# Propuesta de arquitectura para facturación y pago por proximidad de servicios ubicuos en el contexto colombiano

Milton Ausecha Penagos
*mausecha@unicauca.edu.co*

Javier Imbús Guzmán
*jimbus@unicauca.edu.co*

Zeida Solarte
*zsolarte@unicauca.edu.co*

Oscar Caicedo
*omcaicedo@unicauca.edu.co*

*Grupo de Ingeniería Telemática, Universidad del Cauca, Popayán, Colombia*

Fecha de recepción: 19-10-2007 Fecha de selección: 18-04-2008 Fecha de aceptación: 15-01-2008

**ABSTRACT**

Ubiquitous services pretend to interact proactively with the user, proposing solutions to some problems. Those services must to be billed in a secure and efficient form in order to guarantee confidence between customer new services tha fulfill the customer's expectation. For this reason, ubiquitous computing is a new research area that looks for the provisión of services in a transparent way for the user in mobile environments. However, ubiquitous services have the problem of a non-existent protocol that fulfils all the mobility, identity and context requirements of such services. This paper describes the development of a ubiquitous services pilot that pretends to fulfill such requirements.

**KEY WORDS**

Ubiquitous services, Service discovery, Bluetooh, mobility, web services.

**RESUMEN**

Se busca que los nuevos servicios lleguen al usuario en cualquier lugar y hora, de forma transparente y brindando la posibilidad de acceder a los mismos mediante diferentes dispositivos y tecnologías de acceso. Los servicios ubicuos buscan adelantarse a las acciones del usuario para no solo esperar su intervención, sino también para proponerle soluciones a sus problemas y ayudarlo proactivamente con sus tareas. Estos servicios deben ser facturados de forma segura y eficiente para que los establecimien-

tos comerciales puedan brindar un servicio con la certeza de no perder capital debido a fallas en los procesos de facturación y el cliente pueda confiar en que se le facturará únicamente la cantidad correspondiente a los productos y servicios adquiridos, por esto se hace necesario proponer una arquitectura que permita garantizar las operaciones de pago y facturación brindando un alto nivel de seguridad que repercuta en la confianza del usuario y contribuya de forma considerable a la masificación del servicio. Por ello el grupo WapColombia y el GIT (Grupo de Ingeniería Telemática) de la Universidad del Cauca proponen una arquitectura que se adapta a las condiciones del contexto colombiano, para de esta forma contribuir en la construcción de una realidad, que cada día es más cercana gracias a la llegada al país de nuevas tecnologías, como NFC y RFID, que en conjunto con otras ya existentes como certificados digitales, algoritmos de cifrado, entre otros, permitirán innovar para garantizar seguridad en las transacciones financieras.

**PALABRAS CLAVE**

Computación ubicua, RFID, NFC, entidad certificadora, arquitectura, encriptación.

**Clasificación Colciencias: Tipo 1**

## 1. INTRODUCCIÓN

En la actualidad el concepto de computación ubicua es muy popular en países como Japón y Suiza, y día a día despierta mayor interés en los profesionales de las telecomunicaciones de todo el mundo.[1] El término Ubicuidad en el entorno de las telecomunicaciones fue definido por Mark Weiser, quien lo acuñó por primera vez en su artículo titulado: "El computador para el siglo 21" en el Scientific American Ubicomp en 1991,[2] en este artículo se proyectaba un ambiente dotado de un conjunto de recursos, los cuales brindarían no solo capacidades de comunicación a los usuarios mediante el acceso a múltiples dispositivos en cualquier lugar y a cualquier hora, sino que además lo harían de forma transparente y personalizada, gracias a un conocimiento previo del contexto de usuario.[1]

De otro lado, en los últimos veinte años el comercio electrónico móvil ha crecido explosivamente gracias al desarrollo de Internet, tecnologías de comunicaciones inalámbricas y dispositivos móviles, desempeñando un papel cada día más importante en nuestras vidas.[3] Al mismo tiempo la tecnología RFID (Radio Frequency IDentification), en donde un lector se comunica con una etiqueta por medio de radio frecuencia, ha despertado gran interés tanto en la industria como en la academia,[3] por lo cual en un futuro cercano todos los servicios de datos móviles estarán integrados a tecnologías de este tipo, y si además se considera que los servicios de datos contribuirán con el 70%-80% de las ganancias de los Proveedores de Servicios de Telecomunicaciones, se tiene que el futuro de los servicios basados en RFID es prometedor, especialmente el Servicio de Pago Móvil, que será la principal aplicación de RFID en el área de las telecomunicaciones.[4]

Aunque el pago desde dispositivos móviles es un campo incipiente a nivel nacional, con la llegada de nuevas tecnologías al país, entidades financieras, comerciantes y usuarios empiezan a manifestar interés por estas nuevas formas de pago, con lo cual entes reguladores como el Ministerio de Comunicaciones afrontan retos legislativos, que ya se empiezan a abordar con la creación del Decreto 2870 de 2007, que tiene en cuenta las diferentes áreas donde es posible una convergencia: los servicios, equipos terminales, redes o medios de transmisión, y mercados. Este decreto de convergencia abre el camino para que personas o empresas que no cuentan con grandes recursos económicos, participen en el mercado de las telecomunicaciones, el cual cada vez es más dinámico y competitivo, especialmente en el área de los servicios.

Los servicios de pago móvil hacen parte de la convergencia descrita anteriormente, por lo cual el planteamiento de una arquitectura para un sistema de pago que garantice transacciones seguras se convierte en una necesidad para la sociedad colombiana, la cual debe ser abordada teniendo en cuenta las limitaciones tecnológicas, de regulación y los retos sociales que implica el desarrollo de una aplicación de este tipo en el contexto nacional, además ya se han sentado en el país las bases legales para el uso de la factura digital con el decreto 1929 que la define como un documento equivalente a la factura

física en papel que soporta las transacciones de bienes y servicios y que para efectos fiscales su expedición, entrega, aceptación, conservación y exhibición, debe hacerse en un formato electrónico de conservación y la tecnología de información autorizados.[5] Por estas razones el Grupo de Ingeniería Telemática de la Universidad del Cauca está llevando a cabo los primeros pilotos como un acercamiento a una implementación real, y prepara gradualmente a los usuarios para la llegada de las nuevas tecnologías móviles.

El presente documento está estructurado de la siguiente manera, inicialmente se presenta un Marco Conceptual donde se explican las características de los servicios ubicuos y se definen las propiedades de un sistema de pago en un entorno ubicuo. Luego se presenta la arquitectura propuesta y se describe el proceso de pago llevado a cabo por un cliente al hacer uso del sistema; después se especifica la función de cada una de las entidades, que hacen parte de la arquitectura por medio de un caso de estudio y se compara frente a otras formas de pago implementadas en el mundo.

Finalmente se presentan las conclusiones y trabajos futuros que surgen al proponer esta arquitectura.

## 2. MARCO CONCEPTUAL

*A. Servicios ubicuos*

La esencia de la computación ubicua es la creación de ambientes saturados con capacidades de computación y comunicación, que se integran a la vida de las personas. Este entorno implica retos, algunos de los cuales ya han sido afrontados en el proceso de maduración que han sufrido sus dos antecesores: Los Sistemas Distribuidos y la Computación Móvil.[6]

Las características más relevantes de los sistemas distribuidos que se retoman en la computación ubicua son:[6] comunicación remota, tolerancia a fallos, alta disponibilidad, acceso a información remota y seguridad. Mientras que de la computación móvil se retoman características como: sistemas de redes móviles, acceso móvil a información, gestión adaptativa de recursos y sensibilidad de la locación.

Sin embargo, con la computación ubicua aparecen retos nuevos, como uso efectivo de espacios inteligentes, invisibilidad, escalabilidad localizada y enmascaramiento de desigualdades tecnológicas del entorno.[6]

Los servicios de comunicación en la vida diaria llegarán a ser más personalizados, y las capacidades que hagan uso del contexto y de las preferencias del usuario serán cada vez más importantes. Por esto se hacen necesarias herramientas y entidades en la red que permitan un fácil acceso a los servicios, un rendimiento y funcionamiento óptimos, pero sobre todo que garanticen comunicaciones seguras y confiables.[7] Desde este punto de vista se puede dar una definición más precisa de los servicios ubicuos:[7] Un entorno ubicuo comprende una infraestructura de red y un conjunto de recursos, que brindan capacidades de comunicación a los usuarios mediante el acceso a múltiples dispositivos en cualquier lugar y a cualquier hora, de forma transparente y personalizada, gracias a un conocimiento previo del contexto

de usuario, garantizando siempre la seguridad y confiabilidad de la comunicación, tanto a los clientes como al proveedor del servicio.

*B. Servicio de pago en entornos ubicuos*

En el modelo de comercio móvil clásico, la gente accede a internet usando su dispositivo móvil para seleccionar sus productos y ordenarlos en línea.

Pero muchos pagos no se efectúan de esta forma. En lugar de buscar la información del producto en internet antes de su elección, las personas interactúan con su ambiente o el medio que las rodea.[3] Normalmente cuando una persona desea obtener información de los productos cercanos, incluyendo información detallada del artículo y del vendedor, recurre a un conocido o a un aviso publicitario, con lo cual puede obtener los siguientes resultados: la persona no obtiene la información que necesita, así que recurre a otros medios como internet; otras personas le pueden brindar información sobre el producto, pero ésta no es útil ya que puede estar desactualizada; y finalmente, algunas personas le pueden brindar información útil acerca de un producto, pero ésta no es determinante para saber si está tomando la mejor opción.[3] Pero la selección del artículo es solo el primer paso para su compra, que inicia el siguiente proceso:

- Selección del artículo en la página Web
- Adición del artículo a la cuenta del usuario, si no se tiene se crea una con la información del comprador.
- Si la cuenta no tiene el respaldo de una tarjeta de crédito o cuenta bancaria, el usuario debe consignar el valor del artículo en la cuenta del vendedor.
- Si la cuenta tiene el respaldo de una tarjeta de crédito o cuenta bancaria, el usuario debe autorizar el traspaso de dinero a la cuenta del vendedor.
- El usuario recibe una confirmación de la transacción, que es generalmente una factura enviada a su casa.

En un entorno ubicuo, una vez seleccionado el producto, se realiza su pago y facturación, al igual que en cualquier transacción, pero con algunas características especiales:

- Se crea una cuenta de usuario con los datos y gustos personales.
- El sistema le informa al usuario la existencia de un artículo de su interés, por medio de una tecnología inalámbrica.
- El usuario observa los detalles del artículo desde su teléfono móvil y lo adiciona a su cuenta.
- El usuario realiza el pago por medio de una tecnología de campo cercano.
- El usuario recibe una confirmación de la transacción por medio de un mensaje de texto, en su teléfono móvil, y la factura en su correo electrónico.

Las interacciones de computación ubicua son típicamente espontáneas y de breve duración, con la posibilidad de ser iniciadas sin intervención de los usuarios e involucrando numerosos servicios dispersos, geográficamente confiables y no confiables. De acuerdo con las características anteriores se identifican los siguien-

tes requerimientos en un sistema de pago de computación ubicua: espontaneidad, eficiencia, seguridad, privacidad, flexibilidad, usabilidad y despliegue.[8]

*Espontaneidad:* La espontaneidad es una característica inherente y deseable de las interacciones ubicuas, que establece que los sistemas de computación ubicua deben ser diseñados con la suposición de que un grupo de usuarios participantes es altamente dinámico e impredecible. En términos de sistemas de pago, esto significa que es altamente improbable que los individuos entren en relaciones de larga duración con los diferentes proveedores de servicio que puedan encontrar.[8]

*Eficiencia:* Cuando se refiere a pagos que impliquen transacciones de medio o alto valor, la eficiencia de los sistemas de pago de computación ubicua está relacionada con la confianza que debe existir entre los usuarios y los proveedores de servicio. Cuando muchos pagos pequeños están implicados, es importante que el proceso del pago sea ligero y eficiente; caracterizado por la baja transferencia de datos y bajos costos tanto en lo computacional como en lo financiero.[8]

*Seguridad:* Claramente la seguridad es una consideración importante en cualquier sistema de pago y debe ser utilizada para evitar fraudes tales como hurto, falsificación de dinero, y evasión del pago. Los ambientes de computación ubicua, que brindan servicios a cualquier hora y en cualquier lugar, son más vulnerables a violaciones de seguridad que ambientes controlados que pueden ser asegurados físicamente. Los problemas de seguridad también se presentan debido a la falta de establecimiento de relaciones de confianza entre los usuarios finales y los proveedores de servicio.[8]

*Privacidad:* Muchos sistemas de pago como las tarjetas de crédito y las transferencias de dinero requieren que los usuarios faciliten información personal como nombre y números de cuenta durante la transacción. Se puede dar el caso en el que los usuarios no desean divulgar esta información pero necesitan pagar por los servicios. Además, sin los mecanismos adecuados para proteger la privacidad, la información de pago podría ser combinada con información del contexto que proporciona detalles de las actividades de los usuarios.

*Flexibilidad:* Los sistemas ubicuos deben seguir el principio de la volatilidad y no deben asumir ninguna configuración específica de red, de dispositivos y/o de usuarios, con lo cual se pueden identificar dos casos especiales: operación desconectada e indisponibilidad del dispositivo. La operación desconectada es un modo de operación que permite a los clientes continuar accediendo a servicios durante fallas temporales de un depósito de datos compartido o de una conexión de red. En el segundo caso, es importante que las interacciones de los usuarios con los ambientes de computación ubicua no dependan exclusivamente de un dispositivo móvil, ya que existe la posibilidad de que un cliente no tenga su dispositivo móvil cerca, pero todavía necesite hacer uso del servicio de pago.[8]

*Funcionalidad:* Se refiere al grado de comodidad y a la utilidad percibida por los usuarios, en el momento de

hacer uso del sistema de pago ubicuo, es un aspecto crucial si se tiene en cuenta el gran número de transacciones que una persona podría realizar durante el curso de un día normal. Por ejemplo, los usuarios esperarán un nivel de servicio comparable al existente con las tarjetas de crédito y las cuentas bancarias. Problemas como confianza, responsabilidad, contabilidad y aseguramiento se deben tratar adecuadamente para que los usuarios acepten el sistema. La mayoría de los usuarios no aceptaría un sistema que permita que se lleven a cabo transacciones financieras sin su intervención; al mismo tiempo, no es práctica la participación del cliente en todas las transacciones especialmente cuando estas son de bajo valor. Por lo tanto, los diseñadores de los sistemas de pago se enfrentan al reto de balancear estas necesidades contradictorias.[8]

*Despliegue:* Para tener éxito, el sistema de pago de computación ubicua se debe poder emplear a gran escala. En términos prácticos, debe soportar tanto nuevos servicios como los ya existentes.[8]

Anteriormente se definieron las características más importantes que debe tener cualquier servicio de pago ubicuo, y teniendo en cuenta que el servicio de facturación y pago desarrollado pretende ser un servicio con estas características, a continuación se relacionan cada una de ellas con la solución propuesta.

El servicio de pago implementado es espontáneo, ya que los usuarios lo pueden iniciar en cualquier momento, en alguno de los puntos de venta POS, siempre y cuando ya esté registrado en el sistema y tenga una cuenta de usuario. El proceso de pago es corto debido a las propiedades de las tecnologías y herramientas empleadas, por lo cual es poco probable que el cliente entable una relación de larga duración con el sistema en el momento del pago. Los bajos costos de operabilidad y el empleo de herramientas de libre acceso incrementan la eficiencia del servicio.

En un sistema de pago, la seguridad en las transacciones y la privacidad de la información suministrada por los clientes, son dos aspectos trascendentales para generar confianza tanto en los usuarios como en el proveedor del servicio. En el sistema se hace uso de la infraestructura de llave pública, que permite realizar la autenticación de los usuarios y cada una de las entidades que conforman el sistema mediante el empleo de credenciales, además de garantizar la integridad de la información con el cifrado de la misma, para lo cual se requiere el uso de certificados digitales emitidos por autoridades certificadoras.

La naturaleza ubicua del servicio de facturación y pago desarrollado lo hace un sistema flexible frente a otras formas de pago tradicionales, en donde la usabilidad del sistema es un aspecto determinado en gran parte por la experiencia de cada individuo al momento de utilizar el servicio, por lo cual es algo difícil de percibir por los desarrolladores. Pero si se tienen en cuenta el grado de aceptación de las tarjetas de crédito por parte de los usuarios y las mejoras que un sistema de pago móvil presenta frente a estas formas de pago tradicionales, se puede garantizar en gran medida la funcionalidad que representa la solución propuesta para las personas.

Al no ser necesario llevar consigo una tarjeta ni digitar claves en equipos extraños se mejora la experiencia del usuario final que percibe el servicio como fácil de utilizar.

El sistema propuesto ha sido desarrollado sobre plataformas robustas y con herramientas de libre acceso, que lo hacen no solo escalable ante un aumento en el número de usuarios, sino integrable a soluciones y sistemas similares.

*C. RFID y NFC*

RFID y NFC son tecnologías que merecen especial atención en la computación ubicua. RFID se refiere a cualquier sistema que permita la transmisión de números de identificación sobre radio, obteniendo una identificación automática con capacidades de almacenamiento y recuperación remota de datos, mediante el uso de dispositivos llamados etiquetas.[9] Un sistema RFID se compone de dos partes fundamentales: la etiqueta (transponder) y el lector. Una etiqueta RFID es un pequeño objeto que puede ser adherido o incorporado en un producto, animal o persona, que está compuesto de un microcontrolador, una antena (cableada o impresa con tinta de carbón conductivo) que habilita la recepción y la respuesta a solicitudes de radio-frecuencia desde un transmisor/receptor (tranceiver) RFID, y un material de encapsulación de polímero que envuelve la antena y el microcontrolador.[9] El lector es quien inicia el proceso de identificación al generar un campo RF en una frecuencia específica, definida por un sistema en particular, con lo cual causa una diferencia de voltaje por medio de un acoplamiento capacitivo o inductivo.[9] La etiqueta detecta este cambio y después de un proceso de autenticación opcional, gracias a un mecanismo de respuesta del lector, responde transmitiendo la identificación que posee.[9]

NFC es una tecnología que involucra Identificación de Radio Frecuencia (RFID) de corto alcance y posibilita la transferencia de datos entre un dispositivo móvil y un sistema de servicios, por simple contacto entre aquél y una placa NFC.[10] NFC se diferencia de las demás tecnologías RFID o de proximidad en que su distancia de funcionamiento es corta y depende del diseño de la etiqueta y del lector, pero, generalmente, el radio de acción es muy pequeño; esto es una ventaja a la hora de atender servicios que implican una necesaria privacidad, como es el caso de un proceso de facturación y pago. Además, NFC va más allá de RFID en el sentido que es un protocolo simétrico, donde los lectores pueden leer de etiquetas y de otros lectores directamente, es decir, se pasa de transferir datos en un solo sentido a un proceso bidireccional.[10]

## 3. ARQUITECTURA DE PAGO Y FACTURACIÓN

Una arquitectura para pago y facturación de servicios ubicuos debe estar estructurada de forma tal que sus diferentes componentes permitan satisfacer las necesidades de los usuarios desde el punto de vista del servicio prestado, pero al mismo tiempo debe garantizar la protección de la información a intercambiar, por lo cual es necesario hacer énfasis en el manejo en la seguridad de cada bloque y sus conexiones, ya que un sistema es tan seguro como su elemento más inseguro.

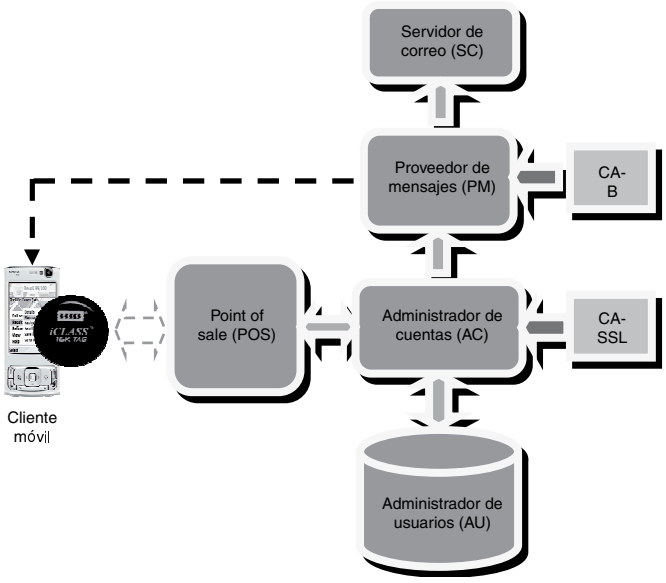



**Figura 1.** Arquitectura para pago y facturación de servicios móviles ubicuos

La arquitectura propuesta (Figura 1) tiene los siguientes componentes: un Cliente Móvil, que permite al usuario realizar pagos, un POS (Point of Sale) capaz de recibir pagos de móviles habilitados con interfaces de contacto cercano, un Administrador de Cuentas (AC) que es el núcleo de la arquitectura y le recibe todas las peticiones de transacción, un Administrador de Usuarios (AU), que almacena toda la información concerniente a las cuentas de los diferentes usuarios del sistema, principalmente las credenciales de cada uno de ellos que son generadas por el AC, un Proveedor de Mensajes (PM) encargado de enviar mensajes de información al móvil seguro del usuario, y finalmente un servidor de correo que envía la factura digital a la cuenta de correo del usuario.

Se tienen además dos entidades certificadoras, CA – SSL, que se encarga de certificar al Administrador de Usuarios y CA – B (Certificate Authority - Billing), que certifica al proveedor de mensajes y en especial le proporciona un certificado para firmar digitalmente las facturas enviadas a las cuentas de correo de los usuarios del servicio.

*A. Proceso de pago y facturación*

El proceso de pago y facturación se describe a continuación.

El usuario accede al servicio mediante su teléfono móvil, el cual como requisito debe tener dos interfaces de comunicación, la primera de tipo contactless o por contacto cercano, que es necesaria al momento de efectuar el pago; la segunda una interfaz inalámbrica que le permita acceder a una red de área amplia con el fin de recibir los mensajes de confirmación cuando la transacción sea exitosa.

Con la interfaz de contacto cercano que puede ser una etiqueta RFID o

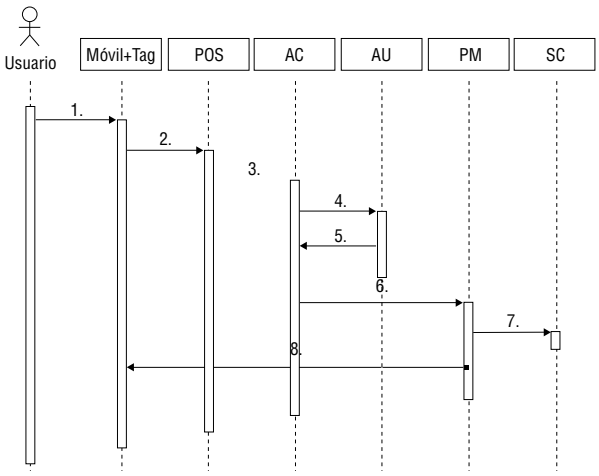
un elemento NFC, el móvil se puede comunicar con el POS de forma confiable, al realizarse autenticación mutua y cifrada de la información transmitida, para de esta forma distribuir la seguridad y no dejarla como responsabilidad única de un servidor central.

Para obtener la información acerca de la capacidad de pago del usuario, el POS debe comunicarse de forma segura con el Administrador de Cuentas, el cual se comunica con la mayoría de los bloques de la arquitectura, el AU debe estar certificado por una CA (Certification Authority) para poder cifrar todos los mensajes de la comunicación. El AC se comunica directamente con el Administrador de Usuarios que maneja la información de los usuarios activos y su correspondiente capacidad de pago.

El Administrador de Cuentas debe notificarle al usuario el resultado de la transacción a través del PM, que debe contar con acceso a la interfaz inalámbrica del móvil. El PM también se encarga de realizar el envío de la factura electrónica, la cual debe estar firmada digitalmente por una segunda CA, que se ha denominado CA-B (CA – Billing), esta prueba de compra digital se envía al correo electrónico que el usuario proporciona al crear su cuenta. El proceso completo es ilustrado en el diagrama de la Figura 2.

*B. Creación de cuenta*

Para el proceso de creación de cuenta se añade un nuevo componente a la arquitectura general, denominado Punto de Creación de Cuentas (PCC). Este componente permite realizar




1. Selección de compra
2. Envío de credenciales
3. Envío de información de compra
4. Petición de validación de información
5. Validación de transacción
6. Solicitud de mensaje de información
7. Envío de factura digital
8. Envío de mensaje de información

**Figura 2.** Diagrama de secuencia del proceso de pago y facturación

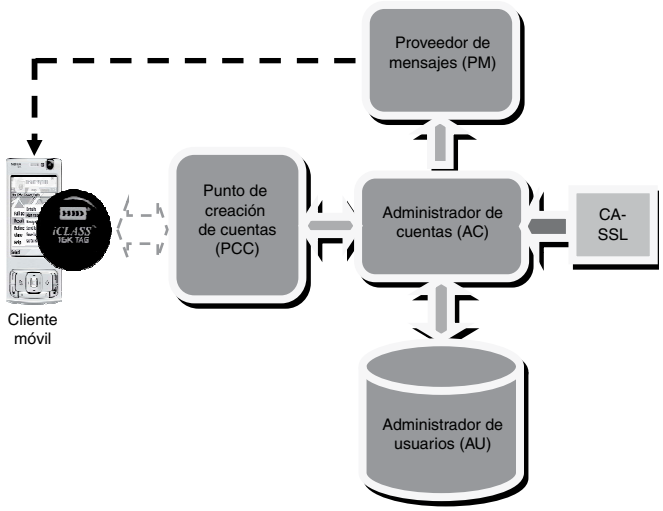



**Figura 3.** Arquitectura para creación de cuenta

operaciones como creación de cuenta para un nuevo usuario, bloqueo de cuenta en caso de presentarse un reporte de robo del dispositivo móvil y eliminación de cuentas.

El usuario debe crear una cuenta para usar el sistema, en este proceso se asigna una etiqueta RFID a su teléfono móvil, en la que se graban mediante una conexión segura los datos de cuenta necesarios para realizar el proceso de pago. El resultado de este proceso se envía en un mensaje a través de la otra interfaz inalámbrica del dispositivo móvil.

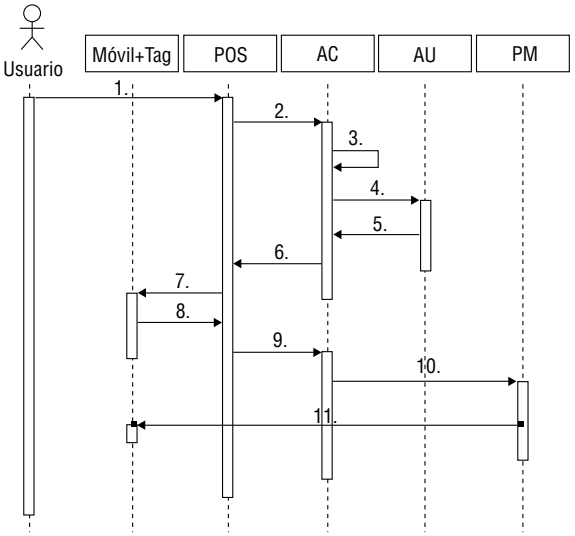
El proceso de grabación en la etiqueta se realiza mediante el PCC, este se comunica con el AC, como se muestra en la Figura 3, y le hace una petición de creación de cuenta, el AC crea uno o varios identificadores para el nuevo usuario y los envía al AU para que sean registrados.

Al obtener un resultado satisfactorio de la operación de registro, el AC envía esta información al PCC para que los datos de cuenta sean grabados en la etiqueta del dispositivo móvil. Toda la información transferida durante este proceso se cifra, y si es necesario se refuerza la seguridad con autenticación mutua y firma digital sobre los datos transmitidos. Además el AC debe estar certificado por una entidad confiable, como Verisign, Thawte o Global Trust que son empresas muy conocidas y dedicadas a la comercialización de varios tipos de certificados. Finalmente el PM se encarga de hacer llegar un mensaje al usuario para darle la bienvenida al sistema de pago o en caso de algún inconveniente informarle que no fue posible crear su cuenta y qué debe hacer para poder acceder al servicio, tal como se aprecia en el diagrama de la Figura 4.

## 4. CASO DE ESTUDIO

*A. Implantación de un servicio de pago por proximidad en un ambiente ubicuo.*

A continuación se describen los detalles de implantación de cada




1. Solicitud de creación de cuenta
2. Envío de información del usuario
3. Creación de identificadores
4. Registro de identificadores
5. Confirmación de registro
6. Envío de identificadores
7. Grabación de etiqueta
8. Confirmación
9. Confirmación
10. Petición de envío de mensaje de bienvenida al sistema
11. Envío de mensaje de bienvenida

**Figura 4.** Diagrama de secuencia del proceso de creación de cuenta

una de las partes de la arquitectura propuesta.

### *Teléfono Móvil*

El teléfono móvil utilizado por el usuario para acceder al servicio debe contar con una interfaz de contacto cercano para efectuar el pago; existen dos opciones para cubrir este aspecto: emplear una etiqueta RFID o usar un teléfono NFC. Según la que se utilice cambia el modelo de negocio.

Al usar un teléfono NFC, tal como el Nokia 6131 NFC, se puede consultar la información que se encuentra en la etiqueta dentro del teléfono mediante un *Trusted Midlet* que se comunica con un *Java Card Applet* instalado en el elemento seguro NFC.[11] El *applet* nunca inicia una comunicación, solamente espera a que un *midlet* que debe ser seguro, lo haga mediante comandos APDU (Application Protocol -Data Unit); únicamente un *midlet* firmado con un *code-signing certificate* es considerado seguro, con lo cual es asociado al dominio *trusted third party* del teléfono y puede acceder a las API restringidas de java.

Empresas como Thawte y Verising cobran alrededor de US500 por un certificado con vigencia anual. Adicional a esto es necesario tener en

cuenta que el elemento seguro NFC puede ser accesible únicamente mediante llaves de autenticación, por lo cual, para efectuar un desarrollo debe realizarse una operación de desbloqueo del elemento seguro NFC. En el caso del teléfono de Nokia, existe un Servicio de Desbloqueo mediante una midlet que agrega llaves de autenticación conocidas, con el fin de permitir el proceso de desarrollo de aplicaciones.[11]

La segunda opción que se tiene para la interfaz de contacto cercano es usar etiquetas RFID, que tienen características muy adecuadas para la implementación de la arquitectura, como son:

- Comunicaciones confiables a alta velocidad, sin arriesgar la seguridad de los datos.
- Nivel elevado de seguridad con autenticación mutua, codificación de datos, y llaves diversificadas de 64-bit para permitir la lectura/escritura.
- Suficiente memoria de lectura/escritura como para almacenar varias plantillas biométricas.
- Sistema de archivos separados para garantizar seguridad, lo que permite implementar numerosas aplicaciones.
- Cumplimiento de los estándares ISO 15693[12] y 14443B[13] para las comunicaciones sin contacto.

Toda la transmisión de datos por radiofrecuencia entre la tarjeta y el lector se codifica con un algoritmo seguro que normalmente pertenece al fabricante del lector, no obstante también se utilizan técnicas de cifrado estándar de la industria para reducir el riesgo de robo o manipulación de información. Para más seguridad aún, los datos de la tarjeta también pueden protegerse con encriptación DES (Data Encryption Standard) o triple DES, y el tiempo necesario para llevar a cabo las operaciones de encriptación se mantiene bajo, de forma que las transacciones se realizan en menos de 100 milisegundos, en el caso de una aplicación típica segura de billetera electrónica.[14]

### *POS*

Se debe implementar con un lector capaz de establecer una comunicación segura con la etiqueta RFID que garantice un nivel de seguridad adecuado. Básicamente el punto de venta o pago está compuesto por un lector y un computador conectado a este, en el cual debe haberse instalado una aplicación que utilice el API proporcionado por el fabricante del lector. Algunas opciones disponibles son lectores de fabricantes como Omnikey y HID Global que ofrece lectores de la serie iCLASS, de los cuales se eligió el RW100[15] como unidad lectora. En este punto la seguridad se basa en autenticación mutua entre las etiquetas y el equipo de lectura, además de la encriptación de la información mediante cifrado triple DES, que se puede realizar mediante el SDK que proporciona el fabricante escrito en Visual Basic para plataforma Windows, pero debido a que se busca el mayor nivel de seguridad posible en la estación de pago, se optó por trabajar con la distribución Debian Etch de Linux y desarrollar directamente sobre esta plataforma mediante NetBeans IDE. En el POS debe ir instalada una aplicación cliente que es básicamente

una aplicación de escritorio escrita en Java, con acceso al protocolo serial definido por el fabricante (ya que este protocolo es independiente de la plataforma) mediante JNI y además con capacidades de comunicación con un servicio web Java. Esta aplicación se utilizará para establecer una comunicación segura con el lector ya que se puede implementar autenticación mutua entre ellos y así los identificadores de un usuario que han sido almacenados en la etiqueta asociada a su móvil y posteriormente enviar esta información al AC mediante la utilización de un protocolo seguro como HTTPS (HTTP Over SSL).

### *Administrador de cuentas (AC)*

El Administrador de Cuentas es un bloque fundamental de la arquitectura ya que interviene con la mayoría de los bloques definidos y debe establecer una comunicación segura con cada uno de ellos, además debe ser lo suficientemente flexible como para poder interactuar con aplicaciones de escritorio, Bases de Datos, Directorios que implementen LDAP[16] (Lightweight Directory Access Protocol) como openLDAP[17] y el proveedor de mensajes definido.

En esencia es un Servicio Web Java, desarrollado con NetBeans IDE que hace uso de Metro,[22] un stack para el desarrollo de Servicios Web seguros y es desplegado sobre GlassFish v2 que es un servidor de aplicaciones gratuito y de código libre, distribuido con la licencia CDDL y la GNU GPL. GlassFish tiene como base al Sun Application Server.[23] El AC tiene la capacidad de atender solicitudes por parte de un cliente, que en este caso es el POS, solicitando verificación de la información leída de la etiqueta asociada a un móvil, o creación de identificadores cuando un nuevo usuario necesita acceder al servicio.

El AC debe conectarse con la base de datos, repositorio o directorio, que administre los usuarios, en este caso se ha elegido un servidor de directorio LDAP. El AC se comunica con él mediante JNDI (Java Naming and Directory Interface), que es la interfaz de la plataforma Java para conexión con servicios de nombres y directorios.[24]

### *Administrador de usuarios*

La información de cada usuario debe ser almacenada y para ello existen diferentes clases de bases de datos y directorios, de forma que cuando un usuario realice un pago se pueda validar su información personal, números de cuenta, permisos, y certificados de forma muy rápida, por lo cual se sugiere una implementación de LDAP, como openLDAP, para realizar la administración de usuarios, ya que permite consultas con tiempos de respuesta muy bajos.

El protocolo LDAP, además de permitir un manejo jerárquico y sistemático en la información de los usuarios, lo cual es muy útil por el modelo del negocio implementado en un sistema de pago, también posibilita varias formas de acceso, como JNDI.

LDAP es adecuado para implementar sistemas de autenticación/autorización centralizada, o para sistemas donde se guarda gran cantidad de registros y se requiere un uso constante de los mismos. Pero se pueden usar métodos alternativos para el proceso de autenticación como Kerbe-

ros v5 o Digest-MD5 que se acoplan perfectamente con openLDAP y dejar este último únicamente para realizar la autorización. Para usar Kerberos es necesario hacer uso de GSSAPI (Generic Security Services Application Programming Interface) en AC, a través de JNDI y realizar la configuración necesaria en openLDAP, además de correr los demonios de Kerberos en Linux.

### *Proveedor de mensajes*

Con el fin de enviar información de servicio a los usuarios se ha definido el PM, que mediante mensajes Wap Push puede notificar al comprador de una transacción efectuada satisfactoriamente o de inconvenientes debido a que el saldo en cuenta no fue suficiente, al momento de realizar la adquisición de un producto o servicio.

Los mensajes pueden enviarse mediante una Gateway SMS o un Push Proxy Gateway tal como Kannel[18] que corre sobre Linux, o APIs de Java como jSMS,[19] que actúan como interfaz entre la red cableada y la red inalámbrica, permitiendo la comunicación entre los componentes arquitecturales soportados en una infraestructura cableada y el dispositivo móvil del usuario.

Gracias a la compatibilidad directa entre el Servicio Web y jSMS, además de las facilidades de configuración que proporciona esta API, es una opción sobresaliente para formar parte en la implementación de un servicio de pago por proximidad.

### *Servidor de correo*

Debido a que la gran mayoría de teléfonos móviles en el país son de gamas media y baja y no están en capacidad de leer documentos como archivos pdf, formato en el cual se podría enviar la factura electrónica firmada, se hace necesario el uso de un servidor de correo, ya sea mediante un API como Java Mail o servicios de correo como Postfix o Sendmail corriendo bajo Linux.

Java Mail posee un diseño universal y abstracto que lo hace más difícil de usar y las clases requeridas (o archivos .jar) son bastante pesadas en términos de espacio requerido en disco. Por consiguiente, si pequeñas aplicaciones o dispositivos embebidos necesitan capacidades de mensajería tal como e-mail o SMS, deben implementar sus propios mecanismos para enviar y recibir correos.[20]

Por su parte, jSMS provee una API pequeña para SMS y correo que fácilmente puede ser adaptada a pequeños dispositivos.

Básicamente se necesita un servicio de correo que permita enviar como archivo adjunto la factura electrónica firmada digitalmente a la cuenta de correo proporcionada por el usuario al crear su cuenta de uso del servicio, también que el servicio de correo se pueda comunicar de forma segura con el Administrador de Usuarios.

### *Entidades certificadoras*

Es necesario garantizar que la información enviada de un módulo a otro sea auténtica e íntegra.

Auténtica en cuanto a que se pueda saber a ciencia cierta que un módulo determinado envió el mensaje y prevenir ataques de suplantación. Íntegra en cuanto a que se garantice que el mensaje no ha sido modificado. Esto se puede garantizar mediante el

uso de PKI (Public Key Infraestructure), la cual implica la generación de un par de llaves (pública y privada) para identificar a un usuario determinado, y el uso de funciones Hash. En PKI se necesita de una autoridad certificadora confiable que emita certificados cuyo contenido sean llaves públicas de las entidades con las que se establece comunicación.[21]

En esta arquitectura se muestran dos tipos de entidades certificadoras. Con CA-SSL se hace referencia a una entidad certificadora externa como Verisign o Thawte, las cuales comercializan certificados SSL que permitirían validar la identidad del Administrador de Cuentas.

El segundo tipo de entidad certificadora es necesaria para generar los certificados que permitan firmar la factura electrónica, las opciones de implementación para este caso son openSSL y entornos gráficos que usan SSL como XCA que funciona tanto con Linux como con Windows.

Otra herramienta muy útil es keytool, que hace parte de la plataforma Java y se encarga de generar parejas de llaves públicas y privadas, certificados autofirmados y almacenes de claves o keystore.

*B. Comparación*

No existe una clasificación única para los sistemas de pago móvil, debido a los diferentes aspectos que se deben tener en cuenta en este tipo de transacciones, que limitan y caracterizan el sistema. La ubicación del usuario, el monto a pagar, el proveedor del servicio, el instante y el medio utilizado para el pago, son los rasgos más sobresalientes en un sistema de pago y que además permiten su caracterización.[25]

Basándose en los aspectos nombrados en el párrafo anterior se puede definir el tipo de pago propuesto en este artículo; el cual es un sistema POS (Point of Sale) al requerir la presencia del usuario en el punto de venta; las cantidades de dinero que maneja son pequeñas, y lo convierten en un sistema micropago diseñado para ser administrado por un sistema independiente soportado en Entidades Financieras, y basado en tokens que se transfieren del usuario al vendedor en tiempo real.[26]

En todo el mundo han sido planteados diversos sistemas y arquitecturas para pagos móviles, en diferentes escenarios y con características distintas, por lo cual no existe un estándar o Modelo Global para un Sistema de Pago Móvil. Esta falta de normalización se debe a la competencia entre Entidades Financieras y Operadores de Telefonía Móvil por el control del mercado; y a la diversidad de escenarios donde se requiere un sistema de Pago móvil, cada uno con necesidades específicas, que caracterizan y limitan la solución de pago. En la Tabla 1 se comparan dos medios de pago implementados en el mundo, con el sistema de pago propuesto, donde se puede apreciar la dificultad para crear un medio de pago estándar.

En la Tabla 1 se aprecian sólo 3 soluciones de pago de varias que se han implementado en el mundo, y cada una ha sido creada para una necesidad específica en un contexto concreto. Incluso existen soluciones con la misma lógica, pero que emplean tecnologías distintas, por ejemplo

**Tabla 1.** Sistemas de pago

| | LIPSO | PAYBOX | Propuesta |
|---|---|---|---|
| Forma de pago | Cargo a la Factura del teléfono Móvil | Se debita de una cuenta Bancaria o Tarjeta de crédito | Se debita de una cuenta Bancaria |
| Instante de pago | Pospago | Pago en Tiempo Real | Pago en Tiempo Real |
| Monto | Micropago | Micropago | Micropago |
| Ubicación del usuario | Pago desde Internet | Persona a Persona (P2P) | Punto de Venta (POS) |
| Según el proveedor | Operador Móvil | Proveedor Independiente/ Intermediario | Proveedor Independiente |

eco-PAY es una solución similar a PAYBOX pero emplea SMS en lugar de un Servicio IVR (Interactive Voice Response), ya que fue creada para el contexto 11 canadiense, donde los SMSs tienen mayor acogida.25 La gran ventaja del sistema propuesto en este artículo frente a los pilotos y sistemas ya establecidos en el mundo, es que ha sido diseñado para el contexto colombiano de una forma tal que pueda funcionar con herramientas libres y pocos recursos económicos. Este sistema de pago permite llevar a cabo transacciones de poco valor en tiempo real, en situaciones comunes para los colombianos, sin la limitante de estar asociado a un operador móvil específico, además de emplear tecnologías de campo cercano creando un entorno ubicuo para los clientes.

## 5. CONCLUSIONES Y TRABAJOS FUTUROS

A pesar de las limitaciones tecnológicas que se tienen en Colombia, es posible llevar a cabo las primeras implementaciones para un sistema de facturación y pago ubicuo. En el momento, tecnologías como NFC y RFID no tienen un uso masivo por parte de los usuarios, pero la construcción de un piloto para pago y facturación desempeña un papel importante como un primer acercamiento de ellas a la población colombiana.

La calidad de un proceso de facturación y pago está medida por la seguridad, la privacidad y la confianza que éste refleje hacia los usuarios en el manejo de los datos personales, y especialmente de la información financiera. Es por esto que el papel que desempeñan las entidades certificadoras adquiere gran importancia en la prestación del servicio, para lograr satisfacción en los usuarios finales.

El panorama colombiano es muy alentador para la implementación de servicios de pago y facturación de nueva generación por la acogida que han tenido en los últimos años las tarjetas débito y crédito, y la enorme demanda de teléfonos móviles en el mercado.

El uso de tecnologías como RFID y/o NFC permitirá incrementar los niveles de seguridad en servicios de pago y facturación, para proteger mejor la identidad del usuario y dificultar la copia de su información, al contrario de como hoy en día se presenta con las tarjetas de banda magnética que son fácilmente duplicables.

Existen diversas opciones de implementación para cada uno de los

componentes de la arquitectura propuesta. En el momento de hacer la selección, se debe evaluar cuidadosamente la compatibilidad entre estos ya que muchos de ellos han sido construidos sobre diferentes lenguajes de programación (Java, C#) y diferentes plataformas (Windows, Linux). Además se deben tener en cuenta los costos que implica cada una de las opciones (equipos, licencias de software y certificados digitales), para así implementar la solución más conveniente.

Algunos trabajos futuros son:

- Implementación de la arquitectura propuesta, teniendo en cuenta las limitaciones de las redes móviles actualmente existentes en el país en cuanto a velocidades de acceso GPRS.
- Pruebas de seguridad sobre la implementación obtenida, que permitan validar la escogencia de soluciones particulares y formular soluciones alternativas en caso de ser necesario.
- Construcción de una plataforma para facturación y el pago de servicios ubicuos en ambientes móviles, que defina los protocolos necesarios para realizar la facturación y el pago de servicios ubicuos en ambientes móviles de forma segura y conveniente, y además establezca recomendaciones para la implementación e implantación de la arquitectura y los protocolos definidos en el contexto colombiano.

## BIBLIOGRAFÍA


1. Ishii Hiroshi. Bottles: A Transparent Interface as a Tribute to Mark Weiser. IEICE Transactions Inf. And Syst, Vol. E87-D, Número 6. p. 1299-1311. Junio 2004.
2. Weiser Mark. The Computer for the 21st Century. Scientific American Ubicomp. Septiembre 1991.
3. Z Weiping, W Dong, S Huanye, Dep. of Computer Science & Engineering, Shanghai Jiaotong University: Mobile Rfid Technology For Improving M-Commerce. IEEE International Conference on e-Business Engineering. 2005
4. L Wei, Z Chenglin, Z Wei, Z Zheng ,Z Feng, L Xiaoji, F Jielin, K KyungSup: The Gprs Mobile Payment System Based On Rfid. Communication Technology, 2006. ICCT '06. International Conference on. Noviembre 2006.
5. Espaldarazo a la Factura Electrónica. Revista Dinero – Sección Tecnología. p. 66 - 67. Junio de 2007.
6. Satyanarayanan M, Carnegie Mellon University. Pervasive Computing: Vision and Challenges. Personal Communications. p. 10 - 17. Agosto 2001.
7. Sunaga H, Takemoto M, Yamato Y, Yokohata Y: Ubiquitous Life Creation Through Service Composition Technolgies. World Telecommunications Congress 2006 - WTC2006.
8. P Boddupalli, F Al-Bin-Ali, N Davies, A Friday, O Storz, M Wu, Department of Computer Science University of Arizona, Arizona, United States: Payment Support In Ubiquitous Computing Environments. Fifth IEEE Workshop

on Mobile Computing Systems & Applications. 2003.

9. Roussos G. Birkbeck College, University of London. Enabling RFID in Retail. IEEE Computer Magazine, Vol 39. p. 25 – 30. Marzo 2006

10. Anokwa Y, Borriello G, Pering T, Want R, Computer Science and Engineering University of Washington Seattle: A User Interaction Model for NFC Enabled Applications. Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, 2007.

11. Nokia 6131 NFC SDK: User's Guide. Forum Nokia. Julio de 2007.

12. WG8 Working Group 8 ISO/IEC JTC1/SC17. Project Details on: ISO/IEC 15693, Vicinity cards (VICCs). Disponible en: http://www.wg8.gipp.com/sd1.html#15693

13. WG8 Working Group 8 ISO/IEC JTC1/SC17. Project Details on: ISO/IEC 14443, Proximity cards (PICCs). Disponible en: http://www.wg8.gipp.com/sd1.html#14443.

14. Tag iCLASS Datasheet. HID Global. 2007. Disponible en: http://www.hidcorp.com/documents/iclass_tag_ ds_es.pdf

15. iCLASS® RW100, RW300, RW400 Readers Datasheet. HID Global. Abril de 2007. Disponible en: http://www.hidcorp.com/documents/iclass_rw10 0_300_400_ds_en.pdf

16. Lightweight Directory Access Protocol (LDAP): The Protocol. IETF Proposed Standard RFC 4511. Junio de 2006. Disponible en: http://tools.ietf.org/html/rfc4511.

17. The OpenLDAP Project Overview. OpenLDAP Project Foundation. 2007. Disponible en: http://www.openldap.org/project/

18. Kannel: Open Source WAP and SMS Gateway – Overview. The Kannel Group. 2006. Disponible en: http://www.kannel.org/overview.shtml

19. jSMS – Java SMS & MMS API – Overview. Object XP. 2007. Disponible en: http://www.objectxp.com/products/jSMS/

20. JavaMail API Specification. Sun Microsystems, Inc. 2007. Disponible en: http://java.sun.com/products/javamail/reference/ api/index.html

21. Varela Rubén. Criptografía, Una Necesidad Moderna. Revista Digital Universitaria, Vol. 7. Departamento de Seguridad en Cómputo en DGSCA, UNAM. Julio de 2006. Disponible en: http://www.revista.unam.mx/vol.7/num7/art56/j ul_art56.pdf

22. What is Metro? GlassFish Metro. Disponible en: https://metro.dev.java.net/discover/

23. GlassFish. GlassFish Community. Disponible en: https://glassfish.dev.java.net/public/users.html

24. Java Naming and Directory Interface (JNDI). Sun Microsystems, Inc. 2008. Disponible en: http://java.sun.com/products/jndi/

25. Ondrus J, Pigneur Y, INFORGE - Ecole des HEC University of Lausanne, Switzerland: A Disruption Analysis in the Mobile Payment. Proceedings of the 38th Annual Hawaii International Conference on System Sciences. 2005.

26. Vásquez A, Depto, Ing. Eléctrica y Computación, UACJ (Universidad Autónoma de Ciudad Juárez): Estándares de Métodos de Pago por Móvil. Revista Cultura Científica y Tecnológica CULCyT, 2006.

## CURRÍCULOS

**Zeida María Solarte.** Ingeniera Electrónica de la Universidad del Cauca, en 1990. Especialista en Redes y Servicios Telemáticos, por la Universidad del Cauca en 1999. Magíster en Ingeniería, área Telemática, Universidad del Cauca, en 2005. Profesora titular de la Corporación Universitaria Autónoma de Occidente de Cali.

**Oscar Mauricio Caicedo.** Ingeniero en Electrónica y Telecomunicaciones, Universidad del Cauca, 2001. Especialista en Redes y Servicios Telemáticos, Universidad del Cauca, 2003. Magíster en Ingeniería, área Telemática, Universidad del Cauca, 2006. Coordinador del grupo de interés en desarrollo de aplicaciones móviles e inalámbricas W@PColombia y miembro del grupo de Ingeniería Telemática.

Docente del departamento de Telemática de la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca.

**Milton Royers Ausecha Penagos.** Estudiante del programa de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca, candidato a recibir el título en 2008. Durante el período 2007-2008 se desempeñó como vicepresidente de la rama estudiantil IEEE de la Universidad del Cauca, y coordinador del comité académico del Cuarto Seminario Nacional de Tecnologías Emergentes en Telecomunicaciones TET 2007, evento organizado por este grupo estudiantil en la ciudad de Popayán.

Actualmente se encuentra realizando su trabajo de tesis en servicios de pago y facturación para servicios ubicuos y pertenece al semillero de investigaciones en aplicaciones móviles e inalámbricas W@PColombia en el área de nuevos servicios.

**Javier Fernando Imbús Guzmán.** Estudiante del programa de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca, candidato a recibir el título en 2008. Durante el período 2005-2006 se desempeñó como vicepresidente de la Fundación Pulsos FIET, y organizador de la tercera jornada FIET, evento organizado en la ciudad de Popayán. Actualmente se encuentra realizando su trabajo de tesis en servicios de pago y facturación para servicios ubicuos y pertenece al semillero de investigaciones en aplicaciones móviles e inalámbricas W@PColombia en el área de nuevos servicios.