Seguridad basada en parámetros SIM para entornos de comercio electrónico móvil

SIM parameter-based security for mobile e-commerce settings

Francisco Orlando Martínez Pabón,[1] Jaime Caicedo Guerrero,[2] Rodrigo Hernández Cuenca,[3] Oscar Mauricio Caicedo Rendón[4] y Javier Alexander Hurtado Guaca[5]

RESUMEN

Los requerimientos de seguridad son los más exigentes en el dominio del comercio electrónico. Cuando se habla de comercio electrónico móvil los requisitos a nivel de seguridad no solo conservan su nivel de exigencia, sino que se debe mantener un equilibrio entre el grado de seguridad que se requiere y las capacidades de los dispositivos, tanto a nivel hardware como de usabilidad. Estas características exigen el diseño de modelos con un esquema simple de autenticación y autorización transparente para los usuarios, que además garantice la integridad de la información que se intercambia durante cualquier transacción electrónica. Como respuesta a esta necesidad, el Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas W@PColombia, ha desarrollado la plataforma P3SIM con el objeto de brindar las facilidades necesarias para la construcción de aplicaciones móviles seguras basadas en parámetros SIM; a través de un *framework*, un ambiente de compilación y de simulación como sus principales componentes, la plataforma P3SIM combina las ventajas de identificación que proporciona el módulo SIM con las capacidades que en materia de seguridad ofrecen API como SATSA y JavaCard en el entorno Java ME, una de las plataformas más utilizadas en el desarrollo de aplicaciones para dispositivos móviles. Igualmente, a través del desarrollo de un prototipo aplicado al contexto del comercio electrónico móvil, no solo se demuestran las facultades de la plataforma para operar en ambientes seguros sino también su capacidad de adaptación a los requerimientos de seguridad fijados por el entorno.

Palabras clave: cifrado simétrico, cifrado asimétrico, comercio electrónico móvil, firma digital, java card, módulo de identificación de suscriptor, SATSA.

ABSTRACT

Security requirements are more demanding in the e-commerce domain. However, mobile e-commerce settings not only insist on security requirements, they also require balance between security levels and hardware and usability device ability. These features require designing models having simple authentication and authorisation scheme which also ensures information integrity for each e-transaction. The Mobile and Wireless Applications' Development Interest Group W@Pcolombia thus developed the P3SIM platform so that mobile applications might include SIM parameter-based security features. The P3SIM platform's framework and compilation and simulation settings combines the advantages of identification provided by the SIM module with the security features provided by SATSA and Java Card APIs for Java ME environments, one of the most-used platforms for mobile application development. Developing an m-commerce-based prototype not only shows the platform's ability to operate in secure environments, it also shows its ability to comply with environmental security requirements.

Keywords: symmetrical coding, asymmetric coding, mobile e-business, digital sign, java card, subscriber identification module, SATSA.

Recibido: agosto 17 de 2006
Aceptado: abril 27 de 2007

[1] Ingeniero en electrónica y telecomunicaciones y Estudiante M. Sc., Ingeniería, Área Ingeniería Telemática, Universidad del Cauca, Colombia. Docente, Departamento de Telemática, Universidad del Cauca, Colombia. Coordinador, Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas, W@PColombia. Investigador, Grupo de Ingeniería Telemática, GIT. Socio Fundador, Software Architect de la Empresa Software Mobile Solutions, Parquesoft. fomarti@unicauca.edu.co

[2] Ingeniero en electrónica y telecomunicaciones, Universidad del Cauca, Colombia. Investigador, Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas, W@PColombia. Ingeniero de desarrollo de aplicaciones móviles, Toppmobile S.A., jcaicedo@unicauca.edu.co

[3] Ingeniero en electrónica y telecomunicaciones, Universidad del Cauca, Colombia. Investigador, Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas –W@PColombia. Ingeniero de Desarrollo, Colombia Games. rhernandez@unicauca.edu.co

[4] Ingeniero en electrónica y telecomunicaciones, Especialista, en Redes y Servicios Telemáticos y M. Sc., en Ingeniería, Área Ingeniería Telemática, Universidad del Cauca, Colombia. Docente, Departamento de Telemática - Universidad del Cauca, Colombia. Coordinador, Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas, W@PColombia. Investigador, Grupo de Ingeniería Telemática, GIT. Socio Fundador y Director de Proyectos, Empresa Software Mobile Solution, Parquesoft. Asesor de Proyectos, Empresa Seratic Ltda. omcaicedo@unicauca.edu.co

[5] Ingeniero en electrónica y telecomunicaciones, Especialista en Redes y Servicios Telemáticos y Estudiante M. Sc., en Ingeniería, Área Ingeniería Telemática, Universidad del Cauca, Colombia. Docente Departamento de Telemática, Universidad del Cauca, Colombia. Director, Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas –W@PColombia. Investigador, Grupo de Ingeniería Telemática – GIT. Socio Fundador, Software Developer de la Empresa Software Mobile Solutions – Parquesoft. javhur@unicauca.edu.co

Introducción

El medio inalámbrico que utilizan los servicios móviles los hace más susceptibles a problemas relacionados con seguridad en comparación con los medios cableados. Uno de los entornos donde la seguridad es un factor clave, es precisamente el comercio electrónico móvil. Los mecanismos de seguridad en el escenario móvil han tenido una evolución continua y especialmente importante en los últimos años, dada la motivación que ha surgido en torno a las aplicaciones de comercio electrónico (Baudín de la Lastra, 2005; Sutton, 2005); desde que ingresó al mercado la telefonía celular digital GSM a inicios de los años noventa, se ha prestado especial atención a los mecanismos que garantizan la seguridad de las comunicaciones tanto de voz como de datos, con estándares como el GSM 02.48 (SIM Toolkit Secure Messaging; ETSI, 1999).

Sin embargo, una solución segura en el ámbito del comercio electrónico móvil no solo se reduce a un problema de construcción de mecanismos de seguridad más complejos (v.g. Certificados digitales, algoritmos de cifrado), sino que debe existir un balance entre el nivel de seguridad que se ofrece y las limitaciones de los dispositivos móviles. Estas limitaciones no solo están relacionadas con el rendimiento (capacidad de procesamiento y memoria), sino también con la usabilidad. Las limitaciones del teclado numérico del teléfono pueden conducir a los usuarios a una selección poco rigurosa de sus claves de acceso, prefiriendo contraseñas cortas, por ejemplo, que no son precisamente las más seguras.

Es necesario diseñar un modelo de autenticación más simple y transparente para al usuario, al tiempo que se garantice la integridad y el no repudio de la información que se intercambia en un entorno de comercio electrónico móvil. Para satisfacer esta necesidad, el Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas W@PColombia, perteneciente al Grupo de Ingeniería Telemática (GIT) de la Universidad del Cauca, ha diseñado la plataforma P3SIM para facilitar el desarrollo de aplicaciones móviles seguras basadas en parámetros del Módulo de Identificación de Suscriptor (SIM), proponiendo un modelo de autenticación transparente para el usuario, ajustado a la usabilidad y seguridad que requieren entornos tan exigentes como el comercio electrónico móvil. Este trabajo constituye un complemento importante a otros proyectos que se han realizado al interior del grupo en el área del comercio electrónico móvil, específicamente en el campo de seguridad (plataforma Mercurio; Caicedo, Cerón, Chamorro, Martínez y Hurtado, 2006) y la adaptación de algunos procesos ligados al sector de artesanía en el entorno móvil (Caicedo, Martínez, Gómez y Hurtado, 2005).

A continuación, en la primera parte, se presentan algunas generalidades sobre seguridad en entornos de comercio electrónico móvil; luego se plantean los modelos de autenticación para aplicaciones de comercio electrónico móvil y se describen los componentes fundamentales de la plataforma P3SIM; posteriormente se describe un prototipo de comercio electrónico móvil construido con P3SIM, para finalmente exponer algunos trabajos futuros y las conclusiones del trabajo realizado.

Generalidades sobre seguridad en entornos de comercio electrónico móvil

El comercio electrónico móvil o *m-commerce* se define como: *Cualquier transacción con valor cuantificable económicamente que se ejecuta por medio de la Red de Telecomunicaciones Móviles* (Baudín de la Lastra, 2005). El comercio electrónico móvil no es más que una respuesta de las telecomunicaciones ante las tendencias sociales presentes, ya que cada día existen más personas que por sus hábitos laborales y de vida se encuentran en continuo movimiento y no disponen de mucho tiempo. En general, se puede hablar del comercio electrónico móvil como una variante del comercio electrónico convencional, donde los aspectos básicos que garantizan el éxito del servicio son: el atractivo, la utilidad de los contenidos y el nivel de seguridad ofrecido al usuario (Shaffer, 2000).

Otra característica de gran importancia es procurar un acceso universal que garantice la disponibilidad del servicio desde cualquier dispositivo móvil, y que los consumidores sean reconocidos como usuarios únicos independientemente del dispositivo de acceso. A esta característica se la denomina multiacceso, y es considerada un requisito básico para cualquier proveedor de comercio electrónico móvil, como una nueva estrategia para la captación de clientes. Las aplicaciones más comunes del comercio electrónico móvil están representadas fundamentalmente por la compra de artículos en portales o tiendas virtuales, mercadeo sensible con respecto a la ubicación geográfica del cliente, transacciones bancarias y recepción de información desde sitios *web*, como por ejemplo, resultados de apuestas, acciones de la Bolsa, noticias, etc.

Problemas que enfrenta el comercio electrónico móvil

A pesar de todas las ventajas que presenta el comercio electrónico móvil y las expectativas que genera en un futuro próximo, existe una serie de factores que dificultan su implantación y desarrollo frente a las soluciones de comercio electrónico convencionales (Anonymous, 2002). Estos inconvenientes están relacionados con las características del entorno inalámbrico (menor ancho de banda, latencia más baja, menos estabilidad en las conexiones, disponibilidad menos previsible) y limitaciones de los teléfonos móviles (procesadores menos potentes, menor capacidad de memoria, limitaciones en el consumo de potencia, pantallas de tamaño reducido; Ghosh, 2001), pero más allá de estos factores, el talón de Aquiles del comercio electrónico móvil está asociado sin lugar a dudas al tema seguridad (Ponce, 2002).

Para acceder a los servicios móviles es necesario establecer una comunicación de datos entre dos entidades, para lo

cual se requiere de al menos tres elementos básicos: el emisor del mensaje, el receptor del mismo y un soporte físico por el cual se transfieren los datos. En el caso de acceso a servicios móviles la comunicación se realiza a través de un medio inalámbrico, lo cual implica un riesgo mayor para la información que en los entornos alambrados. Técnicas como *Bluejacking* (envío de mensajes a dispositivos *bluetooth* sin autorización), *BlueSnarfing* (aprovecha el modo visible de un dispositivo *Bluetooth* para extraer información) o los mismos virus informáticos, son prueba de ello (Peláez, 2005, pp. 4-5).

Para la prestación de servicios de comercio electrónico móvil de forma segura se deben tener en cuenta cuatro aspectos básicos (Moreno, 2005), (Caicedo, Cerón, Chamorro, Martínez y Hurtado, 2006):

Autenticidad: todas las entidades participantes en una transacción deben estar debidamente identificadas antes de iniciar el proceso, con el objeto de evitar la transferencia de datos confidenciales a una persona o entidad no deseada que pueda hacer uso malintencionado de los mismos.

Confidencialidad: los datos enviados en una comunicación no deben ser leídos por una persona o entidad distinta al destinatario final; si esto ocurre, el espía no debe tener la capacidad de entender el mensaje enviado.

Integridad: es necesario asegurar que los datos enviados en una comunicación lleguen sin modificaciones a su destino final. Esto implica que la información no ha sido alterada, borrada, reordenada o copiada en el transcurso.

No repudio: se debe asegurar que una vez enviado un mensaje con datos importantes o confidenciales el destinatario de los mismos no pueda negar haberlos recibido, o en el caso del emisor este no pueda negar haberlos enviado.

Mecanismos de cifrado

Debido a las vulnerabilidades que existen en el entorno en el cual se ejecutan los servicios de comercio electrónico móvil, uno de los procesos más importantes es el cifrado de la información. Los mecanismos de cifrado se dividen en dos grandes grupos (Fúster, Martínez, Encinas, Montoya y Muñoz, 2001):

Simétrico: es aquel en donde se utiliza la misma clave tanto para cifrar como para descifrar la información.

Asimétrico: se basa en la infraestructura de clave pública PKI, donde se utiliza una pareja de claves: una pública, conocida por todos, y otra privada, sólo conocida por el usuario a quien le es asignada. Un mensaje puede ser cifrado por cualquier persona usando la clave pública ya que es globalmente conocida, aunque únicamente el poseedor de la clave privada podrá descifrarlo. Recíprocamente, un mensaje cifrado con la clave privada sólo puede ser cifrado por su poseedor, mientras que puede ser descifrado por cualquiera que conozca la clave pública.

Debido a que el cifrado asimétrico es computacionalmente costoso (lo que redunda en grandes tiempos de procesamiento), se acostumbra a utilizar una combinación de cifrado simétrico con asimétrico, proceso conocido como cifrado híbrido. Mediante el cifrado de clave pública se comparte una clave para el simétrico. En cada mensaje la clave simétrica utilizada es diferente, por lo que si un atacante pudiera descubrir la clave simétrica meramente le valdría para ese mensaje y no para los restantes. PKI (Public Key Infraestructure) usa sistemas de cifrado híbridos. La clave simétrica es cifrada con la pública, y el mensaje saliente es cifrado con la simétrica, todo combinado automáticamente en un solo paquete. El destinatario usa su clave privada para descifrar la simétrica y acto seguido usa la simétrica para descifrar el mensaje.

Otro mecanismo para brindar seguridad a las transacciones realizadas en redes como Internet es la firma digital. Su finalidad es la de garantizar la autoría de la misma y la integridad de grandes cantidades de datos. Un mensaje firmado es completamente legible, no está cifrado, es como una postal firmada. Para generar una firma digital lo primero que se hace es generar un resumen o *hash* del mensaje a firmar. Dicho resumen es mucho más pequeño (de 128 a 160 bits) que el mensaje original, irreversible (del *hash* no se puede obtener el mensaje), y es muy difícil encontrar otro que tenga el mismo resumen. El proceso que sigue es cifrar dicho *hash* con una clave asimétrica, la privada. Finalmente se envía al destinatario el mensaje, la firma y un certificado digital del emisor. Para verificar la firma se hace el proceso inverso, es decir, la firma se descifra con la clave pública del certificado digital y se obtiene un *hash*. Luego se calcula el *hash* del mensaje a comprobar y finalmente se compara con el *hash* anterior. Si son iguales se garantiza que el que lo firmó fue el poseedor de la clave privada (ya que se ha podido descifrar con la pública) y que el documento no ha sido modificado (ya que los *hash* coinciden). Si cualquiera de estas dos condiciones no se cumplen se obtiene lo que se suele llamar una "rotura de firma".

Niveles de seguridad

La filosofía que se maneja en muchas ocasiones en el comercio electrónico móvil es: "un leve retardo es un precio pequeño a pagar por una transacción segura". Para adoptar las medidas de seguridad adecuadas los diseñadores de servicios de comercio electrónico móvil deben encontrar un balance entre las expectativas de los usuarios con respecto al rendimiento de las aplicaciones y las implicaciones de la seguridad de una transacción. Esto causará que los servicios se ubiquen dentro de uno de varios estratos según las necesidades de seguridad requeridas en el servicio móvil (Hattangady y Davis, 2002).

*Seguridad de bajo nivel***.** Cuando la información importante o personal no está en peligro o el valor de una transacción es bastante bajo, la seguridad de una aplicación se puede salvaguardar adecuadamente con técnicas como el cifrado

simétrico. Es usado básicamente en compras pequeñas y transacciones en puntos de venta (v.g., la compra de boletos para el cine). Los usuarios de esta categoría en el mercado se caracterizan por su impaciencia.

Seguridad de nivel medio. Una aplicación de billetera electrónica, que almacena en el dispositivo móvil información personal como el número de la licencia de conducción, tarjeta de crédito y el pasaporte, es ejemplo típico de una aplicación con necesidades de seguridad de medio nivel. La adición de técnicas de seguridad más complejas se obtiene a expensas de la sensibilidad y el retraso de las operaciones generales del dispositivo del cliente.

*Seguridad de alto nivel***.** Las aplicaciones con estas necesidades de seguridad generalmente deben utilizar módulos dedicados HW/SW (*Hardware*/*Software*) de seguridad constituidos por generadores *hardware* de números aleatorios; memoria *hardware* protegida, donde las claves pueden ser almacenadas, y canales seguros de entrada-salida. El módulo SIM (Suscriptor Identification Module) en redes GSM, RUIM (*Removable User Identity Module*) para redes CDMA (*Code Division Multiple Acces*) o UICC (*Universal Integrated Circuit Card*) para redes UMTS (*Universal Mobile Telecommunications System*) es un ejemplo de este tipo de elementos de seguridad.

Modelos de autenticación para entornos de comercio electrónico móvil

En general para hacer uso de cualquier servicio de comercio electrónico móvil lo primero que el usuario debe hacer es autenticarse ante el proveedor del servicio. Desde esta perspectiva, el modelo tradicional de autenticación sugiere la utilización de un *login* y un *password* bajo dos aproximaciones:

- Digitando la información de autenticación (*login* y *password*) cada vez que se quiera hacer uso del servicio.
- Digitando la información de autenticación tan solo la primera vez que se hace uso del servicio, de forma tal que la aplicación almacene estos datos en algún tipo de repositorio (como un *RecordStore* en una aplicación Java ME) (Muchow, 2001, pp. 271-273), haciendo innecesario el posterior ingreso de los mismos.

La primera aproximación tiene serios inconvenientes desde el punto de vista de usabilidad; dadas las limitaciones de introducción de texto a través del teclado numérico del teléfono móvil, la digitación continua del *login* y el *password* se traduce en desperdicio de tiempo e incluso dinero por el uso de la red cuando algunos de los parámetros es incorrecto y se requiere una nueva introducción de ellos. Igualmente, como una consecuencia directa de este comportamiento, los usuarios pueden optar por utilizar contraseñas cortas, fáciles de recordar pero también fáciles de vulnerar. En cuanto a la segunda aproximación, aunque corrige de alguna manera el problema de usabilidad de la primera, tiene el inconveniente de almacenar los parámetros en un repositorio local que puede ser vulnerado en cualquier momento.

Autenticación basada en parámetros SIM

A través de la plataforma P3SIM, que será descrita posteriormente, se propone un nuevo modelo de autenticación que busca mejorar la usabilidad del modelo tradicional al tiempo que garantiza una protección efectiva de la información. En este caso, el componente más importante en el proceso de autenticación es la tarjeta SIM del teléfono móvil. El Módulo de Identificación de Suscriptor (SIM), brinda a los usuarios de las redes de telefonía móvil una verdadera movilidad e independencia y se convierte en un elemento de identidad único de los usuarios frente a la red de su operador; a través de este modelo de autenticación se propone que los parámetros almacenados en la SIM puedan hacer parte del proceso de identificación no solo ante el operador sino también ante los proveedores de servicios de comercio electrónico móvil.

Las tarjetas SIM son una clase especial de tarjetas inteligentes con una CPU de 8/16 bits y frecuentemente con capacidades de memoria EEPROM entre 32 y 64 kilobytes. En cuanto a la estructura lógica, los archivos en la SIM están organizados en una estructura jerárquica y pueden ser de tres tipos: MF (archivo maestro), DF (archivo dedicado) o EF (archivo elemental). La Figura 1 muestra las relaciones estructurales generales que pueden existir entre estos archivos, los cuales están compuestos por un encabezado que define la estructura y atributos del mismo, internamente manejado por la SIM, y opcionalmente por un cuerpo que contiene los datos del archivo.

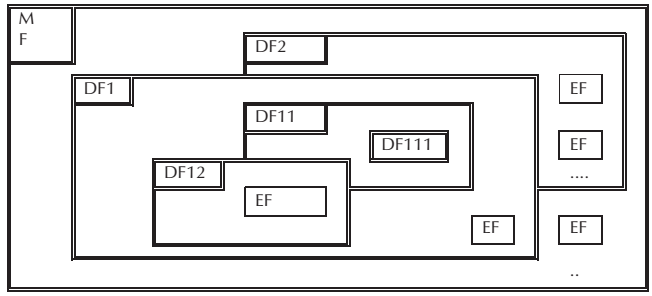

Figura 1. Relaciones estructurales de los archivos en la SIM

La esencia del esquema de autenticación basado en parámetros SIM consiste en brindar a las aplicaciones que acceden a servicios de comercio electrónico móvil el acceso a dos parámetros que identifiquen unívocamente a cualquier usuario; se debe gestionar un parámetro de conocimiento público y otro de conocimiento restringido. Después de un estudio profundo de los archivos almacenados en la tarjeta SIM se llegó a la conclusión de que los dos parámetros que cumplen estas condiciones son el ICCID (*Identification Integrated Circuit Card*) y el IMSI (*International Mobile Subscriber Identity*).

El ICCID es un archivo de diez bytes que no tiene ningún tipo de restricción para ser leído pero no puede ser modificado; esta característica lo convierte en un candidato ideal para ser usado de alguna manera como el *login* del usuario. El IMSI es

un parámetro de ocho bytes (en la mayoría de los casos) que sólo puede ser leído mientras se haya introducido el CHV1 (o PIN), lo que implica que si por alguna razón un usuario pierde su SIM, el IMSI no podrá ser leído (a menos que el CHV1 sea introducido correctamente) (3GPP, 2005).

De acuerdo a este modelo, durante el proceso de autenticación el dispositivo móvil le envía al proveedor del servicio los parámetros SIM y crea una clave que se almacena en la tarjeta, lo cual es transparente al usuario. Para acceder de forma segura al servicio de comercio electrónico móvil se crea una clave simétrica con base en el IMSI, (ocho bytes que se pueden utilizar en cualquier orden y repitiéndose de la forma que quiera definir el proveedor del servicio, según sea la longitud para la clave requerida) que debe ser manejada por el dispositivo móvil (gestionándola en la tarjeta SIM) y por el proveedor del servicio. Una vez se crea la clave simétrica el dispositivo móvil logra acceder de forma segura al servicio cifrando cualquier información de común acuerdo entre los actores del sistema. Para la realización de transacciones se pueden utilizar diferentes mecanismos de acuerdo al nivel de seguridad requerido y al volumen de información intercambiado. Por ejemplo, si se requiere enviar una gran cantidad de información sin importar la confidencialidad pero se debe garantizar el no repudio y la integridad de la misma, se puede recurrir a la firma digital.

Para llevar a acabo la implementación del modelo, es necesario dotar a las aplicaciones de las capacidades necesarias para acceder a los parámetros de la SIM. En el próximo apartado se describen las tecnologías adoptadas por P3SIM para llevar a cabo este proceso.

Tecnologías para la implementación de un modelo de autenticación basado en SIM

SIM Application Toolkit (SAT) y Java Card

Los organismos de estandarización de las redes de telefonía celular como la ETSI[6] y el 3GPP[7] han definido estándares para la arquitectura, funcionalidad, desarrollo y ciclo de vida de las aplicaciones que residen en el módulo SIM, dando origen a herramientas como SAT (SIM Application Toolkit), el cual es definido en la especificación técnica GSM 11.14 (ETSI, 1996). SAT especifica y define una serie de interfaces que garantizan la interoperabilidad entre el módulo SIM y el equipo móvil independientemente del fabricante de uno u otro elemento. Sin embargo, los procedimientos definidos por SAT sólo facilitan a las aplicaciones el acceso a servicios básicos de voz y mensajería corta (SMS) (Guthery, 2001).

Dada la necesidad de interoperabilidad, portabilidad y facilidad de programación de aplicaciones para tarjetas inteligentes como la SIM que provienen de diversos fabricantes, nace Java Card (Attali, Caromel, Courbis, Henrio y Nilsson, 2001), una respuesta de la famosa plataforma de desarrollo Java (Gosling, Bill, Steele y Bracha) a las limitadas capacidades de las tarjetas inteligentes, incluyendo por supuesto los módulos SIM. La plataforma Java Card fue diseñada y desarrollada desde un principio, específicamente para proporcionar seguridad a las tarjetas inteligentes. Como una plataforma neutral, la tecnología Java Card está implementada sobre una amplia diversidad de soluciones para tarjetas inteligentes ofreciendo varios niveles de seguridad. Las características modernas del lenguaje de programación Java proporcionan un rico arreglo de herramientas de desarrollo confiable y seguro de aplicaciones. La Java Card Virtual Machine separa la aplicación de los niveles inferiores de *hardware* y el sistema operativo. El Java Card API estándar provee una interfaz uniforme para tarjetas inteligentes heterogéneas, y por otro lado, agrega facilidades específicas para el manejo de transacciones con tarjetas inteligentes (atomicidad de un grupo de operaciones, objetos persistentes, *Applet firewall*, cifrado simétrico/asimétrico, firma digital, etc.) (Chen, 2005).

La especificación GSM 03.19 define el SIM API, una extensión del API Java Card, el cual le permite a los programadores de aplicaciones acceder a las funciones y datos descritos en la especificación técnica 11.11 (3GPP, 2005) y 11.14 (3GPP, 2004) de tal forma que los servicios basados en SIM se puedan desarrollar y cargar sobre la tarjeta rápidamente, y si es necesario, de forma remota una vez que la tarjeta SIM Java Card ha sido emitida.

Java ME y SATSA

La especificación SATSA (*Security and Trust Services API*), definida a través de JSR-177 (*Java Specification Request* 177; JSR 177 Expert Group, 2004, pp. 1-3), establece una serie de paquetes opcionales para la plataforma Java ME (Java Micro Edition). El propósito principal es especificar una colección de API que proporcionen servicios de confianza y seguridad a través de la integración de un elemento de seguridad denominado SE (*Security Element*). Un SE es un componente en un dispositivo Java ME que provee los siguientes beneficios:

- Almacenamiento seguro de datos confidenciales, tales como llaves privadas de usuario, certificados de claves públicas, credenciales, información personal y otros.
- Operaciones criptográficas que soportan protocolos de pagos, integridad de datos y confidencialidad de datos.
- Un ambiente de ejecución para el despliegue de funcionalidades relacionadas con seguridad.

[6] ETSI (European Telecomunication Standard Institute). http://www.etsi.org

[7] 3GPP (3rd Generation Partnership Project). http://www.3gpp.org

Un SE puede ser representado de varias formas. Las tarjetas inteligentes son las más usadas comúnmente para implementar un SE ya que están ampliamente desplegadas en los teléfonos móviles. Alternativamente, un SE puede estar totalmente implementado en *software*. Esta especificación no excluye cualquiera de las posibles implementaciones para un elemento de seguridad; sin embargo, algunos de los paquetes son optimizados para implementarse en tarjetas inteligentes.

La plataforma P3SIM

El Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas – W@PColombia, de la Universidad del Cauca, desarrolló la plataforma P3SIM con el objeto de brindar a los desarrolladores de servicios móviles sobre redes de 2.5G y 3G las facilidades necesarias para implementar las características de seguridad que requieren, basado en un modelo de acceso con parámetros SIM. Para cumplir este objetivo, la Plataforma de Seguridad para Servicios Móviles basada en SIM Card P3SIM ha sido estructurada en tres componentes principales (Caicedo y Hernández, 2006):

- Un *framework* para construcción de aplicaciones.
- Un ambiente de compilación Java Card.
- Un ambiente de simulación.

El *framework* ofrece una interfaz de programa de aplicación (API), que tiene asociado un Applet Java Card alojado en la tarjeta SIM y un grupo de clases Java ME que implementan un conjunto de métodos de alto nivel para el manejo de cifrado/descifrado simétrico o asimétrico y el manejo de firma digital. El ambiente de compilación es de uso opcional, y permite un proceso de compilación sencillo para un Applet Java Card en caso de que el proveedor de servicio quiera manejar un Applet propietario. El ambiente de simulación se crea debido a la inexistencia de una herramienta que permita simular en un ambiente de desarrollo de aplicaciones Java ME el acceso a parámetros GSM y el uso de cifrado asimétrico dentro de la tarjeta SIM. Este ambiente de simulación se complementa con el entorno Aspects Developer (Aspects Software, 2006).

Como se muestra en la Figura 2, la arquitectura del *framework* P3SIM está compuesta por las siguientes clases:

- *SECApplet*: es una clase Java Card que implementa todas las facilidades criptográficas y SAT (SIM Application Toolkit) que serán utilizadas, como por ejemplo, almacenamiento y generación de claves, cifrado asimétrico y acceso a parámetros GSM.
- *P3SIM*: es la clase principal de la plataforma, esta provee los métodos estáticos que pueden ser invocados por los desarrolladores que deseen hacer uso del *framework*.
- *ResourceManager*: clase encargada del manejo de los recursos necesarios para instalar el SECApplet en la tarjeta SIM.
- *CommManager*: clase encargada del manejo de las comunicaciones entre la clase P3SIM y el Applet de seguridad SECApplet instalado en la tarjeta SIM del móvil. Para realizar sus tareas se soporta en la clase BeanConnector.
- *BeanConnector*: clase que realiza los procesos de comunicación con el Applet de seguridad a bajo nivel, manipula los datos y los bytes necesarios para la generación de las *command* APDU con las cuales se comunica P3SIM y el Applet de seguridad instalado en la tarjeta SIM.
- *SymmetricManager*: clase encargada del manejo de la criptografía simétrica, posee métodos necesarios para el cifrado y descifrado utilizando el algoritmo DES.
- *DigestManager*: clase encargada de la generación de *MessageDiggest* utilizando el algoritmo SHA-1, además permite la comparación de dos *MessageDiggest* a fin de verificar la validez de una firma.

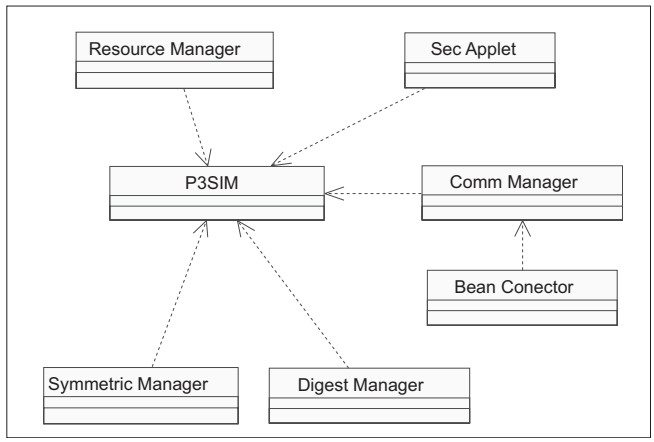

Figura 2. Arquitectura del framework P3SIM

A través de este *framework*, la plataforma P3SIM ofrece actualmente los siguientes servicios:

- Obtener parámetros del módulo SIM como el IMSI, ICCID, LOCI (Location Information) y el SST (SIM Service Table).
- Crear, obtener o actualizar dos claves DES, un par de claves RSA (de 1.024 bits) del usuario y una clave pública RSA de otra entidad.
- Cifrar y descifrar información de forma simétrica con cualquiera de las dos claves DES. Así se logra garantizar la integridad y confidencialidad de la información.
- Cifrar y descifrar información con cualquiera de las tres claves RSA, lo que permite intercambiar información entre la aplicación Java ME y el proveedor del servicio, garantizándose la integridad, confidencialidad de la información y el no repudio.
- Calcular y verificar una firma digital con el objeto de garantizar la integridad de grandes cantidades de información recibidas desde el proveedor del servicio y el no repudio.

Dadas las características de la plataforma P3SIM, se plantea una arquitectura de referencia en capas para el desarrollo de aplicaciones seguras en entornos de comercio electró-

nico móvil que acceden a los parámetros SIM del teléfono (Figura 3).

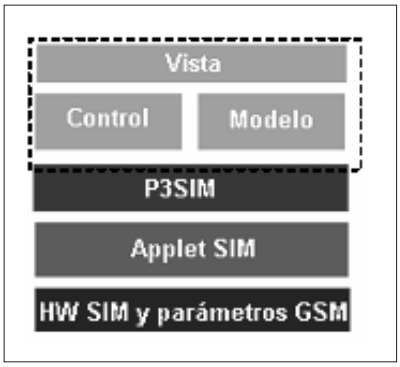

Figura 3. Arquitectura de referencia para el desarrollo de aplicaciones seguras con P3SIM

En la parte baja de la torre se encuentra el *hardware* de la SIM (que incluye a los métodos nativos) y los parámetros GSM, dentro de los cuales son de especial interés el IMSI y el ICCID. La siguiente capa la conforma un Applet Java Card que implementa los métodos para acceder a los parámetros SIM, permite gestionar claves simétricas, asimétricas, certificados digitales, y cifrar pequeñas cantidades de información con criptografía asimétrica. La siguiente capa está conformada por el *framework* P3SIM, que se encarga de abstraer la complejidad del intercambio de bytes entre el móvil y la tarjeta SIM y además implementa los métodos de cifrado simétrico y generación de *hash* (usado en la firma digital). En los siguientes niveles se encuentra el dominio de la aplicación, ilustrado a través del patrón Modelo-Vista-Control (MVC), uno de los más utilizados en el área de desarrollo de aplicaciones para dispositivos móviles.

Prototipo de validación de comercio electrónico móvil

En esta sección se describe un prototipo de servicio de comercio electrónico móvil que emplea el modelo de autenticación basado en parámetros SIM. En términos generales, el prototipo hace uso de las APIs de SATSA (a través del *framework* P3SIM) para comunicarse con un Applet Java Card en la tarjeta SIM, según lo planteado en la arquitectura de referencia. Para el prototipo se utilizaron tarjetas USIMERA de Axalto con soporte para Java Card. En la Figura 4 se exhibe la arquitectura de la aplicación que reside en el teléfono móvil, y la Figura 5 ilustra el diagrama de casos de uso del prototipo implementado.

El prototipo se basa en una arquitectura simple en la cual la clase ECommerceMIDlet controla el ciclo de vida de la aplicación y accede a las facilidades de la plataforma P3SIM para comunicarse con el módulo SIM e ingresar al servicio. Las clases restantes gestionan la interfaz gráfica de la aplicación.

Como se puede observar en el diagrama de casos de uso del prototipo, se propone un modelo mediante el cual el usuario realiza inicialmente una suscripción al servicio de comercio electrónico móvil. Durante este proceso, introduce sus datos personales, los cuales son enviados por la aplicación al servidor adicionando los parámetros IMSI e ICCID del módulo SIM para que sean registrados por parte del proveedor. Cuando el usuario desea acceder al servicio posteriormente, el proceso de autenticación estará basado en estos parámetros SIM, evitando el uso de un *login* y contraseña como se plantea en el modelo tradicional.

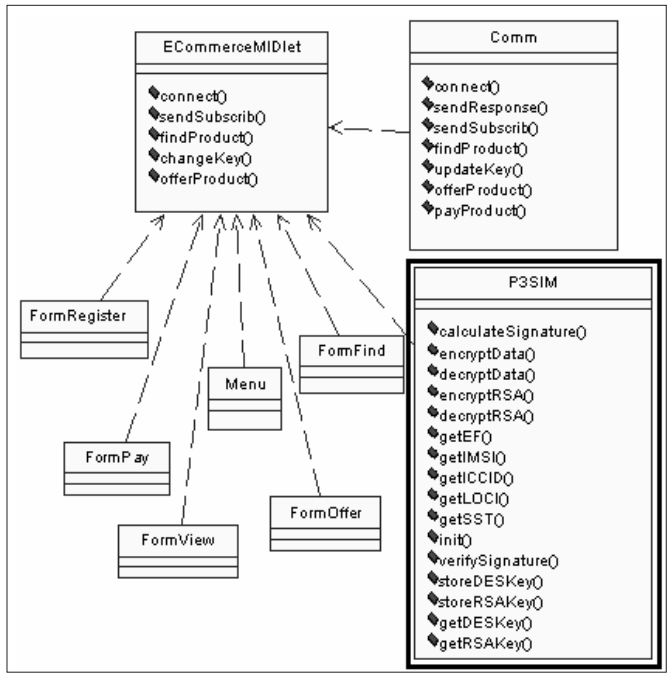

Figura 4. Arquitectura de la aplicación cliente

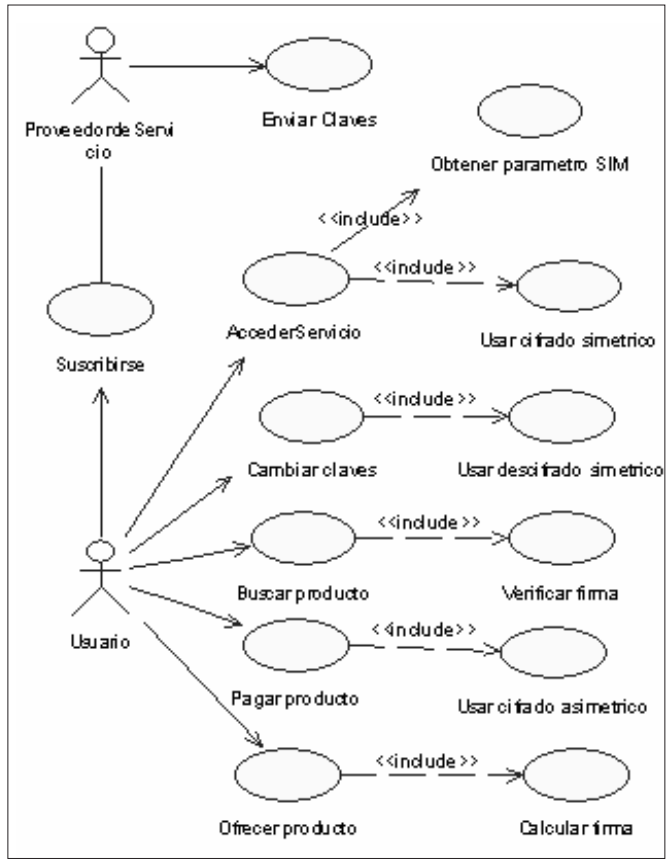

Figura 5. Diagrama de casos de uso del prototipo

Las ventajas del uso de la plataforma P3SIM no solo se reflejan en el proceso de autenticación, sino también en cualquiera de las operaciones clásicas que se pueden encontrar en un portal de comercio electrónico convencional. Cuando el usuario desea ofrecer un producto introduce en el teléfono móvil la información básica del producto (nombre, descripción, precio) y opcionalmente toma una fotografía del producto si el teléfono ofrece esta capacidad o la adiciona desde el sistema de archivos; esta información es enviada al servidor junto con la firma digital, garantizando la integridad y el no repudio de la información. Igualmente, cuando el usuario consulta la información de un producto el proveedor del servicio envía la información junto con su firma digital, de tal manera que la aplicación en el teléfono móvil no desplegará el contenido a menos que la firma sea válida. En el caso de una transacción electrónica el prototipo utiliza un cifrado asimétrico para el valor de la tarjeta de crédito o cuenta bancaria (según sea el caso), de tal manera que esta información es intercambiada de forma segura a través de la red. La Figura 6 muestra algunas pantallas del prototipo implementado.

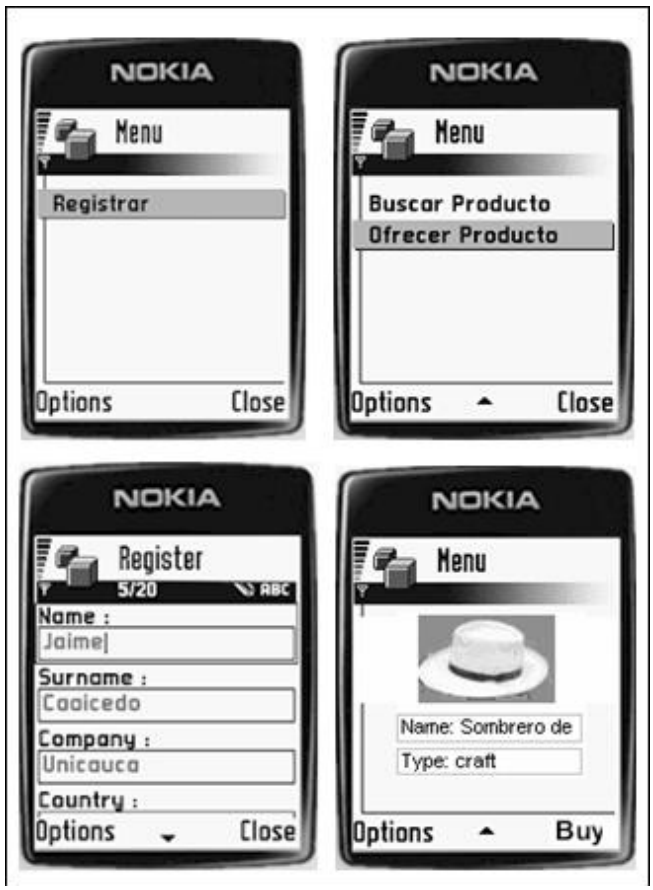

Figura 6. Interfaces del prototipo

Trabajos futuros

Una de las grandes limitaciones para el desarrollo del proyecto fue la ausencia de teléfonos con soporte para SATSA en el mercado colombiano; por esta razón fue necesario desarrollar las pruebas en un entorno de simulación. Sin embargo, el despliegue de teléfonos con soporte para SATSA no se ha hecho esperar (v.g. algunos teléfonos de la reciente serie N de Nokia, como el N91), y se espera que estos modelos amplíen su cobertura en el mercado global a favor de la construcción e implementación de aplicaciones móviles seguras como sugiere este proyecto.

Uno de los trabajos a futuro que se plantean es la ampliación del número de algoritmos manejados por parte del *framework* P3SIM, ya que hasta ahora únicamente se soporta DES para el cifrado simétrico y RSA para el asimétrico, pero Java Card y SATSA brindan la posibilidad de manejar otros como 3DES, AES, DSA y EC (Elliptic Curve). Por otro lado, es factible implementar una gestión más robusta de la firma digital por parte del *framework*, al introducir más funciones *hash*, más mecanismos de *padding* (relleno) y certificados digitales para cada usuario. Otro trabajo interesante es la incorporación de esquemas de seguridad basados en XML, que han tomado un gran auge gracias a los servicios *web* (Caicedo, Martínez, Gómez y Hurtado, 2005), (JSR 105 Expert Group, 2005).

Conclusiones

El talón de Aquiles del comercio electrónico móvil es sin lugar a dudas la seguridad. La adición de nuevos y más complejos mecanismos de seguridad como certificados digitales o algoritmos de cifrado precisan de un desarrollo cuidadoso que mantenga un equilibrio entre el nivel de seguridad que se ofrece y las capacidades de los dispositivos móviles. Estas capacidades no solo imponen restricciones en cuanto a capacidad de procesamiento o memoria disponible, sino también a nivel de usabilidad. Un modelo de autenticación tradicional donde existe la necesidad de introducir un *login* y un *password*, no es precisamente el más cómodo para los usuarios, dadas las limitaciones del teclado numérico del teléfono.

A través del desarrollo de la plataforma P3SIM se abren nuevas posibilidades para el desarrollo de aplicaciones seguras en entornos de comercio electrónico móvil, ya que reúne las ventajas de identificación que proporciona el módulo SIM, ampliamente desplegado en las redes de telefonía móvil modernas, y las capacidades que ofrece en materia de seguridad API como SATSA y Java Card en el entorno de las aplicaciones Java ME, la plataforma más exitosa para el desarrollo de aplicaciones móviles en el mundo.

P3SIM define un modelo de autenticación totalmente transparente para el usuario, lo cual incrementa la usabilidad de las aplicaciones de comercio electrónico móvil al tiempo que se proporciona un mayor nivel de seguridad en cualquiera de las operaciones básicas que se realizan tradicionalmente en un portal de comercio electrónico. Aunque el despliegue de API como SATSA o Java Card es aún reciente, el Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas W@PColombia, ha creado un precedente importante a partir de la construcción de P3SIM para el desarrollo de aplicaciones seguras, en uno de los entornos más exigentes

y de mayores perspectivas a futuro como efectivamente lo es el comercio electrónico móvil.

Bibliografía

3GPP, Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface., 3GPP TS 11.14, Sophia Antipolis Cedex, Francia, 3GPP PartnerShip Program, Sep., 2004.

3GPP, Specification of the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface., 3GPP TS 11.11, Sophia Antipolis Cedex, Francia, 3GPP PartnerShip Program, Jul., 2005

Anonymous., M-commerce advocates should heed e-commerce failures. , USA Today, Vol. 130, No. 2683, April., 2002, pp. 10.

Aspects Software, Aspects Developer V 2.1.05., Aspects Software, Enero, 2006. Disponible en: http://www.aspects-sw.com/pdf/aspects_developer.pdf

Attali, I., Caromel, D., Courbis, C., Henrio, L. and Nilsson, H. An integrated development environment for Java Card., Computer Networks, Vol. 36, No. 4, Jul., 2001, pp. 391-405

Baudín de la Lastra, R., Comercio electrónico móvil. Una realidad., Tecnología y Sociedad, SEMA Group., 2005. Disponible en: http://www.coit.es/publicac/publbit/bit120/tecno.html

Caicedo, O., Cerón, D., Chamorro, D., Martínez, F. y Hurtado, J., Arquitectura para la Provisión Segura de Servicios en Redes de Telefonía Móvil (Mercurio)., Memorias del IV Congreso Iberoamericano de Telemática CITA 2006, Monterrey, ITESM, mayo, 2006.

Caicedo, J. y Hernández, R. , Plataforma de acceso a servicios desde dispositivos móviles, utilizando parámetros de autenticación basados en SIM Card en redes GSM., Tesis presentada a la Universidad del Cauca, para optar al grado de Ingeniero en Electrónica y Telecomunicaciones, 2006.

Caicedo, O., Martínez, F., Gómez, M., and Hurtado, J., Architectures for Web Services Access from Mobile Devices., Memorias del Third Latin American Web Congress La Web 2005, Buenos Aires, Sociedad Argentina de Informática e Investigación Operativa SADIO, nov., 2005, pp. 93-97.

Chen, Z., Java Card Technology for Smart Cards., 1a ed., Massachussets, Addison Wesley, 2000, pp. 20-30.

ETSI, Security mechanisms for the SIM Application Toolkit., GSM 02.48 Spec, Sophia Antipolis Cedex, Francia, European Telecommunications Standard Institute, Jul., 1999.

ETSI, Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface., GSM 11.14 Spec, Sophia Antipolis Cedex, Francia, European Telecommunications Standard Institute, Dec., 1996.

Fúster, A., Martínez, D., Encinas, L., Montoya, F. y Muñoz, J., Técnicas criptográficas de protección de datos., 2a ed., México, Alfaomega, 2001, pp. 115-164.

Ghosh, A., Software security and privacy risks in mobile e-commerce., Association for Computing Machinery, Communications of the ACM, Vol. 44, No. 2, Feb., 2001, pp. 51-57

Gosling J., Bill, J., Steele, G. and Bracha G., Java(TM) Language Specification., 3a ed., Santa Clara, Addison-Wesley Professional, 2005, pp. 1-10.

Guthery, S. and Cronin, M., Mobile Application Development with SMS and the SIM Toolkit., 1a ed., New York, McGraw-Hill Professional, 2001, pp. 5-10

Hattangady, S. and Davis, C., Reducing the security threats to 2.5G and 3G wireless applications., Texas Instruments Wireless Terminals Business Group., Texas Instruments, Ene., 2002. Disponible en: http://focus.ti.com/pdfs/vf/wireless/securitywhitepaper.pdf.

JSR 105 Expert Group, XML Digital Signature APIs., Java Community Process Program, Santa Clara, California, Sun Microsystems Inc, Jul., 2005.

JSR 177 Expert Group, Security and Trust Services API (SATSA) for Java MicroEdition., Java Community Process Program, Santa Clara, California, Sun Microsystems Inc, Jul., 2004, pp. 1-3.

Moreno, L., Transacciones Seguras (II)., HTMLWeb.net, BJS Software, 2005. Disponible en: http://www.htmlweb.net/seguridad/ssl/ssl_2.html.

Muchow, J., Core J2ME Technology & MIDP., 1a ed., New York, Prentice Hall, 2001, pp. 1-15.

Peláez, D., Seguridad en Dispositivos Móviles: Bluetooth., escert.upc.edu, Equipo de Seguridad para la coordinación de emergencias en Redes Telemáticas., 2005. Disponible en: http://escert.upc.edu/_pub/articulos/seguridad_dispositivos_moviles.pdf.

Ponce, D. A., Contribución al desarrollo de un entorno seguro de m-commerce., Tesis presentada a la Universidad Politécnica de Catalunya, para optar al grado de Doctor en Ingeniería Telématica, 2002.

Shaffer, R., M-commerce: Online selling's wireless future., Fortune, Vol. 142, No. 2, Jul., 2000, pp. 262

Sutton, N., Carriers join forces for mobile commerce., Computing Canada, Vol. 31, No. 17, Nov., 2005, pp. 1-12