Plataforma para el acceso a servicios desde dispositivos móviles utilizando parámetros de autenticación basados en SIM Card

Services Access Platform from Mobile Devices using SIM based Authentication Parameters

Recibido 14 de septiembre de 2006, aprobado 15 de junio de 2007.

Francisco Martínez
Estudiante de Maestría en Ingeniería. Coordinador del Grupo W@PColombia y miembro del Grupo de Ingeniería Telemática-GIT, Universidad del Cauca. Popayán, Colombia.
fomarti@hotmail.com ✉

Rodrigo Hernández
Ingeniero en Electrónica y Telecomunicaciones. Ingeniero de desarrollo de aplicaciones móviles, Toppmobile S.A. Miembro del Grupo W@PColombia. Cali, Colombia.

Jaime Caicedo
Ingeniero en Electrónica y Telecomunicaciones. Ingeniero de desarrollo de aplicaciones móviles, Colombia Games. Miembro del Grupo W@PColombia. Bogotá, Colombia.

Oscar Caicedo
MSc en Ingeniería. Coordinador del Grupo W@PColombia y miembro del Grupo de Ingeniería Telemática-GIT, Universidad del Cauca. Popayán, Colombia.

Javier Hurtado
Especialista en Redes y Servicios Telemáticos. Director del Grupo W@PColombia y miembro del Grupo de Ingeniería Telemática-GIT, Universidad del Cauca. Popayán, Colombia.

PALABRAS CLAVES
Firma digital, ICCID, IMSI, Java Card, Módulo SIM, SATSA.

KEY WORDS
Digital signature, ICCID, IMSI, Java Card, SIM Module, SATSA

RESUMEN
El acceso seguro a servicios desde terminales móviles implica un equilibrio entre el grado de seguridad requerido 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. Como respuesta a esta necesidad, el Grupo 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.

ABSTRACT
Services secure access requires a balance between the security level and device hardware and usability capabilities. These features require the design of models with a simple authentication and authorization scheme that also assure the information integrity. To solve this issue, the W@PColombia Group, developed the P3SIM platform in order to mobile applications may include security features based on SIM parameters.

INTRODUCCIÓN

El medio inalámbrico que utilizan los servicios móviles los hace más susceptibles a problemas relacionados con seguridad en comparación con los medios cableados. Desde que ingresó al mercado la telefonía celular digital GSM a inicios de los años 90, 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) [1]. Sin embargo, proporcionar un acceso seguro a servicios en redes de telefonía móvil requiere un balance entre el nivel de seguridad que se ofrece y las limitaciones de los dispositivos móviles. Estas limitaciones no sólo están relacionadas con el rendimiento (capacidad de procesamiento y memoria) y el medio que utilizan para intercambiar la información, 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.

Por esta razón, es necesario diseñar un modelo de autenticación simple y transparente para el usuario, que garantice la integridad y el no repudio de la información que se intercambia cuando se accede a un servicio específico desde un dispositivo 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 construido la plataforma P3SIM para facilitar el desarrollo de aplicaciones móviles seguras basada en los parámetros del Módulo de Identificación de Suscriptor (SIM) con propósitos de autenticación. W@PColombia logró un modelo transparente para el usuario ajustado a la usabilidad y seguridad que requieren los exigentes entornos del mundo moderno. 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) [2] y la adaptación de algunos procesos ligados al sector de artesanía en el entorno móvil [3].

MODELOS DE AUTENTICACIÓN PARA ACCESO A SERVICIOS DESDE DISPOSITIVOS MÓVILES

En general, para acceder a un servicio típico (comercio móvil, acceso a bases de datos, aplicaciones a nivel de intranet, etc.) a través de un dispositivo 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 una contraseña bajo dos aproximaciones:

a. Digitando la información de autenticación (login y contraseña) cada vez que se quiera hacer uso del servicio.

b. Digitando la información de autenticación tan sólo 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 [4]) haciendo innecesario el ingreso posterior 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 la contraseña se traduce en desperdicio de tiempo e incluso dinero por el uso de los recursos de la red cuando algunos de los parámetros es incorrecto y se requiere una nueva introducción del mismo. Igualmente, como una consecuencia directa de este comportamiento, los usuarios pueden optar por utilizar contraseñas cortas, fáciles de recordar pero también fáciles de vulnerar. Al respecto, actualmente existen en el mercado algunas iniciativas para autenticación desde dispositivos móviles que pueden ser enmarcadas dentro de esta aproximación; RSA, la división Seguridad de EMC, ha implementado una solución denominada RSA SecurID cuyo soporte ha sido extendido a dispositivos JME y plataformas Windows Mobile [5]. La idea básicamente radica en

proporcionar un mecanismo de autenticación basado en un password o código aleatorio que se usa sólo una vez y cambia cada cierto tiempo previamente establecido; de esta manera, el usuario inicialmente debe introducir su código PIN en la interface de la aplicación móvil y recibe un código o password RSA SecurID; posteriormente el usuario introduce dicho código como password en la aplicación que se desea asegurar y ésta lo envía para que su validación sea realizada por un software denominado RSA Authentication Manager; para cada acceso el password generado será diferente. Siguiendo esta misma línea, la empresa DeepNet Security ofrece dos soluciones para autenticación desde dispositivos móviles: Mobile 2x2 [6] ofrece un mecanismo de autenticación de doble vía a través de la misma filosofía de generación de passwords aleatorios que se usan una sola vez. Esta versión está dirigida a dispositivos Windows Mobile, Java ME, Symbian y Palm; por otro lado, la misma compañía ofrece la solución Mobile Pass [7] orientada a dispositivos de bajas capacidades que ofrece la entrega de los passwords aletorios a través de un mecanismo simple, pero al mismo tiempo universal, como SMS (Short Messaging Service).

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. Aunque en [2] se propone el uso de SRS (Secure Record Store) como mecanismo de almacenamiento persistente seguro del lado del dispositivo móvil, el grado de seguridad alcanzado no es tan alto como el que proporcionan módulos dedicados Hardware/Software de tipo SIM [8], WIM (Wireless Identity Module) [9], o WLAN Smart Card [10]. En este último caso, a pesar de la importancia que representa el hecho de llevar mecanismos de autenticación más seguros a los entornos WLAN, emulando de alguna manera lo que la SIM representa en las redes GSM [11], la plataforma que aquí se plantea está destinada fundamentalmente a entornos de redes de telefonía móvil.

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; a través de este modelo de autenticación, se propone que los parámetros almacenados en la SIM hagan parte del proceso de identificación no solo ante el operador sino también ante los proveedores de servicio.

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 128 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) [12].

La esencia del esquema de autenticación basado en parámetros SIM consiste en brindar a las aplicaciones el acceso a dos parámetros que identifiquen unívocamente a cualquier usuario. Después de analizar los archivos almacenados en la tarjeta SIM se llegó a la conclusión que los dos parámetros que cumplen estas condiciones son el ICCID (Integrated Circuit Card Identification) y el IMSI (International Mobile Subscriber Identity). El ICCID es un archivo de 10 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 8 bytes (en la mayoría de los casos) el cual 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) [13] [14].

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; este procedimiento puede realizarse durante la fase de suscripción al servicio, por ejemplo. Para acceder de forma segura al servicio, se crea una clave simétrica con base en el IMSI que debe ser gestionada por el dispositivo móvil (a través de la tarjeta SIM) y por el proveedor; de esta manera, el dispositivo móvil puede realizar transacciones 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 de la misma pero sí su integridad, entonces se debe usar la firma digital; por otro lado, si se requiere enviar poca información garantizando su integridad y confidencialidad entonces se debe usar el cifrado asimétrico.

LA PLATAFORMA P3SIM

OBJETIVOS Y RETOS DE IMPLEMENTACIÓN

El Grupo de Interés en el Desarrollo de Aplicaciones Móviles e Inalámbricas – W@PColombia de la Universidad del Cauca, desarrolló la Plataforma de Seguridad para Servicios móviles basada en SIM Card - P3SIM con el objeto de brindar a los desarrolladores de servicios móviles sobre redes de 2.5G y 3G las facilidades necesarias para adicionar características de seguridad a sus aplicaciones, de acuerdo con un modelo de autenticación basado en parámetros SIM.

El primer objetivo que se trazó para la construcción de P3SIM fue proporcionar un Framework simple y liviano que se encargara de abstraer la complejidad del intercambio de bytes entre la aplicación móvil y la tarjeta SIM. En segundo lugar, era indispensable que el Framework construido pudiera ampliarse (con algoritmos de cifrado más complejos) y ser personalizado según las necesidades de los proveedores de servicios. Para cumplir a cabalidad con los objetivos mencionados anteriormente, la disponibilidad de un ambiente de simulación que permitiera testear las aplicaciones Java ME desarrolladas y las versiones futuras de la plataforma se convirtió en un factor fundamental y en el principal reto en la construcción de P3SIM. Se invirtió un gran esfuerzo en la construcción de dicho ambiente puesto que las herramientas de simulación proporcionadas por el Wireless Toolkit de Sun [15] son bastantes limitadas y genéricas, ya que fueron construidas para comunicar una aplicación Java ME con una tarjeta inteligente de propósito general y no con un módulo SIM; por otro lado, proporciona métodos de cifrado muy sencillos (no manejan esquemas de cifrado asimétrico, por ejemplo), que deben ser complementados. Teniendo en cuenta las limitaciones anteriores, fue necesario diseñar un módulo que permitiera la comunicación entre el Wireless Toolkit y una herramienta externa capaz de manipular parámetros SIM (como el IMSI y el ICCID) y que, además, facilitara la comunicación con tarjetas SIM reales. Después de evaluar diferentes alternativas en el mercado, la herramienta seleccionada fue Aspects Developer [16], un Entorno de Desarrollo para smart cards que ofrece una librería (dll) a través de cual se habilita la comunicación con sistemas externos (el Wireless toolkit, en nuestro caso). De esta manera, el ambiente de simulación es el resultado de un híbrido entre las capacidades del Wireless Toolkit de Sun y Aspects Developer que se comunican a través de una aplicación Java SE; esta aplicación contiene un módulo JNI (Java Native Interface) que a través de Sockets habilita la comunicación entre estas dos herramientas.

CARACTERÍSTICAS DE LA PLATAFORMA

De acuerdo con los objetivos planteados en la sección anterior, la plataforma P3SIM ha sido estructurada en tres componentes principales:

- Un Framework para construcción de aplicaciones
- Un ambiente de compilación Java Card [17].
- 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, los cuales implementan un conjunto de métodos de alto nivel para el manejo de cifrado/descifrado simétrico o asimétrico y el manejo de firma digital a través de APIs como SATSA (Security and Trust Services API) [18]. 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 desee gestionar 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 al interior de la tarjeta SIM, como se explicó anteriormente.

Como se muestra en la Figura 1, la arquitectura del Framework P3SIM se compone de 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 generación y almacenamiento de claves, cifrado asimétrico y el acceso a parámetros GSM. Esta clase puede ser modificada para ampliar las capacidades del framework, como fue planteado en los objetivos para la construcción de la plataforma.
- *P3SIM:* Es la clase principal de la plataforma. Provee los métodos estáticos que pueden ser invocados por los desarrolladores que hagan uso del Framework.

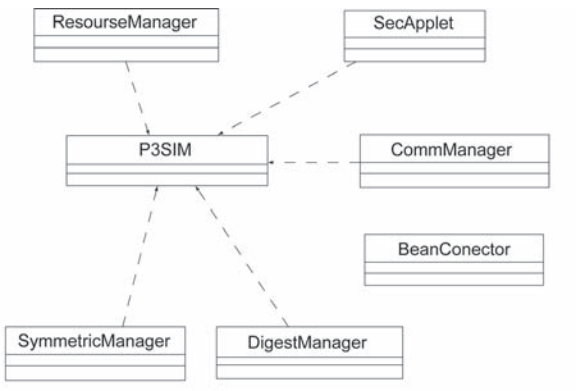

Figura 1. Arquitectura del framework P3SIM.

- *ResourceManager*: Es la clase encargada del manejo de los recursos necesarios para instalar el SECApplet en la tarjeta SIM.
- *CommManager:* Es la 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:* Es la 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 (Application Protocol Data Units) con las cuales se comunica P3SIM y el Applet de seguridad instalado en la tarjeta SIM.
- *SymmetricManager:* Es la clase encargada del manejo de la criptografía simétrica. Posee métodos necesarios para el cifrado y descifrado utilizando el algoritmo DES.
- *DigestManager:* Es la clase encargada de la generación de MessageDiggest y utiliza el algoritmo SHA-1, además permite la comparación de dos MessageDiggest a fin de verificar la validez de una firma.

A través del Framework descrito, la plataforma P3SIM ofrece 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 1024 bits) del usuario y una clave pública RSA de otra entidad [19].
- 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, lo cual garantiza la integridad, confidencialidad 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 que requieran acceso seguro a servicios desde dispositivos móviles, basado en los parámetros SIM del teléfono (Figura 2).

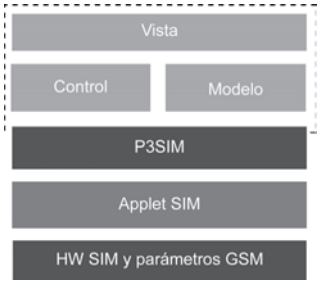

Figura 2. Arquitectura de referencia para el desarrollo de aplicaciones seguras con P3SIM.

En la parte baja de la torre se encuentra el hardware de la SIM (que incluye 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 permite, finalmente, cifrar pequeñas cantidades de información con criptografía asimétrica. La siguiente capa está conformada por el Framework P3SIM el cual se encarga de abstraer la complejidad del intercambio de bytes entre el móvil y la tarjeta SIM e implementa los métodos de cifrado simétrico y generación de hash (usado en la firma digital). En el siguiente nivel 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).

PRUEBAS DE LA PLATAFORMA P3SIM

Uno de los elementos clave en las pruebas de unidad de la plataforma P3SIM es la descarga y puesta en operación del Applet, que se descarga a la tarjeta SIM. En primer lugar, se diseñaron algunos archivos de prueba que contienen los comandos que gestionan las funciones del Applet, como se muestra a continuación:

```
powerup;
echo “Select SECApplet”;
0x00 0xA4 0x04 0x00 0x08 0xa0 0x0 0x0 0x0 0x62 0x1 0xd 0x1 0x7F;
echo “Solicitud de mi clave DES”;
0x70 0x01 0x00 0x00 0x00 0x08;
echo “Solicitud de la otra clave DES”;
0x70 0x02 0x00 0x00 0x00 0x08;
echo “actualizacion de mi clave DES”;
0x70 0x11 0x00 0x00 0x08 0x55 0x54 0x53 0x52 0x51 0x50 0x58 0x59 0x7F;
echo “Solicitud de mi clave DES”;
0x70 0x01 0x00 0x00 0x00 0x08;
echo “Solicitud de la otra clave DES”;
0x70 0x02 0x00 0x00 0x00 0x08;
echo “actualizacion de la otra clave DES”;
0x70 0x12 0x00 0x00 0x08 0x79 0x78 0x76 0x75 0x74 0x73 0x72 0x71 0x7F;
echo “Solicitud de mi clave DES”;
0x70 0x01 0x00 0x00 0x00 0x08;
echo “Solicitud de la otra clave DES”;
0x70 0x02 0x00 0x00 0x00 0x08;
echo “recalcula mi clave DES”;
0x70 0x21 0x00 0x00 0x00 0x7F;
echo “Solicitud de mi clave DES”;
0x70 0x01 0x00 0x00 0x00 0x08;
powerdown;
```

Luego de este proceso se comprobó el funcionamiento correcto de los métodos que acceden a los parámetros SIM y los que se encargan de gestionar el cifrado y descrifado de la información. En el primer caso, fue necesario recurrir a las capacidades del entorno Aspects Developer, ya que el Java Card Kit [20] de Sun no soporta esta funcionalidad. En el segundo caso, se utilizó la herramienta "cref" del Java Card Kit para simular una tarjeta cargada en el SECApplet y por medio de la utilidad "apdutool" se envió el archivo de comandos mostrado anteriormente, obteniendo las respuestas específicas para cada uno de los comandos enviados.

Para completar la integración de la plataforma, las pruebas de sistema fueron ejecutadas a través de los siguientes procedimientos:

- La instalación del Applet en la SIM simulada, por parte de un MIDlet.
- Crear una clave DES con base en un parámetro SIM.
- Obtener una clave simétrica de la tarjeta simulada y luego cifrar/descifrar información con dicha clave.
- Obtener un Hash de cualquier información, con los algoritmos soportados por SATSA.
- Generar y verificar una firma digital, para ello el Wireless Toolkit de Sun debe acceder a la tarjeta SIM simulada.

Se utilizaron tarjetas SIM Java Card Axalto USIMERA de 128 Kb y sólo fue posible descargar los applets empleando la herramienta VIEWS Professional, propietaria de Axalto. Otras herramientas como "Interoperable Loader" de la SIM Alliance no arrojaron resultados satisfactorios. A través de la realización de estas pruebas fue posible comprobar que el ambiente de simulación desarrollado proporciona las facilidades requeridas para que los desarrolladores realicen los tests de sus aplicaciones Java ME, las cuales acceden a parámetros SIM a través de SATSA, de forma transparente.

Finalmente, es necesario resaltar algunos aspectos importantes relacionados con el rendimiento de la plataforma P3SIM. Las capacidades computacionales exigidas a los dispositivos móviles habilitados para desempeñarse dentro de un entorno seguro se ven incrementadas proporcionalmente al nivel de seguridad requerido. De esta forma, es lógico que la integración de las capacidades de la plataforma P3SIM dentro de una aplicación móvil exija una cuota de recursos computacionales adicionales por parte del dispositivo que ejecuta la aplicación. En términos generales, las pruebas realizadas permiten afirmar que la cantidad de memoria extra exigida al integrar las capacidades de P3SIM, puede ser considerada como moderada y muy acorde a los niveles de seguridad y confiabilidad exigidos, como lo muestran las gráficas obtenidas a través del monitor de memoria del Wireless Toolkit (Figura 3). Sin embargo, la posibilidad de optimización de los algoritmos para disminuir el costo computacional permanece ligada a la implementación de las APIs de SATSA que realice el fabricante del dispositivo.

En cuanto al consumo de ancho de banda, P3SIM no incrementa el tráfico de datos del usuario puesto que la información útil es cifrada, pero se conserva la longitud del mensaje original a diferencia de los modelos de cifrado de información basados en XML, los cuales han demostrado un incremento significativo en el tráfico de datos entre la aplicación móvil y el servidor, a pesar de los esfuerzos que se han realizado para su compactación.

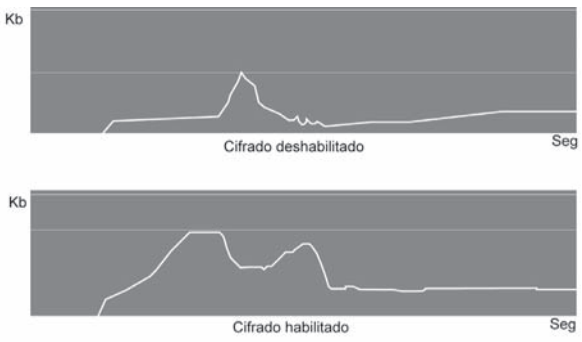

Figura 3. Consumo de memoria P3SIM.

PROTOTIPO DE VALIDACIÓN

Para validar las funcionalidades de la plataforma, se implementó un prototipo 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. En la Figura 3 se muestra la arquitectura de la aplicación que reside en el teléfono móvil y 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 y acceder 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, el usuario introduce sus datos personales y éstos son enviados por la aplicación al servidor, adicionando los parámetros IMSI e ICCID del módulo SIM, para que sean registrados por parte del proveedor del servicio. Cuando el usuario desea acceder al servicio posteriormente, el proceso de autenticación se basa en estos parámetros SIM, lo cual evita el uso de un login y contraseña como se plantea en el modelo tradicional.

Las ventajas del uso de la plataforma P3SIM no sólo se reflejan en el proceso de autenticación, sino también en cualquiera de las operaciones clásicas que se puede 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 los datos. 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; logrando así

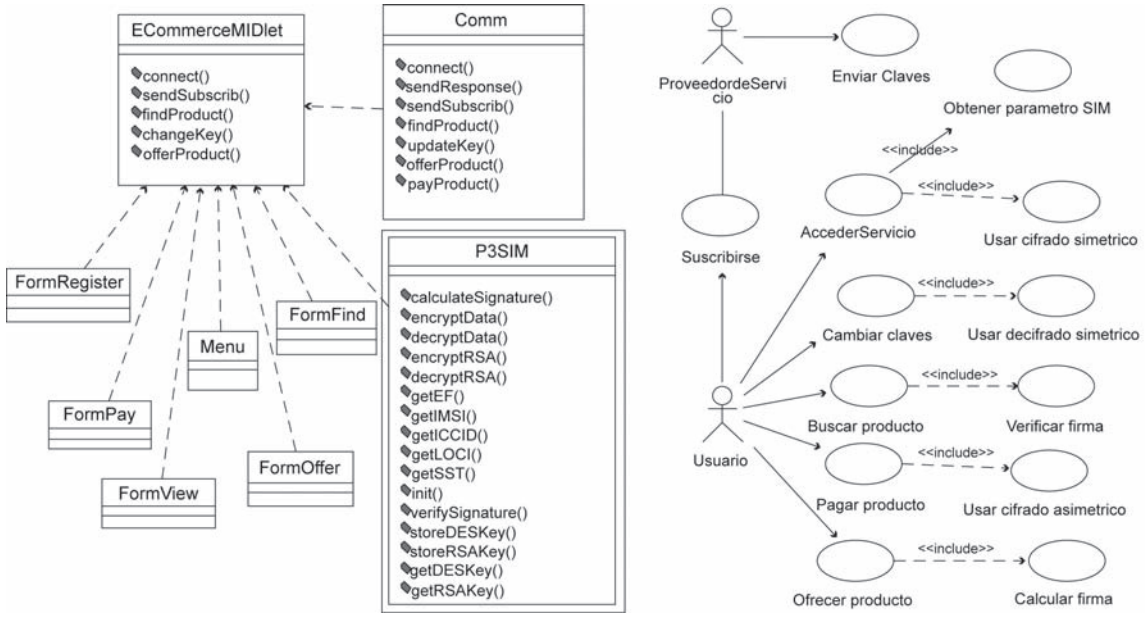

Figura 4. Arquitectura de la aplicación cliente.

un proceso de autenticación en ambos sentidos. En el caso de una transacción electrónica, el prototipo utiliza cifrado asimétrico para el número 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.

Como conclusiones importantes acerca del prototipo de validación es importante resaltar que el solo hecho de almacenar las claves tanto simétricas como asimétricas en una tarjeta inteligente como la tarjeta SIM, brinda al sistema un nivel de seguridad importante. Por otro lado, el framework P3SIM se ha construido basado en premisas de seguridad ampliamente usadas y probadas, como por ejemplo las utilizadas en la clave RSA privada del usuario a la cual sólo se le permite ser creada o actualizada, pero nunca puede ser obtenida o extraída de la tarjeta SIM. Finalmente, la plataforma P3SIM brinda la flexibilidad requerida para realizar transacciones con el nivel de seguridad requerido: por ejemplo, usar cifrado simétrico para intercambiar un gran volumen de información que no requiere un alto nivel de seguridad o usar el cifrado asimétrico para intercambiar un pequeño volumen de información con requerimientos de seguridad exigentes, como en el caso del intercambio del número de tarjeta de crédito o cuenta bancaria, descrito previamente.

CONCLUSIÓN

La plataforma P3SIM ofrece nuevas posibilidades para el desarrollo de aplicaciones móviles que requieren acceso seguro, al tiempo que mejora la usabilidad a través de procesos de autenticación totalmente transparentes para el usuario. P3SIM reúne las ventajas de identificación que proporciona el módulo SIM, ampliamente desplegado en las redes de telefonía móvil modernas, y las capacidades que ofrecen en materia de seguridad APIs como SATSA y JavaCard en el entorno de las aplicaciones Java ME, la plataforma más exitosa para el desarrollo de aplicaciones móviles en el mundo. Aunque el despliegue de APIs como SATSA o Java Card es incipiente en los terminales actuales, el grupo 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 mayor despliegue actualmente, como lo es la telefonía móvil.

REFERENCIAS

[1] ETSI.
Security mechanisms for the SIM Application Toolkit., GSM 02.48 Specification

[2] O. Caicedo, D. Cerón, D. Chamorro, F. Martínez, y J. Hurtado.
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 de 2006

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

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

[5] EMC News.
RSA Broadens Reach of RSA SecurID® Two-Factor Authentication Solution with Expanded Support for Leading Mobile Device Platforms. EMC, Abril, 2007. Disponible en: http://www.emc.com/news/emc_releases/showRelease.jsp?id=5053&printtest123=PRINTABLE

[6] DeepNet Security, Mobile 2x2™.
DeepNet Security, Enero, 2007. Disponible en: http://www.deepnettechnologies.com/products/mobile2x2.asp

[7] DeepNet Security, MobilePass™.
DeepNet Security, Enero, 2007. Disponible en: http://www.deepnettechnologies.com/products/mobilepass.asp

[8] 3GPP.

Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) Interface, Junio, 2006. Disponible en: http://www.3gpp.org/ftp/Specs/html-info/1111.htm

[9] WAP Forum

Wireless Identity Module - Part: Security, WAP Forum, Julio, 2001. Disponible en: http://www.wapforum.org/tech/documents/WAP-260-WIM-20010712-a.pdf

[10] WLAN Smart Card Consortium

WLAN-SIM Specification Version 1.0. , WLAN Smart Card Consortium, Octubre, 2003. Disponible en: http://wlansmartcard.org/specs/WLAN-SIM-V1.pdf

[11] A. Ahmad, R. Chandler, A. Dharmadhikari, y U. Sengupta.

"SIM-Based WLAN Authentication for Open Platforms". *Technology Intel Magazine*, Agosto, 2003. Disponible en: http://www.pcparents.com/technology/magazine/communications/wi08031.pdf

[12] S. Redl, M. Weber, y M. Oliphant.

GSM and Personal Communications Handbook Norwood: Artech House,1a ed., 1998, pp. 303 – 344.

[13] 3GPP

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

[14] S. Guthery y M. Cronin.

Mobile Application Development with SMS and the SIM Toolkit. New York: McGraw-Hill Professional, 1a ed., 2001

[15] Sun MicroSystems, Sun Java Wireless Toolkit for CLDC.

Enero, 2006. Disponible en: http://java.sun.com/products/sjwtoolkit/

[16] Aspects Software

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

[17] Z. Chen.

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

[18] JSR 177 Expert Group

Security and Trust Services API (SATSA) for Java MicroEdition., Java Community Process Program, Sun Microsystems Inc, Julio 2004, pp. 1-3.

[19] A. Fúster, D. Martínez, L. Encinas, F. Montoya, y J. Muñoz.

Técnicas criptográficas de protección de datos. México, Alfaomega, 2a ed. 2001, pp. 115-164.

[20] Sun MicroSystems

Java Card Development Kit., Marzo, 2006. Disponible en: http://java.sun.com/products/javacard/dev_kit.html

BIBLIOGRAFÍA

Sun Microsystems.

J2ME Specification. Disponible en: http://java.sun.com/j2me/index.jsp.

D. Peláez.

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.

D.A. Ponce.

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.

SIM Alliance Web Site

Disponible en: http://www.simalliance.org/

Axalto. USIMERA

The USIM card for 3G services. Disponible en: http://www.axalto.com/wireless/usimera.asp