Device*), que permita la creación de una gran variedad de nuevos servicios y aplicaciones basados en acceso seguro p. Ej. transacciones bancarias, pagos, venta de tiquetes, etc.

Actualmente no existe una organización que provea un ambiente de desarrollo aceptado globalmente para el comercio electrónico móvil. Algunas iniciativas han sido emprendidas por varias organizaciones con el fin de promover ciertos protocolos, estándares y soluciones de seguridad; sin embargo no han tomado el camino adecuado para seguir los requerimientos del PTD, el cual esencialmente pone en el centro del mundo del comercio electrónico móvil, al usuario, permitiéndoles mantener el control de su ambiente de seguridad y establecer enlaces seguros con un amplio rango de proveedores y aplicaciones, posiblemente sin los servicios de un servidor intermedio.

El amplio éxito de la telefonía móvil y los cientos de millones de teléfonos móviles que serán vendidos en un futuro cercano significa que un gran número de personas en el mundo estarán involucradas en el comercio electrónico móvil. Con el fin de dar soporte a este crecimiento, se creo el MeT, (*Mobile electronic Transactions*), el cual

[1] Para estimular el uso de servicios inalámbricos, los operadores, desarrolladores de aplicaciones y empresas deben crear servicios que sean fáciles de utilizar e incorporar un alto nivel de confiabilidad y seguridad.

tiene como objetivo adoptar un crecimiento coherente del mercado del comercio electrónico móvil, apuntando a asegurar que las aplicaciones que utilizan transacciones seguras sean desarrolladas con una experiencia coherente de usuario (CUE, *Consistent User Experience*) en el uso de diferentes tipos de teléfonos, tecnologías de acceso y escenarios de uso.

MeT fue inicialmente conformado por Ericsson, Motorola y Nokia, actualmente se han adicionado otros fabricantes tales como Panasonic, Siemens, Sony y en los últimos días NEC[2], los cuales son una conexión importante y representativa para la industria telefónica móvil. Estas compañías comparten la visión de un mercado coherente y creciente como resultado de una experiencia consistente de usuario independiente del dispositivo, red o servicio.

3.1 ASPECTOS Y FUNCIONES IMPORTANTES DEFINIDOS POR MET PARA UN SISTEMA SEGURO

3.1.1 Modelo de referencia del sistema

3.1.1.1 Elementos claves del modelo de referencia

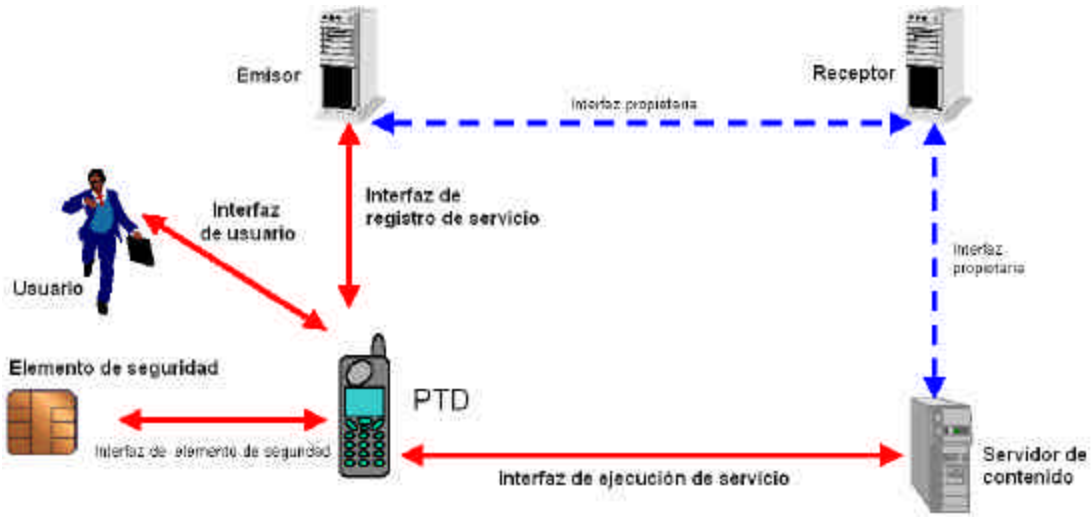

Figura 3-2 Modelo de referencia del sistema

[2] 2 de octubre de 2001, MeT. *Press Releases*. [Consulta: 20 noviembre de 2001]. Disponible en: http://www.mobiletransaction.org/pressreleases/october2.html

La Figura 3-2 muestra el modelo de referencia para MeT. En muchos escenarios el emisor, receptor y/o servidor de contenido pueden ser reducidos en dos o hasta en una entidad; no obstante, aquí se pretende mostrar los principios básicos del modelo, los cuales son aplicables a la mayoría de los ambientes.

Los principales elementos presentados en el diagrama son los siguientes:

(i) PTD: El teléfono móvil del usuario es el Personal Trusted Device (PTD). El PTD es utilizado para establecer el ID (identificación) del usuario y autorizar transacciones (con una firma digital). El PTD incluye un elemento de seguridad que contiene el par de llaves públicas del usuario y certificados raíz (utilizados para verificar otros certificados). El elemento de seguridad puede ser implementado en cualquiera de las siguientes formas: *(a) combinado*, card SIM/WIM (*Suscriber Identity Module*/*WAP Identity Module*); *(b) una tarjeta inteligente WIM; (c) en un dispositivo removible* que contenga la funcionalidad WIM; *(d) Un hardware*, el elemento de seguridad dentro del teléfono; o *(e) un software* de elemento de seguridad en el teléfono. El PTD también contiene certificados de servicio de usuario o certificados de URLs[3].

(ii) Servidor de contenido: A través de éste el proveedor de servicio proporciona contenido. En los entornos, local y remoto, el contenido se envía desde el servidor de contenido y se presenta al usuario en el PTD. En entornos personales, el contenido puede desplegarse en otro dispositivo.

En el caso de los entornos locales o remotos, el servidor de contenido puede ser accedido a través de cualquier proxy (p. Ej. Una gateway WAP).

De esta forma una aplicación corriendo en un servidor de contenido puede solicitar al usuario realizar una autorización (firmar la transacción) y el PTD estará en capacidad de realizar esta función utilizando la interfaz de ejecución de servicio.

(iii) Receptor: El receptor de transacciones proporciona un solo punto de contacto entre emisores y proveedores de servicio. En los escenarios de transacciones (tal como pago por cuenta de cobro), el papel del receptor es proporcionar las reglas del negocio y conexiones entre los múltiples proveedores y receptores. No todos los

[3] El servicio de certificados y certificados de URLs son proporcionados por el usuario y no por los proveedores del servicio, p. Ej. Bancos o Autoridades de Certificación.

escenarios de uso necesitan de un receptor; en algunos escenarios tampoco el proveedor de contenido interactúa directamente con el emisor o el proveedor de contenido y el emisor son la misma entidad.

(iv) Emisor: El emisor proporciona el servicio de certificación para una cuenta en particular. En general, la razón de ser de una cuenta o un usuario de una cuenta, es el servicio ofrecido por el emisor. Esta cuenta podría asociarse con un valor monetario o con los datos de un usuario. El servicio de certificado permite al emisor identificar al usuario.

3.1.1.2 Interfaces

MeT define las siguientes interfaces en el modelo de referencia del sistema:

- Interfaz de ejecución de servicio desde el PTD al servidor de contenido.
- Interfaz de registro de servicio desde el PTD al emisor (también se refiere al servicio de registro del proveedor).
- Interfaz de usuario entre el PTD y el usuario.
- Interfaz del elemento de seguridad entre el PTD y un elemento de seguridad removible.

Interfaz de ejecución de servicio: Esta interfaz se utiliza para realizar transacciones seguras con un servidor de contenido.

Interfaz de registro de servicio: Esta interfaz se encuentra entre el emisor y el PTD y se utiliza para cargar certificados de servicio sobre el PTD. El emisor puede ser un proveedor de servicios financieros, tal como un banco o un departamento de crédito de un almacén, cuyo servicio pretende utilizar el usuario.

Interfaz de usuario: Esta interfaz representa las interacciones con el usuario que son necesarias para realizar transacciones MeT. Involucra: (1) Presentación de información al usuario sobre el PTD. (2) Peticiones de entradas y (3) Aceptación de entradas y reenvío apropiado de éstas. Una interfaz de usuario consistente (con un alto nivel de abstracción) contribuye a dar mayor seguridad al usuario.

Interfaz de elemento de seguridad: Esta interfaz se ubica entre el Elemento de seguridad y dos entidades en el PTD: la capa de transporte y la capa de aplicación.

La interfaz define las interacciones relativas a la verificación de usuario, procesamiento criptográfico, etc. que se definen en las especificaciones, WAP para WIM[4]. Se deben seguir las especificaciones de la interfaz WIM para los Elementos de Seguridad removibles. En el caso de los elementos de seguridad no removibles la interfaz puede ser propietaria de acuerdo al fabricante del PTD. Ejemplos de elementos de seguridad no removibles son los Elementos de Seguridad hardware embebidos y Elementos de Seguridad Software.

3.1.2 Ambientes

Los entornos en los cuales MeT habilita transacciones se clasifican en tres categorías: **remoto**, **local** y **personal**.

3.1.2.1 Ambiente Remoto

En este entorno la conexión entre el servidor de contenido y el PTD establece por medio de PLMN (*Public Land Mobile Nerwork*), como la red celular GSM.

El acceso desde WAP a Internet se realiza a través de una gateway WAP. La gateway WAP ejecuta las funciones de conversión del servidor proxy de protocolo WAP a protocolos de Internet, como se muestra en la Figura 3-3. Alternativamente el servidor de contenido puede contener la gateway WAP.

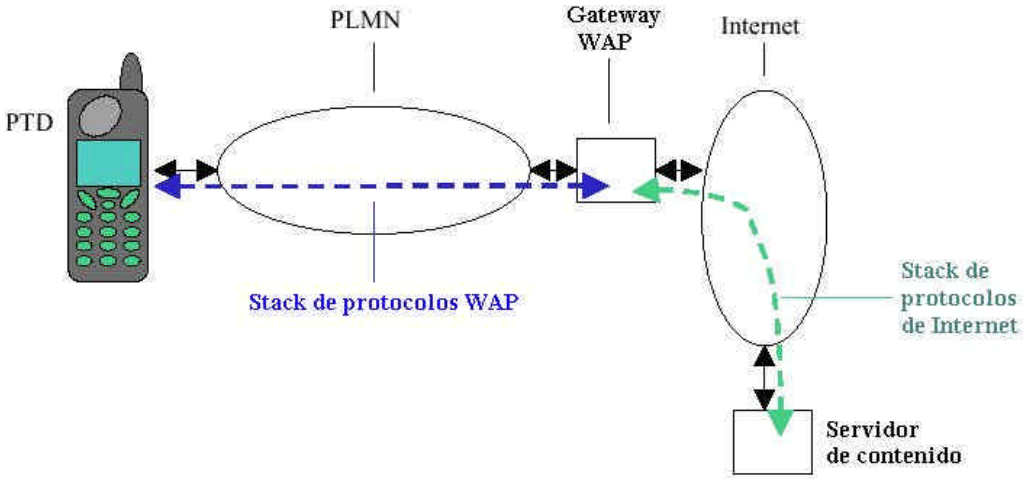

Figura 3-3. Ejemplo de ambiente remoto MeT

[4] "Wireless Identity Module Specification", WAP Forum, 05-11-1999. URL: http://www.wapforum.org/

3.1.2.2 Ambiente local

En el ambiente local las transacciones son iniciadas bajo tecnologías inalámbricas de corto rango, como Bluetooth. Una aplicación típica sería, venta de artículos al por menor utilizando pago con cuenta de cobro realizada desde un PTD.

La Figura 3-4 muestra una topología típica. El nodo de acceso Bluetooth está localizado en el mismo lugar donde se entrega el servicio, (de acuerdo al ejemplo anterior este sería un almacén de venta al por menor). Por esta razón el proveedor de servicio puede tener la capacidad de ofrecer contenido basado en la localización del usuario.

Para utilizar el stack de protocolos WAP sobre conexiones Bluetooth es necesario utilizar los mecanismos de seguridad disponibles en la especificación de WAP, como WTLS[5], de tal forma que sea posible proporcionar autenticación en el servidor y sesiones seguras.

En el ambiente local MeT no confía en la autenticación y encriptación Bluetooth para validar el contenido del servidor y ofrecer sesiones seguras; por el contrario utiliza WTLS para proporcionar estas facilidades.

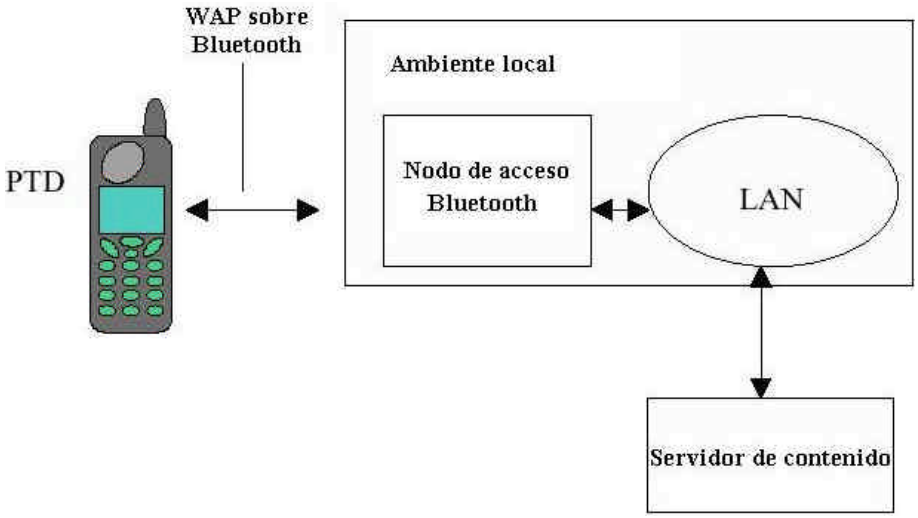

Figura 3-4. Ambiente local típico MeT

[5] "Wireless Transport Layer Security Specification", WAP Forum, 05-11-1999. URL: http://www.wapforum.org/

3.1.2.3 Ambiente Personal

En el ambiente personal el PTD habilita transacciones seguras desde otros dispositivos de comunicaciones (un PC, por ejemplo). El PTD participa en la autenticación y autorización haciendo posible certificar servicios y realizar firmas de operaciones requeridas por su elemento de seguridad. Así, el usuario puede utilizar otros dispositivos de comunicación sin tener que personalizarlos.

Un ejemplo de este ambiente es cuando un PTD usuario, conectado a un PC, navega en un site que requiere autenticación por medio de Internet utilizando el protocolo de la capa de transporte seguro, (TSL). El certificado para este site ya debe haber sido proporcionado al usuario y la llave privada asociada al certificado debe estar almacenada el Elemento de Seguridad del PTD, de esta forma el PC puede pedir al PTD realizar las operaciones criptográficas, solicitándole la llave privada, para autenticación y autorización de usuario. Exceptuando las operaciones de firmado, el PC maneja todas las operaciones relacionadas con el protocolo TSL. EL PC y el PTD pueden comunicarse utilizando tecnologías inalámbricas tales como Bluetooth, IrDA[6] o conexiones físicas por medio del USB o del puerto serial.

El ambiente personal habilita a dispositivos externos para acceder a las funciones del PTD, (p. Ej. almacenamiento de llaves), haciendo el uso de la seguridad inherente al Elemento de Seguridad. Esto habilita la promulgación de certificados de servicios para ser utilizados a través de diferentes métodos de acceso. Otros dispositivos podrán ejecutar las funciones MeT en el PTD utilizando la interfaz de ejecución de servicio personal.

[6] Especificación del sistema Bluetooth - parte A (Core) y parte B (Profiles), v1.0B 01-12-1999 URL: http://www.bluetooth.com/

Infrared Data Association. URL: http://www.irda.org/

Figura 3-5. Ambiente personal MeT

3.1.3 Funciones Principales

Las transacciones MeT esta construidas sobre un conjunto de funciones núcleo las cuales son reutilizadas en diversas aplicaciones o escenarios de uso. Las funciones núcleo son las siguientes:

1. Inicialización
2. Registro
3. Establecimiento de sesión segura
4. Autenticación
5. Autorización de usuario

3.1.3.1 Inicio del PTD

La inicialización del PTD permite equipar al Elemento de Seguridad con el par de llaves públicas iniciales y el certificado raíz CA, (*Certificate Authority*) necesarios para realizar transacciones MeT seguras. Algunos elementos de seguridad pueden ser entregados al usuario pre-inicializados –en el caso de WIMs, con un par de llaves privadas iniciales y un certificado raíz CA ya implantados. Un PTD además puede tener acceso a múltiples elementos de seguridad.

Las llaves pueden ser proporcionadas externamente a través de Elementos de Seguridad removibles, como en el caso de tarjetas SWIM (*Subscriber Wireless*

Identity Module, combinación de SIM y WIM), de tarjetas WIM o de otros elementos removibles con la funcionalidad WIM y su respectiva interfaz. Por otro lado las llaves pueden ser generadas internamente por un Elemento de Seguridad embebido. Los aspectos relacionados con la generación de llaves en una interfaz de usuario segura, se especifican en el documento "MeT *Consistent User Experience*".

Los certificados cliente almacenados en el elemento de seguridad tienen etiquetas que se despliegan al usuario para identificación del certificado y cuando se requiere introducir un PIN para desbloquear el certificado.

El certificado raíz CA puede ser proporcionado como una parte de la inicialización del proceso. El proceso para descargar los certificados raíz en entornos locales y remotos está especificado en, "*Wireless Public Key Infrastructure Definition*"[7]. Estos certificados contienen las llaves públicas del los CAs raíz quienes emiten los certificados para las transacciones de lo usuarios. Puede haber más de un certificado CA raíz.

3.1.3.2 Registro (Personalización)

El registro es por medio del cual un proveedor de servicios asocia una identidad de usuario con una cuenta de servicio. Esto se realiza asociando un certificado de servicio de usuario con el servicio. El proceso de registro personaliza el PTD para el usuario.

En MeT el PTD registra un servicio con el fin de tener asignados certificados de servicios a su par de llaves (se utilizan pares de llaves separadas para autenticación y firma). Siguiendo la recomendación WPKI, el PTD debe ser capaz de manejar completamente los certificados y las URLs almacenadas en él.

Un concepto fundamental de MeT es que a los certificados de múltiples servicios de diferentes proveedores pueden asignárseles un par de llaves común. Los certificados de servicios no necesitan ser almacenados en el elemento de seguridad, ya que no son susceptibles como la llaves privadas.

[7] "Wireless Public Key Infrastructure Definition", WAP Forum, 24-10-2000. URL: http://www.wapforum.org/

El proceso de certificación se define en WPKI. Este involucra peticiones en línea desde el PTD a un portal PKI, el cual redirecciona la petición al CA. El CA genera el certificado y envía el certificado completo o la URL directamente al PTD. El CA almacena el certificado emitido en su base de datos de llaves públicas.

Las fases de inicialización y registro pueden ser combinadas con algunos certificados de registro siendo estos proporcionados durante la inicialización.

3.1.3.3 Establecimiento de Sesión Segura

Una sesión segura se compone de: Confidencialidad, integridad de datos y de un servidor de autenticación. Idealmente una sesión segura se ubica entre el PTD y el servidor de contenido; sin embargo, la tecnología actual, aún no permite esto.

En entornos locales y remotos las sesiones seguras son proporcionadas por la capa segura del protocolo WAP, WTLS. Actualmente, de acuerdo con el *WAP June 2000 conformance release*, WTLS opera solamente desde el PTD a la gateway WAP. Esto proporciona sesiones seguras cuando el servidor de contenido esta localizado en la gateway WAP. Cuando el servidor de contenido esta separado de la gateway, las sesiones seguras pueden ser establecidas utilizando una aproximación de 2 fases que involucra el uso de WTLS entre el PTD y la gateway WAP, y SSL o TSL entre la gateway WAP y el servidor de contenido. En este caso la gateway WAP debe ser segura y confiable.

Las versiones futuras de WAP ofrecerán una capa de transporte segura end-to-end utilizando procesos de redirección del PTD a una gateway localizada en el servidor de contenido.

3.1.3.4 Autenticación

La autenticación de usuario permite verificar al proveedor del servicio si el usuario esta habilitado para utilizar el servicio, sin embargo es necesario tener en cuenta que no todos los servicios requieren de autenticación de usuario. Por ejemplo, una tienda Web donde el acceso a las “vitrinas” de compra están abiertas a todos los visitantes no requiere de autenticación (Aunque la compra, como tal, si requiere de autorización). Por otro lado, un servidor de contenido que maneja información

delicada por ejemplo un servidor de banca, requiere autenticación de usuario antes de proporcionar contenido.

MeT utiliza WTLS clase 3 para realizar la autenticación de usuario. Esto permite a la gateway WAP establecer la identidad del usuario por medio del certificado de servicio del usuario relacionado con la llave pública almacenada en el PTD. La autenticación del PTD es establecida por el envío desde el servidor al PTD de una petición, la cual el PTD firma y retorna.

La verificación del usuario es establecida por medio de la entrada del PIN de acceso el cual sólo conoce el usuario. Este PIN permite acceder el par de llaves utilizadas para la autenticación.

Como se planteó en el establecimiento de sesión, la autenticación es para la gateway WAP y no necesariamente para el servidor de contenido. Una futura capa de seguridad WAP end-to-end permitirá la autenticación a una gateway localizada en el servidor de contenido.

Es tan esperada como necesitada una capa de aplicación adicional para las funciones de autenticación, ésta estará encaminada a de métodos que involucren WAP, Bluetooth y otros estándares básicos de MeT.

3.1.3.5 Autorización por el usuario

La autenticación es el medio por el cual el proveedor de servicio asegura que el usuario ha visto y aceptado el contrato de la transacción. La autorización se realiza por medio de un contrato de transacción firmado digitalmente utilizando una llave privada asociada con un certificado de servicio de usuario. El contrato de transacción firmado puede ser almacenado por el proveedor de servicio como una prueba de la autorización de la transacción.

Ejemplos de uso de autorización por usuario son aprobaciones de pago en tiendas o de transacciones bancarias, a través del web.

MeT utiliza la función *signText* de WMLScript[8], para autorización. Esta función opera de la siguiente forma. SignText, (signText) es una función de WMLScript, que

[8] "WMLScript Crypto Library Specification", WAP Forum, 05-11-1999. URL: http://www.wapforum.org/

contiene un objeto de tipo *stringToSign*. El servidor de contenido construye un contrato en el *stringToSign*. El script es enviado al PTD donde el *stringToSign* (contrato) es desplegado en la pantalla de teléfono. Si el usuario acepta el contrato, debe entrar un PIN, este es el proceso de verificación de usuario para autorización. Si el PIN introducido es correcto, el *stringToSign* es firmado con la llave privada del PTD y retornado al servidor de contenido. Este contrato firmado es la prueba para el servidor de contenido dé la autorización de la transacción por parte del usuario.

3.1.4 Especificación De La Tecnología De Seguridad

3.1.4.1 WTLS, (TSL para WAP)

Las principales características de WTLS son:

- Basado en TSL/SSL
- Soporta protocolos basados en datagramas (p. Ej. UDP/TCP)
- Proporciona ancho de banda y optimización de memoria
- Proporciona actualización en línea para conexiones de larga duración
- Soporta algoritmos criptográficos
    - Encriptación: RC5, DES, 3DES, IDEA
    - Integridad: HMAC con SHA-1, MD5
    - Intercambio de teclas: RSA, Diffie-Hellman, ECC
- Proporciona opciones de autenticación: anónimo, autenticación de servidor, autenticación de servidor y cliente

3.1.4.2 WIM (interfaz con el Elemento de Seguridad)

WIM, tal como se define en WAP, en MeT sirve como la interfaz de definición del elemento de seguridad removible. Su implementación física incluye:

- Tarjeta inteligente (SIM u otra).
- Otro módulo hardware no falsificable

Los estándares aplicables son los siguientes:

- ISO7816-4 (almacenamiento, verificación de PIN, etc.)
- ISO7816-8 (operaciones criptográficas)
- PKCS#15 (formato de información)

La funcionalidad principal de WIM incluye:

- Autenticación de cliente WTLS
- Manejo de sesiones seguras
- Firmas digitales

3.1.4.3 WMLScript signText

Funcionalidad

- Aplicación de autorización de niveles de transacción
- Proporcionar seguridad – almacenamiento de firma como prueba de autorización de un servicio

3.1.5. Dispositivo Personal Confiable, (PTD, Personal Trusted Device*)*

El amplio éxito de la telefonía móvil y los cientos de millones de teléfonos móviles que serán vendidos en un futuro cercano significa que un amplio número de personas en el mundo estarán involucradas en el comercio electrónico móvil. Así, las especificaciones MeT apuntan a asegurar que las aplicaciones que utilizan transacciones seguras sean desarrolladas con una experiencia coherente de usuario (CUE, *Consistent User Experience*) en el uso de diferentes tipos de teléfonos, tecnologías de acceso y escenarios de uso.

MeT adopta y extiende las tecnologías y estándares de la industria existente, basándose en WAP por WTLS (*Wireless Transport Layer Security*), WIM (*Wireless Identity Module*) y WPKI *(Wireless Public Key Infrastructure*).

Para su uso define tres tipos de interfaz:

- La interfaz de registro de servicio

- La interfaz de ejecución de servicio
- Interfaz con el usuario, aspectos referentes a la experiencia de usuario en el manejo de transacciones seguras con el PTD.

Y opera en los ambientes ya definidos:

- El ambiente remoto o mundo de la Internet móvil.
- El ambiente local o físico.
- El ambiente personal o doméstico.

3.1.5.1. Definición del PTD, interfaces y entidades relevantes

Considerando el teléfono móvil como un PTD, los siguientes aspectos son relevantes:

- Debe ser personal, controlado y utilizado por una persona y llevado por una persona la mayor parte del tiempo.
- Debe tener una plataforma de aplicación por medio de la cual se asocian interfaces para transacciones relacionadas con servicios tales como de banca, pagos, etc.
- Debe tener una función de seguridad requerida para servicios relacionados con transacciones: sesiones seguras, autenticación y autorización.

EL PTD contiene un elemento de seguridad, que es utilizado para proteger la información más importante, (p Ej. las llaves privadas), utiliza un mecanismo para verificación de usuario; solamente ante una autenticación exitosa el PTD puede ser utilizado para realizar transacciones. La verificación de usuario se ejecuta en el elemento de seguridad (p. Ej. Tarjetas inteligentes que ejecutan operaciones criptográficas solamente después de recibir un PIN introducido por el usuario).

Con el fin de acceder a múltiples servicios, el PTD utiliza una base de datos de certificados para servicios específicos. En ella, se puede encontrar ya sean los certificados o enlaces a la localización del certificado (URLs).

Adicionalmente, el PTD puede contener una base de datos de transacciones (para contratos y cobros/entradas).

En la Figura 3-6, se muestran las interfaces y entidades definidas por el MeT para el PTD,

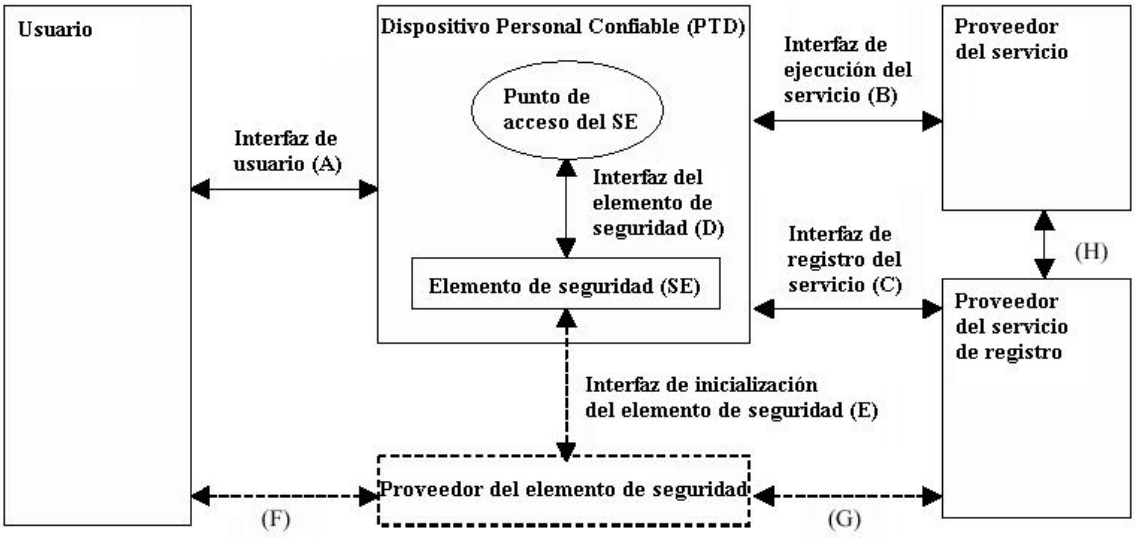

Figura 3-6. Interfaces definidas y entidades definidas para el PTD[9]

Usuario: Es la persona que posee el PTD.

PTD: Elemento utilizado para realizar transacciones electrónicas móviles. Contiene el elemento de seguridad.

Elemento de seguridad: Es utilizado para guardar llaves criptográficas y realizar operaciones utilizando estas llaves.

Proveedor del elemento de seguridad: Proporciona el elemento de seguridad al usuario, como parte del PTD o de forma separada.

Proveedor del servicio: Es una entidad compañera del PTD en aplicaciones de transacción, (en contraste con otras aplicaciones como por ejemplo la de registro).

Proveedor de servicio de registro: Proporciona el servicio de certificado al usuario (un certificado de usuario relacionado con un servicio). Aquí no hay distinción entre el papel de la autoridad de registro tradicional (RA, *Registration Authority*)y la autoridad de certificado (CA, *Certificate Authority*).

[9] Nota: Las líneas punteadas indican que un elemento o interfaz no está presente en todas las configuraciones y son utilizadas únicamente en situaciones específicas.

3.1.5.1.1 Interfaz de usuario

La interfaz de usuario (A) cubre interacciones entre el usuario y el PTD. El propósito de su definición es asegurar una experiencia de usuario coherente, caracterizada por los siguientes aspectos:

- Conocimiento del servicio/marca utilizado.
- Conocimiento de la seguridad del entorno.
- Verificación de usuario.
- Conocimiento de la firma digital
- Acceso a contratos firmados digitalmente.
- Acceso a objetos entregados (cobros/entradas).

3.1.5.1.2 Interfaz de ejecución de servicio

La interfaz de ejecución de servicio (B) define ahora como el PTD accede a un servicio de transacciones electrónicas móviles. Esto incluye algunas funciones: sesión segura, autenticación de usuario y autorización por usuario.

- **Sesión segura y autenticación**

  El establecimiento de una sesión segura como se indica en WTLS trae consigo los siguientes aspectos:

  - Negociación de parámetros de seguridad (algoritmos criptográficos y tamaño de la llave)
  - Intercambio de llaves basado el algoritmos de llaves públicas, resultado en llaves simétricas para encriptación de mensajes y protección de integridad.
  - Autenticación del servidor basado en un servidor de certificado (la autenticación de servidor es necesaria para prevenir que un impostor interprete el servicio).

  Durante una sesión segura, el PTD contiene información acerca de lo siguiente:

  - La identidad del servicio, basado en un certificado de servicio.

- Protección de sesión basado en parámetros relacionados: algoritmos y longitud de llaves.

- **Autenticación de usuario**

  Una función opcional durante el establecimiento de sesión es la autenticación del PTD al servicio (WTLS clase 3). El servicio realiza la petición de autenticación del PTD y el usuario debe aprobar la autenticación introduciendo su PIN.

  Durante este proceso se utiliza al elemento de seguridad. La autenticación del PTD combinada con la verificación de usuario, al PTD y al elemento de seguridad, tiene como resultado la autenticación del usuario para el servicio, (esto ocurre cuando el usuario introduce el PIN el cual se envía al elemento de seguridad).

  La verificación de usuario en el PTD es necesaria solamente una vez después de abrir el elemento de seguridad. Después de esto hasta que el SE es cerrado, la autenticación puede ser realizada varias veces.

- **Autorización por el usuario**

  Esta interfaz presenta al usuario un documento o datos de transacción, con el fin de que éste los autorice, El servicio puede guardar éstos datos como prueba de confirmación, (p. Ej. Documento firmado digitalmente).

  La autorización por el usuario es implementada utilizando la función de WMLScript signText.

  En la función singText se realiza:

  - El servicio proporciona un texto para ser firmado y el certificado de usuario requerido.
  - El usuario confirma el texto y el certificado que se esta utilizando.
  - Se ejecuta la verificación de usuario en el PTD, (el usuario ingresa un PIN, que es enviado al elemento de seguridad).
  - El texto (desmenuzado) es enviado al elemento de seguridad.

Note que el usuario necesita reingresar el PIN para cada autorización. La verificación de usuario requerida para autorización es diferente que la requerida para autenticación.

3.1.5.1.3 Interfaz de registro de servicio

La interfaz de servicio de registro (C) define como el PTD se registra en un servicio en particular. Esto incluye los pasos para petición y entrega de un certificado de servicio (el certificado de usuario especifico para ese servicio), como se define en WPKI.

3.1.5.1.4 Interfaz de elemento de seguridad

La interfaz del elemento de seguridad (D) define las interacciones pertinentes a la verificación y proceso criptográfico (interfaz WIM). Su funcionalidad define lo siguiente:

- Control de dispositivo (abrir, cerrar).
- Verificación, incluyendo verificación de gestión de datos (cambiar, desbloqueo de un PIN)
- Acceso a datos para lectura de certificados y otros datos
- Autenticación WTLS y gestión de sesión
- Firma digital

3.1.5.1.5 Interfaz de inicialización del elemento de seguridad

La interfaz de inicialización del elemento de seguridad (E) es utilizada para creación de llaves, certificados iniciales, PINs, etc. (Durante la fabricación de una tarjeta WIM).

3.1.5.1.6 Interfaz proveedor del elemento de seguridad – Usuario

Esta interfaz (F) cubre aspectos de entrega del elemento de seguridad e información relacionada, tal como PINs iniciales al usuario (cuando un operador entrega una tarjeta SWIM y PINs WIM al usuario).

3.1.5.1.7 Interfaz de registro de servicio Proveedor-Proveedor del Elemento de seguridad

La interfaz entre el proveedor del servicio de registro y el proveedor del elemento de seguridad (G) cubre aspectos de entrega de información acerca del elemento de seguridad, como los certificados requeridos para verificar la autenticidad del elemento de seguridad y las llaves asociadas.

3.1.5.1.8 Interfaz Proveedor de registro de servicio - Proveedor de servicio

La interfaz entre el proveedor de registro de servicios y el proveedor de servicio (H) cubre la entrega de información relacionada con PKI, tal como certificados raíz y otros CA, información de revocación de certificados, etc.

3.1.5.2. Elemento de Seguridad

El elemento de seguridad (SE, *Security Element*) es utilizado para guardar claves criptográficas y ejecutar operaciones utilizando estas llaves, puede ser removible o no removible.

Un SE removible, debe ser implementado de acuerdo a la especificación WIM[10]. Puede ser implementado como un IC *(Integrated Circuit*) o algún otro elemento hardware removible.

La funcionalidad de un SE basado en una tarjeta IC es implementada como una aplicación de tarjeta inteligente WIM. Esta puede residir en una tarjeta utilizada por una red inalámbrica de identificación de suscriptor, como una tarjeta GSM, ISM[11], una tarjeta USIM, (*Universal Subscriber Identity Module*) [12] o una auxiliar.

Un elemento no removible se implementa como un módulo hardware embebido o como un módulo software con procesamiento criptográfico.

[10] "WAP Identity Module Specification," WAP Forum. URL: http://www.wapforum.org/

[11] Sistemas de telecomunicaciones celular digital (Fase2+); Especificación del módulo de Identidad del suscriptor – Mecanismo móvil (SIM – ME) Interfaz (GSM 11.11 versión 5.4.0).

[12] 3G TS 31.102 Especificación Técnica, Plan de asociación de 3ra Generación; Grupo de especificaciones técnicas; Características de una aplicación USIM.

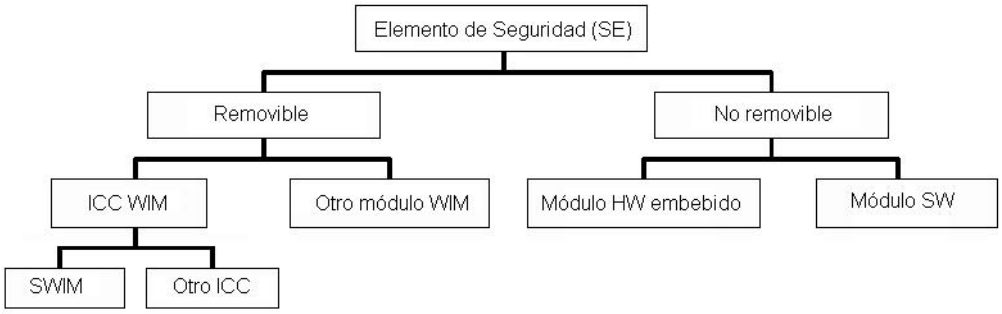

Figura 3-7. Conformación del Elemento de Seguridad, SE.

3.2 REQUERIMIENTOS DE SEGURIDAD PARA EL PTD

Según su concepción el PTD (Personal Trusted Device), es un dispositivo diseñado para una amplia aplicabilidad con el fin de consolidar propósitos de seguridad concisos en servicios de banca, pagos, ventas e identificación y autenticación corporativas. Aquí se presentan requerimientos de seguridad, genéricos, para un dispositivo confiable.

El propósito del PTD es que sea utilizado para múltiples aplicaciones que requieren seguridad, como transacciones bancarias, pagos, ventas, identificación corporativa, etc. Aquí se presentan los requerimientos sobre la implementación de estas funciones de forma segura. Según esto los requerimientos deben ser:

- Suficiencia, importancia para que el PTD sea aceptado por proveedores de servicio y usuario, para los servicios propuestos.
- Realismo, se relaciona a la vez con mercado y costo, esto es que el PTD este disponible para un amplio rango de consumidores.

3.2.1 Elemento de seguridad

En el caso de los elementos de seguridad removibles, la funcionalidad de la interfaz esta de acuerdo a la especificación WAP para WIM. Para elementos de seguridad embebidos, esta funcionalidad es asumida para cubrir al menos:

- Operaciones con llaves privadas
- Funcionalidad relacionada con la verificación de usuario, donde la verificación de usuario se requiere para obtener acceso a otras funciones.

Es recomendable que un elemento de seguridad sea evaluado ya que éste es el punto crítico en la seguridad del PTD, en la carga de operaciones con llave privada y verificación de usuario.

La evaluación debe cubrir aspectos de diseño, implementación físicos y de administración de seguridad. Éste debe ser realizado de acuerdo al "*Criterio común para evaluación de seguridad de tecnologías de información V 2.0*"[13], con un adecuado perfil de protección según el, "*Criterio común para evaluación de seguridad de tecnologías de información. Perfil de protección para circuitos integrados de tarjetas inteligentes con software embebido, Versión 2.0*"[14].

En las diferentes opciones del elemento de seguridad hay diferentes aspectos. Estos requerimientos se concentran en WIM para tarjetas inteligentes y en otros tipos de SE.

3.2.1.1 Implementación de SE

Generación de número aleatorio

En ausencia de otros requerimientos se recomienda que el SE cumpla a cabalidad con los requerimientos de aleatoriedad que se definen más adelante.

3.2.1.2 Iniciación de SE

La iniciación de SE se cubre supliendo al SE con la funcionalidad básica (p. Ej. Sistema operativo de tarjeta inteligente y aplicación), generación de par de llaves, PIN y certificados iniciales.

3.2.1.3 Generación de Llave

Se requiere que las llaves tengan un tamaño mínimo de :

- Llave RSA 1024 bits
- Llave ECC 160 bits

[13] http://csrc.nisr.gov/cc/ccv20/ccv2list.htm

[14] Common Criteria for Information Technology Security Evaluation. Protection Profile Smart Card Integrated Circuit With Embedded Software. Version 2.0 Issue June 1999. URL: http://www.eurosmart.com

Para generación de llaves, deben utilizarse números aleatorios imprevisibles. Esto asegura la utilización de un número suficiente de llaves, es decir, que sea altamente improbable que se generen llaves similares.

La generación de llaves puede tomar lugar en el SE mismo o pueden ser generadas aparte y luego ser transferidas, en este caso es necesario que el ambiente de transferencia sea evaluado.

3.2.1.4 Generación y entrega de PINs iniciales

En un elemento de seguridad removible (WIM), el PIN inicial es generado, guardado en el SE y entregado al usuario de una forma segura.

De acuerdo a la especificación para WIM, se requiere que:

- El PIN de acceso (PIN-G) proteja la contraseña de autenticación (o múltiples contraseñas de autenticación), contraseñas de sesión, etc.
- El PIN de firma (PIN-NR) proteja la contraseña de firma (contraseña de no repudiación); en caso de que existan múltiples contraseñas cada contraseña de firma se protege con un PIN de firma.

Adicionalmente, se recomienda que:

- Un PIN de acceso (PIN-G) habilitado no pueda ser deshabilitado.
- Un PIN bloqueado (debido a ingresar un PIN incorrecto varias veces) puede ser desbloqueado por usuarios con un código de desbloqueo.
- Los PINs iniciales y códigos de desbloqueo son diferentes para cada tarjeta y en el caso de SWIM, diferente dependiendo de la red en que este suscrito, (p. Ej. GSM).
- El PIN de acceso inicial (PIN-G) y de firma (PIN-NR) son diferentes (en caso de múltiples PIN de firma, todos son diferentes).
- El PIN inicial es estregado en una forma similar al de una tarjeta de crédito bancaria, (p. Ej. Por correo a la dirección de residencia).
- Los usuarios tienen la capacidad de cambiar el PIN (proporcionando el PIN actual).

En un elemento de seguridad embebido, típicamente el usuario define los PINs y los códigos de desbloqueo.

3.2.1.5 Certificados iniciales

Al menos en el caso de un WIM, el proveedor almacena los certificados iniciales en el SE (p. Ej. Las claves son generadas antes de ser entregadas del WIM al usuario). Ellos son determinados para ser utilizados como Certificados de Dispositivo (como se explica en [WPKI]). Un Certificado de Dispositivo es un mecanismo por medio del cual se proporciona el servicio de registro en línea para:

- Verificar autenticidad de claves y SE
- Poner en ejecución aceptación de procedimientos por el SE

3.2.1.6 Entrega del SE al usuario

Cuando un SE es entregado al usuario, contiene el par de llaves iniciales, certificados y PINs. Los PINs iniciales son entregados al usuario de una forma segura.

3.2.1.7 Gestión de SE

La gestión del SE abarca las acciones que son realizadas después de que es entregado al usuario.

3.2.1.8 Desbloqueo de PINs

En caso de que el usuario pierda su PIN y bloquee el SE por tratar de acceder a él de una forma incorrecta (o bloquee al SE de otra forma), el usuario puede obtener in código de desbloqueo por medio de un centro de proveedor de servicios de SE, después de una apropiada verificación de usuario. La verificación de usuario se basa en la descripción física de este y en su capacidad para responder ciertas preguntas. También es posible que un código de desbloqueo sea entregado por medio de correo a su dirección de domicilio.

3.2.1.9 Revocación

Sí el SE (o el PTD completo es robado), el usuario puede contactar el proveedor de servicio SE. El proveedor de servicio SE puede o no ofrecer la revocación del servicio para ser utilizado por los proveedores de servicio. Si esta revocación de servicio esta disponible, el proveedor de servicio de registro puede revocar certificados de servicio emitidos para claves en el SE. Si esta revocación de servicio no esta disponible, el usuario debe contactar cada proveedor de servicio de registro de forma separada.

3.2.2 Aspectos de seguridad de implementaciones de SE especiales

3.2.2.1 Tarjeta inteligente de seguridad WIM

Una tarjeta inteligente alberga aplicaciones WIM, el cual es tema para especificar los requerimientos de una tarjeta inteligente, p. Ej. Resistencia contra tarjetas inteligentes basadas en propiedades eléctricas, tiempo, etc.

Una tarjeta multi-aplicación con WIM tiene los siguientes aspectos:

- Aislamiento de datos indispensables WIM (llaves privadas); otras aplicaciones podrían tener acceso controlado, a datos WIM
- Posible uso en común de PINs WIM con otras aplicaciones.

En una tarjeta SWIM, el conjunto de herramientas para desarrollo de aplicaciones SIM (SAT, *SIM Application Toolkit*) puede tener acceso a datos WIM. Esto puede ser permitido para descargas nativas de aplicaciones SAT, (binarias). Las políticas de estos aspectos debe ser establecida en la manifestación práctica del emisor SWIM, (*SWIM issuer Practice Statement*).

3.2.3 Ambiente operativo

Muchas implementaciones de PTD no permiten que se descarguen programas nativos, aún si se trata de recursos de acceso no restringido.

Los PTD que permiten que este tipo de código sea descargado, deben tener un mecanismo que verifique la autenticidad de éste. El mecanismo puede estar basado en, p. Ej. Código firmado donde una llave pública (llave raíz confiable) es

almacenada en el PTD original y el código descargado es verificado utilizando esta llave. El mecanismo debe estar en la capacidad de indicar al usuario si el código no puede ser autenticado, en este caso el código puede ser instalado a riesgo del usuario[15].

3.2.4 Requerimientos criptográficos

3.2.4.1 Generación de números aleatorios[16]

El PTD utiliza números aleatorios para los siguientes propósitos:

- Cliente aleatorio WTLS/TLS
- Material secreto pre-master WTLS/TLS
- Encriptación de llave pública WTLS/TLS RSA (con operación RSA)
- Aleatorio, para firma digital.

En algunos casos WIM o algún otro elemento de seguridad, es utilizado como una fuente de números aleatorios. Sin embargo el Equipo Móvil (ME, *Mobile Equipment*) debe tener números aleatorios disponibles para los casos en que el WIM no este disponible o no se utilice p. Ej. WTLS con servidor de autenticación, únicamente se implementa sin utilizar WIM.

La generación de números aleatorios tiene 2 aspectos: Utilizar un Seudo generador de números aleatorios (PRNG, *Pseudo Random Number Generator*) y producir semillas aleatorias que son utilizadas como entradas al PRNG. Un PRNG necesita ser sembrado (inicializado y resembrado) con datos aleatorios “verdaderos”, preferiblemente desde recursos físicos, Un PRNG es necesario para mezclar datos aleatorios originales, parte de los cuales no necesariamente son de buena calidad, y no producen una cantidad suficiente de datos aleatorios.

El Equipo Móvil debe tener un PNRG que sea compatible con:

[15] Las políticas que permiten que el usuario instale código sin autenticar aún no se encuentran definidas

[16] "Randomness Recommendations for Security", IETF RFC 1750, D. Eastlake, S. Crocker, J. Schiller, December 1994. URL: ftp://ftp.isi.edu/in-notes/rfc1750.txt.

- X9.17 (otro algoritmo de encriptación como RC5, puede ser utilizado en lugar de DES)
- FIPS 186-2 basado en SHA-1.
- Otro PRNG que este bien documentado y analizado por un tercero especializado en evaluación de seguridad.

El equipo móvil debe utilizar semillas aleatorias, las cuales se colectan utilizando recursos múltiples. Se recomienda una semilla mínima de 128 bits, donde solamente los bits que no son predecibles, deben ser contados.

3.2.4.2 Grado de encriptación

De acuerdo con los requerimientos para protección de transacciones con datos financieros, se recomienda que para la capa de transporte segura (WTLS) y otras, soporte encriptación de 128 bits o mayor, “grado alto”. Para interoperabilidad se recomienda que también soporte encriptación de 56 bits, “grado medio”. Además que para implementaciones se utilice alto grado de encriptación en lugar de grado medio (p. Ej. En un hanshake WTLS se recomienda encriptación de 128 bits como primera opción y de 56 bits como segunda opción). Las implementaciones no deben utilizar encriptación de 40 bits.

3.2.5 Reloj de tiempo real

Para verificación de tiempo de validez de certificados y otros propósitos se recomienda que el PTD disponga de un reloj de tiempo real. Este reloj puede ser ajustable por el usuario.

El reloj puede soportar zonas horarias.

3.2.6 Entrada de PIN

Durante la entrada del PIN, debe haber un teclado con todas la teclas. Los caracteres del PIN no deben ser desplegados en pantalla.

El mínimo de caracteres en un PIN debe ser de 4. El elemento de seguridad puede requerir un longitud mínima (de 4 a 8 dígitos); cuando se ingresa un nuevo PIN

(para cambio o desbloqueo), el dispositivo móvil debe obligar al usuario a ingresar mínimo esta cantidad de dígitos.

3.2.7 Activación y desactivación del SE

Después de ingresar el PIN de acceso, el SE se activa (significa que la autenticación relacionada esta funcionalmente disponible). Después de desactivado el PIN debe ser reingresado. El dispositivo móvil controla la desactivación p. Ej. Para una tarjeta WIM, el dispositivo móvil cierra el canal cuando la desactivación es necesaria.

Se recomienda que en una implementación de PTD tenga un temporizador de inactividad, así el SE es desactivado después de un cierto tiempo de inactividad. El PTD puede permitir que el usuario cambie el tiempo límite de inactividad. Se recomienda un valor por defecto de 5 minutos.

3.2.8 Aspectos de la interfaz de usuario

Esta parte se cubrirá más ampliamente cuando se hable de la experiencia coherente de usuario. Aquí se tratarán solamente algunos aspectos sobre los requerimientos de seguridad.

Se requiere que, existan en la interfaz elementos siempre disponibles para:

- Ingreso de PIN, gestión de PIN
- Firma
- Indicador de sesión segura

Los elementos de despliegue dedicados pueden ser únicamente controlados por el PTD y no por aplicaciones de red.

En relación con la sesión segura actual, se requiere que el PTD despliegue al usuario:

- Detalles del certificado del servidor (tipo, proveedor, tiempo de validez, huella digital)
- Parámetros de seguridad (intercambio de llaves, algoritmos de encriptación, algoritmos MAC y tamaño de las llaves);

Y en caso de utilizarse autenticación de cliente se recomienda que el PTD despliegue:

- Detalles de certificado de usuario (tipo, proveedor, validez, huella digital)

  El certificado de huella digital se calcula como un resumen criptográfico SHA-1 del contenido del certificado completo y se despliega como un valor hexadecimal.

3.3 DESCRIPCIÓN DE UNA COMPRA EN UNA TIENDA SEGURA.

El siguiente escenario de uso describe como un usuario realiza un pago con una cuenta en una tienda WAP la cual es accedida por medio de un PTD de usuario en una red inalámbrica. El proceso de pago entre la tienda WAP y la entidad encargada del pago, no se muestra aquí ya que la interfaz de este proceso no se encuentra definida por el MeT, debido a que corresponde a un servicio de Internet fija.

3.3.1 Condiciones iniciales

1. El usuario tiene una cuenta con servicio de pago. Esta cuenta puede ser de varios tipo: prepago, postpago, crédito, débito.
2. El servicio de pago proporciona un mecanismo de transferencia de fondos desde una cuenta de usuario a la cuenta del vendedor.

3.3.2 Preparación del servicio

Algunos criterios preliminares deben ser cumplidos pro el usuario y el vendedor a fin de que el escenario sea válido:

El usuario debe:

1. Poseer un PTD que permita realizar autenticación de usuario, establecer sesiones seguras, crear firmas digitales y almacenar certificados.
2. Iniciar el PTD
3. Registrar el servicio de pago y recibir un certificado de servicio del proveedor de la cuenta.

El vendedor debe:

1. Establecer relaciones con un proveedor de servicios de pago.

Las secuencias de mensajes que se muestran a continuación corresponden a los siguientes casos:

- Transacción exitosa, Figura 3-8.
- Llave de firma incorrecta, Figura 3-9.

3.3.3 Carta de mensajes

3.3.3.1 Transacción exitosa

La Figura 3-8 muestra una transacción exitosa por medio de la cual el usuario navega en una tienda WAP selecciona productos y paga por ello utilizando el PTD.

Ver página siguiente...

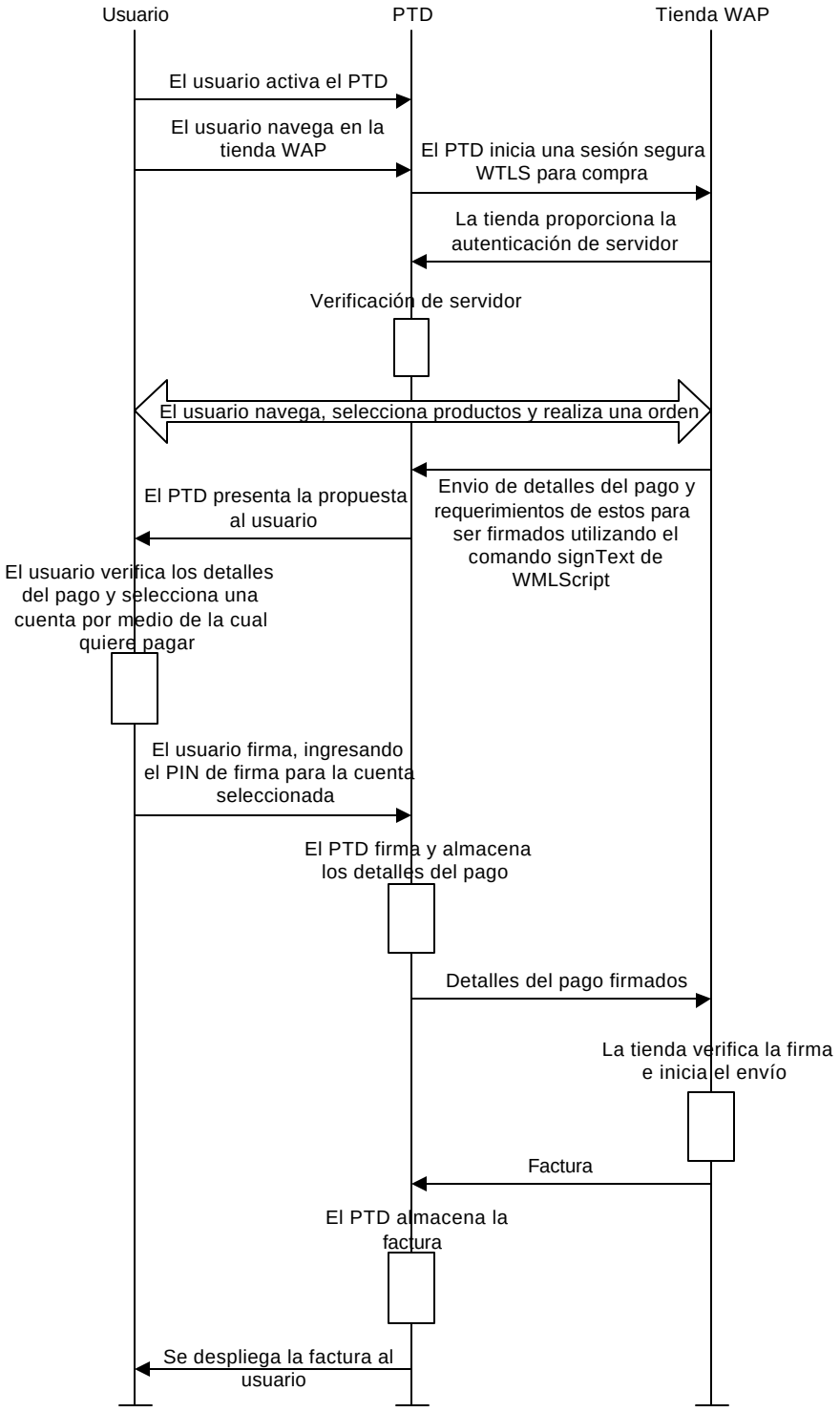

Figura 3-8. Transacción exitosa

Note que en la Figura 3-8, dependiendo del sistema de pago, la verificación de usuario puede ser ejecutada, ya sea por el vendedor WAP o por la estructura del sistema de pago. El almacenamiento del recibo por el PTD requiere la definición de una tipo de contenido, el cual todavía no esta disponible en WAP.

3.3.3.2 Firma con una llave de firma, incorrecta

En este escenario el usuario acepta la transacción pero firma con una llave que no corresponde a la cuenta seleccionada. La tienda determina que la firma no es válida y regresa una notificación diciendo que el pago no es aceptado.

El flujo de mensajes es el mismo hasta el punto donde la transacción es presentada al usuario. La Figura 3-9 muestra el flujo de mensajes desde este punto en adelante.

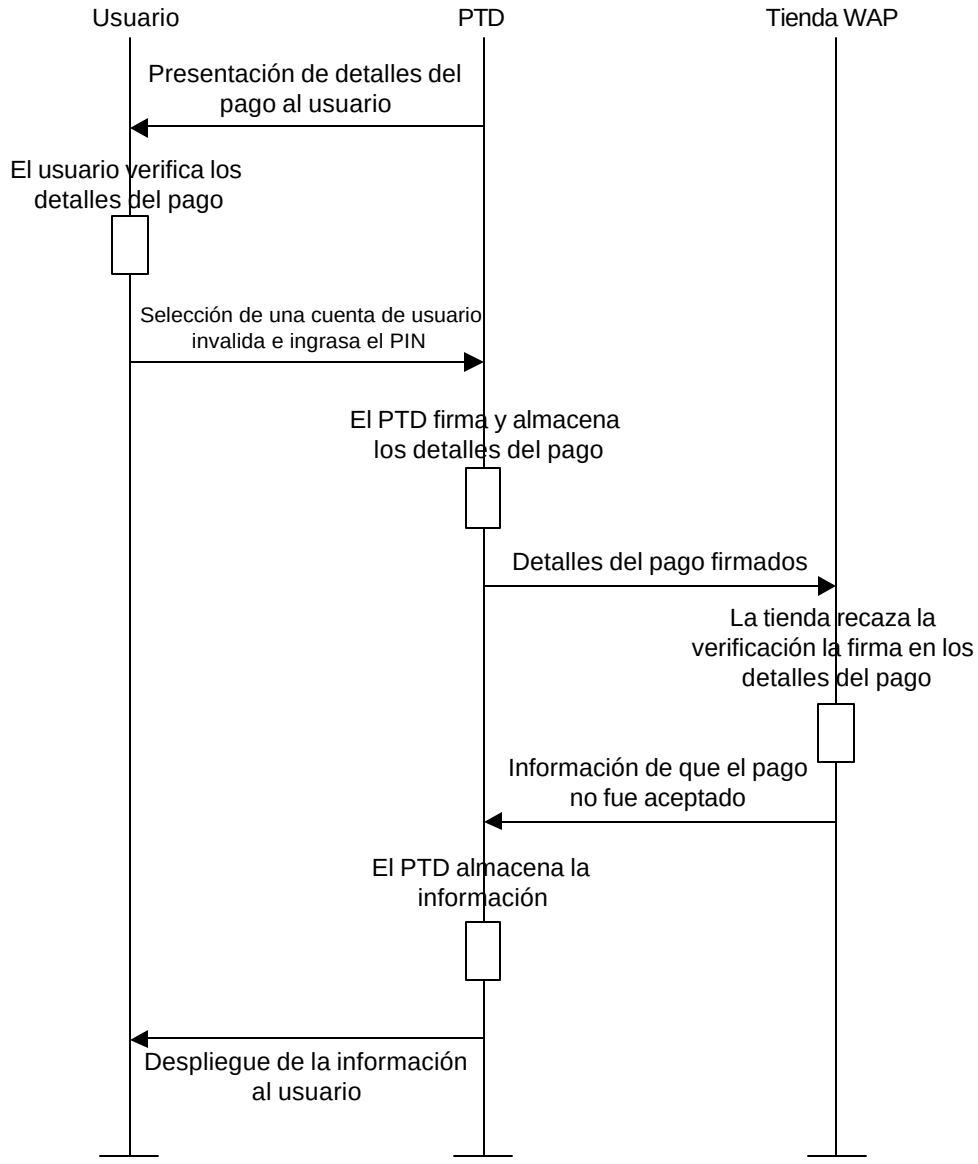

Figura 3-9. Llave de firma incorrecta

3.4 DESCRIPCIÓN DE UNA TRANSACCIÓN BANCARIA EN WAP

El siguiente escenario describe como un usuario interactúa con un banco que ofrece transacciones utilizando WAP. El usuario establece una sesión segura con el banco utilizando el PTD sobre una red inalámbrica y autoriza la transferencia de fondos entre cuentas.

3.4.1 Preparación del servicio

Con el fin de que el usuario acceda a su cuenta por medio de servicios de banca WAP, deben cumplirse los siguientes requisitos preliminares:

El banco debe:

1. Ofrecer acceso a WAP para servicios de banca a través de una gateway segura.
2. Implementar un mecanismo de firma por medio del cual el usuario se registra para acceder a una cuenta WAP.
3. Emitir un certificado de servicio al usuario para identificación del servicio de banca WAP y autenticación del usuario al banco. (Esto es parte del proceso de registro del PTD)

El usuario debe:

2. Mantener una cuenta con el banco proveedor del servicio
3. Poseer un PTD que pueda ejecutar autenticación, establecer sesiones seguras, crear firmas digitales y almacenar certificados.
4. Iniciar el PTD.
5. Registrarse con el servicio de banca WAP y recibir el certificado del servicio del banco.

Las secuencias de mensajes que se muestran a continuación corresponden a los siguientes casos:

- Transacción exitosa, Figura 3-10.
- Fallo en la autenticación del usuario, Figura 3-11.
- Cancelación de la transacción por parte del usuario, Figura 3-12.
- Firma de usuario no-valida, Figura 3-13.

3.4.2 Secuencia de mensajes

3.4.2.1 Transacción exitosa

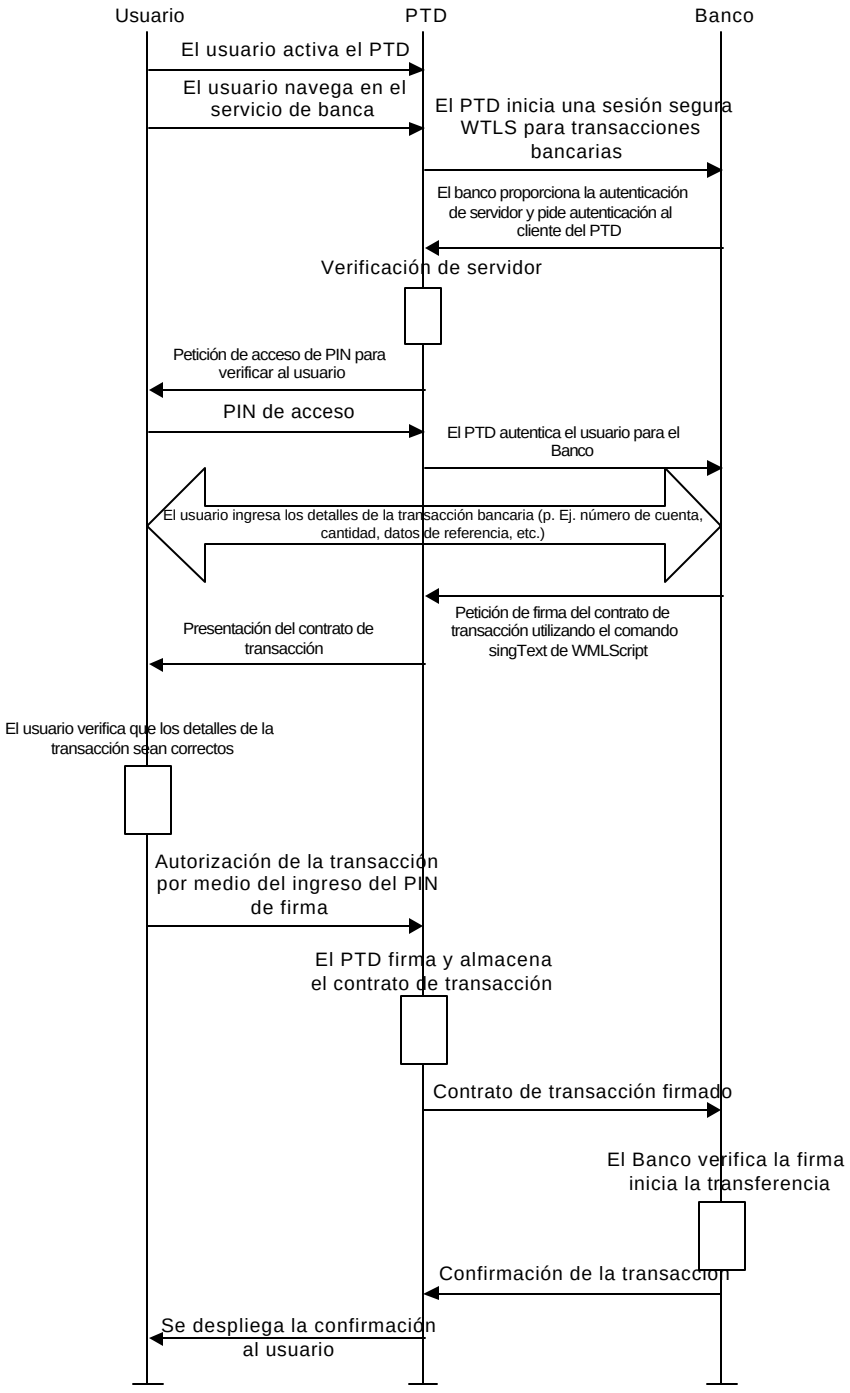

Figura 3-10. Transacción exitosa

3.4.2.2 Fallo en la autenticación de usuario

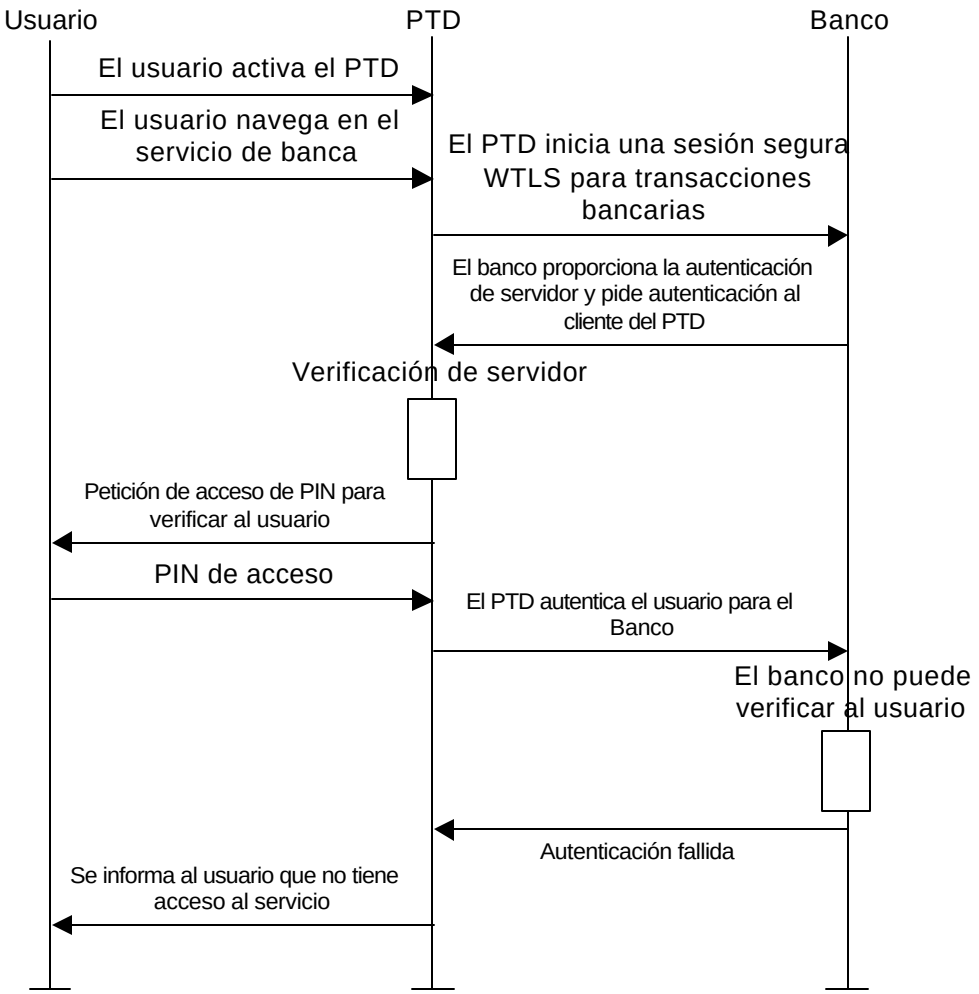

Figura 3-11. Fallo en la autenticación de usuario

3.4.2.3 Cancelación de la transacción por parte del usuario

En este caso el flujo de mensajes es el mismo que en la Figura 3-10 hasta que el banco realiza la petición a usuario de la firma de transacción. La continuación del flujo de mensajes se muestra a continuación en la Figura 3-12.

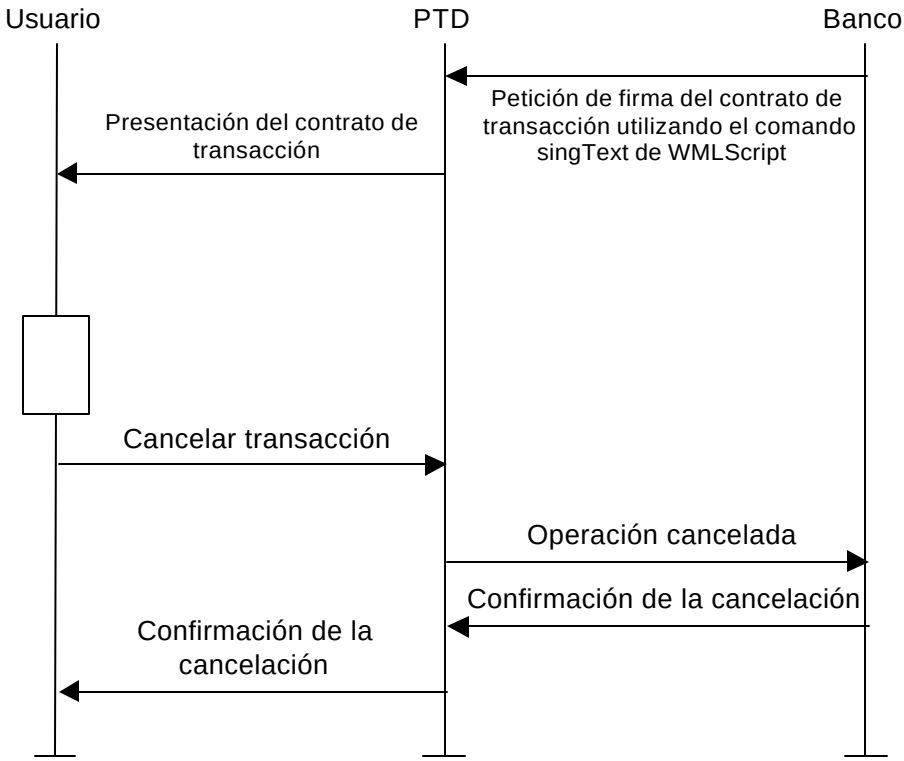

Figura 3-12. Cancelación de la transacción por el usuario

3.4.2.4 Firma de usuario invalida

En este caso el usuario firma la transacción, pero la llave utilizada para la firma no es valida para firmar las transacciones en este servicio. El flujo de mensajes es el mismo que en la Figura 3-10 hasta la petición de la firma de la transacción al usuario. La continuación del flujo de mensajes se muestra a continuación en la Figura 3-13.

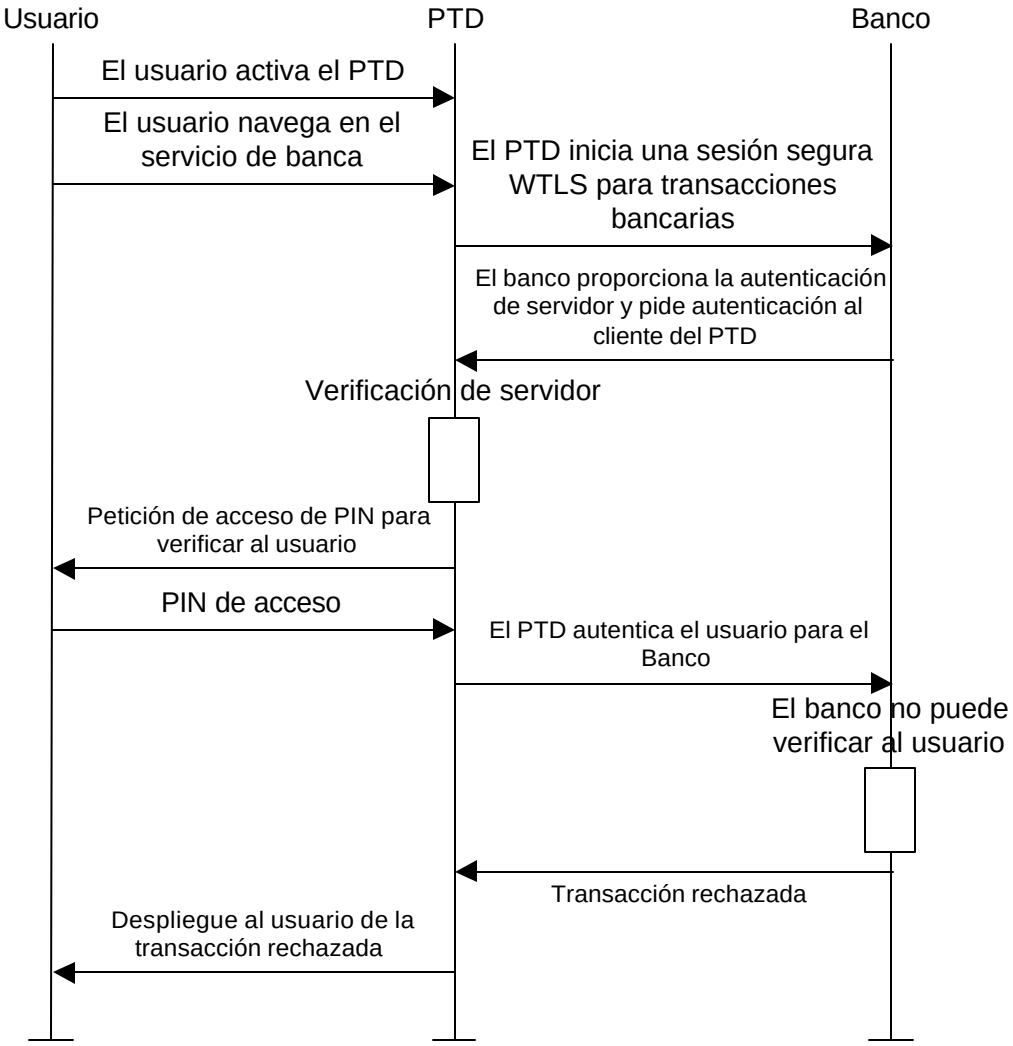

Figura 3-13. Firma de usuario no-válida

3.5 AUTORIZACIÓN PARA CUENTAS DE PAGO UTILIZANDO UN SERVIDOR SET WALLET

El estándar SET especifica el protocolo para pago con tarjeta de crédito para redes abiertas. El estándar fue publicado ya hace varios años; sin embargo, la aceptación en el mercado ha sido bastante lenta hasta ahora. Una de las razones son la difícil aceptación de la responsabilidad por parte de los clientes y la estructuración de los comerciantes.

No obstante, actualmente existen indicios de que la aceptación de SET como protocolo para pago, cambiará en los próximos años. Primero que todo, Visa y

MasterCard todavía fomentan el uso de SET; para utilizar un servidor SET Wallet, la instalación en el cliente es muy simple, (p. Ej. El cliente SET Wallet es albergado en un servidor en nombre del tarjeta habiente y no en el del PC); en segundo lugar la responsabilidad de transacciones fraudulentas en SET será cambiada de comerciante/adquisidor al emisor con el fin de incentivar a los comerciantes a utilizar SET – hoy en día los comerciantes cargan con la mayor parte de la responsabilidad del pago del tarjeta habiente.

Es este escenario de uso se describe al servidor SET Wallet, el cual es albergado por el emisor – p. Ej. El tarjeta habiente (PTD en aplicaciones MeT) es autenticado directamente por el emisor. Esto satisface uno de los requerimientos 3D en "3D SET" promovido por VISA.

La tarea de un servidor SET Wallet, es ejecutar y firmar una transacción de pago SET en nombre del tarjeta habiente. Sin embargo, antes de firmar la transacción de pago, el emisor debe autenticar al cliente móvil – el nivel de seguridad puede ser escogido de acuerdo a las políticas del emisor y puede variar desde un simple nombre de usuario y contraseña hasta una firma digital. Es conveniente que el emisor obtenga una prueba a través de una firma digital del tarjeta habiente, que intenta comprar; por otra parte, es particularmente importante si el emisor esta en capacidad de asumir la responsabilidad final de la transacción. La autenticación de usuario y la autorización de pago puede ser combinada en una sola acción, una firma digital del tarjeta habiente en el PTD sobre el pedido.

Los pasos de una transacción convencional de un servidor SET Wallet para un cliente, basada en PC son:

1. Al final de la fase de compra se solicita al usuario una marca de tarjeta y un método de usuario; como respuesta a esta petición el usuario escoge "Servidor SET Wallet".
2. El comerciante envía un mensaje de iniciación de pago (también conocida como *Wakeup*) al cliente en el PC; el mensaje incluye, descripción del pedido, cantidad y la marca de la tarjeta.
3. Cuando el navegador recibe el mensaje de la iniciación de pago, inicia una aplicación. Esta aplicación que trae una URL guardada o una entrada de

usuario correspondiente al servidor SET Wallet, envía el mensaje de iniciación de pago a esta dirección. Seguidamente servidor completa la transacción SET a nombre del tarjeta habiente.

4. Finalmente, el tarjeta habiente se autentica de algún modo (el mecanismo para esto esta fuera del alcance de SET, pero dentro del control de la tarjeta del emisor).

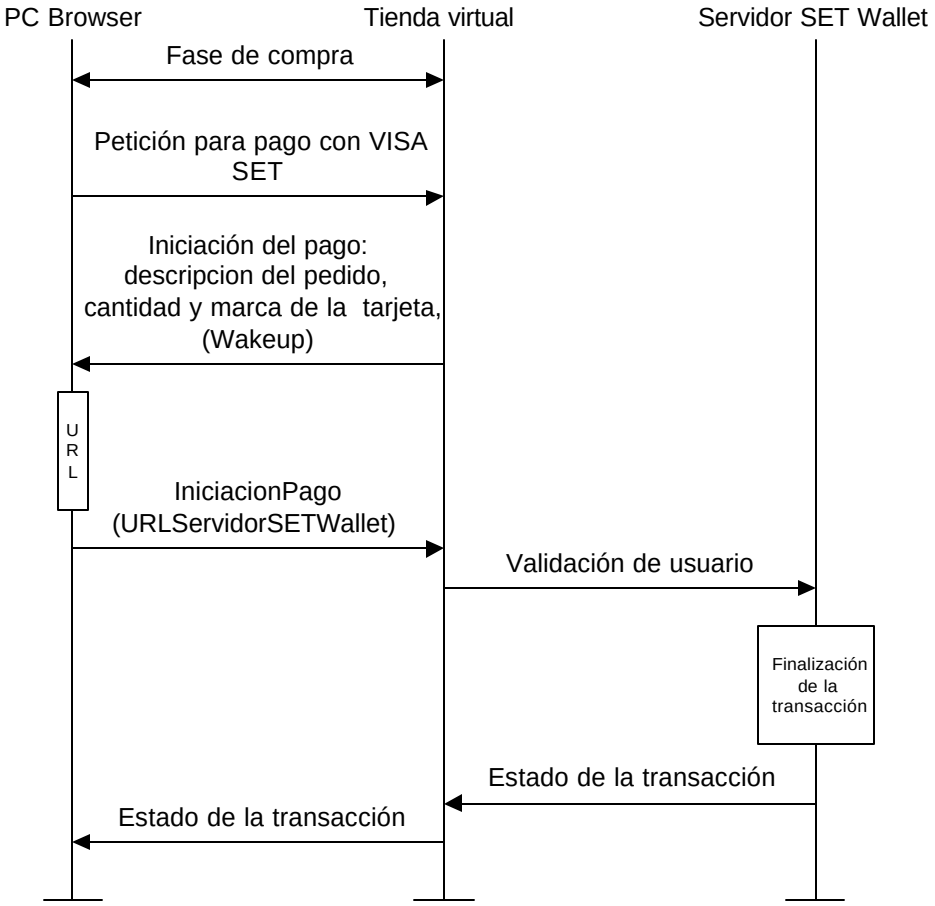

Figura 3-14. Transacción convencional con un servidor SET Wallet

En el escenario de uso MeT, la transacción es mapeada a una transacción utilizando el PTD (teléfono), como se resume a continuación.

1. El PTD envía una página de chequeo al servidor comerciante sobre un canal WTLS seguro. Esto ocurre en la fase de compra.

2. El servidor comerciante envía un deck ECML (*Electronic Commerce Modeling Language*) al PTD para buscar la dirección de la URL del servidor Wallet. Después de recibir el deck ECML del servidor comerciante, el navegador del PTD inicia una aplicación de llenado de formularios ECML con la cual se escribe la URL del servidor Wallet, después el usuario selecciona el nombre del servidor. Así, el formulario completo, conteniendo la dirección del servidor Wallet, es enviado al servidor comerciante.
3. El comerciante emite un comando de redirección al PTD, enviándolo al servidor SET Wallet.
4. Cuando el PTD recibe una confirmación del mensaje de redireccionamiento, el emisor recupera un mensaje de inicio de pago SET (también conocido como mensaje SET *Wakeup*) enviado por el comerciante.
5. El emisor despliega una ventana al tarjeta habiente que contiene la descripción del pedido y el costo (costo neto) y hace la petición de la firma digital. Si la verificación de la firma es exitosa el emisor ejecutará la transacción SET a nombre del usuario.
6. Una vez terminada la transacción SET, el usuario es redireccionado al comerciante quien despliega los resultados de la transacción de pago.

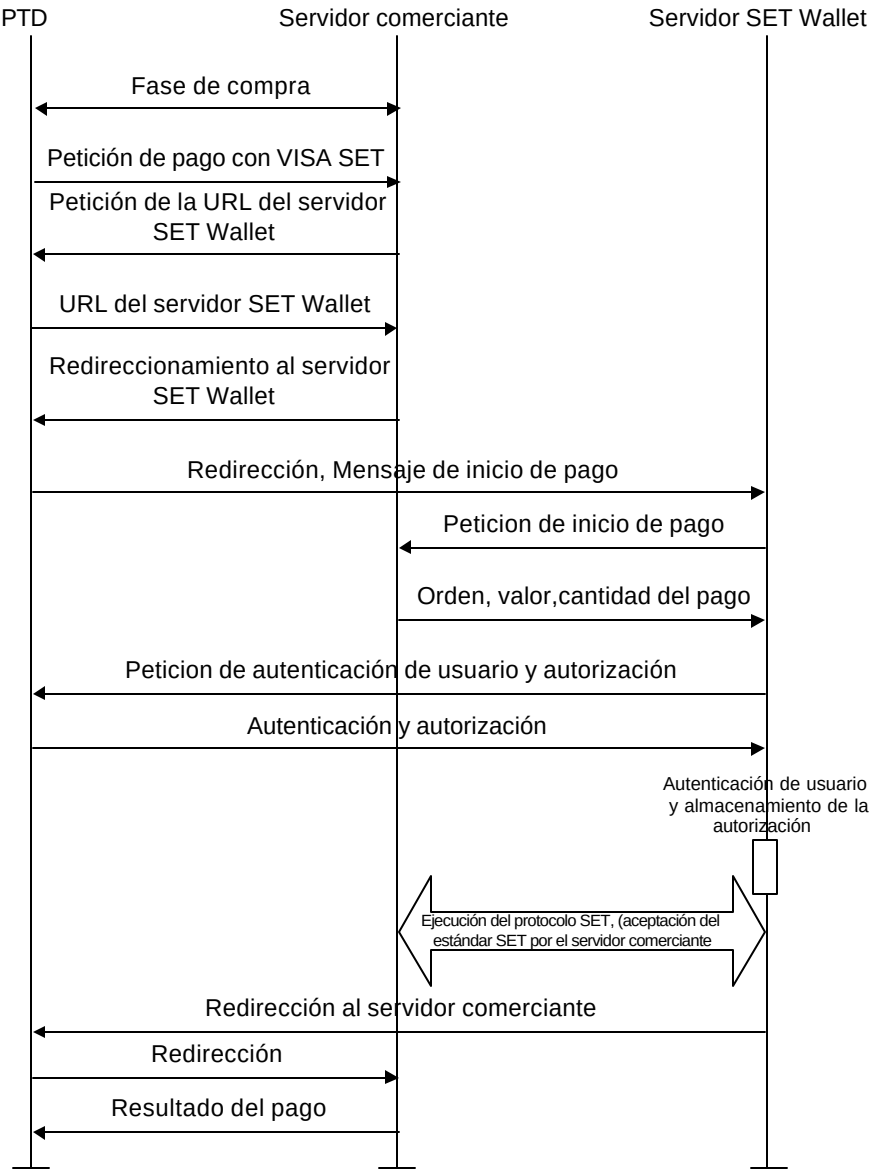

Figura 3-15. Transacción utilizando un servidor SET Wallet, desde un PTD

3.5.1 Modelo del sistema de referencia

El modelo de uso involucra las siguiente entidades: Usuario, Teléfono móvil (PTD), Comerciante, Propietario y emisor de la cuenta.

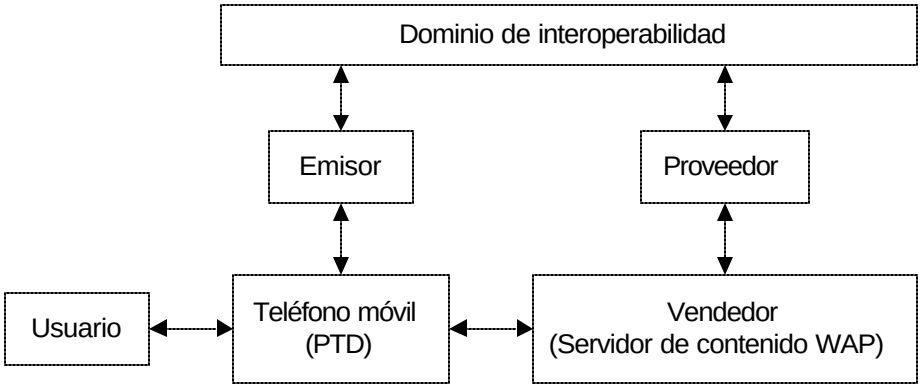

Figura 3-16. Modelo de referencia para pago de cuentas

La Figura 3-17 muestra el mismo modelo de referencia ligeramente mejorado, p. Ej. Considera todos los componentes requeridos para ejecutar una transacción basada en un servidor SET Wallet con autorización MeT

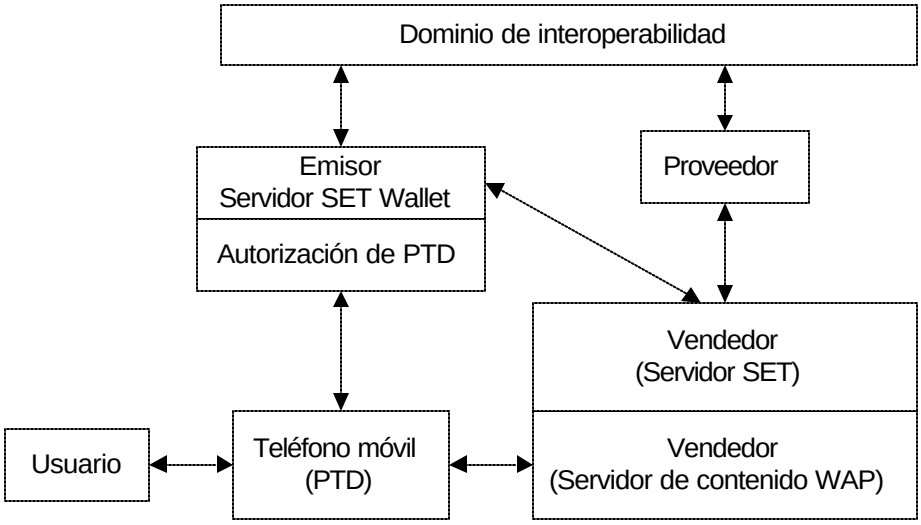

Figura 3-17. Modelo de referencia mejorado: Autorización MeT para servidor SET Wallet

En el modelo de referencia mejorado, el Emisor, comerciante y propietario proporcionan todo el soporte SET. Por otra parte el emisor alberga el SET Walllet para el tarjeta habiente y ofrece una interfaz adicional para su autenticación. El servidor SET del comerciante es separado de su software de contenido WAP. El propietario opera una gateway de pago SET que sirve de interfaz a la red bancaria existente.

Note que el modelo de referencia mejorado introduce un nuevo flujo de mensajes entre el emisor y el comerciante. Este flujo representa al tarjeta habiente – Los mensajes del comerciante, en SET, con el emisor ahora juegan el papel del tarjeta habiente.

3.6 MeT, Experiencia Consistente de Usuario (CUE, Consistent User Experience)

Actualmente, no hay una única organización para proporcionar un framework para e-commerce móvil. Hay algunas iniciativas emprendidas por organizaciones y compañías para promover ciertos protocolos, soluciones de seguridad y estándares. Sin embargo, no hay enfoques sobre los requerimientos para el PTD que permitan al usuario mantener el control sobre el ambiente de seguridad, utilizar el PTD en un amplio rango de aplicaciones y establecer enlaces seguros a proveedores de contenido arbitrarios, posiblemente sin los servicios de un servidor fijo intermedio.

La exitosa adopción de éste framework depende de la aceptación global del PTD por los usuarios. Con el fin de facilitar tal aceptación MeT define la Experiencia consistente de usuario, la cual se concentra en los factores de utilidad del PTD.

Para tal propósito, CUE, (Consistent User Experience) define el modelo de uso del PTD que trae a cuenta la percepción del usuario de éste. Tal modelo enriquece la funcionalidad definida por el framework MeT que define los aspectos de utilidad para proveer al usuario una experiencia consistente cuando utiliza un PTD para transacciones móviles.

El propósito de la especificación CUE es definir y describir los elementos de los PTDs para crear una experiencia consistente de usuario en transacciones electrónicas móviles, manteniendo la utilidad y consistencia de los PTDs.

CUE define solamente las partes de la transacción que son dependientes del fabricante del PTD, no define el comportamiento de una aplicación o la presentación de la interfaz de usuario.

3.6.1 Experiencia consistente de usuario

3.6.1.1 Consistencia

La consistencia en la interfaz de usuario permite a las personas transmitir su conocimiento y habilidades desde una aplicación a otra. La consistencia en una interfaz visual ayuda a las personas a aprender fácilmente a reconocer en lenguaje gráfico de la interfaz.

Aún tareas simples pueden volverse difíciles de ejecutar si los usuarios no pueden tomar ventaja de sus conocimientos anteriores. Por ejemplo, la terminología utilizada en navegadores WAP del año 2000 varía entre teléfonos de diferentes fabricantes, que aunque son pequeñas pueden confundir al usuario.

Con el fin de que la terminología utilizada sea consistente, las aplicaciones pueden ser coherentes en dos formas, interna y externamente.

Internamente consistente significa que el comportamiento de la interfaz de usuario tiene sentido con respecto a otras partes de la aplicación. Por ejemplo, si un atributo de un objeto es modificable utilizando un menú de tipo pop-pup, entonces el usuario espera que los otros atributos del objeto sean modificables de una forma similar. Se debe tratar de evitarle al usuario el menor número de "*sorpresas*" posibles.

La consistencia externa significa que la interfaz de usuario es consistente con el ambiente sobre el que funciona. Esto incluye consistencia con el sistema operativo y el conjunto típico de operación que corre dentro del sistema operativo. Una de las formas, ampliamente reconocida, de consistencia externa es la conformidad con los estándares interfaz – usuario; sin embargo existen muchos otros métodos tal como lenguajes tipo script estandarizados, arquitecturas plug-in o métodos de configuración.

3.6.1.2 Experiencia de usuario

La importancia de la experiencia de usuario ha sido tratada en varias publicaciones.

De acuerdo al Nielsen Norman Group[17] la experiencia de usuario se define como sigue:

> *"La experiencia del usuario abarca todos los aspectos de interacción del usuario final con la compañía, sus servicios y sus productos. El primer requerimiento para una experiencia de usuario ejemplar es conocer exactamente las necesidades del consumidor, sin causar confusión o molestias, próxima a la simplicidad y elegancia que producen los productos que son una satisfacción para el propietario; son una satisfacción utilizarlos"*

Una buena experiencia de usuario es especialmente crítica para la supervivencia de los negocios en línea, así la decisión de comprar depende cada vez más y más de la accesibilidad y presentación del producto más que del producto mismo. De acuerdo con Userlab Inc.[18], el principal déficit de las aplicaciones (Web) de el dominio de e-commerce es que el "62% del los compradores web no les gusta tener que buscar algo que ellos quieren comprar" mientras que "El 40% de la gente nunca regresa al sitio web después de una mala experiencia".

Sin embargo, una buena experiencia de usuario no necesariamente depende solamente de un buen diseño de la interfaz. Considerando a un usuario que ingresa a diferentes aplicaciones, una buen experiencia de usuario depende de la posibilidad de transferencia de la experiencia de una aplicación a otra. El "re-uso" de una experiencia ya aprendida facilita el manejo de otras aplicaciones.

3.6.1.3 Percepción del contexto de uso

3.6.1.3.1 Percepción de un ambiente seguro

Cuando se utiliza un PTD, el promedio de usuarios no conoce mucho acerca de riesgos o técnicas de seguridad que existen y utilizan durante las transacciones. Para el usuario, debe haber una forma cerciorarse de la seguridad del ambiente.

[17] Nielsen Norman Group URL: http://www.nngroup.com

[18] Userlan Inc. URL: http://userlab.com

El usuario debe percibir si el nivel de seguridad proporcionado por el ambiente tecnológico, es adecuado para el tipo de transacción que esta realizando y que riesgos de la transacción están correctamente estimados.

Se debe presentar al usuario la información acerca del contexto en el cual las transacciones se están ejecutando de una forma consistente. Por ejemplo la información relacionada con una sesión de seguridad puede ser desplegada al usuario. El usuario debe percibir en que parte de la tansacción se encuentra mientras se realiza la autenticación. Por ejemplo, mediante el despliegue del resultado de la autenticación.

3.6.1.3.2 Percepción de uso/marca

Tener una marca conocida es un elemento importante cuando se está construyendo un móvil e-commerce confiable, es decir, un proveedor de servicio de una marca conocida basado en la confiabilidad de su buen nombre, (en el caso de que lo sea, claro esta) y sobre una experiencia de usuario previa.

Los símbolos de la marca son diseñados para asegurar al usuario sobre la seguridad de ese lugar. Como, cuando y donde el símbolo de la marca es mostrado es importante. La consistencia en la presentación de símbolos de marca hace fácil para el usuario notarlos y asegurarse de que el servicio es digno de confianza.

3.6.2 Seguridad

Para el usuario, debe haber una forma de asegurarse de las funciones de seguridad que se ejecutan en el PTD. El PTD debe ser significado de protección a la información personal y a la funciones que se ejecutan y que tienen relación con esto. Por ejemplo, un PIN, (*Personal Identity Number*) debe ser desplegado en el PTD en una forma tal que un curioso no sea capaz de verlo o descifrarlo.

3.7 CONCLUSIONES

La introducción de WAP ha hecho posible acceder a servicios de Internet móvil entre ellos las transacciones móviles. Sin embargo, la postura más realista a la hora

de abordar el tema de la seguridad consiste en reconocer que el acceso a Internet a través de dispositivos móviles se encuentra aún en un estado naciente. El soporte masivo por parte de la industria es un esfuerzo reciente que obtendrá su fruto a medida que se vaya implantando GPRS y, más adelante, los sistemas de tercera generación (UMTS).La madurez de la tecnología, mediante estándares ampliamente aceptados y soportados, llevará a la consecución de los niveles de seguridad necesarios para hacer del acceso móvil a Internet la herramienta idónea para el comercio electrónico, el ocio y la prestación de servicios personalizados.

4. SISTEMAS DE LOCALIZACIÓN EN SISTEMAS MÓVILES

4.1 INTRODUCCIÓN

Aunque asociar una ubicación geográfica con información es un proceso que nació como muchos de los adelantos en comunicaciones para aplicaciones militares, rápidamente fue adoptada para los servicios marítimos y de aviación comenzando con los sistemas de radar hasta los sistemas de posicionamiento global; mas adelante viendo como esta tecnología podía servir para salvar vidas se aplico a los servicios de emergencia y hoy en día se pueden aplicar a muchos aspectos de los negocios para ayudar a:

- Escoger un sitio
- Identificar un mercado potencial
- Planificar una red de distribución
- Dibujar territorios de venta
- Ubicar recursos, entre otros.

Todos estos ítems involucran cuestiones de geografía:

- ¿Donde se localizan los clientes actuales o potenciales?
- ¿En que vecindario o área censal viven consumidores con un mismo perfil?
- ¿Dónde se ubican mis competidores?
- ¿Qué zonas no son importantes?

A veces las interrogantes abarcan demasiados factores y otras veces son bastante específicas: ¿Qué construcciones se encuentran en una determinada zona? ¿sus ocupantes tienen determinados ingresos mínimos? y ¿Están a menos de cinco minutos caminando del punto de interés?.

Las personas mantienen sus mismos comportamientos y necesidades, tanto en los entornos que les son familiares como en los que no lo son, en su país como fuera de él, tanto en el automóvil, como si van a pie. Por ejemplo, la gente necesita, esté donde esté, encontrar un sitio para comer, una farmacia, un cajero, una parada de taxi, etc. Incluso, las necesidades aumentan cuando se viaja al extranjero para visitar las curiosidades turísticas, para orientarse, para encontrar fácilmente un hotel, para localizar una oficina de cambio de moneda. En el automóvil, estas personas pueden tener necesidad de otros servicios adicionales, tales como una ayuda a la navegación para orientarse en una ciudad desconocida, asistencia automovilística si este se estropea, etc. Hoy en día, un viajero no previsor (aquel que no ha consultado los lugares en Internet, que no compró una guía, que no reservó habitación en un hotel, o no confirmó su plaza en el avión…) pierde mucho tiempo y su teléfono móvil no le será de mucha ayuda. Esta persona es un usuario insatisfecho del teléfono móvil y, por lo tanto, un cliente a contentar con unos servicios de uso sencillo y más eficaces.

Existe un amplio y variado abanico de servicios móviles que se basan en la posición, pero, entre ellos, hay cuatro que, en potencia, presentan más probabilidades de mayores beneficios.

a) Servicios de información

Encontrar el servicio “equis” más próximo, disponer de la información del tráfico de las carreteras, beneficiarse de una guía de navegación en una ciudad que no se conoce, obtener el plano de calles, son ejemplos de los servicios basados en la posición, una nueva fuente de ganancias para los operadores. La información que se busque dependerá de los objetivos de los clientes y del estilo de vida de los usuarios:

- En una relación del tipo “empresa / consumidor particular”, este nuevo medio de información será explotado por las empresas. El conocer la posición de los abonados, que disponen de este servicio opcional, permite a las empresas el envío de campañas de publicidad o de promoción de productos de la zona.
- En una relación del tipo “consumidor particular / empresa”, es precisamente el propio abonado el que solicita su posición a fin de recibir una información

precisa del entorno, en función de la posición en que se encuentra en ese momento. El usuario puede solicitar información acerca de los servicios existentes en los alrededores (restaurantes, gasolineras, farmacias, etc.), pero también puede solicitar información sobre el tráfico de las carreteras.

- En una relación del tipo "consumidor particular / consumidor particular", el abonado puede localizar a sus amigos, a los miembros de su familia o todavía más ampliamente, al círculo de miembros de una comunidad a la que él esta adherido (deporte, música, cine, etc.).

b) Servicios de emergencia

Se trata de servicios de emergencia tanto públicos como privados, que pueden ser utilizados igualmente por los viandantes o los conductores. Los servicios públicos de urgencias, que pueden pedir la intervención de las fuerzas de seguridad públicas.

c) Servicios de seguimiento de vehículos y de personas

Estos servicios que son, por lo general, del tipo "entre-empresas" se encargan de la gestión de las flotas y, para ello, localizan un recurso externo para optimizar su explotación, su gestión o para asegurar su seguridad. Por recurso externo, se entiende una persona en un vehículo a motor o no (camionero, repartidor, técnico de mantenimiento, agente de seguridad…) o un objeto (coche, camión, remolque, contenedor o cualquier otro equipo o material).

d) Servicios de operador

La explotación de las informaciones de posición permiten mejorar los servicios en campos muy diversos como la planificación de la red, la calidad del servicio, la optimización de los en la entrega y adjudicación de los canales de radio y la tarificación.

Esta nueva forma de percibir los servicios de información basados en la localización nace en 1994 gracias al despliegue del Sistema Global para Comunicaciones Móviles (GSM: Global System for Mobile Communications); posteriormente en 1995 Ericsson y Nokia empiezan el estudio para el desarrollo de esta tecnología, logrando así que en 1996 Ericsson lance su primera plataforma denominada Sistema de Posicionamiento Móvil (MPS: Mobile Positioing System).

El primer informe y orden de regulación (FCC Regulación 47 CFR 20.18 (e)) es impuesto en julio de 1996 por la Comisión Federal de Comunicaciones (FCC: Federal Communications Com ission) cuyo requerimiento a los operadores es de informar de la localización de móviles en caso de llamadas de emergencia E-911 y para el 1 de octubre de 2001 “permitir la capacidad de identificar la latitud y longitud de una unidad móvil realizando una llamada de emergencia 911, en un radio de no más de 125 metros en el 67% de todos los casos”.

La iniciación de la estandarización GSM ANSI/ETSI ocurre desde 1997 con la fase uno que trata la descripción del Servicio y posteriormente se continuó con la fase dos, que corresponde a la descripción funcional y arquitectural del sistema, completando la estandarización en 1999.

Estos servicios utilizan principalmente cuatro métodos para determinar la posición llamados Cell-ID (identificador de Célula), Diferencia de tiempo de arribo o llegada (TDOA), Enhanced Observed Time Difference (E-OTD) y GPS (Sistema Global de Posicionamiento). Los servicios de posición utilizan alguno de los diferentes métodos disponibles para determinar la posición y todos tienen alguna limitación. Mientras que unos necesitan cambiar la tarjeta SIM o incluso el propio terminal, otros implican cambios en la red. Estas modificaciones, que el método elegido trae consigo a la cadena global de telecomunicación, tienen su reflejo en el impacto que acarrea en las inversiones de los operadores. De ahí que el interés se centre en minimizar estos impactos.

A continuación se da una breve introducción a los cuatro métodos en orden creciente según su precisión:

- Cell-ID, identificador de célula: La precisión depende de la densidad de la red celular. Si con el fin de mejorar la precisión, se tiene no sólo en cuenta el Cell-ID, sino también dos medidas radio eléctricas de la red, se habla entonces de Cell-ID++. Este sistema aprovecha las medidas de potencia recibidas de las células vecinas (Network Measurement Results o NMR) y el mecanismo de sincronización del canal de radio en el sentido terminal móvil-estación base (Timing Advance o TA) en GSM. En los sistemas de tercera generación, se utiliza la medida del tiempo empleado por las ondas de radio en completar el recorrido entre E/R (Round Trip Time o RTT).

- La diferencia de tiempo de llegada (TDOA) determina la posición de un móvil basado en la triangulación. Este sistema usa las mediciones de diferencia de tiempo para convertirlas en distancias constantes a dos estaciones base (focos) para definir una curva hiperbólica. La intersección de dos hipérbolas determina la posición.
- OTD (Diferencia de Tiempo Observada): Es necesario diferenciar estos métodos teniendo en cuenta la generación a la que pertenece la red celular. En el caso del GSM, se habla de E-OTD (OTD mejorado, que se describe más adelante). Este método sólo aporta un poco más de precisión que el proporcionado por el Cell-ID ++.
- GPS Asistido: Basado en la constelación de satélites GPS y en la ayuda del servidor de referencia en la red celular, este método ofrece la precisión más exacta.

Hoy en día se están implementando estas y nuevas tecnologías para las redes de segunda y tercera generación, las cuales pretenden definitivamente introducir los servicios de localización como algo necesario y común para los usuarios.

4.2 LOCATION INTEROPERABILITY FORUM (LIF)

El Foro de Interoperabilidad en Localización (LIF: Location Interoperability Forum) es un foro abierto nacido en septiembre 26 del 2000 por Motorola, Ericsson y Nokia, que pretende establecer un sistema común, simple, seguro y ínteroperatible, capaz de ofrecer servicios de localización desde cualquier tipo de terminal móvil con independencia de la interfaz utilizada.

4.2.1 Visión

- Definir un método de acceso simple y seguro que permita a los dispositivos inalámbricos acceder la información de localización proporcionadas por las redes inalámbricas, independiente de la interfaz de radio y los métodos posicionando.
- Promover normas para definir los métodos de localización y sus arquitecturas de apoyo.

- Establecer una gran red de trabajo que ayude a la estandarización y especificación de métodos comunes y procedimientos para probar y verificar los diferentes métodos y tecnologías de posicionando.

4.2.2 Estructura del LIF

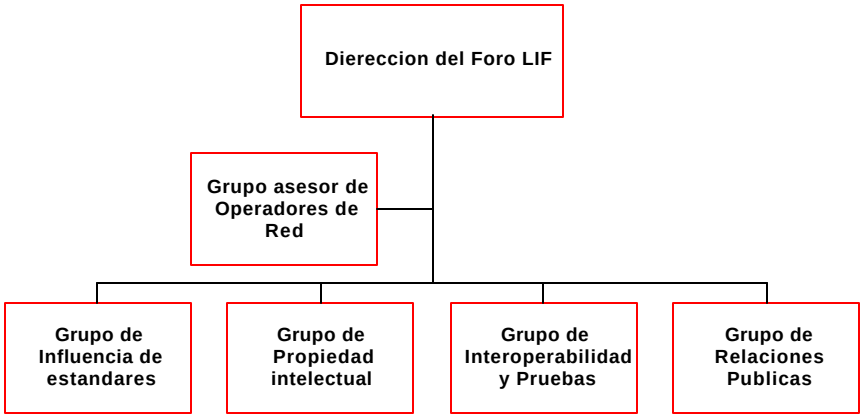

Figura 4-1. Estructura LIF

4.2.3 Categorías de Servicios de localización

El foro ha clasificado los servicios de localización en tres categorías, dependiendo de su exactitud, como se muestra en la Tabla 4-1.

Categorías de los Servicios de Localización	
Categoría 1 **El Nivel de Servicio básico**	Localización de todos los microteléfonos, basado en la celda o en la exactitud celular mejorada.
Categoría 2 **El Nivel de Servicio reforzado**	Localización de todo nuevo microteléfono con la exactitud mejorada a un costo razonable.
Categoría 3 **El Nivel de Servicio extendido**	Localización de nuevos microteléfonos con la exactitud alta y superior (comparado con la Categoría 2), el costo depende de la opción del cliente.

Tabla 4-1. Categorías de los servicios de localización

Las soluciones de localización automática se dividen en dos grandes grupos: Aquellas que están basadas en las capacidades de la red (Network-based method)

y aquellas que están basadas en las capacidades del terminal (handheld based). Esta clasificación es la utilizada por la FCC de los EEUU en sus reglamentaciones.

4.3 MÉTODOS BASADOS EN LAS CAPACIDADES DE LA RED

4.3.1 Cell Global Identity (Cell ID)

Es el método más simple para localizar un terminal móvil y se basa en la hipótesis de que la cobertura geográfica de una celda se ajusta a la prevista por los estudios de cobertura radio (Figura 4-2). Dado que un terminal móvil está conectado (cuando está en conversación) a una estación base, se supone que el terminal móvil se encuentra geográficamente en la zona donde se ha previsto que esa estación base sea la más idónea para atenderle, por lo tanto, para asegurar una localización fiable, se requiere establecer unos mapas precisos de cobertura de las estaciones base, utilizando herramientas precisas de planificación celular. Por ello se hace necesario amoldar los planos para transformarlos a un formato descriptible y fácil de usar, lo cual se logra utilizando los polígonos llamados “de Voronoi” (Figura 4-5) que ofrecen la posibilidad de determinar los contornos geométricos de las células, además es posible afinar la localización utilizando las medidas de RTT (Round Trip Time) efectuadas por la estación base (Figura 4-4) que puede medir el tiempo entre la emisión de una trama (en el sentido descendente, desde la estación base hacia el terminal móvil) y la recepción de la trama correspondiente (en el sentido ascendente, desde el terminal móvil hacia la estación base). Utilizando esta medida, la estación base puede calcular la distancia entre ella y el terminal móvil, con una precisión de alrededor de 80 metros permitiendo así reducir la zona de incertidumbre; pero esta información es de poca utilidad en el caso de una celda atendida por una antena omnidireccional; entonces para ofrecer una mejora en la precisión se utiliza un arreglo de antenas que sectorizan la celada, como podemos ver en la Figura 4-3.

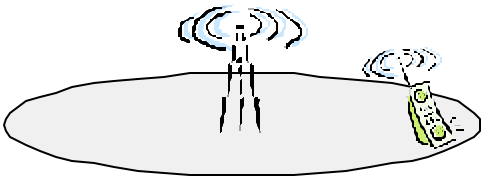

Figura 4-2. Cobertura de radio

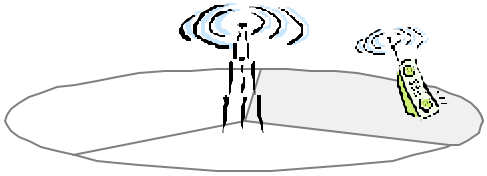

Figura 4-3. Celda sectorizada

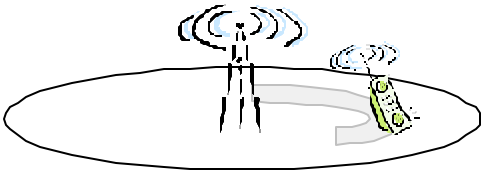

Figura 4-4. Cobertura con RTT

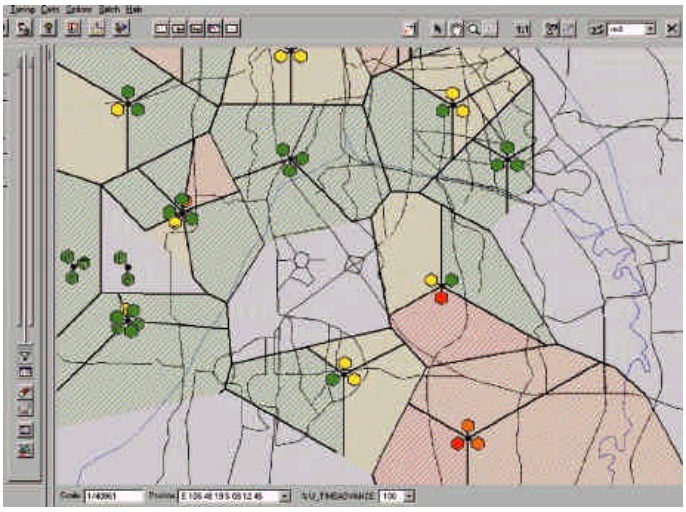

Figura 4-5. Polígonos de Voronoi

Contrariamente a lo que ocurre con los sistemas de segunda generación, en los que un terminal móvil sólo tiene comunicación con una única estación base, en los sistemas de tercera generación un terminal móvil puede estar en comunicación con varias estaciones base en las situaciones de “soft handover” (transferencia intercelular). Una dificultad suplementaria subyace en el hecho de que las

estaciones base a las que el terminal móvil está conectado pueden cambiar varias veces por segundo, esto obliga a introducir un método que permita identificar a la celda más representativa de la posición geográfica del terminal móvil. Se puede, por ejemplo, preguntar al terminal móvil qué estación recibe la señal mejor o realizar un tratamiento estadístico sobre qué celdas utiliza el terminal. Esta última solución permite afinar aún más la precisión de la localización, determinando la zona de la célula en la que se encuentra el terminal móvil. Los métodos basados en las coberturas de las células pueden ser suficientemente válidos para los servicios que no necesiten de una precisión inferior a unos cientos de metros. La ventaja de estos métodos radica en su bajo coste de despliegue y de funcionamiento, al mismo tiempo que se pueden implantar por todo lo ancho del amplio parque de terminales móviles (ya que no requieren ningún desarrollo en los propios terminales), pero la principal dificultad con estos métodos está en predecir correctamente la cobertura geográfica de las células; la mejor estación base no es siempre la más próxima físicamente. La fiabilidad y la precisión de la posición residen en la exactitud de las predicciones de radio, Fig.4-5.

4.3.2 Diferencia de tiempo de arribo o llegada (TDOA)

La técnica TDOA (Time Difference Of Arrival) trabaja midiendo el tiempo exacto de llegada de una señal de radio enviada desde un móvil y recibida por tres o más unidades de medida (handover asíncrono). Ya que las ondas de radio viajan a la velocidad de luz, si se calcula la diferencia en tiempo de llegada a las estaciones celulares, es posible calcular hipérbolas en que el dispositivo transmisor se localiza. La técnica TDOA utiliza típicamente las antenas ya montadas, lo cual hace que este método trabaje con los móviles existentes, es decir, no hay ninguna modificación al microteléfono requerido y sólo requiere las modificaciones a la red (ver Figura 4-6).

En los ambientes de multitrayecto (áreas urbanas) puede ser necesario hacer las mediciones con cuatro antenas para superar los efectos del multitrayecto.

El Centro de Localización de Servicio Móvil (SMLC: Service Mobile Location System) calcula los valores de diferencia de tiempo de llegada (TDOA) substrayendo los valores de Tiempo de llegada (TOA: Time Of Arrival), calculando la posición del móvil por triangulación hiperbólica sabiendo que:

a) Las coordenadas geográficas de las unidades de medida son conocidas.
b) El desfase de tiempo entre las unidades de medida involucradas en la medición es conocida, esto genera los valores RTD (Real Time Difference).

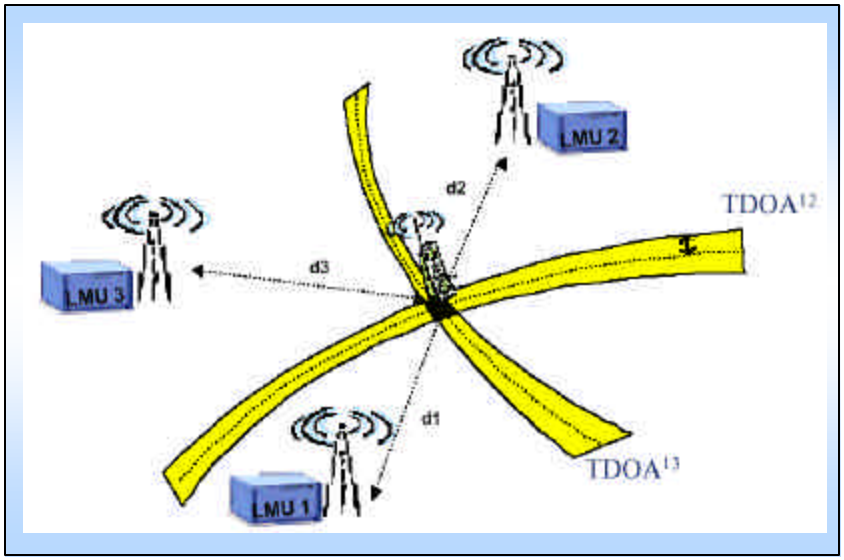

Figura 4-6. Método de localización TOA

Las señales de acceso son usadas por un detector TOA en las unidades de medida que están escuchando, y cuando ocurre una petición de posicionamiento se seleccionan las unidades que deben medir el TOA de la señal de la Estación Móvil (MS: Mobile Station – Estación Móvil) y además se configuran para escuchar a la frecuencia correcta, obligando al MS a realizar un handover asíncrono; bajo las tales circunstancias, el MS transmite hasta 70 señales de acceso (320 ms) con una potencia y canal de trafico especifico. Cada unidad de medida realiza las medidas de TOA, integrando las señales recibidas reforzando así la sensibilidad, esto se hace aplicando una técnica de rechazo por multitrayectoria para medir con precisión el tiempo de llegada de la señal con línea de vista, aumentando la probabilidad de descubrimiento y medida. La presencia de diversidad, por ejemplo la diversidad de antena y salto en frecuencia mejorarán la capacidad de rechazo por multitrayectoria y por consiguiente la exactitud en la medida.

Cuando una aplicación requiere la posición de un móvil, tiene que enviar una petición al SMLC con la identidad del móvil y el parámetro de nivel de exactitud;

dependiendo de este nivel de exactitud, el SMLC decide cuántas Unidades de Medida de Localización (LMU: Location Measure Unit - unidades de medida de localización) deben ser incluidas en la petición de posicionamiento. Una vez recopilados los valores de TOA medidos junto con el parámetro de exactitud, el SMLC utiliza las medidas de TOA y en combinación con la información sobre las coordenadas de las LMU's y los valores RTD se genera una estimación de la posición. El SMLC entrega la estimación de la posición junto con una estimación de incertidumbre a la aplicación.

El método TDOA requiere hardware adicional (LMU's) para medir el tiempo de llegada de las señales con precisión. Existen opciones de implementación diferentes para este método de posicionamiento. Por ejemplo, es posible o integrar las unidades de medición en los BTSs o implementarlas como unidades autosuficientes; en caso de que se selecciones este tipo de configuración, la comunicación entre las unidades de medida y la red se lleva a cabo preferentemente con una interfaz de radio. Las unidades autosuficientes pueden tener antenas separadas o antenas con una BTS existente.

4.4 MÉTODOS BASADOS EN LOS TERMINALES

4.4.1 Enhanced Observed Time Difference (E-OTD)

La posición del MS es determinada deduciendo los componentes geométricos de los retardos de tiempo desde las Estaciones Base (BTS: Base Tranceiver Station) a un MS. Para las redes sincronizadas, el MS mide tiempo relativo de llegada de las señales de varios BTSs y para las redes no sincronizadas, las señales se reciben por un punto de medición fijo, conocido como la LMU de la cual se sabe su posición.

Las medidas son realizadas por el MS sin ningún hardware adicional. Para las medidas de sincronización del Tiempo de Diferencia Observado (OTD: Observed Time Difference) [1]

[1] **NOTA:** En este documento, el término OTD se usa para referirse a una cantidad de tiempo, considerando que el E-OTD se usa para referirse a un método del posicionamiento.

pueden usarse señales normales o silenciosas; cuando la transmisión de los BTSs no está sincronizada, la red necesita medir la RTD entre ellas y para obtener la triangulación exacta se necesitan por lo menos tres BTSs geográficamente distintas. Basado en los valores del OTD medidos, la ubicación del MS puede ser calculada por la red celular y es llamado "MS-assisted", o si toda la información necesaria está disponible en el MS, en el propio MS, se llama "MS-based".

4.4.2 Tipos del Cálculo para la posición.

La estimación de la localización es realizada por una Función de Cálculo de Posición (PCF: Position Calculation Function) que puede estar localizada en el MS o en la red. Existen dos maneras de calcular la posición de un móvil utilizando E-OTD, conocidas como tipo hiperbólico o tipo circular, las cuales usan la misma arquitectura de la red, las funciones MS, LMU y los cálculos de la PCF.

4.4.2.1 Tipo Hiperbólico

Hay tres medidas básicas del tiempo asociadas con este tipo de cálculo:

- Diferencia de Tiempo Observada (OTD). Es el intervalo de tiempo medido por un MS entre la recepción de señales de dos Estaciones (BTS) de la red celular. La señal del BTS_1 se recibe en un tiempo t_1 , y la señal del BTS_2 se recibe en un tiempo t_2, así los OTD valorados en este caso son: $OTD = t_2-t_1$. Si las dos señales llegan exactamente al mismo tiempo, entonces OTD = 0.
- Diferencia de Tiempo Real (RTD). Es la diferencia de sincronización relativa en la red entre dos BTSs. Si la BTS_1 envía un estallido en el momento t_3, y el BTS_2 en el momento t_4, el RTD entre ellos es: $RTD = t_4 - t_3$.
- Diferencia de Tiempo Geométrica (GTD). Se refiere a la diferencia de tiempo entre la recepción (por un MS) de estallidos de dos estaciones base diferentes debido a la geometría. Si la longitud del camino de la propagación entre la BTS_1 y la MS es d_1, y la longitud del camino entre la BTS_2 y el MS es d_2, entonces $GTD = (d_2 - d_1) / \upsilon$ dónde υ es la velocidad de las ondas de radio.

La relación entre estas tres cantidades es: GTD = OTD - RTD. GTD es una cantidad relacionada con la geometría de la localización (las posiciones del móvil y

BTSs); GTD es la cantidad real que es útil para los propósitos de la localización, ya que contiene la información sobre la posición del MS, por lo tanto si sólo se conocen los valores de OTD y RTD, la localización no puede calcularse.

La estimación de la posición puede calcularse en el MS o en la red dependiendo de la aplicación. Cualquiera que sea el método utilizado, la estimación de la localización es calculada del GTD, basado en el hecho de que es posible localizar el MS que observa un valor GTD constante (d2-d1= constante) entre dos BTSs formando una hipérbola. El MS puede localizarse en la intersección de dos hipérbolas obtenida con tres BTSs y dos GTDs. Si más GTDs están disponibles es posible que el área de localización sea más exacta.

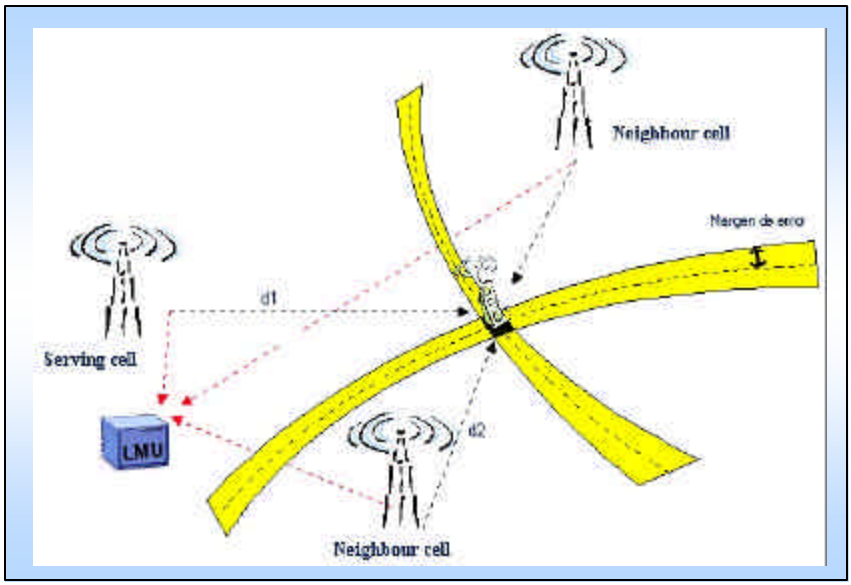

Figura 4-7. Método de localización E-OTD Hiperbólico

En la Figura 4-7 la línea negra punteada representa el GTD determinado, es decir, representa una diferencia constante en la distancia a dos BTSs. El resultado de la medida no es exacto, así el área amarilla representa el área de incertidumbre para la medida de OTD. El área negra es la intersección de las hipérbolas, que es la posición más probable calculada donde se encuentra el MS.

4.4.2.2 Tipo circular

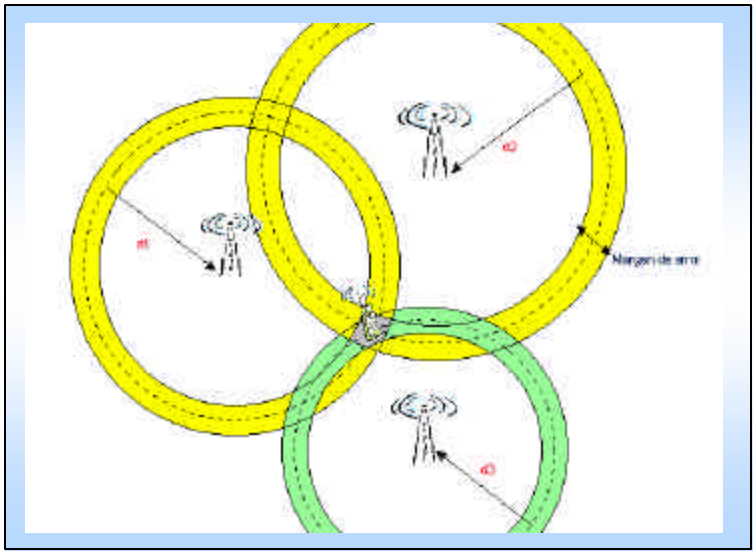

Figura 4-8. Método de localización E-OTD circular

Este tipo de cálculo de localización no mide las diferencias de tiempo al MS y LMU recibidas por las señales provenientes de las BTSs. Más bien, mide el tiempo de llegada de esas señales individualmente. Hay cinco medidas asociadas con este el tipo de E-OTD:

- Tiempo Observado en el MS (MOT), que es una señal que llega de un BTS. Éste es un tiempo medido contra el reloj interior del MS.
- Tiempo Observado por el LMU (LOT), en una señal que llega de un BTS. Éste es un tiempo medido contra el reloj interior del LMU. Habrá un desplazamiento de tiempo ε generalmente entre el reloj interior del MS y el reloj interior del LMU.
- La Distancia Geométrica de MS a BTS (DMB).
- La Distancia Geométrica de LMU a BTS (DLB).

Estas cantidades están relacionadas por:

$$DMB - DLB = u\left(MOT - LOT + e\right)$$

Ecuación 4-1

En donde υ es la velocidad de las señales (la velocidad de las ondas de radio). Hay tres cantidades desconocidas subsecuentemente (la posición de $MS_{(x,y)}$, y la

compensación del reloj ε) , ya que tenemos estas incógnitas, se deben contar por lo menos con tres BTS, para así generar una ecuación por cada una. Éste es el mismo número de BTSs que se requiere para el tipo hiperbólico de E-OTD.

La posición del MS se define por la intersección de círculos concéntricos generados por las BTSs comunes a las observaciones hechas por el MS y LMUs, como se muestra en la Figura 4-8.

Los tipos hiperbólicos y circulares difieren en la relación entre el margen de error del MS y la posición geográfica del MS al BTSs. En todo los otros respetos la aplicación es idéntica. La Figura 4-9, muestra como es la precisión de este método dependiendo de la zona.

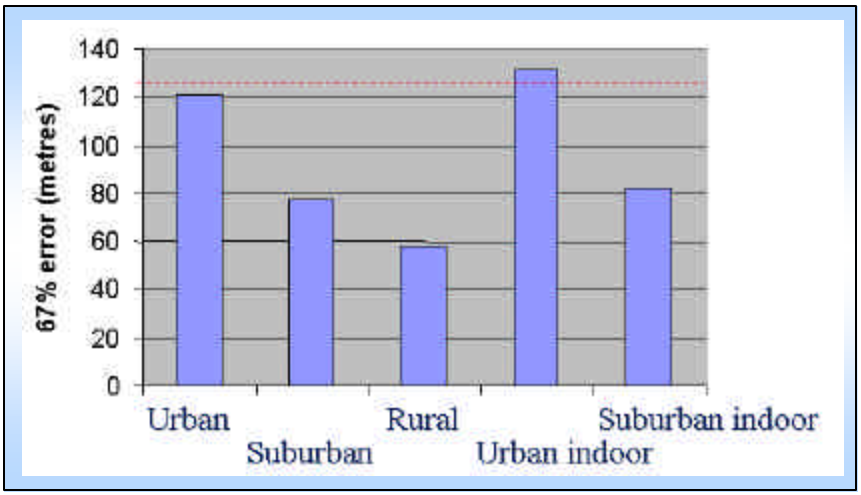

Figura 4-9. Resultado simulación

4.4.3 Global Positioning System (GPS)

En un Sistema de Posicionamiento Global (GPS: Global Positioning System) se pueden distinguir tres segmentos o áreas bien diferenciadas:

El segmento espacial: Término técnico que incluye los satélites del sistema. Estos transmiten información horaria, posición del satélite e información sobre el estado del satélite (salud y efemérides), para cada uno de los 24 satélites que orbitan a una altitud de aproximadamente 20,183.61 kilómetros sobre la superficie de la Tierra.

El segmento de usuario: Compuesto por los usuarios y sus receptores. Cada usuario posee un receptor GPS para recibir las señales provenientes de los

satélites. El usuario no transmite nada hacia el satélite y, por tanto, este no tiene conocimiento del mismo permitiendo así que el sistema no tenga limite de usuarios para su uso al mismo tiempo.

El segmento de control: Los satélites están controlados y monitoreados por estaciones en tierra que comprueban el estado y posición de los satélites. Los parámetros orbitales, los comandos de mantenimiento y las correcciones de tiempo son actualizados periódicamente desde tierra. NAVSTAR tiene cinco estaciones de control en Hawai, Isla Ascensión, Diego García, Kwajalein y Colorado Spring.

Tanto NAVSTAR como GLONASS suministran dos tipos de señales. Una utilizada en el campo militar que posee una precisión mucho mayor que la suministrada para uso civil, a la cual se le introducen una serie de errores aleatorios controlados desde las estaciones en tierra. Esta señal es de libre uso y sin costo alguno por su utilización.

4.4.3.1 ¿Cómo funciona el GPS?

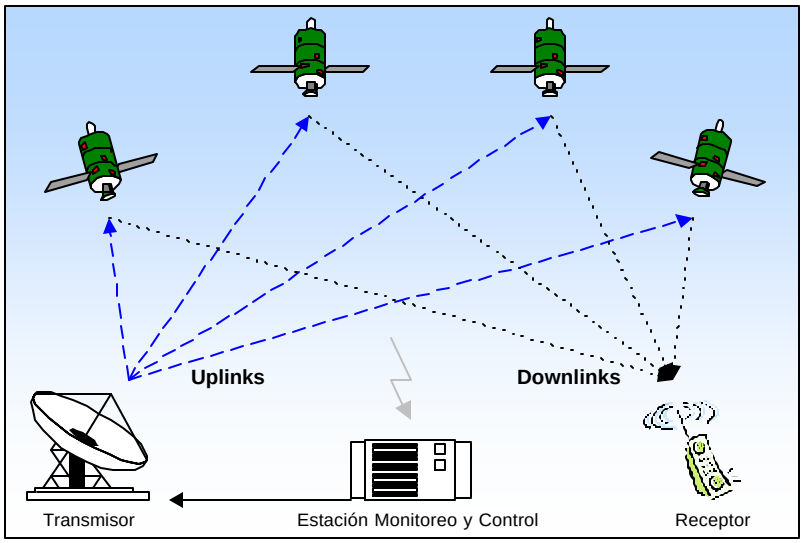

Figura 4-10. Sistema GPS típico

El Sistema del Posicionamiento Global (GPS) proporciona los medios para determinar la posición, velocidad, y tiempo alrededor del planeta, usando satélites que emiten señales de radio, las cuales permiten calcular la posición de un receptor que a menudo se encuentra en la superficie de la Tierra. Un sistema GPS

generalmente consiste en satélites, receptores y estaciones de monitoreo y control como se muestra en la Figura 4-10. Los cuatro satélites mostrados en la Figura 4-10 emiten las señales de radio desde el espacio, transmitiendo una Señal serial Directa de Espectro Ensanchado (DS-SS: Direct Séquense – Spread Spectrum) a 1.023 Mchip/sec[2] con un período de código de un milisegundo; todos los satélites transmiten a 1575.42 MHz usando CDMA; la señal DS-SS de cada satélite se modula con un mensaje de navegación que incluye el tiempo exacto y una descripción de la posición del satélite.

La medida del posicionamiento para el receptor de GPS está basado en el tiempo de llegada (TOA); cuando 4 o más satélites están en línea de vista con el receptor (o la antena del receptor), son determinadas la latitud, longitud, y altitud del receptor, y según la calidad del servicio, la precisión de esta medida varia. El servicio que esta disponible para las aplicaciones comerciales e incluso para la determinación de la posición telefónica móvil es denominado Servicio de Posicionamiento Estándar (SPS: Standard Positioning Service). El SPS proporciona la exactitud de la posición horizontal dentro de un círculo de 100 metros de radio 95% del tiempo pero para lograr mejor exactitud se usan las técnicas de corrección diferencial; GPS diferencial (DGPS), que puede reducir el error de la posición por debajo de los 5 metros.

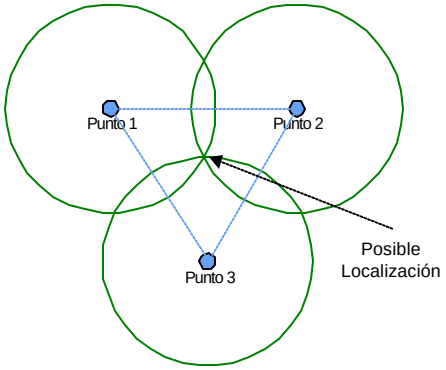

Figura 4-11. Tiempo de llegada TOA

La Figura 4-11. se usa para mostrar una vista bidimensional simplificada del principio TOA; el sistema determina la posición basado en la intersección en el rango de los círculos, el cual es calculado del tiempo de transmisión de señal que se

2

deduce multiplicando el tiempo por la velocidad de la señal. Tres medidas del rango determinan una única posición y el nivel de exactitud geométrica es mayor dentro del triángulo formado por los centros de los tres círculos y disminuye gradualmente como uno se mueva fuera del triángulo. GPS usa el mismo principio dónde el círculo se vuelve la esfera en el espacio y por lo cual necesitamos una cuarta medida, que es sacada del desfasamiento del reloj del receptor.

Para resolver el desfase entre el reloj del receptor y reloj del satélite, es usado un cuarto satélite, en caso de que los relojes de los satélites no estén sincronizados, por medio de la central de control en tierra son inmediatamente sincronizados manteniendo siempre un alto nivel de exactitud. Como resultado, pueden calcularse la posición del receptor y desplazamiento del reloj de las ecuaciones:

$$P_1 = \sqrt{(x-x_1)^2 + (y-y_1)^2 + (z-z_1)^2} + c(dT_1 - dt)$$

$$P_2 = \sqrt{(x-x_2)^2 + (y-y_2)^2 + (z-z_2)^2} + c(dT_2 - dt)$$

$$P_3 = \sqrt{(x-x_3)^2 + (y-y_3)^2 + (z-z_3)^2} + c(dT_3 - dt)$$

$$P_4 = \sqrt{(x-x_4)^2 + (y-y_4)^2 + (z-z_4)^2} + c(dT_4 - dt)$$

Ecuación 4-2

donde $(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3) y (x_4, y_4, z_4)$ es la posición conocida de los satélites, P_1, P_2, P_3 y P_4 son seudo rangos medidos, *c* es la velocidad de luz y dT_1, dT_2, dT_3, dT_4, son las condiciones conocidas del reloj de los satélites basados en un tiempo GPS, las cuales son deducidos por el receptor gracias al mensaje de navegación del satélite, y *dt* es una variable desconocida que mide el retardo o desfase del tiempo GPS. Para la simplicidad, varias condiciones de error se han omitido en las ecuaciones anteriores. El término de la raíz cuadrada representa el rango geométrico entre el satélite y receptor, y todas las otras condiciones contribuyen a las medidas del seudo rango.

Hay cuatro funciones principales para un receptor GPS convencional:

- Medición de la distancia de los satélites al receptor pudiendo determinar los seudo rangos (fases del código).

- Extracción del tiempo de llegada de la señal de los mensajes contenidos en la transmisión del satélite.
- Cálculo de la posición de los satélites evaluando los datos efímeros que indican el tiempo de llegada.
- Determinación de la posición del receptor y el tiempo base GPS del receptor usando los artículos de los datos anteriores.

4.4.3.2 GPS-Asistido

La idea básica es establecer una red sincronizada GPS, la cual tenga receptores en áreas despejadas que le permitan operar continuamente y que además este conectada con la red GSM, para que cuando ocurra un requerimiento de posición esta red pueda mandar datos de ayuda que permitan aumentar la precisión del receptor GPS. Si se lleva a cabo propiamente la asistencia GPS, el método debe ser capaz de:

1. Reducir el tiempo de cálculo.
2. Aumentar la sensibilidad del sensor.
3. Consumir menos poder del microteléfono.

Si el receptor GPS no sabe su localización aproximada, no podrá determinar los satélites visibles o estimar el rango y frecuencia Doppler de estos, por lo cual tiene que investigar completamente la fase del código lo cual toma de 0 a 1023 chips y la frecuencia espacial que varia de –4kHz a +4khz para localizar los satélites visibles, además de que los movimientos relativos entre los satélites y el receptor hace que la búsqueda tome un tiempo más; por consiguiente, existe un parámetro importante para evaluar la calidad de un receptor denominado TTFF (Time To First Fix). Para GPS autónomo, este tiempo podría ser superior a 10 minutos, obviamente inaceptable para las aplicaciones como E911, pero se puede reducir el TTFF de un receptor a unos segundos si se transmiten datos de ayuda utilizando la red sincronizada GSM, esto reduce significativamente la búsqueda de fase del código y frecuencia espacial, además, debido a la disponibilidad del mensaje de navegación de satélite transmitida vía red celular,

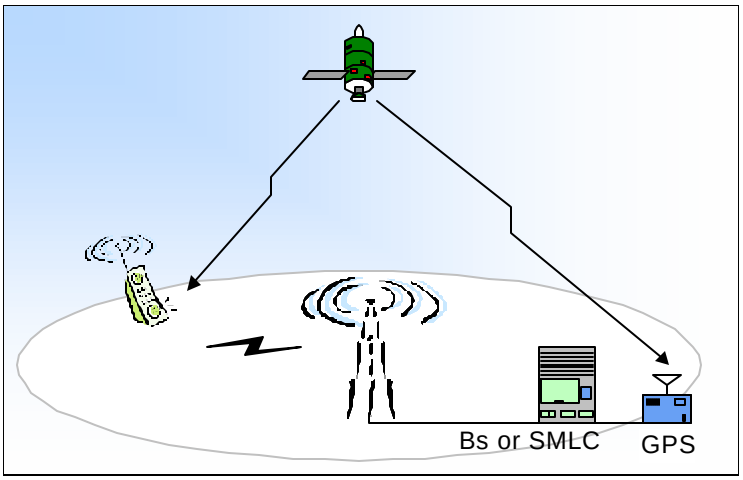

Figura 4-12. Sistema GPS Asistido

puede ayudar también al receptor cuando las señales del satélite son demasiado débiles para demodular la información útil; también reduce la dispersión de poder del microteléfono yendo al "modo ocioso" siempre que no halla necesidad de los servicios de localización. Ver Figura 4-12.

4.5 SISTEMA DE POSICIONAMIENTO MÓVIL

Existen varias compañías que ofrecen sistemas de posicionamiento. El problema con estas compañías y sus sistemas es que no son compatibles entre ellas, haciendo que los diseñadores de aplicaciones tengan que escoger solo un tipo de sistema, perdiendo así parte del mercado potencial de usuarios. Gracias al foro LIF se intentará regularizar las tecnologías de posicionamiento haciendo más fácil para diseñadores de aplicaciones alcanzar un mercado más amplio.

4.5.1 Ericsson MPS (Mobile Positioning System)

El Sistema de Posicionamiento Móvil (MPS: Mobile Positioning System) de Ericsson utiliza varias técnicas de posicionamiento diferentes, como E-OTD, A-GPS y CGI+TA. Su propósito es proporcionar a los usuarios finales su posición para poder brindar comunicación verdaderamente personalizada a través del teléfono móvil u otros dispositivos móviles de una forma segura y confiable.

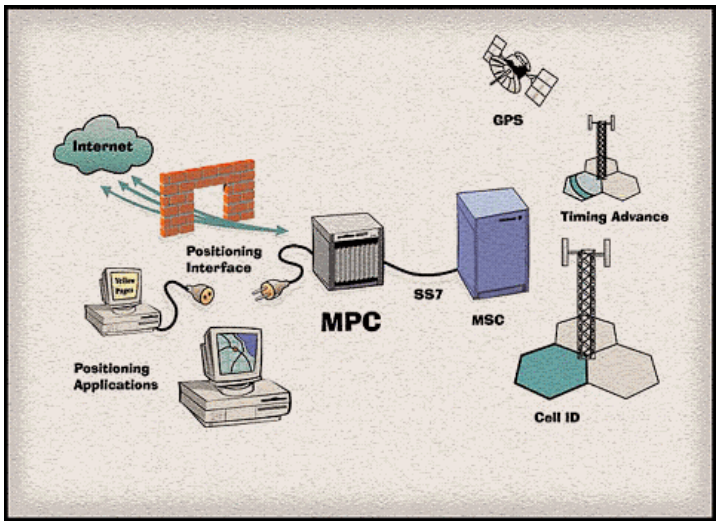

Figura 4-13. Sistema de posicionamiento móvil

El MPS consiste en un servidor, llamado Centro de Posicionamiento Móvil (MPC: Mobile Positioning Center) y extensiones de software para el operador de la red móvil. El MPS utiliza el Protocolo de Posicionamiento Móvil (MPP: Mobile Positioning Protocol) basado en el Protocolo de Transferencia de HiperTexto (HTTP: HyperText Transfer Protocol) para la comunicación con el MPC.

La información de la posición móvil se entrega al MPC vía la red GSM. El MPC calcula las coordenadas, las cuales se usan para aplicaciones proporcionadas por el operador o por los Proveedores del Servicio de Internet (ISP: Internet Service Providers). La exactitud de la ubicación de un móvil depende de la técnica que se utilice; actualmente la exactitud es aproximadamente de 150 metros en las áreas rurales y en las áreas urbanas es según los tamaños de la celda, entre mas pequeña sea, la exactitud será mayor.

Características del MPS

- No requiere ninguna modificación al teléfono móvil GSM.
- Ruta hacia el futuro.
- Asegura el desarrollo de aplicaciones con una API abierta que soporta el despliegue del mercado y permite a los diseñadores crear aplicaciones independientemente del sistema de posicionamiento móvil.
- Sistema comercial integrado en la red.

- El sistema es totalmente escalable.
- Se requieren cambios mínimos en la red celular y en el software.

4.5.1.1 Solicitudes

Una solicitud se emite enviando una petición HTTP GET al MPC. La sintaxis para la solicitud es:

http://my.positioning.server/PositionRequest/Direct.asp?<ParameterList>

La lista de parámetros (*ParameterList)* es una lista de nombres con su valor. La sintaxis para la lista del parámetro es:

name=value&name=value&name=value..

Por ejemplo:

http://my.positioning.server/PositionRequest/Direct.asp?USERNAME=xxx &

PASSWORD=yyy&POSITION_ITEM=46701234567&POSITION_TIME=(time now)

Se pueden posicionar múltiples MSs en una sola solicitud de URL. Esto se hace agregando más parámetros de POSITION_ITEM separados por comas o guiones para posicionar un rango de MSs.

Por ejemplo:

POSITION_ITEM=4670010000,4670010005-4670010010

Los parámetros USERNAME, PASSWORD, POSITION_ITEM y POSITION_TIME son obligatorios y hay también varios parámetros optativos como POSITION_DELAY y POSITION_FORMAT.

4.5.1.2 Respuesta y Valores de retorno

La respuesta está en un formato de texto muy similar al Lenguaje de Marcación de HiperTexto (HTML: HyperText Markup Language) con etiquetas o títulos específicos MPP. Una contestación exitosa para un MS puede parecerse a lo que se muestra en las líneas siguientes:

<Head RequestID=2.965239225.3800 AnswerID=1>
<MS=46777100009

```
        RequestedTime=20000830085447+0200
        Error=0
        GeodeticDatum=WGS-84
        HeightDatum=NotAvailable
        CoordinateSystem=LL
        PositionFormat=IDMS0

        <PositionData
                <PositionArea
                        Time=20000830085400+0200
                        <Area=Arc
                                <Area=Point
                                        Latitude=N561242
                                        Longitude=E153221
                                >
                                InnerRadius=6600
                                OuterRadius=7123
                                StartAngle=30
                                StopAngle=150
                        >
                >
                <PositionArea
                        Time=20000830085449+0200
                        LevelOfConfidence=100
                        <Area=CircleSector
                                <Area=Point
                                        Latitude=N561242
                                        Longitude=E153221
                                >
                                StartAngle=30
                                StopAngle=150
                                Radius=7123
                        >
                >
        >
>
<Tail RequestID=2.965239225.3800>
```

La primera etiqueta PositionArea incluye el valor del Timing Advance y la segunda son los datos de la celda que esta atendiendo al móvil. Si el MS está ocupado y ha habido un handover, sólo se entregan lo datos de la etiqueta PositionArea.

4.5.1.3 Limitaciones

Debido a que el MPP esta basado en HTTP, tiene todas las limitaciones inherentes a este.

4.5.1.4 Seguridad

MPS ofrece seguridad basada en SSL (Secure Socket Layer) entre la aplicación y el MPC. Además, para poder hacer una solicitud de localización a una estación móvil se debe tener el nombre del usuario y la contraseña.

4.5.1.5 Privacidad

Con MPS no hay forma de desactivar la funcionalidad de posicionamiento sin apagar el terminal móvil, pero se pueden utilizar métodos de encriptación para evitar saber quien es el dueño del móvil y en el caso de m-commerce se pueden evitar los mensajes de broadcast.

4.6 EJEMPLO DE UN SERVICIO DE LOCALIZACIÓN

4.6.1 Servicios de localización prestados por la empresa Amena.

Amena, del Grupo Auna, es un operador de telefonía móvil del mercado español que comenzó a prestar sus servicios con cobertura nacional el 25 de Enero de 1999.

Amena ofrece un conjunto de servicios basados en la localización, denominados servicios ¿Dónde?, que permite a las empresas gestionar sus recursos humanos y materiales, reemplazando los métodos tradicionales de trabajo por una nueva forma de entender los negocios basada en las nuevas tecnologías, potenciando la movilidad y la comunicación con sus colaboradores, y a los usuarios obtener un gran número de servicios a través de su móvil.

Las posibilidades del servicio de localización de Amena le permite al usuario obtener información acerca de restaurantes, farmacias, tráfico, gasolineras o cajeros, realizando una localización automática de la posición actual del móvil para ofrecerle información sobre los lugares más próximos solicitados. También puedes introducir

una carretera para acceder a información en ruta y además, selecciona la opción "Cómo ir a" para conocer el itinerario a seguir para llegar a cualquier parte.

Figura 4-14. Menú

Figura 4-15. Zona

Cuando se accede al servicio de ¿Dónde?, a través del teléfono móvil, lo primero que se puede observar (Figura 4-14) es el menú de los lugares de los cuales se tienen datos. En la figura 4-15 se debe seleccionar si desea la información total del la ciudad o solo los mas cercanos.

Figura 4-16. Criterios

Figura 4-17. Resultado

En la figura 4-16 se toman otros datos de criterio y en la figura 4-17 se da el resultado de las gasolineras.

5 ANÁLISIS DE REQUERIMIENTOS DEL SOFTWARE Y ANÁLISIS DEL SOFTWARE DE LA APLICACIÓN MÓVIL

5.1 DEFINICIÓN Y CARACTERIZACIÓN DEL SISTEMA OBJETIVO

5.1.1 Esencia del sistema

Con el advenimiento de nuevas tecnologías habilitadoras de los procesos de comunicación aparecen nuevos servicios que pueden ser implementados con grandes beneficios para las empresas.

Este es el caso de WAP, una tecnología para el desarrollo de aplicaciones inalámbricas que ofrece nuevos horizontes en la forma y uso de Internet abriendo un amplio abanico de posibilidades para aplicaciones que pueden ganar efectividad gracias a la movilidad y disponibilidad de las aplicaciones inalámbricas.

Teniendo en cuenta lo anterior, se ha planteado el desarrollo de un **SERVICIO DE GESTIÓN DE PEDIDOS** basado en tecnologías web y WAP, (*Wireless Application Protocol*), que ofrecerá a las empresas suscriptoras capacidades para recibir y gestionar pedidos desde terminales móviles WAP por parte de los usuarios del servicio (Clientes).

5.1.2 Descripción general del sistema

El sistema tendrá módulos que permiten a las empresas gestionar sus productos, agentes vendedores, clientes y móviles de distribución de productos. De igual

forma, los clientes suscritos podrán realizar pedidos a diferentes empresas, gestionar su perfil y personalizar su presentación para disponer en el terminal WAP de un menú a su medida; el cliente podrá generar nuevos pedidos teniendo como base un pedido anterior para minimizar el tiempo en el cual se encuentra al aire utilizando recursos de la red brindándole ahorro en el tiempo de ejecución de sus pedidos.

5.2 ANÁLISIS DEL DOMINIO DEL PROBLEMA

5.2.1 Declaración del problema

5.2.1.1 Descripción del problema

El auge de los sistemas de información utilizando medios de acceso masivo, tal como Internet, ha permitido a muchas empresas aumentar su competitividad, permitiendo vender sus productos, en línea, a tal punto que actualmente el comercio electrónico en Internet es más una necesidad que un privilegio, la razón más importante es la dramática diferencia de costos en la realización de operaciones; por ejemplo, según la American Bankers Association[▣], el costo que genera una venta de un pasaje aéreo por teléfono es de 8 dólares mientras que por Internet es de 0,01. Además las posibilidades que hoy en día ofrece las tecnologías de Internet, permiten desarrollar alternativas comerciales de una manera efectiva y con posibilidades de expandir sus capacidades.

Las tecnologías de Internet son fácilmente adaptables a los cambios de la empresa, cuentan con alta tolerancia a fallos, alto rendimiento, acceso casi global y con niveles de seguridad aceptables que permiten cumplir condiciones de confidencialidad, integridad, autentificación e irrenunciabilidad. Además, como soporte para el comercio electrónico permite la utilización de sistemas de pago electrónico tales como pago con tarjeta de crédito, debito, cheques, órdenes de pago electrónicos, dinero virtual, micro-pagos, etc. los cuales aplican modernas técnicas de

[▣] American Banking Association, http://www.aba.com

encriptación (procedimientos de cifrado, firma digital y certificados, entre otros) para garantizar seguridad.

Aunque estos sistemas han sido diseñados para estar disponibles un 100% del tiempo, en la mayoría de los casos es el usuario quien no cuenta con el acceso en los momentos claves, debido a que se necesita de un PC para poder acceder a Internet.

La aparición de tecnologías para desarrollo de aplicaciones inalámbricas, sobre todo en el campo del Internet móvil abren nuevas posibilidades de expansión para aplicaciones que soportan estos servicios, ofreciendo disponibilidad y movilidad en el momento en que realmente se necesitan, mediante teléfonos móviles, PDAs, HandHeld, etc.

Así, es posible pensar en que el modelo de atención de clientes de muchas empresas, puede ser imitado y optimizado en un alto grado utilizando estas tecnologías, sin embargo, es de vital importancia, pensar en el cliente final que deber ser quien perciba de forma clara y evidente los beneficios que esto podría traer consigo.

De acuerdo a lo anterior, se quiere crear un servicio de aplicación de apoyo a la fuerza de ventas con el fin de que las empresas que manejan un modelo similar se reúnan de forma tal que se beneficien de las ventajas de tener un contacto con sus clientes y agentes casi en tiempo real, (agilización en el proceso de despacho de pedidos, optimización del proceso de control de salida y llegada de productos a la empresa, etc.), y sus clientes la observen como una comunidad de fácil acceso.

5.2.1.2 Propósito del sistema a desarrollar

La aplicación debe proporcionar los siguientes aspectos:

- Permitir al administrador de la empresa gestionar sus agentes de ventas y agentes distribuidores, productos pedidos y clientes.
- Proveer soporte para la actualización de inventario

- Permitir al cliente o agentes realizar pedidos desde la mayor parte de sitios posible y en cualquier momento.
- Proporcionar al cliente o agente escoger los productos y ofertas que más se ajusten a sus necesidades, con el fin de que solamente se le muestre la información le interesa.
- Permitir al cliente verificar su estado de cuenta en cada una de las empresas en donde haya realizado algún pedido.
- Facilitar al agente la verificación del estado de las cuentas de sus clientes.
- Ofrecer un nivel de seguridad aceptable para garantizar confiabilidad en el manejo de la aplicación.
- Ofrecer funciones que optimicen las transacciones, como recuperación y reutilización del último pedido realizado y recuperación de sesión.
- Almacenar los pedidos realizados en el menor tiempo posible, casi en tiempo real.
- Permitir al administrador de la aplicación gestionar las suscripciones de las empresas que utilizan los servicios, mediante la generación de estadísticas y de las funciones propias de la gestión.

5.2.2 Diccionario de dominio

Administrador del sistema: Es quien se encarga de administrar y velar por la consistencia del sistema en el cual los clientes, las empresas y los agentes se apoyan para realizar el proceso de compra-venta.

Administrador: Es quien está a cargo de la empresa, es quien supervisa el entorno interior, exterior para el bien de la organización o empresa en que se desempeñan.

Agente distribuidor: Es la persona que visita al cliente para entregarle productos previamente pedidos u ofreciéndolos sin necesidad de que sean pedidos con anticipación.

Agente visitador: Es quien atiende clientes solamente para recibir pedidos.

Carrito de compras: Similar al de un proceso de venta tradicional este se refiere al conjunto de productos que un cliente pretende comprar.

Categoria: Se refiere al tipo de empresa, según el tipo de productos que ofrece.

Ciudad: Nombre de la ciudad donde se encuentra la empresa o donde el agente o el usuario hacen el pedido para ser despachado.

Cliente: Es quien esta interesado en realizar una compra utilizando la aplicación y que además esta registrado en el sistema.

Código: Numero que identifica la empresa o agente.

CodigoEmpresa: Es un número que se asocia a un producto para identificar a que empresa pertenece, así todos los productos de una empresa tendrán un mismo CodigoEmpresa.

Contraseña: Conjunto de caracteres encriptados que permiten seguridad.

Descripción: Contiene datos que dan una idea de lo que se quiere describir.

Dirección: Contiene la dirección real del los usuario en general del sistema.

E-mail: Dirección de correo electrónico de los usuario del sistema.

Existencia: Es la cantidad de productos que se encuentran disponibles para la venta.

Nombre: Contiene los nombre de los cliente, Agente y Empresas.

Producto: Son los artículos que una empresa ofrece a sus clientes.

Teléfono: Numero donde se puede contactar los usuario del sistema.

Tipo: De acuerdo al valor que tome se identifica la modalidad de un agente, (Agente visitador o Agente distribuidor).

Usuario: Hace referencia a todo aquel que intenta ingresar o realizar alguna acción utilizando el sistema.

Valor: Hace referencia al costo que tiene el producto para un cliente.

Zona: Hace referencia a las localidades a las cuales un agente debe atender.

5.2.3 Modelo del dominio

5.2.3.1 Diagrama general

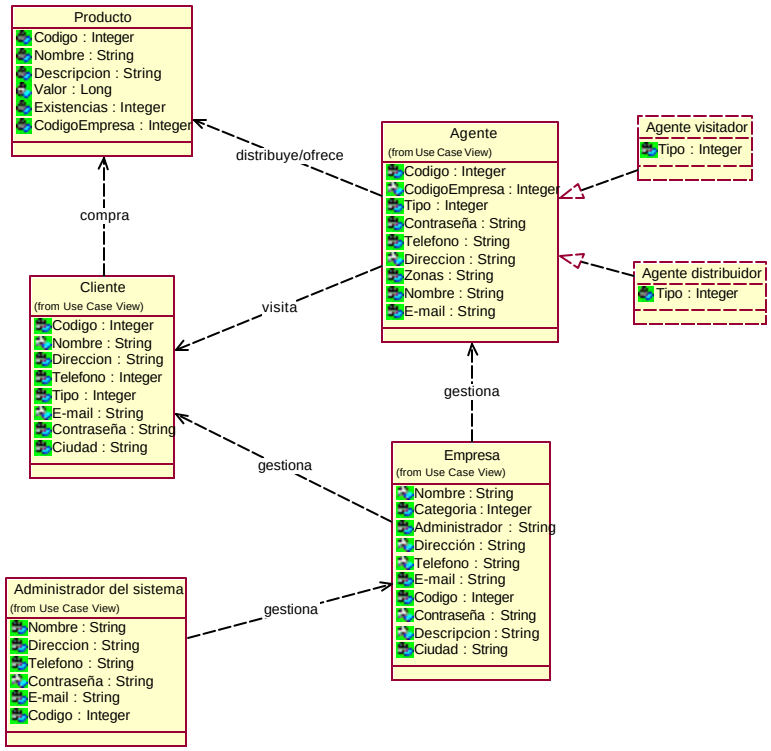

Figura 5-1. Modelo del dominio del sistema, diagrama general

5.2.3.2 Jerarquías de especialización

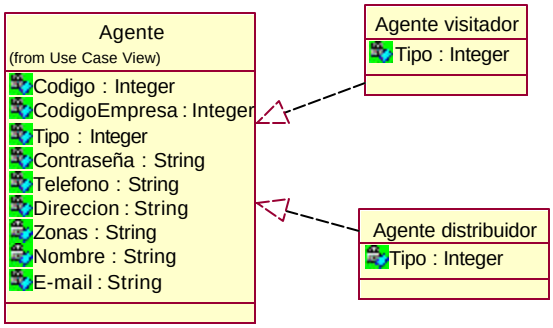

Figura 5-2. Jerarquías de especialización

5.3 DEFINICIÓN DEL MODELO DE DESARROLLO ESPECÍFICO

5.3.1 Modelos que describirán el sistema

Según la metodología establecida para el desarrollo de los modelos que describirán el sistema y teniendo en cuenta el alcance del proyecto, se describirán los siguientes modelos:

- Análisis de requerimientos del software.

  En el cual se incluye:

  - Especificación de requerimientos, para ello se debe realizar: Definición el propósito del sistema, identificación de las funciones, especificación de atributos y restricciones y maquetas de los formatos de entrada y salida.

  - Modelo del dominio: Consta de un diagrama de clases, que tiene como propósito identificar los elementos fundamentales del sistema y un diccionario de datos con el fin de establecer un vocabulario común entre los participantes del proyecto.

  - Casos de uso de alto nivel: Que tiene como objetivo la identificación de los actores y los casos de uso del sistema.

  - Análisis de riesgos.

- Plan del software, con el cual se definen los recursos, actividades, cronograma y el presupuesto necesario para el desarrollo del software.
- Referencias bibliográficas.

- Análisis del software.

Tiene como objetivo, representar el comportamiento del sistema con base en los conceptos del dominio del problema, sin entrar aún en los detalles de la solución, para ello se deben definir:

- Casos de uso abstractos, complementados con las maquetas de interfaces de usuario.
- Diagrama de paquetes de análisis.
- Diagrama de clases de análisis, con el fin de identificar las responsabilidades, atributos, relaciones y requerimientos especiales de las clases de análisis.
- Diagramas de interacción del sistema, con el cual se describe el comportamiento del sistema con la realización de los casos de uso teniendo en cuenta las interacciones entre las clases de uso de análisis.
- Diagramas de estados.
- Primera versión del manual de usuario.

- Diseño del software:

En él se representa los componentes con los cuales se construye el software, las interacciones entre ellos y su comportamiento. Para tal fin el modelo contiene:

- Casos de uso reales: En el cual se realiza una descripción entre las interacciones reales entre el sistema y sus usuarios.

- Diagrama de paquetes de diseño: Se describen los subsistemas creados para estructurar los elementos del modelo de diseño y sus interfaces.
- Diagrama de clases de diseño.
- Diagramas de interacción: Se describe el comportamiento del sistema por medio de la realización de los casos de uso, teniendo en cuenta las interacciones entre las clases de diseño. Para esto también se requieren de los diagramas de secuencias y de colaboración.
- Diagrama de estados.
- Diagrama de implantación, con el cual se describe la arquitectura del sistema en tiempo de ejecución, considerando el hardware necesario, tipos de conexiones y lugares de ejecución de los diferentes componentes.
- Descripción de la arquitectura.
- Segunda versión del manual de usuario.

- Implementación y pruebas del software

5.3.2 Fundamentos metodológicos a utilizar

Para el desarrollo del sistema se seguirá básicamente el M.R.D.P. complementado por el Proceso Unificado (UP) utilizado para el desarrollo de programas mediante el paradigma de orientación a objetos.

5.3.3 Organización del recurso humano

Considerando la importancia del recurso humano en el Ambiente de Desarrollo y que de su organización los resultados que se obtengan en el desarrollo de cada fase, se han determinado los siguientes objetivos:

- Establecer roles claramente definidos con el fin de potencializar la competencia y especialización de las personas involucradas en el proyecto.
- Contribuir a la creación y enriquecimiento de la base de conocimiento de la organización (Universidad del Cauca) en la cual se desarrolla el proyecto.
- Buscar el aseguramiento de calidad en todos los niveles del proceso de desarrollo y del producto final.

5.3.4 Roles

El grupo consta de tres integrantes para los cuales hemos definido tres roles específicos:

5.3.4.1 Desarrollador

- Diseñar con y para reusabilidad.
- Seguir los lineamientos metodológicos en el proceso de desarrollo.
- Cumplir con las tareas asignadas, de acuerdo al cronograma planteado.

5.3.4.2 Auditor

El Auditor tendrá como funciones:

- Verificar la consistencia de los modelos desarrollados.
- Revisar y encargarse de hacer las correcciones pertinentes a los subproductos del proceso de desarrollo.
- Vigilar el avance del proyecto.

5.3.4.3 Orientador

Las funciones de los orientadores son:

- Dar las especificaciones y establecer tareas a desarrollar.

- Supervisar el proceso de desarrollo.
- Asesorar al personal del proyecto en la aplicación de la metodología utilizada en el desarrollo.

El personal asignado a cada uno de los roles es el siguiente:

Debido a que el Proceso de Desarrollo será realizado por un grupo de tres personas, los roles de desarrollador y de auditor serán rotados para cada modelo de la siguiente forma:

- Análisis de requerimientos software:
  - Desarrollador: Fernando Alonso Mejía Londoño.
  - Auditor: María Alejandra Dulcey Morán.
- Análisis del software:
  - Desarrollador: María Alejandra Dulcey Morán.
  - Auditor: Fernando Alonso Mejía Londoño
- Diseño del software:
  - Desarrolladores: Fernando Alonso Mejía Londoño.
  - Auditor: María Alejandra Dulcey Morán.

Y en todas las fases de desarrollo:

- **Orientadores :** Ing. Esp. Diego Andrés Acosta Ortiz, Ing. Javier Hurtado.

5.3.5 Ambiente de soporte

5.3.5.1 Plataforma para el desarrollo

Para el desarrollo del proyecto, teniendo en cuenta el alcance de este proceso se elige como plataforma el sistema operativo *Windows 2000 Professional*.

5.3.5.2 Base de datos de ingeniería

En la base de conocimiento/experiencia del grupo se cuenta con la experiencia adquirida en los cursos anteriores, en las cuales se desarrollaron documentos similares para el desarrollo de un proyecto, además se espera enriquecer esta base con el desarrollo de este proyecto.

En esta base se cuenta con:

- Documentos de diseño.
- Especificaciones de diseño.
- Manuales de usuario.
- Prototipos.
- Reporte del desempeño organizacional y de las actividades.
- Documentos que se desarrollan teniendo como soporte el MRDP.

Estos documentos y datos se encuentran almacenados en medios magnéticos y en documentos escritos.

5.3.5.3 Software para modelamiento

Para el modelamiento del sistema se cuenta con la herramienta de desarrollo de Rational Software Corporation, Rational Rose, con la cual se desarrollaran las distintas vistas de UML, que se realizarán siguiendo el modelo definido por el UP.

5.3.5.4 Software de aplicación

Para el desarrollo de documentos se utilizará la aplicación de Microsoft Office, Microsoft Word. Además para el desarrollo de prototipo o maquetas de interfaz de usuario, (considerando que se realizará una aplicación web), se utilizará DreamWeaver de Macromedia, editores de código como EditPlus o PHPCoder, servidor Apache web server y gestor de base de datos MySQL.

5.3.5.5 Infraestructura física

Para el desarrollo del proyecto disponemos de la casa de cada uno de los integrantes y de las instalaciones de la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca.

5.3.6 Modelo del proceso de desarrollo

Como modelo del proceso de desarrollo es una adaptación que complementa al modelo en espiral de Boehm. En el cual se plantean mínimo cuatro ciclos cada uno con cuatro fases:

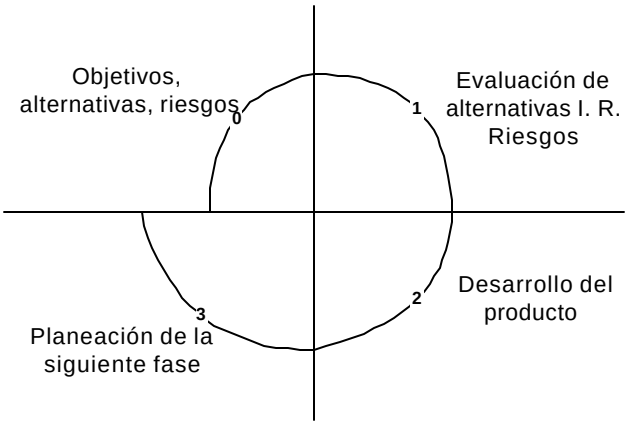

Figura 5-3. Módelo en espiral de Boehm

En cada ciclo se plantea el desarrollo de:

C0: Modelo del Dominio.

C2: Modelo de especificaciones

C3: Modelo funcional.

C4: Modelo ejecutivo.

5.4 CONSTRUCCIÓN DEL MODELO DE ESPECIFICACIONES

5.4.1 Árbol de funciones

5.4.1.1 Funciones de la empresa

1. Validar acceso

2. Realizar búsqueda

    2.1 Realizar búsqueda de pedidos

        2.1.1 Por empresa

        2.1.2 Por agente

        2.1.3 Por número de pedido

    2.2 Realizar búsqueda de productos

    2.3 Realizar búsqueda de clientes

    2.4 Realizar búsqueda de agentes

3. Verificar pedido

4. Modificar estado de pedido, (pendiente, atendido, enviado, cancelado)

5. Modificar datos (relacionados con los agentes, clientes y productos)

6. Gestionar agentes

    6.1 Adicionar agentes

    6.2 Modificar datos de agente

6.3 Eliminar agente

7. Gestionar clientes

7.1 Adicionar clientes

7.2 Modificar datos de cliente

7.3 Eliminar cliente

8. Gestionar productos

8.1 Adicionar productos

8.2 Modificar datos de producto

8.3 Eliminar producto

5.4.1.2 Funciones del agente

1. Validar acceso
2. Realizar pedido en nombre de un cliente
3. Modificar pedido de un cliente
4. Cancelar pedido de un cliente
5. Modificar contraseña

5.4.1.3 Funciones del cliente

1. Validar acceso
2. Realizar pedido
3. Modificar pedido
4. Cancelar pedido

5. Modificar contraseña

5.4.1.4 Funciones del administrador del sistema

1. Gestionar empresas

    1.1 Adicionar empresas

    1.2 Modificar datos de empresa

    1.3 Eliminar empresa

2. Gestionar administradores

    2.1 Adicionar administradores

    2.2 Modificar datos de administrador

    2.3 Eliminar administradores

5.4.2 Modelo de casos de uso

5.4.2.1 Diagrama general

Ver página siguiente …

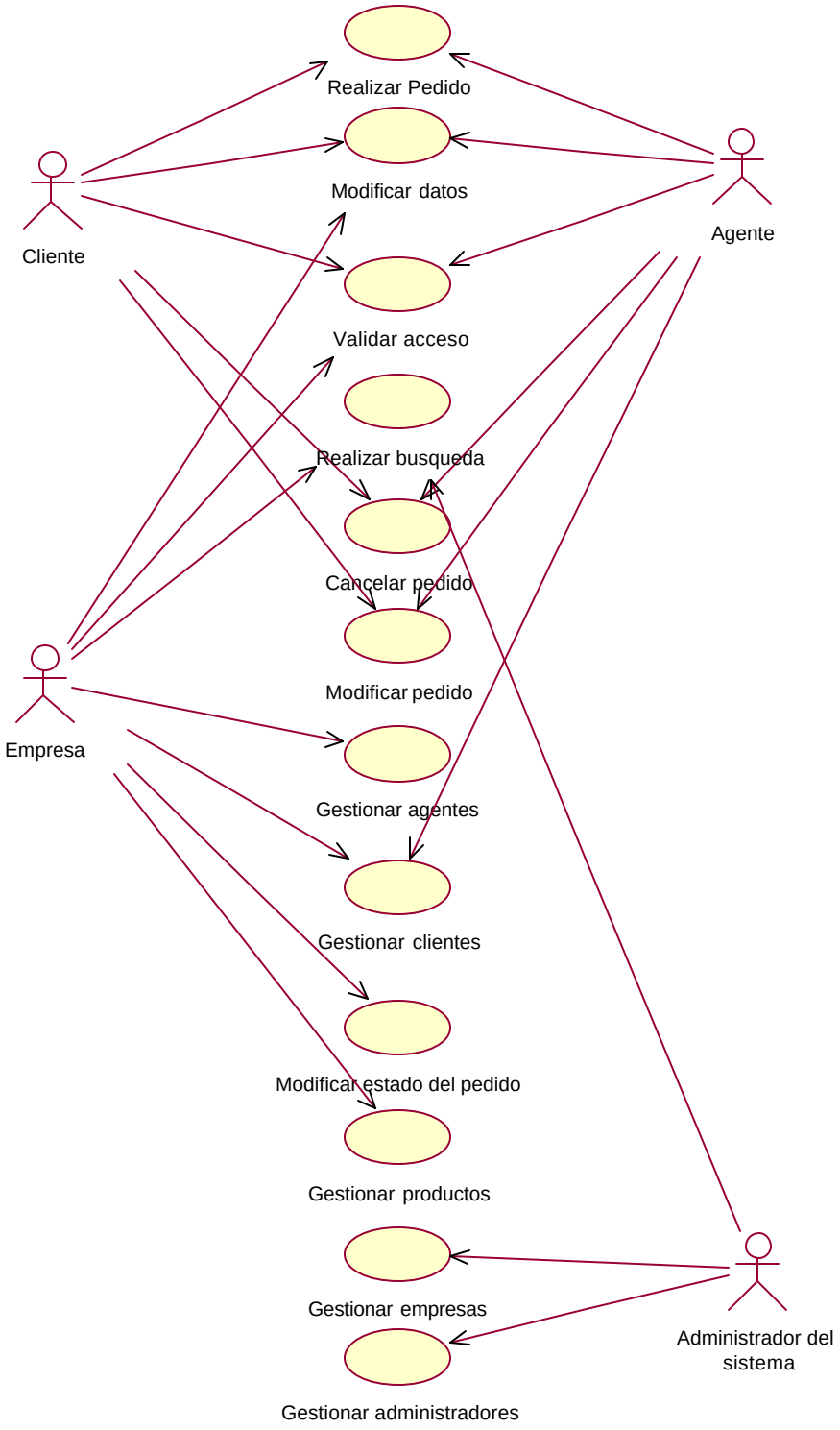

Figura 5-4. Modelo de casos de uso, diagrama general

5.4.3 Descripción de alto nivel de los casos de uso

- ***Caso de uso:* CancelarPedido**

  Actores: Agente, cliente

  Tipo: Secundario

  Descripción: Permite que un usuario o un agente cancele un pedido, antes de que este sea enviado.

- ***Caso de uso: GestionarAdministradores***

  Actores: Administrador del sistema

  Tipo: Secundario

  Descripción: Un administrador del sistema, puede adicionar, eliminar o modificar sus datos o los de otros administradores del sistema.

- ***Caso de uso: GestionarAgentes***

  Actores: Empresa

  Tipo: Primario

  Descripción: Permite a la empresa adicionar, eliminar o editar los datos relacionados con sus agentes de ventas y verificar su desempeño.

- ***Caso de uso: GestionarClientes***

  Actores: Empresa, Agente

  Tipo: Primario

  Descripción: Por medio de este caso de uso la empresa puede adicionar, eliminar o modificar los datos de sus clientes, y conocer su record de compras y pedidos realizados.

- ***Caso de uso: GestionarEmpresas***

  Actores: Administrador del sistema

  Tipo: Primario

Descripción: Por medio de este caso de uso el administrador de la aplicación puede adicionar, eliminar o modificar los datos de las empresas que exhiben sus productos a través de la aplicación.

- ***Caso de uso: GestionarProductos***

Actores: Empresa

Tipo: Primario

Descripción: Utilizando este caso de uso la empresa puede modificar el catálogo de productos que presenta al usuario, es decir, puede adicionar, eliminar o modificar la presentación de éstos.

- ***Caso de Uso: ModificarDatos***

Tipo: Secundario

Actores: Cliente, Agente, Empresa

Descripción: Permite modificar los datos referentes al cliente, agente o empresa, es decir, dirección, teléfono, e-mail, contraseña, etc.

- ***Caso de uso: ModificarEstadodelPedido***

Actores: Empresa

Tipo: Primario

Descripción: Este caso de uso se utiliza cuando un pedido realizado por un cliente ya ha sido atendido, o ya ha llegado a su destino, con el fin de que el cliente pueda conocer el progreso del pedido que ha realizado.

- ***Caso de Uso: ModificarPedido***

Tipo: Secundario

Actores: Cliente, Agente

Descripción: Permite al cliente o agente modificar el contenido de un pedido, recientemente realizado y que no ha sido despachado aún.

- ***Caso de Uso: RealizarBúsqueda***

  Tipo: Secundario

  Actores: Empresa y administrador del sistema.

  Descripción: Permite al usuario buscar específicamente un producto, empresa, agente, cliente o pedido.

- ***Caso de uso: RealizarPedido***

  Tipo: Primario

  Actores: Cliente, Agente

  Descripción: Este caso de uso permite al cliente o agente realizar la selección de los productos que desea introducir en un carrito de compras y realizar la solicitud de estos, de una forma similar a como se realiza en una tienda convencional.

- ***Caso de Uso: ValidarAcceso***

  Tipo: Primario

  Actores: Cliente, Agente, Empresa

  Descripción: Por medio de la introducción de algunos datos se realiza la validación e identificación de los usuarios que intentan ingresar al sistema, con el fin de cumplir con los niveles de seguridad básicos y mostrar la interfaz adecuada dependiendo de sí se trata de un cliente, agente, empresa o administrador del sistema. De igual forma permite que el sistema este en la capacidad de manejar perfiles de usuario.

5.5 ANÁLISIS DE RIESGOS

- **Cambios o reformas trascendentales en las especificaciones que soportan las tecnologías utilizadas.**

  Probabilidad: Media

  Impacto: Alto

Estrategia: Debido a que el sistema se esta desarrollando pensando en la funcionalidad del producto y no en la tecnología a utilizar, en caso de existir alguna eventualidad que implique cambios sustanciales en la tecnología utilizada, es posible reutilizar gran parte del diseño que realizado.

- **Perdida temporal o parcial del recurso humano**

  Probabilidad: Baja

  Impacto: Alto

  Estrategia: Aunque es muy difícil prever alguna perdida de recurso humano, hemos tratado de que el tiempo destinado al desarrollo de la aplicación, sea aprovechado al máximo y si es posible, adelantarlo con el fin de evitar pérdidas dada la eventualidad mencionada. Además se documentarán debidamente todas las actividades realizadas.

- **Baja aceptación de la aplicación desarrollada**

  Probabilidad: Media

  Impacto: Alto

  Estrategia: Se realizarán visitas y estudios a empresas que manejen un esquema similar al que se pretende implantar con el fin de que la aplicación no cause traumatismos en el cumplimiento de las funciones que se realizan en esos lugares.

- **Debido a que es necesario desarrollar la aplicación para el dispositivo móvil, basandose en un emulador, es probable que la aplicación desarrollada no se adapte al dispositivo real.**

  Probabilidad: Media

  Impacto: Medio

  Estrategia: Aunque es muy poco probable que se disponga de un dispositivo móvil todo el tiempo en que se desarrolla la aplicación, se realizarán pruebas,

tanto de navegación como de desempeño de la aplicación, en el momento en que se disponga de él.

5.6 CASOS DE USO ELEMENTALES EXTENDIDOS, PARA LA APLICACIÓN WAP

Esta parte del análisis del software[1], se incluye aquí teniendo en cuenta la importancia del diseño de las interfaces de usuario para una aplicación que utiliza como soporte hardware un dispositivo con fuertes limitaciones, tales como tamaño y resolución de la pantalla reducidos, baja capacidad de procesamiento, teclado pequeño, y además con limitaciones en la velocidad de transmisión de datos debido a la tecnología en la cual esta soportado WAP, (CDPD).

El diseño de las interfaces de usuario que se muestra a continuación fue realizado teniendo en cuenta las limitaciones ya mencionadas, es decir, tratando de reducir al máximo las incomodidades que el usuario debe enfrentar al utilizar un dispositivo WAP, para navegar en Internet. Para esto, se manejaron dos aspectos importantes: reducción del número de interacciones que el usuario debe realizar con el teclado e interacción de la aplicación con el servidor de aplicaciones.

[1] Los paquetes y diagramas de clases de análisis, asi como los diagramas de interacción del sistema se incluyen en el anexo A: “Análisis del software para la aplicación móvil”

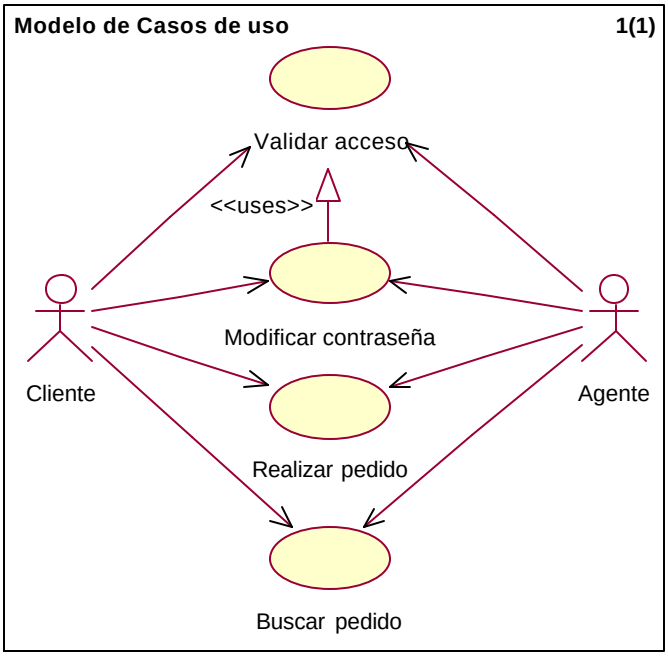

Figura 5-5. Casos de uso elementales

5.6.1 Validar Acceso

Actores: Cliente, Agente

Propósito: Permitir al sistema identificar al usuario, de tal forma que sea posible mostrarle contenidos personalizados y asegurar que el pedido enviado sea realizado por un usuario registrado.

Resumen: Este caso de uso, exige al usuario que desea realizar un pedido, estar registrado en el sistema. Además permite la identificación del tipo de usuario para mostrarle el contenido adecuado de acuerdo a su perfil, atendiendo a las limitaciones del dispositivo WAP.

Tipo: Primario.

Precondiciones: Ninguna

Referencias cruzadas: 5.4.3.2.1, 5.4.1.3.1

Escenario:

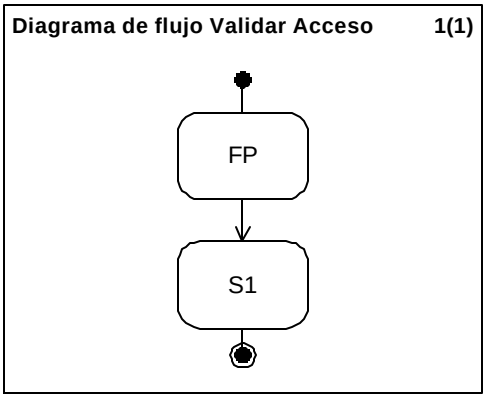

Figura 5-6. Escenario de uso, Validar acceso

Flujo Principal: Cuando el usuario escoge en la interfaz inicial la opción "Ingresar", se despliega la interfaz que le solicita la introducción del "nombre de usuario" y "contraseña".

Figura 5-7. Menú principal

Figura 5-8. Petición de introducción de nombre de usuario y contraseña

La opción Aceptar (Presionar el botón "Yes") solamente se encuentra disponible, cuando el usuario introduce un carácter. Si el usuario escoge la opción Cancelar, vuelve a la interfaz anterior, (FP, Figura 5-7)

Subflujo S1: Menú de usuario

Si la contraseña introducida es correcta [E1], se le despliega al usuario el menú personalizado de acuerdo al perfil almacenado. El menú incluye las opciones:

- Empresas, (Ver empresas)
- Modificar contraseña
- Buscar pedido
- Salir

Figura 5-9. Menú de usuario registrado

Flujo de Excepción E1: Si la contraseña y/o el nombre de usuario no son correctos se le muestra al usuario la siguiente interfaz:

Si el usuario presiona el botón Aceptar, se vuelve a realizar la validación de los datos introducidos, si escoge la opción Cancelar, vuelve al menú principal.

Figura 5-10. Introducción de nombre de usuario o contraseña incorrectos

5.6.2 Modificar contraseña

Actores: Cliente, Agente

Propósito: Permitir al usuario registrado, modificar la contraseña de acceso a su perfil.

Resumen: Por medio de este caso de uso el usuario puede modificar la contraseña de acceso a su perfil. Para esto es necesario que introduzca la contraseña anterior, introduzca la contraseña nueva y posteriormente la confirme.

Tipo: Secundario

Precondiciones:

- El usuario debe ser un usuario registrado
- El usuario debe haber iniciado una sesión antes de intentar cambiar la contraseña

Referencias cruzadas: 5.4.1.2.5, 5.4.1.3.5

5.6.3 Validar acceso

Escenario:

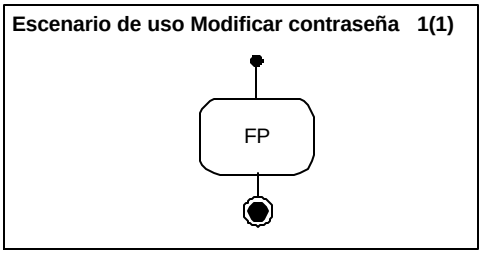

Figura 5-11. Escenario de uso modificar contraseña

Flujo principal FP: Modificar contraseña

Cuando el usuario escoge en el menú principal la opción modificar contraseña, se despliega la siguiente interfaz

Figura 5-12. Modificar contraseña

En esta interfaz, se solicita la introducción de la contraseña actual, posteriormente la nueva contraseña y finalmente la confirmación de esta última.

Si la nueva contraseña es igual a la confirmación, [E1], se despliega la siguiente interfaz:

Figura 5-13. Modificación de contraseña exitosa

Esta interfaz regresará automáticamente después de un tiempo al menú principal; sin embargo, el usuario también lo puede hacer de forma manual escogiendo la opción Volver.

Flujo de excepción E1: Confirmación de contraseña incorrecta

Si la confirmación de la contraseña no es igual a la nueva contraseña, se despliega la siguiente interfaz

Figura 5-14. Modificación de contraseña incorrecta

La opción aceptar se hace disponible, solamente, si el usuario ha introducido algún caracter. Si el usuario escoge la opción Aceptar, se realizará nuevamente la validación de la nueva contraseña y la confirmación de esta; si escoge la opción cancelar volverá al menú principal y no se realizará el cambio de contraseña.

5.6.4 Realizar pedido

Actor: Cliente, Agente

Propósito: Proporcionar al cliente o agente realizar pedidos desde un dispositivo móvil.

Resumen: Este caso de uso permite al cliente o agente realizar la selección de los productos que desea introducir en un carrito de compras y realizar la solicitud de estos, de una forma similar a como se realiza en una tienda convencional. En el caso de los pedidos que realiza un agente, son asignados a un cliente a cargo de dicho agente.

Este caso de uso también permite al usuario navegar por las empresas y productos; sin embargo si no se encuentra registrado no se le permite realizar pedidos.

Tipo: Primario.

Precondiciones:

- Para realizar un pedido, el usuario debe ser un Cliente o Agente autenticado.
- Para enviar la solicitud del pedido debe haber al menos un producto en el carrito de compras.

Referencias cruzadas: 5.4.1.2.2, 5.4.1.3.2

5.6.5 Validar acceso

Escenario:

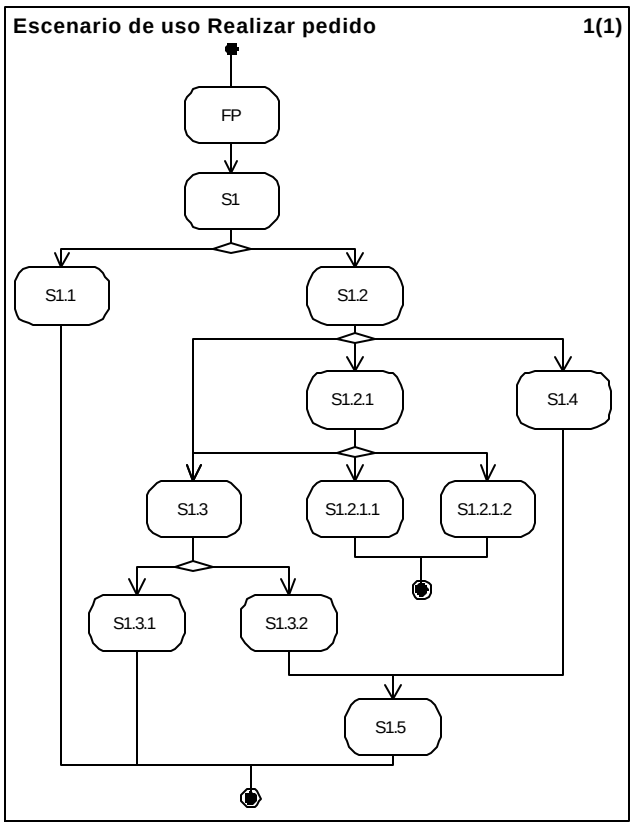

Figura 5-15. Escenario de uso, Realizar pedido

Flujo principal FP: Listar empresas

Después de que el usuario se ha validado como Agente o Cliente de una empresa, tiene la posibilidad de iniciar el catálogo de compras, en este catálogo se incluyen las empresas en las cuales él se encuentra registrado y sus respectivos productos.

La primera interfaz que se muestra al usuario son las empresas en las cuales el se encuentra registrado, en el caso del Cliente; en el del agente no se muestra ésta interfaz ya que solamente pertenece a una empresa[2].

[2] Si un agente desea realizar pedidos a otra empresa, debe estar registrado como un usuario diferente, es decir, debe tener, un nombre de usuario diferente para cada empresa a la que pertenezca.

Figura 5-16. Listado de empresas

En esta interfaz el cliente puede escoger la empresa a la cual desea realizar el pedido una vez el usuario escoge una, se le mostrarán los productos que ésta ofrece.

La opción "Ver carrito de compras" solamente se encuentra disponible cuando el usuario ha adicionado al menos un producto en el carrito de compras.

Subflujo S1: Listar productos

Este subflujo se ejecuta cuando el usuario escoge la empresa a la cual va a realizar el pedido, aquí se muestra una lista de productos que ofrece dicha empresa. El usuario puede escoger, ver el producto en detalle o volver para ver la interfaz anterior, que en este caso es la lista de empresas, (Figura 5-16).

Figura 5-17. Listado de productos de una empresa

Si el usuario escoge la opción "Ver carrito de compras", se le mostrará la interfaz que le permite ver los productos que ha adicionado y los detalles del pedido, (valores, cantidades, etc.).

Subflujo S1.1: Detalles del producto

Esta interfaz se muestra al usuario cuando realiza un clic sobre un producto, (presiona el botón “Yes” cuando el cursor esta sobre un producto), aquí se muestran detalles como: Precio, referencia, empresa proveedora y una breve descripción.

Figura 5-18. Detalles del producto

Esta interfaz es la que permite al usuario adicionar productos al carrito de compras; si el usuario escoge la opción Cancelar, volverá a la interfaz anterior en la que se le muestran los detalles del producto; si escoge la opción adicionar el producto, se le muestra la siguiente interfaz:

Figura 5-19. Confirmación de la adición del producto al carrito de compras

Ésta interfaz regresa al catálogo de productos después de 2 segundos; sin embargo también cuenta con la opción Seguir, para que el usuario lo haga de forma manual.

Subflujo S1.2: Vistas del carrito

Cuando el usuario escoge la opción “Ver carrito de compras”, se le muestra la siguiente interfaz:

Figura 5-20. Vistas del carrito de compras

En esta interfaz se le muestra una lista de opciones para ver el carrito de compras:

Vista por items, en esta vista se muestran todos los items pedidos sin importar la empresa; Vista por empresa, aquí se muestran los productos clasificándolos por empresa; Eliminar productos, esta opción permite al usuario eliminar productos del carrito de compras; Volver a empresas o Volver a productos, dependiendo de donde el usuario haya llamado a esta interfaz; y vista detallada la cual muestra uno a uno de forma detallada los productos que se encuentran en el carrito de compras.

Subflujo S1.2.1: Vista de empresas a las que se les ha realizado pedido

Ha este subflujo se puede llegar desde la interfaz de vistas del carrito, (subflujo S1.2) de dos formas:

- Desde la opción eliminar artículo o,
- Desde la opción ver carrito de compras, por empresas.

Cuando el usuario escoge alguna de estas dos opciones, se le muestra la siguiente interfaz:

Figura 5-21. Listado de las empresas a las cuales se les ha pedido productos

La cual contiene la lista de empresas a las cuales el usuario ha realizado pedido de productos, cuando el usuario escoge una de las empresas listadas, se ejecutará una acción dependiendo de la opción escogida en la interfaz anterior, es decir, si en la interfaz anterior seleccionó eliminar articulo; se mostrará al usuario una lista de los productos pedidos; pero si la opción de la interfaz anterior es ver carrito de compras por empresas, se mostrará al usuario la información detallada del pedido realizado.

Si el usuario ha escogido previamente la opción eliminar productos del carrito la opción “Vaciar carrito”, se hace disponible.

Finalmente si el usuario escoge la opción “Volver a vistas del carrito”, regresará a la interfaz de vistas del carrito, (Figura 5-20).

Subflujo S1.2.1.1: Eliminar producto pedido

Para facilitar al usuario la eliminación de productos del carrito de compras, se le muestra una lista de los productos que ha seleccionado de una empresa, previamente escogida, en la siguiente interfaz:

Figura 5-22. Interfaz de usuario, Eliminar producto

Si el usuario escoge la opción empresas, se le mostrará el listado de empresas de la interfaz anterior, (Figura 5-21); si escoge la opción eliminar se le pide una confirmación, por medio de la cual el usuario puede decidir si continuar con la eliminación del producto o volver a la interfaz anterior.

Figura 5-23. Confirmación de eliminación de un producto del carrito de compras

Subflujo S1.2.1.2: Vaciar carrito

Este subflujo se inicia cuando el usuario escoge la opción vaciar carrito de compras de la interfaz anterior, (Subfujo S1.2.1), entonces se le muestra una interfaz de confirmación, por medio de la cual el usuario puede aceptar o cancelar la eliminación de todos los artículos que contiene el carrito de compras.

Figura 5-24. Confirmación de la eliminación de todos los productos del carrito de compras

Si el usuario escoge la opción aceptar se eliminan todos los productos del carrito de compras y vuelve al catálogo de productos o empresas, según de donde se haya llamado la interfaz de vista del carrito de compras, (Figura 5-16, Figura 5-17); si escoge la opción cancelar, regresa a la interfaz de vistas del carrito de compras, (Figura 5-20).

Subflujo S1.3: Vista por artículos

Este subflujo puede ser iniciado cuando el usuario escoge la opción Vista por items del carrito de compras o después de escoger una empresa, de la cual quiere ver los productos que ha pedido hasta el momento, (Ver carrito te compras>Vista por

empresa>empresa1). En esta vista se muestran detalles de los productos pedidos como:

- Referencia del producto pedido
- Cantidad pedida
- Valor unitario x Cantidad de productos
- Valor total del pedido

Y opciones como:

- Realizar pedido
- Volver a la interfaz anterior
- Ver detalles de un producto

Figura 5-25. Vista por items del carrito de compras

Subflujo S1.3.1: Realizar pedido

Este subflujo se inicia cuando el usuario hace escoge la opción realizar pedido en el subflujo anterior, (subflujo S1.3).

Para el caso del agente, se realiza la petición de introducción del código del agente al cual él va a representar y posteriormente se presenta un informe del estado de la transacción él cual incluye el número asignado a la transacción realizada.

En el caso del Cliente únicamente se le presenta la información del estado de la transacción.

Figura 5-26. Realizar pedido

La opción Aceptar, únicamente aparece cuando el usuario introduce algún carácter; si el usuario escoge la opción Aceptar se realiza la petición del pedido, [E1] y se le da el número de la transacción realizada; si el usuario escoge la opción cancelar, regresa a la interfaz anterior, (Vista por artículos, Figura 5-25)

Subflujo S1.3.2: Detalles del producto pedido

Cuando el usuario escoge ver los detalles del producto, en la interfaz de "Vista del pedido por artículos", (Subflujo 1.3), se le muestran los detalles del producto seleccionado como se muestra a continuación:

Figura 5-27. Detalles del producto pedido

La información presentada incluye:

- Nombre del producto.
- Empresa proveedora
- Cantidad pedida
- Valor unitario
- Descripción del producto

Mediante esta interfaz el usuario puede cambiar la cantidad de productos a pedir.

Si el usuario escoge la opción volver, regresa a la interfaz anterior, (Vista por items, Figura 5-25).

Subflujo S1.4: Vista detallada de productos

En este subflujo se presentan al usuario uno a uno los productos que ha pedido, ordenados por empresa. La información presentada de cada producto es la siguiente:

- Empresa proveedora
- Nombre del producto
- Referencia
- Valor unitario
- Cantidad
- Descripción

Y con las siguiente opciones:

- Modificar cantidad
- Volver a vistas del carrito
- Ir al siguiente producto

Figura 5-28. Vista detallada de los productos del carrito de compras

Subflujo S1.5: Modificar cantidad

Este subflujo se inicia cuando el usuario hace un clic sobre la cantidad del producto, en la vista detallada que se muestra en la interfaz anterior, (Subflujo S1.3.2, Figura 5-27). Su finalidad es permitir al usuario cambiar la cantidad que desea pedir de un producto específico, mediante la siguiente interfaz:

Figura 5-29. Modificar cantidad del producto pedido

La opción Aceptar, únicamente aparece cuando el usuario ha introducido un número, si escoge la opción Cancelar, regresa a la interfaz anterior, (Detalles del producto pedido, Figura 5-27)

Flujo de excepción E1: No existe el código del usuario

En caso de que el agente introduzca un código que no esté registrado, o que no se le haya asignado, se muestra la siguiente interfaz:

Figura 5-30. Código de cliente incorrecto

La cual contiene el siguiente mensaje:

"El código del cliente, que usted ha introducido, no existe o no se le ha asignado. Por favor contacte al administrador de su empresa"

Cuando el usuario hace clic en aceptar, regresa a la interfaz de petición del código del cliente,(Figura 5-26).

5.6.6 Buscar pedido

Actores: Cliente, Agente

Propósito: Permitir al usuario, recuperar un pedido realizado anteriormente, con el fin de que este sea cancelado, (si aun no ha sido atendido por la empresa), o reenviado como uno nuevo.

Resumen: En este caso de uso el usuario puede recuperar los últimos 5 pedidos realizados a una empresa o encontrar un pedido realizado anteriormente. Posteriormente modificarlo para reenviarlo como uno nuevo ó cancelarlo, (solamente en caso de que aún no haya sido atendido por la empresa).

Tipo: Primario.

Precondiciones:

- Debe haberse realizado al menos un pedido.
- Solamente pueden realizar búsqueda de pedidos los usuarios registrados en el sistema.
- Los agentes solamente pueden acceder a los pedidos de los clientes que tienen asignados.

Referencias cruzadas: 5.4.1.2.3, 5.4.1.2.4, 5.4.1.3.3, 5.4.1.3.4

Casos de uso: Validar acceso

Escenario:

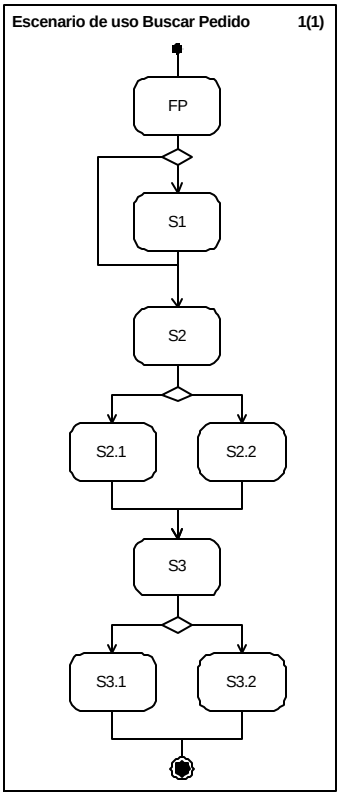

Figura 5-31. Escenario de uso, Buscar Pedido

Flujo principal, FP: Búsqueda de pedido

El caso de uso se inicia cuando el usuario escoge en la interfaz principal, (Figura 5-9), buscar pedido, entonces se le muestra una interfaz que realiza la petición de la letra inicial de la empresa a la cual realizó el pedido que está buscando, en el caso del Cliente; o la petición de introducción del código del cliente , en el caso de Agente.

Figura 5-32. Introducción de la inicial de la empresa

Si el usuario registrado es un Agente, la interfaz inicial, será la siguiente:

Figura 5-33. Introducción del código del cliente

Esta interfaz permite al usuario ingresas el código del cliente del cual desea buscar un pedido.

Si el usuario escoge la opción Aceptar, se iniciará la búsqueda de las empresas que empiezan por el caracter o caracteres introducidos, ó la búsqueda del cliente con el código introducido, [E1]; si por el contrario escoge la opción volver regresará a la interfaz inicial, (Figura 5-9). La opción Aceptar (Presionar el botón “Yes”) solamente se encontrará disponible, cuando el usuario introduce un carácter.

Subflujo S1: Listado de empresas

Aquí se muestra al Cliente una lista de empresas a las cuales ha realizado pedidos y empiezan por la letra que introdujo en la interfaz anterior.

Esta interfaz únicamente se presenta al cliente ya que el Agente solamente tiene acceso a la información correspondiente de la empresa a la cual representa.

Figura 5-34. Lista de empresas

Si el usuario escoge la opción ver, se realizará la búsqueda de los últimos 5 pedidos realizados a esa empresa, [E1], si de lo contrario escoge la opción Volver, se mostrará la interfaz anterior, (Subflujo S5, Figura 5-32).

Subflujo S2: Criterio de búsqueda

Este subflujo se inicia cuando el agente introduce el código de un cliente registrado, (Figura 5-33) o cuando un cliente introduce escoge la empresa a la cual a realizado pedidos, en la interfaz de la Figura 5-34. Aquí se muestra una interfaz que le permite escoger como realizar la búsqueda del pedido por código o listando los últimos 5 pedidos realizados.

Figura 5-35. Selección del criterio de búsqueda de pedido

Si el usuario escoge la opción Volver se mostrará la interfaz anterior, (Figura 5-34 ó Figura 5-33).

Subflujo S2.1: Búsqueda de pedido por código

Esta interfaz le permite al usuario introducir el código del pedido que desea ver, en este tipo de búsqueda el usuario puede buscar cualquier pedido que se encuentre en la base de datos, [E1].

Figura 5-36. Introducción del número del pedido

Si el usuario escoge la opción Volver se le mostrará la interfaz anterior, (Figura 5-35).

Subflujo S2.2: Listado de los últimos 5 pedidos realizados.

En este subflujo se muestra al usuario una lista de los 5 últimos pedidos realizados a la empresa escogida.

Figura 5-37. Listado de los últimos 5 pedidos

Si el usuario escoge la opción Volver se le mostrará la interfaz anterior, (Subflujo S5.2, Figura 5-35).

Subflujo S3: Detalles del pedido buscado

Aquí, se muestra al usuario los detalles del pedido que escogió en la interfaz anterior, es decir productos pedidos, referencias, valores y valor de la factura. El pedido se muestra de una forma similar a cuando se ve el carrito de compras, es decir, que el usuario tiene la posibilidad de modificarlo y reenviarlo; si el producto no ha sido atendido, el usuario tiene la posibilidad de reemplazarlo por el que acaba de enviar, de lo contrario, el pedido se enviará como uno nuevo. De igual forma si el pedido no ha sido atendido la opción cancelar pedido estará disponible.

Figura 5-38. Interfaz de usuario Detalles del pedido

Si el usuario escoge la opción Volver regresará a la interfaz anterior, (Subflujo S2.1, Figura 5-36 ó Subflujo S2.2, Figura 5-37).

Subflujo S3.1: Cancelar pedido realizado

Cuando el usuario escoge esta opción se cancela el envío del pedido realizado, pidiéndole antes una confirmación.

Figura 5-39. Confirmación de cancelación del pedido

Si el usuario escoge la opción cancelar volverá a la interfaz anterior, (Subflujo S3, Figura 5-38).

Subflujo S3.2: Modificar pedido

Con esta opción el usuario puede volver al catálogo de compras para modificarlo, es decir el carrito de compras se habilita nuevamente para que el usuario pueda realizar cambios sobre el pedido, si el pedido ya ha sido atendido, la única opción que tiene el Cliente o Agente es enviar el pedido como uno nuevo, de lo contrario se le pedirá una confirmación para que el pedido sea enviado en reemplazo del último realizado o como uno nuevo.

Figura 5-40. Tipo de envío del pedido

Flujos de excepción:

Flujo de Excepción E1: En caso de que no se encuentren resultados después de la ejecución de una búsqueda, se desplegará al usuario la siguiente interfaz:

Figura 5-41. Búsqueda no exitosa

Esta interfaz regresará automáticamente después de un tiempo a la interfaz que produjo este flujo de excepción; sin embargo, el usuario también lo puede hacer de forma manual escogiendo la opción Volver.

5.7 DIAGRAMA DE IMPLANTACIÓN

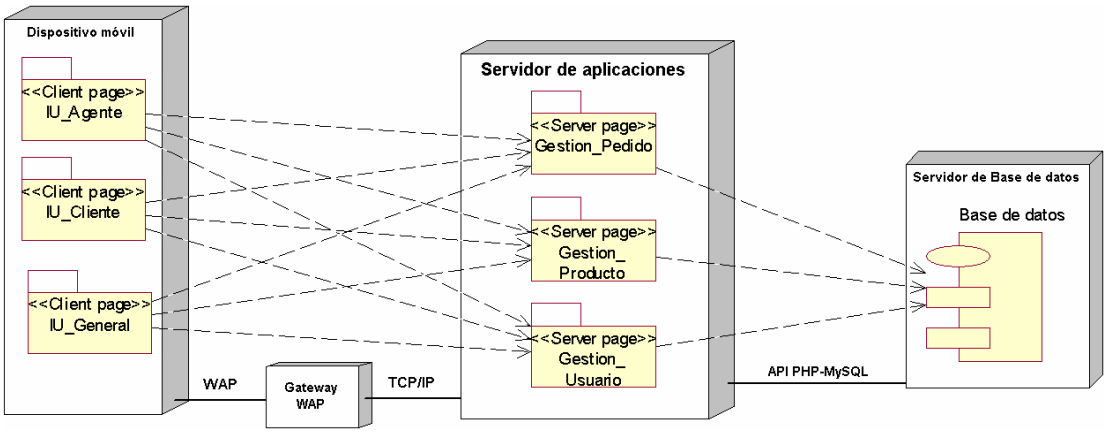

Figura 5-42. Diagrama de implantación

Este diagrama ilustra la distribución física de los componentes del sistema. En primer lugar están las Client page desplegadas en el dispositivo móvil, mediante invocaciones realizadas al servidor de aplicación; en segundo lugar se encuentra una *gateway* WAP la cual hace posible el intercambio de información entre la red fija y la red móvil. Seguidamente está el servidor de aplicaciones el cual alberga las Server page encargadas de construir las Client page. Finalmente se encuentra el servidor de base de datos el cual podría estar implementado en el mismo servidor de aplicación; sin embargo se ilustra de forma separada para describir el caso más general. A continuación se describe en detalle cada uno de estos componentes.

Dispositivo móvil: El dispositivo para el cual fue desarrollada la aplicación, es el R280d de Ericsson, la descripción técnica del dispositivo es la siguiente:

Tipo de acceso	CDPD, TDMA[3].
Versión del naegador	Openwave 3.1
Resolución de la pantalla	101 x 40 pixels
Tamaño del despliegue	3 filas x 15 columnas
Máximo tamaño de. PDU, (Protocol Data Unit)	1492

Tabla 5-1. Descripción técnica del R280d de Ericsson.

Servidor de aplicaciones y de base de datos: Es un PC con sistema operativo *Windows 2000 Professional*, con *Apache Web Server*, como servidor web; *MySQL*, como gestor de base de datos y *PHP*, como lenguaje *scripting* de WML embebido.

En el diagrama también indican los protocolos de comunicación entre componentes hardware. Entre el dispositivo móvil y la gateway se utiliza WAP, (*Wireless Application Protocol*) y entre la gateway y el servidor de aplicaciones se utiliza TCP/IP. Debido a que el servidor de base de datos se encuentra en el mismo servidor de aplicaciones se utiliza el API de PHP para MySQL, para la comunicación entre la paliación y la base de datos.

[3] En Colombia se hace a través de CDPD.

6. CONCLUSIONES, RECOMENDACIONES Y LOGROS

6.1. CONCLUSIONES

Las tecnologías de acceso a Internet desde dispositivos móviles son la próxima gran ola de la tecnología y con ellos el m-commerce puede alcanzar las proyecciones estimadas. Muchas empresas han implementado versiones inalámbricas de sus portales web y se han extendido al reino del m-commerce, ofreciendo a sus clientes, acceso móvil para que puedan realizar transacciones a través de dispositivos inalámbricos a cualquier hora y en cualquier lugar.

Las compañías tradicionales también comienzan a centrarse en iniciativas de m-commerce. Algunas lo hacen para llegar a un grupo más numeroso de clientes que procesen transacciones (por ejemplo, adolescentes), mientras que otras compañías se centran en incrementar el acceso de sus clientes actuales y en mejorar el servicio a los mismos. El e-commerce por sí solo no ofrece el mayor valor a los clientes o la mayor ventaja competitiva a las compañías. Las compañías deberían extender en transacciones de m-commerce ofreciendo diversos recursos relacionados con servicio a través de acceso inalámbrico.

A pesar de la adopción de algunas empresas, del m-commerce, como una nueva forma de hacer negocios, aún hace falta la aceptación por parte de los clientes, de los servicios ofrecidos, esto es debido a que hasta el momento los dispositivos, la red y la infraestructura en general que soporta el m-commerce, no se encuentra del todo preparada para mantener de una forma eficiente y confiable estos servicios, es decir, aún no esta capacitada para satisfacer a plenitud las necesidades de los clientes y sobre todo en el campo B2C, (Business to Consumer).

El éxito del m-commerce estará condicionado a la habilidad de las empresas en crear un modelo de negocios que satisfaga al menos los siguiente aspectos:

- Creación y suministro de servicios independientes de la red que los soporta
- Segmentación de grupos consumidores, de forma tal que permita clarificar cuales son las necesidades más importantes que se deben cubrir en cada grupo y crear soluciones con un evidente valor agregado para cada consumidor.
- Implantación de nuevas plataformas tecnológicas que faciliten el acceso y transacciones en un entorno confiable y seguro.

Teniendo en cuenta las limitaciones de los dispositivos y de la tecnología que actualmente soporta WAP en Colombia; el desarrollo de aplicaciones debe basarse en servicios que exijan escasa interacción con los dispositivos y la red, pero que se perciban como de alto valor agregado, como por ejemplo: aquellos basados en la necesidad de información en tiempo real, (cotizaciones de bolsa, información bancaria, alertas, etc.) y aquellos que contribuyen al apoyo a la fuerza de ventas (B2B, business to business), debido a que es allí donde se puede encontrar un gran potencial de ingresos y economías de escala.

De acuerdo a lo anterior, se desarrollo: iPedidosV1.0, el cual tiene como objetivo incentivar a las empresas a hacer uso de estas tecnologías, especialmente WAP, lo cual permite que Colombia aproveche las ventajas del acceso a Internet desde cualquier lugar y en cualquier momento, “Always-on”.

Este permite a las empresas exponer sus productos a los clientes en un sistema de fácil acceso, según la cobertura del servicio celular se lo permita, y a los clientes las facilidades que trae consigo, el disponer de este servicio las 24 horas del día, de tal forma que sea posible realizar un pedido en cualquier momento, dependiendo de sus necesidades; de esta forma, iPedidos es una nueva alternativa para agilizar los procesos de despacho y venta de los pedidos realizados por un usuario.

Los servicios basados en la posición cubren una inmensa gama de posibles servicios, incluyendo los servicios de proximidad, seguimiento, facturación y

seguridad. Hoy, varias tecnologías están disponibles. Algunas están comercialmente explotables, como el SIM Toolkit o WAP. Algunas no están todavía comercialmente maduras en vista de la necesidad de modificar la infraestructura de la red (EOTD, *Enhanced Observed Time Difference*) o de los terminales (GPS, *Global Positioning System*). En todo caso, cada tecnología de localización tiene su campo preferido de aplicación. En todos estos casos, es vital señalar, como es el caso para las puertas de acceso WAP, que es la composición de la información multifuente enriquecida por la posición y las preferencias del usuario la que hará de los servicios basados en la posición una aplicación clave, ("*Killer application*") para operadores. Los servicios basados en la posición y los de proximidad están introduciendo hoy día un nuevo uso de Internet, con nuevas posibilidades de utilización y oportunidades de negocio. Hemos recorrido un largo camino desde el Internet "tradicional" de los años noventa. Ahora es el momento de la Internet Móvil del Siglo XXI.

Teniendo en cuenta que el m-commerce podría verse como una extensión del e-commerce, el cliente es la base central del desarrollo de aplicaciones; por esto es importante brindar los mecanismos de seguridad suficientes, para que el usuario del sistema, perciba un ambiente confiable; y de fácil uso, es decir coherente con lo ya conocido, (casi intuitivo).

Aunque la, seguridad en los sistemas inalámbricos ha tomado cierta importancia, aún tendrá que afrontar muchos obstáculos. Ya que además de las dificultades que representan la banda estrecha y la baja capacidad de procesamiento de los dispositivos inalámbricos, es necesario tener en cuenta un tercer elemento en la red, la "gateway WAP", la cual representa un punto débil en la infraestructura de la red, debido a que en este punto se hace la traducción del protocolo SSL, (*Secure Sockets Layer*) a WTLS, (*Wireless Transport Layer Security*), dejando los datos vulnerables por un instante.

Aunque el desarrollo de aplicaciones WAP, tiene un futuro prometedor, actualmente no cuenta con las facilidades para mostrar al usuario resultados del todo satisfactorios y atractivos, debido a las limitaciones ya mencionadas. Este obstáculo se hace aún mayor teniendo en cuenta que el usuario espera un servicio muy similar al que ya esta acostumbrado a obtener con el Internet convencional.

Por lo anterior, en el caso de la aplicación WAP, fue necesario pensar en el diseño de interfaces que permitan al usuario ver un servicio funcional, dinámico y de fácil acceso, compitiendo con un teclado poco funcional y un acceso desde el dispositivo móvil al servidor de aplicaciones no muy eficiente. De esta forma, se crearon interfaces que no permiten que el usuario tenga muchas interacciones con el teclado y que reducen al máximo las peticiones que el dispositivo móvil debe hacer al servidor. Ahora bien, no siempre fue posible combinar estos dos aspectos, por lo que en muchos casos dependiendo de la función implementada fue necesario escoger uno de los dos, considerando posibles expansiones del sistema y avances en la tecnología que soporta WAP.

6.2. RECOMENDACIONES

En la siguiente versión de la aplicación WAP, debe contar con un sistema de búsqueda que le permita al usuario encontrar un producto, una empresa o un agente de una forma eficiente y rápida. Para esto es necesario tener en cuenta las preferencias de cada usuario con el fin de reducir la información presentada en cada búsqueda, es decir, se debe mostrar únicamente lo que al usuario le interesa o le podría interesar ver, (en el caso de manejo de publicidad).

Es importante que cuando se disponga de una infraestructura adecuada para el soporte de un nivel de seguridad mayor se implemente en la aplicación WAP el sistema de identificación de usuario, mediante de firmas y certificados digitales, tal como lo especifica el MeT. Con el fin de proteger al usuario y a la entidad prestadora del servicio de fraudes como suplantación, repudiación, etc.

Las interacciones que el usuario tenga que realizar con el teclado del dispositivo celular deben ser mínimas; pero se debe tener en cuenta también, el no exagerar el número de interacciones que el sistema realice con el servidor. Esto debido a las limitaciones tanto de la red prestadora del servicio de transmisión de datos, como del dispositivo inalámbrico.

6.3. LOGROS

En el transcurso del desarrollo del sistema ‡pedidos, se lograron triunfos muy significativos, tanto como para los desarrolladores, integrantes del grupo de interés W@PColombia del GIT, la FIET y la Universidad del Cauca.

El proyecto, participo en eventos como la 3ra. Feria Empresarial de Cauca, realizado en Santo Domingo el 22 de junio del 2001 , en donde el proyecto obtuvo el primer puesto y posteriormente en Expociencia y expotecnología, del 3 al 14 de octubre, del mismo año, en Corferias Bogota, en la cual fue mostrado a entidades de investigación como Colciencias y a diferentes universidades y colegios del país, de forma satisfactoria. Así, podemos afirmar que el desarrollo de este tipo de sistemas tienen grandes probabilidades de éxito y aunque no se disponga de las tecnologías más avanzadas, es posible desarrollar aplicaciones, en este campo, que realmente contribuyan con el desarrollo de nuestro país.

BIBLIOGRAFÍA

- ANDERSON, Christoffer. “GPRS and 3G Wireless Aplications”. Capitulo 14, New York. John Wiley & Sons, Inc, 2001.

- ARTHUR ANDERSEN. *mCommerce Hacia un mundo sin hilos*. [Consulta: diciembre 18 de 2001]. Disponible en: http://www.arthurandersen.com

- GSMBOX. *GSMBOX – mobile news*. [Consulta: febrero 6 de 2002] Disponible en: http://es.gsmbox.com/

- MeT. *“MeT Account-Based Payment” V1.0.* [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MeT. “MeT Authorization for account based payment using a SET Wallet Server” V1.0. [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MeT. “MeT Consistent User Experience” V1.0. [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MeT. “MeT Core Specification” V1.0. [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MeT. “MeT Event Ticketing” V1.0. [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MeT. “MeT PTD Definition” V1.0. [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MeT. “MeT Terminology” V1.0. [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MeT. “MeT WAP Banking” V1.0. [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MeT. “MeT WAP Shopping” V1.0. [Consulta: 17 julio de 2001] Disponible en: http://www.mobiletransaction.org

- MOBILE BUSINESS SERVICES. *mobile-business-services, wireless products and applications.* [Consulta: 30 noviembre de 2001] Disponible en: http://www.mobile-business-services.com/

- NETWORK COMPUTING. *Netmedia - Network Computing Mexico.* Mexico. [Consulta: 20 noviembre de 2001] Disponible en: http://www.netmedia.info/

- NIITTULA, Tommy, Tesis de Maestria: “Extended Mobile Positioning”, Sweden: Institute of Teleinformatics Royal Institute of Technology, Febrero 2001.

- OLAVARRI GUTIÉRREZ, Federico. “Diapositivas Posicionamiento y Localización”. España: Ericsson S.A. Mayo 2001.

- THE FEATURE. *Wireless Devices Present New Security Challenges.* Jason Levitt. *CMP Media Inc.* [Consulta: 17 enero de 2002] Disponible en: http://www.thefeature.com/

- VENTURE DOME . *Venturedome - Home Stream - Analysis*. [Consulta: 19 diciembre de 2001]. Disponible en: http://www.venturedome.com/

- VERISIGN. *WAP Wireless Technology: Security at a New Level.* [Consulta: 30 octubre de 2001]. Disponible en: http://www.verisign.com/

- W@PFORUM. *WAP Developers Area*. [Consulta: Agosto 27 de 2001]. Disponible en: http://www.wapforum.org

ACRÓNIMOS

B2B	Relación de negocios entre proveedores, (Business to Business)
B2C	Relación de negocios proveedor a consumidor, (Business to Costumer)
BTS	Estación Base Transceptora, (Base Transceiver Station)
CA	Autoridad de Ceritificados, (Certificate Authority)
CDMA	Acceso Múltiple por División de Código, (Code Division Multiple Access)
CDPD	Cellular Digital Packet Data.
CeII-ID	Indentificación de Celda Global, (Cell Global Identity)
CUE	Experiencia Consistente de Usuario, (Consistent User Experience)
DGPS	Sistema de Posicionamiento Global Diferencial, (Differential Global Position System)
DS-SS	Señal Serial Directa de Espectro Ensanchado, (Direct Secuence- Spread Spectrum)
EDGE	Velocidades De Datos Mejorados Para Evolución Global (Enhanced Data Rate for Global Evolution)
E-OTD	Difecencia Observada de Tiempo Mejorada, (Enhanced Observed Time Difference)
FCC	Comisión Federal de Comunicación, (Federal Communication Commission)
GPRS	Servicio General de Radio Modo Paquete (General Packet Radio Service)

GPS	Sistema de Posicionamiento Global, (Global Positioning System)
GSM	Sistema Global para Comunicaciones Móviles, (Global System for Mobile Communication)
GTD	Diferencia de Tiempo Geometrica, (Geometric Time Difference)
HTTP	Protocolo de Transferencia de HiperTexto, (Hypertext Transfer Protocol)
IC	Cirtuito Integrado, (Integrated Circuit)
ID	Identificación, (Identification)
IP	Protocolo de Internet, (Internet Protocol)
IrDA	Asociación para Transmisión de Datos Infrarojos, (Infrared Data Association)
LIF	Foro de Estandarización para los sistemas de Localización, (Location Interoperability Forum)
LMU	Unidad de Medida de Localización, (Location Measure Unit)
MAC	Especificación
ME	Equipo móvil, (Mobile Equipment)
MeT	Transacciones electrónicas móviles, (Mobile electronic Transactions)
MMS	Servicio de Mensajería Multimedía, (Multimedia Messaging Service)
MPP	Protocolo de Poscicionamiento Móvil, (Mobile Positioning Protocol)
MPS	Sistema de Posicionamiento Móvil, (Mobile Position System)
MRDP	Modelo de Referencia para el Desarrollo de Proyectos
MS	Sistema Móvil, (Mobile System)
PAP	Protocolo de aplicaciones Push, (Push Application Protocol)
PDA	Asistente digital personal, (Personal Digital Assistant)
PIN	Número de Identifición Personal, (Personal Identification Number)
PKI	Infraestructura de Llave Pública, (Public Key Infrastructure)
PLMN	Red Pública Móvil (Public Land Mobile Network)

PRNG	Pseudo Generador Aleatorio de Números, (Pseudo Random Number Generator)
PTD	Dispositivo personal confiable, (Personal Trusted Device)
RA	Autoridad de Registro, (Registration Authority)
RTD	Diferencia de Tiempo Real, (Real Time Difference)
RTT	Tiempo de Ida y Vuelta, (Round Trip Time)
SAT	Herramienta para Desarrollo de Aplicaciones SIM, (SIM Application Toolkit)
SE	Elemento de Seguridad, (Secure Element)
SET	Secure Electronic Transaction
SIM	Módulo de Identidad de Suscriptor, (Subscriber Identity Module)
SMLC	Sistema de Servicio de Localización Móvil, (Service Mobile Location System)
SMS	Servicio de Mensajería Corta (Short Message Service)
SSL	Capa de conexión segura, (Secure Sockets Layer)
SWIM	Modulo de Identidad de Suscriptor Inalámbrico, (Subscriber Wireless Identity Module)
TA	Tiempo de Ventaja, (Time Advance)
TDOA	Diferencia de Tiempo de Llegada, (Time Difference of Arrive)
TSL	Capa de Transporte Seguro, (Transport Secure Layer)
UML	Lenguaje de Modelado Unificado, (Unified Modeling Language)
UMTS	Servicio Universal de Telefonía Móvil (Universal Mobile Telephone Service)
USB	Bus Serial Universal, (Universal Serial Bus).
USIM	Módulo de Identidad de Suscriptor Universal, (Universal Subscriber Identity Module)

WAP	Protocolo para aplicaciones inalámbricas (Wireless Application Protocol)
WIM	Módulo de Identidad de Suscriptor, WAP (Wap Identity Module)
WPKI	Infraestructura de Llave Pública para aplicaciones inalámbricas, (Wireless Public Key Infrastructure)
WTLS	Capa inalámbrica de transporte seguro, (Wireless Transport Layer Security)