A. Munoz, J. A. Onieva, and J. Lopez, "Perfiles Seguros para Comercio Movil", *III Simposio Español de Comercio Electronico (SCE05)*, pp. 235-244, 2005.
NICS Lab. Publications: https://www.nics.uma.es/publications

Perfiles Seguros para Comercio Móvil

Antonio Muñoz, José A. Onieva y Javier López

Dpto. Lenguajes y Ciencias de la Computación, Universidad de Málaga
29071- Málaga, España
{amunoz, onieva, jlm}@lcc.uma.es

Resumen. Los escenarios de comercio móvil existentes en la actualidad presentan muchas deficiencias. La mayoría de estos escenarios, como no podría ser de otra forma, tienen en cuenta aspectos relativos a la seguridad, prestando especial atención a las propiedades de Autenticación y Autorización. De entre los elementos esenciales que se utilizan para proporcionar estos servicios de seguridad, los perfiles son un elemento común que permiten la personalización de los servicios del usuario móvil. Sin embargo, los perfiles también precisan de una administración segura. En este trabajo presentamos unas consideraciones iniciales respecto a los distintos tipos de perfiles, sus niveles de seguridad para cada tipo, así como indicaciones para el almacenamiento de manera segura. Por lo tanto, analizaremos las distintas alternativas como medio de almacenamiento, discutiéndolas y prestando especial atención a las tarjetas inteligentes.

1. Introducción

El estado actual del *comercio electrónico* es una buena muestra de que la tecnología subyacente no ha alcanzado aún todo su potencial. Esta afirmación es todavía más concluyente si consideramos un área particular del comercio electrónico, como es el caso del comercio en entornos móviles. Durante la segunda mitad de la década de las 90 multitud de predicciones auguraban una rápida y revolucionaria evolución. Así, en 1999, Forrester Research predecía un volumen de 184 billones de dólares en ventas on-line sólo en Estados Unidos [1]. Sin embargo, hasta finales de 2003 sólo se habían alcanzado los 55 billones de dólares. Las cifras parciales en 2004 no hacen concluir que las perspectivas hayan mejorado.

Algunas de las mayores razones atribuidas tanto por la comunidad investigadora como por estudios empíricos a la gran diferencia entre las cifras esperadas y las reales van referidas a la *seguridad* y *privacidad*. Así, un muy elevado número de usuarios no se "enganchan" al comercio electrónico simplemente porque la falta de seguridad y privacidad se traduce en una manifiesta falta de confianza por parte de tales usuarios en la tecnología subyacente de la información y las comunicaciones. Este problema se agudiza por la evolución natural de tales tecnologías, que están llevando al uso masivo y generalizado de dispositivos en entornos móviles. Precisamente, la evolución del comercio electrónico hacia este tipo de entornos, originando el *comercio móvil*, agudiza más, si cabe, los problemas de seguridad y privacidad y, por ende, de la falta de confianza por parte de los usuarios en unos servicios de comercio móvil donde todo es aún menos "tangible" que en el propio comercio electrónico basado en redes cableadas.

El comercio móvil utiliza tecnologías de computación que permiten la interacción entre los usuarios a través de dispositivos móviles y fácilmente portátiles, infraestructuras wireless y cualquier otro elemento que facilite tal interacción y la localización espacio temporal. Dentro de la infraestructura necesaria para llevar a cabo el comercio móvil podemos encontrar procesadores de tamaño limitado, redes, protocolos, servicios y el espacio físico que los rodea (que pasa a ser un elemento más de la computación).

En muchas ocasiones, la interacción de una gama tan variada de componentes es extremadamente difícil, lo cual provoca, como comentábamos antes, que la confianza que en éstas se deposita sea aún menor que en el comercio electrónico más tradicional. La configuración, administración y monitorización de estos dispositivos es complicada, y la aplicación de políticas de seguridad de forma uniforme es prácticamente imposible. Esto se debe a que mientras algunos dispositivos poseen complejos mecanismos de seguridad, otros pueden ser limitados en cuanto a sus recursos, y por lo tanto incapaces de cumplir requisitos de seguridad muy exigentes. Además, los problemas de *autenticación* y *autorización* se vuelven más complejos, precisamente por la capacidad de movilidad de los usuarios y la no utilización de infraestructuras fijas de comunicación [2].

Por otro lado, en estos escenarios es aún más relevante la consideración del derecho a la *privacidad* de los usuarios [3]. Es de vital importancia[1] controlar cómo se usa esta información (lo cual no es estrictamente equivalente al control de acceso a la misma). En ocasiones, distintos actores necesitan acceder a información que por sí misma no supone ninguna amenaza a los individuos (salario medio, productos populares,...), pero que precisa de la compilación de datos más sensibles (salario de un individuo, compras favoritas,..). Por lo tanto, realizar las operaciones privadamente se convierte en el medio que distintas entidades utilizan para pactar (computacionalmente) los distintos usos posibles de datos que puedan ser sensibles y de esta forma prevenir usos no autorizados.

Nuestra consideración es que para obtener un sistema que cumpla con los requisitos de autenticación y autorización, por un lado, y privacidad, por otro, es necesario hacer uso de un nuevo elemento que debe poder ser portátil y susceptible de ser almacenado de forma segura. Se trata de un repositorio de información relacionada con el usuario, red, dispositivos en uso, etc. Esta información será utilizada para los servicios de autenticación, autorización del sistema e incluso para desempeñar tareas como el almacenamiento o caching de las preferencias de cada usuario. Aparece, pues, el concepto de *perfil*. Si, además, tenemos en cuenta la importancia de la seguridad en comercio móvil de tarjetas inteligentes y en concreto en EAP [5], el uso de estas tarjetas para el almacenamiento de perfiles en escenarios de móviles se convierte en trascendental.

Las tarjetas inteligentes son principalmente usadas para la autenticación de usuarios, aunque pueden proporcionar características más atractivas. Si bien limitadas en velocidad y espacio, los chips integrados contienen un microprocesador, ROM, memoria y su propio Sistema Operativo COS (Chip Operating System), en el que varias aplicaciones pueden ejecutarse. A modo de ejemplo, las tarjetas inteligentes pueden usarse como puntos de acceso a servicio móvil. Por otra parte, las tarjetas

---

[1] De hecho, el termino privacidad es quizás uno de los más usados en la provisión de servicios de seguridad a las distintas tecnologías que se investigan y desarrollan en los Planes de I+D de la Sociedad de la Información

inteligentes pueden almacenar información de usuario, invocar servicios y procesar los resultados del mismo de forma temporal. Por esta razón, pensamos que las tarjetas inteligentes son un vehículo para la implementación de los escenarios de comercio móvil, de forma que los usuarios tengan la posibilidad de acceder a los servicios desde cualquier localización usando sus tarjetas inteligentes en dispositivos portátiles como una PDA (Personal Digital Asistant).

Antes de discutir el almacenamiento seguro de los perfiles, estableceremos una clasificación de éstos, examinando el nivel de seguridad de cada tipo, identificando los distintos campos de los cuales se componen, así como los riesgos potenciales asociados a cada tipo de perfil. Con esta línea de desarrollo estructuramos este artículo en las secciones siguientes: en la sección 2 presentamos y desarrollamos la clasificación. En la sección 3, identificamos nuevos campos (que deberán ser almacenados de forma segura) al mismo tiempo que clasificamos los distintos niveles de seguridad para los perfiles. En la sección 4 revisamos las posibles alternativas para el almacenamiento de los perfiles, concluyendo y argumentando que las tarjetas inteligentes son el medio más adecuado para dicha tarea. Finalmente, concluiremos el artículo y apuntaremos las líneas futuras de trabajo.

2. Clasificación de los distintos tipos de perfiles

En la actualidad, existe un amplio campo abierto, así como distintas iniciativas en la tecnología de perfiles debido en gran parte al auge de los entornos móviles en la investigación. De entre las distintas iniciativas existentes, encontramos formatos diseñados para la definición de perfiles (RDF[9], vCard[10], …), marcos de trabajo y middleware para la administración de una posible infraestructura de perfiles (J2ME[11], OSGi,[12] …), técnicas de Inteligencia Artificial que permiten la implementación de perfiles que aprenden y evolucionan de acuerdo al contexto (Lógica difusa, redes bayesianas, …) y finalmente características especiales de los dispositivos que tienen un impacto importante en la forma de definir y administrar los perfiles. Más información, así como las referencias adecuadas a las distintas iniciativas existentes pueden encontrarse en el documento de trabajo [7].

Una alternativa a la definición de perfil presentada en la sección anterior, de la que haremos uso para caracterizar a las distintas entidades de una forma única, expone al perfil como “un repositorio de datos estructurados que influye en otras entidades y que al mismo tiempo supone la localización donde las propiedades y características son almacenadas en estados temporales presentes y pasados”.

Nuestra definición de perfil esta *centrada en el usuario*, ya que empleamos el perfil de usuario como la composición de los perfiles de red, dispositivos, aplicaciones, servicios, contexto. A su vez el perfil de usuario tiene una serie de campos propios con información relativa al usuario en sí, con idea de facilitar la comprensión del presente artículo vamos a diferenciar entre perfil user-centric, que hará referencia a aquel perfil que es composición del resto, frente al perfil de usuario, con sus distintos campos. La justificación de esta composición aparece de una forma sencilla teniendo en cuenta que no tiene sentido hablar de todos estos tipos de perfiles si no están en última instancia ligados a la existencia de un usuario. No obstante, todos estos tipos de perfiles existen por sí solos, e incluso se pueden definir perfiles más detallados o

subconjuntos de los mismos. A estas estructuras las hemos denominado como *subperfiles*.

Los subperfiles presentan las mismas características que los perfiles, con una única restricción: su unión constituye precisamente un perfil; es decir, la unión de todos los subperfiles de un perfil forman el mismo perfil, y además la intersección de cualquier par de subperfiles ligados a un perfil es nula. Con este concepto, podemos distinguir entre subperfiles estáticos o dinámicos en función del momento de creación de los

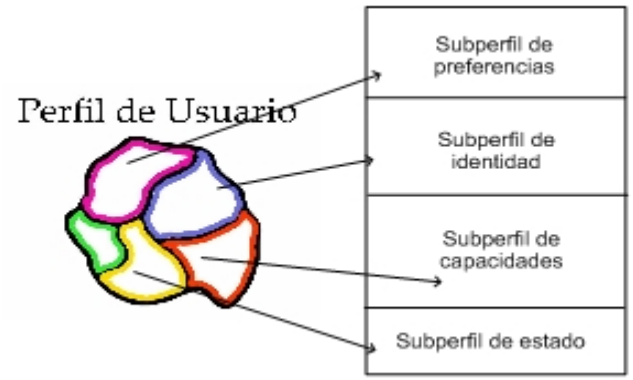

Fig. 1. Composición de un perfil

datos del perfil contenedor. También podemos distinguir entre subperfiles de identidad de usuario, de relación de usuario, de capacidad del usuario y de preferencias del usuario de acuerdo a la semántica de sus datos.

Así, en la figura se muestra como el perfil de usuario esta compuesto por varios subperfiles, a su vez disjuntos entre sí. Así aparecen en la figura los campos de subperfil de preferencias, subperfil de capacidades, subperfil de información de identidad, información del estado actual del usuario y otra información relacionada. Al igual que ocurre con los perfiles de usuario, ésta metodología es extrapolable a los otros tipos de perfiles previamente citados. Así podemos listar los subperfiles de descripción de dispositivos, de descripción hardware de estos dispositivos, de identificación de la información de la red, de seguridad de red, de información IP de red, de carga de información de red, etc., para la composición del perfil de dispositivo. Describimos el perfil de red como una composición de un subperfil de información general de la red y un subperfil de información específica de la red (que más tarde detallaremos). De la misma forma los subperfiles de información general y de información funcional del servicio a proveer se combinan para formar el perfil de servicio. Con respecto a los perfiles de contexto, hemos encontrado que se componen principalmente de un subperfil de localización más un subperfil de información del entorno.

Si profundizamos un poco más en el primer tipo de perfil, y más concretamente en el subperfil que concierne a la identidad de usuario, éste va a tener una serie de campos relativos a la información contenida en los mismos. Entre los campos que podemos encontrar se encuentran: nombre, apellidos, nick, género, fecha de nacimiento, ocupación, idioma(s), dirección, email, teléfono, fax, mensajería

instantánea e incluso un número identificador del usuario en nuestro sistema. Esta información es bastante delicada y por tanto "privada", puesto que este tipo de información está íntimamente relacionada con la identidad del individuo en sí. En otros tipos de subperfiles de usuario, como el de preferencias, aparecen campos como: dispositivos preferidos, sistemas preferidos, aplicaciones preferidas, parámetros de configuración de estas aplicaciones, aplicaciones menos preferidas, servicios preferentes, así como los parámetros de configuración de estos, servicios menos preferentes, modalidades de interacción preferidas y las menos preferidas. Como podemos apreciar, este tipo de información no es tan delicada. Así pues, ¿como almacenar esta información contenida en los perfiles?.

Un ejemplo que nos hará ver la importancia del almacenamiento seguro de los perfiles de una forma mucho más clara es el expuesto en el siguiente escenario: un usuario llamado Katto tiene un dispositivo con interfaz USB en el cual tiene almacenada cierta información relativa tanto a sus datos personales como a sus preferencias de usuario, información que está estructurada en forma de perfil. Katto está de viaje fuera de su ciudad y quiere conectarse a la red con su configuración habitual, para lo cual decide ir a un cybercafe que ha visto en una calle próxima al hotel en que se hospeda. Katto no dispone de mucho tiempo, de manera que quiere hacer uso de los perfiles que lleva consigo en su dispositivo USB para agilizar el proceso. Una vez en el cyber, inserta su dispositivo en uno de los puertos USB de los que dispone la maquina que tiene asignada en el cybercafe. Al hacer esto, todos sus datos personales podrían ser cacheados a la máquina a la que se conecta.

En lo concerniente a los datos relativos a preferencias no hay problema puesto que, en principio, no plantea ningún problema el que esta información quede cacheada en la máquina del cibercafé, puesto que lo más peligroso que puede ocurrir es que a otra persona le guste e intente imitar y tomar como propios los gustos de Katto en la interacción con el PC; datos como el fondo de pantalla, la configuración de los iconos, sonidos, etc. En cambio, en el tema de los datos personales la cosa cambia sustancialmente, puesto que hay contenida información potencialmente peligrosa si es capturada por algún usuario malicioso; datos como pueden ser métodos de acceso, numero de cuentas bancarias, direcciones, contactos, etc.

Por lo tanto, para obtener un buen nivel de seguridad, no debemos olvidar que al menos parte de la información deberá ser almacenada de forma segura para el usuario. Un primer enfoque lo podemos encontrar en el almacenamiento del perfil completo de forma segura, con idea de que en posteriores versiones se relajen las restricciones de seguridad de acuerdo a la semántica de los datos. Este enfoque, al margen de la eficiencia inicial, es el mejor desde un punto de vista práctico, pues nos será más fácil relajar las restricciones de seguridad que, por el contrario, hacerlas más estrictas.

3. Clasificación de los distintos niveles de seguridad para los perfiles

Con todo lo expuesto hasta el momento, establecemos distintas categorías en lo que al nivel de seguridad se refiere, es decir, tendremos ciertos elementos (perfiles, subperfiles o incluso conjuntos de campos pertenecientes a los anteriores) que sean delicados (información personal) y deban ser tratados con mayores medidas de seguridad; y en el extremo opuesto tendremos otros para los que las medidas

necesarias a tomar sean mínimas e incluso nulas. Como es de esperar, entre ambos extremos nos encontraremos un abanico de posibilidades que engloba a la mayor parte de los campos pertenecientes a un perfil, aunque en este trabajo sólo vamos a tratar un caso intermedio en aras de mayor claridad. Dicho esto, pasamos a incluir los distintos campos en sus respectivos niveles de seguridad indicados (*alto, medio y bajo*).

Dado que el perfil de usuario es el perfil que en cierta medida engloba a todos los demás, y dado que este estudio acerca de los perfiles se ha llevado a cabo para entornos centrados en el usuario, vamos a comenzar por él. Como previamente mencionábamos, en éste podemos encontrarnos información relativa a la identidad, relaciones, capacidades y preferencias del usuario, desgranando los campos uno a uno. Además, hacemos su clasificación respectiva dentro de los distintos niveles de seguridad.

- Alto: Nombre, apellidos, género, fecha de nacimiento, ocupación, dirección, email, números de cuentas bancarias, números de teléfono y mensajería instantánea.
- Medio: Identificador de usuario, nick e idioma.
- Bajo: Capacidades y preferencias. También algunos datos relativos a la interacción con los dispositivos.

La información de la *relación* se divide en distintas categorías; así que, en este apartado, tendremos ciertos campos con información muy delicada como pueden ser, la relación con otros usuarios, y qué tipo de relación se mantiene con ellos. Esta entrará pues en el nivel más alto de seguridad. También habrá campos relativos a intereses del usuario que en muchos casos no tienen porqué tratarse con tanto rigor y que englobamos en un nivel medio. Y por último, también habrá relaciones con dispositivos que pueden estar incluidas en un nivel bajo de seguridad.

Los *perfiles de dispositivos* están compuestos a su vez, por un lado del subperfil de características hardware, del subperfil de características software y también por los subperfiles de limitaciones hardware y software. Pensamos que el grado de seguridad que debe ser tomado en cada uno de ellos corresponde a:

- Medio: Algunos datos de los subperfiles de características software, como son: número de serie de la copia instalada, propietario de la copia, nombre del SO, vendedor del SO, versión del SO, revisión del SO, paquetes de seguridad instalados, etc.
- Bajo: Características y limitaciones hardware. Tipos de interfaces, versiones de los interfaces, resolución de la pantalla, tamaño de la pantalla, hardware para la reproducción de audio, tipo de sistema soportado, tipo de teclados, ratón, touchpad, tipo de memoria, tamaño de memoria, velocidad de memoria, reloj de memoria, latencia de memoria, localización de la memoria, familia y tipo de procesador, vendedor, bus, etc.

En cuanto a los perfiles de red, la clasificación es la siguiente:

- Alta: Subperfil de información general con campos como identificación de red, seguridad IP, información de facturación, etc.

- Media: Subperfil de información específica que contiene datos técnicos y de rendimiento de la red. No se trata de información crítica, pero la conjunción de estos datos podría ser utilizada por un agente malicioso.

Los perfiles de *servicio, aplicación y contexto* presentan datos que permiten su clasificación dentro del grupo de bajo nivel, puesto que la información aquí contenida está orientada a facilitar la interacción del usuario con sus dispositivos y el software lo cual no reporta gran riesgo.

4. Tarjetas inteligentes para el almacenamiento de perfiles en entornos de comercio móvil

La idea del uso de perfiles en entornos de comercio móvil está concebida para la movilidad y portabilidad de los mismos por parte del usuario, es decir, la información contenida en los perfiles ha de formar parte del usuario en todo momento. Así que uno de los requisitos imprescindibles que ha de cumplir un dispositivo para el almacenamiento de perfiles va a ser la *portabilidad*. Por otro lado, y como ya hemos citado con anterioridad, habrá cierta información contenida muy delicada en los perfiles, por lo cual será necesario un almacenamiento seguro de los mismos, de manera que el dispositivo de almacenamiento deberá de cumplir una serie de *requisitos mínimos de seguridad*. Una vez hemos esbozado los principales requisitos para un dispositivo destinado al almacenamiento de perfiles, vamos a ver las características que nos aportan las distintas alternativas y porqué hemos llegado a la conclusión de que el uso de tarjetas inteligentes es el más apropiado.

El primer conjunto de dispositivos comentados son los lápices USB, que en el caso concreto tiene unas características muy similares a cualquier dispositivo de almacenamiento masivo que utilice una conexión USB (MMC, SD, HD USB externos, etc.). Estos dispositivos tienen la ventaja de que ser portátiles para el usuario, con lo cual en cualquier momento están con él. No obstante se tratan de dispositivos poco seguros, de manera que si estos fuesen perdidos o robados podrían ser usados sin autorización.

Los dispositivos de almacenamiento masivo locales además de tener el defecto de los anteriores ni tan siquiera son portátiles. Otra alternativa posible es el uso de bases de datos remotas, cuya opción es interesante puesto que cumple tanto los requisitos de portabilidad (si pueden ser accedidas desde cualquier punto) como de seguridad. No obstante, ambas cualidades tienen sus inconvenientes. Con respecto a la seguridad, hay alternativas para acceder a una base de datos de forma remota y segura, alternativas que requieren del uso de ciertas tecnologías que podrían llegar a ser muy costosas para el propósito de acceder a ciertos datos del perfil, puesto que haría falta el establecimiento de un canal seguro, compartición de claves, etc. El otro inconveniente es que el usuario no podría hacer uso de su perfil en un entorno desconectado, lo cual limita de algún modo el requerimiento de portabilidad de los mismos. Al igual que ocurre con estos dispositivos, algo muy similar sucede con otras alternativas como una carpeta compartida en la red, o cualquier medio de almacenamiento virtual.

Otro aspecto fundamental en el que se basa el artículo [8], dónde se muestra cómo para demostrar matemáticamente la seguridad en una transacción, es necesaria la

presencia de dos procesadores cooperando, debiendo ser al menos uno de ellos confiable. Aspecto que nos limita aún más el tipo de dispositivo a usar para contener el perfil, pero a su vez nos refuerza nuestra teoría de usar tarjetas inteligentes para este propósito.

Así, para concluir este punto, tenemos las tarjetas inteligentes, que como es sabido, son dispositivos portátiles cuyo uso se ha extendido entre los usuarios, los cuales utilizan tarjetas inteligentes (en ocasiones sin saberlo) en su vida cotidiana. Cumplen una serie de requisitos de seguridad muy útiles para el almacenamiento de perfiles: son resistentes a manipulación, tienen capacidad criptográfica de cómputo, son capaces de generar claves, utilización del algoritmo RSA, etc. La capacidad de cómputo se estima en la actualidad en 100 MIPS, y los tamaños de memoria pueden alcanzar un megabyte para tarjetas que soporten memorias FLASH [4].

Aunque la capacidad de memoria es muy limitada en la actualidad para almacenar la totalidad de los datos de un perfil completo de usuario, la computación móvil incrementa el uso de procesamiento y memoria proporcionando muchos dispositivos conectados en el entorno al mismo tiempo, de forma prácticamente invisible al usuario [6]. A esto debemos añadir que la tecnología progresa sin cesar, por lo que la capacidad de memoria dejará de ser un obstáculo en un futuro inmediato. Todo esto convierte a las tarjetas inteligentes en el mejor dispositivo para el almacenamiento seguro de perfiles con información delicada.

5. Detalles del Diseño

A la hora de diseñar una aplicación que funcione con tarjetas inteligentes tenemos que tener una serie de consideraciones; como las restricciones de memoria, las cuales pueden suponer una limitación severa en nuestro caso puesto que los perfiles suelen venir estructurados usando variantes del lenguaje de programación XML, con sus respectivas etiquetas de inicio, fin, etc. Además de esto, dentro de la tarjeta tendremos un applet de java, en concreto un *applet de javacard*, que será el software que se ejecute dentro de la tarjeta, y por tanto el que nos proporcione la seguridad inherente a las tarjetas inteligentes como elemento de computación confiable. Las tarjetas inteligentes que existen en el mercado tienen en su mayoría una capacidad muy reducida, unos 64Kb, espacio de memoria en que han de alojarse tanto el applet de javacard mencionado, como los perfiles que tengan que ser portados por el usuario; y adicionalmente la posibilidad de que estas tarjetas inteligentes puedan llevar applets con propósitos distintos.

Otro factor a tener en cuenta es el dispositivo en el cuál va a estar conectada la tarjeta inteligente; para mayor claridad vamos a llamar a este “terminal”. Este tendrá cierta interacción con la tarjeta inteligente, lo cual supone que hará falta un software que se ejecute en el terminal y se comunique con la tarjeta de la manera adecuada, es decir mediante envíos de APDU´s (Application Protocol Data Unit). Además, por las características de la tecnología JavaCard, el inicio de cualquier comunicación entre ambos ha de ser iniciado precisamente por esta aplicación que se ejecuta en el terminal. En aras de facilitar al usuario su interacción, tanto de configuración como de instalación, lo más cómodo para los usuarios sería ver esta aplicación que se lanza en el terminal como un applet de Java, distinto del applet de JavaCard que se ejecuta en

la tarjeta, con objeto de que el usuario no necesite instalar nada. El usuario sólo debería tener previamente instalada una máquina virtual de Java.

6. Conclusiones y líneas de investigación futura.

En la actualidad cada vez más usuarios llevan consigo una tarjeta inteligente, y debido a las características portátiles de las mismas, está van con el usuario casi la mayor parte del tiempo, hecho que se debe en mayor medida al uso masivo de telefonía móvil. Al mismo tiempo, parece claro que los perfiles serán usados por las distintas aplicaciones y servicios. Con la suma de estos hechos concluimos que las tarjetas inteligentes representan la mejor alternativa para el almacenamiento de perfiles de usuario. Las restricciones de memoria presentes no serán ciertas gracias al progreso tecnológico, y su implementación es posible y enriquecedora para los entornos de comercio móviles.

Esto representa una línea de investigación práctica abierta. Los siguientes pasos que nos guíen en esta línea pasan por la elaboración de una clasificación más detallada de los distintos niveles de seguridad (así como su correspondencia con políticas de seguridad existentes). De la misma forma, actualmente estamos trabajando en un protocolo para el almacenamiento y acceso de los datos de un perfil en tarjetas inteligentes de forma segura**,** usando las capacidades criptográficas que estas presentan.

Agradecimientos

El estudio que hemos descrito en este artículo se encuentra parcialmente financiado por el proyecto europeo UBISEC FP6-2002-IST-1, contrato 506926 y por la Consejería de Innovación, Ciencia y Empresa de la Junta de Andalucía bajo el tercer plan de Investigación Andaluz.

REFERENCIAS

[1] Forrester Research. Post-web retail. Sept. 1999. http://forrester.com/.

[2] J. Lopez, R. Oppliger, G. Pernul. Authentication and Authorization Infrastructures (AAIs): A Comparative Survey. Computers & Security Journal. Elsevier (North Holand), Vol. 23, 2004.

[3] M. Brown, R. Muchira. Investigating the relationship between Internet Privacy Concerns and Online Purchasing Behaviour. Journal of Electronic Commerce Research. Vol. 5, No. 1, 2004.

[4] Pascal Urien1, Guy Pujolle.(2003) “A simple security model for emerging 802.11 pervasive Environments“. In *the Proceedings of the SOC'2003 Conference.*

[5] Urien, P., Farrugia, A.J., Pujolle, H., Groot, M.(2002) “EAP. Support in smartcards”, *draft-urien-EAP-smartcard- 01.txt, internet draft, March 2002*.

[6] Weiser, M.(1993) “Some Computer Sciences issues in Ubiquitous Computing”, *Communications of the ACM July 1993, Vol 36, n°7, pp 75-84*

[7] Deliverable D3.1 (2004) “Profile Management, Description and Exchange: Requirements and state of the art analysis” Proyecto UBISEC. http://www.ubisec.org

[8] Goldreich, O. *Towards a theory of software protection*, Proc. 19th Ann. ACM Symp. on Theory of Computing, pp. 182-194. 1987.

[9] http://www.w3.org/RDF/

[10] http://www.w3.org/TR/vcard-rdf

[11] http://java.sun.com/j2me/

[12] http://www.osgi.org/