APLICACIÓN WEB PARA LA ADMINISTRACIÓN DE TARJETAS INTELIGENTES CON GLOBALPLATFORM

Ing. Rita Milena Hernández Díaz[1];

Ing. José Enrique Díaz Ramos[2]

1. *Universidad de Matanzas – Sede "Camilo Cienfuegos", Vía Blanca Km.3, Matanzas, Cuba.* rita.hernandez@umcc.cu

2. *Universidad de Matanzas – Sede "Camilo Cienfuegos", Vía Blanca Km.3, Matanzas, Cuba.* enrique.diaz@umcc.cu

CD de Monografías 2015

ISBN: XXX-XXX-XX-XXXX-X

Resumen

En el presente trabajo se hace un estudio acerca de las tarjetas inteligentes y las tecnologías asociadas, ya que actualmente la mayoría de las aplicaciones que ofrecen servicios a través de la Web haciendo uso de tarjetas inteligentes, necesitan de la instalación de middlewares del lado del cliente. Esto supone un elevado riesgo para su seguridad, debido a que el uso de claves simétricas en el cliente posibilita que puedan ser accedidas por atacantes permitiendo acceso a operaciones que requieren seguridad sobre la tarjeta y los sistemas que la utilizan. Con el objetivo de eliminar los riesgos antes mencionados, se desarrolla una aplicación web para la administración de tarjetas inteligentes con GlobalPlatform 2.1.1 que cuenta con un middleware del lado del servidor, aprovechando las ventajas que ofrece este estándar en cuanto a seguridad.

***Palabras claves**: Web, tarjetas inteligentes, GlobalPlatform, middleware*

ISBN: XXX-XXX-XX-XXXX-X

Introducción

Con el avance de las Tecnologías de la Información y las Comunicaciones se registra una tendencia al uso de dispositivos inteligentes que facilitan y aseguran el proceso de identificación, tal es el caso de las tarjetas inteligentes. Son muchos los escenarios en los que se utilizan estos dispositivos, entre los que se puede mencionar el comercio electrónico con el uso de los monederos electrónicos. También son utilizadas en el control de acceso, este tipo de aplicación suele estar ligada a puertas automatizadas que permiten o impiden el paso físico de una persona a un área determinada. Otro de sus importantes usos en la actualidad, es su vinculación a la firma digital de documentos, o sea, el almacenamiento del certificado digital dentro de la tarjeta. Las tarjetas inteligentes también se han expandido a la esfera de la salud, ya que el uso de la tarjeta anula la necesidad de tener que compartir una inmensa base de datos y tener que hacer réplicas periódicas. Otro de sus usos es en el sector público para el transporte, ya que permite pagar la cuota de autobús sin necesidad de usar efectivo o monedas. En los últimos años las tarjetas inteligentes han ido evolucionando en la tecnología móvil, ofreciendo a los clientes servicios con un mayor beneficio y facilitándoles diferentes aplicaciones y tecnologías desde el móvil.

Formando parte de los procesos enfocados al progreso de la informática y las comunicaciones en Cuba, la Universidad de las Ciencias Informáticas (UCI) en el Centro de Identificación y Seguridad Digital (CISED), específicamente en el departamento de Tarjetas Inteligentes ha venido desarrollando soluciones referentes a esta tecnología, con el fin de obtener productos y servicios basados en tarjetas inteligentes, entre los que se encuentran el SmartCardFramework que permite el desarrollo para aplicaciones de pasaportes electrónicos, licencia de conducción e Infraestructura de Clave Pública (PKI por sus siglas en Inglés), la aplicación SmartCardTool que forma parte del SmartCardFramework, el SmartCoP que es una plataforma para el desarrollo de servicios en línea, entre otras.

ISBN: XXX-XXX-XX-XXXX-X

Para realizar las operaciones de administración en las tarjetas inteligentes que implementan Java Card y GlobalPlatform es necesario instalar un middleware del lado del cliente. Por tanto se hace complejo ejecutar las operaciones de administración, debido a la necesidad de dominar su uso por parte del cliente. Unido a esto para realizar operaciones sobre los dominios de seguridad es necesario que el middleware cuente con las llaves para tener acceso a los mismos. Por cada terminal donde se llevan a cabo las operaciones es necesario contar con las llaves, constituyendo una vulnerabilidad, pues estas al ser simétricas corren el riesgo de ser obtenidas por personal no autorizado, permitiendo el acceso a operaciones que requieren seguridad sobre la tarjeta.

Para dar solución al problema existente se ha tomado como objetivo general: desarrollar una aplicación web para la administración de tarjetas inteligentes mediante la implementación del estándar GlobalPlatform 2.1.1, utilizando la plataforma para el desarrollo de servicios en línea con tarjetas.

Desarrollo

Varias son las empresas que se dedican hoy a desarrollar soluciones haciendo uso de los distintos tipos de tarjetas inteligentes. Una de las empresas líderes es Gemalto, esta ofreció una solución denominada SConnet, la cual tiene como objetivo principal, proporcionar un puente de conexión entre el JavaScript, que corre en la página web de un navegador y la tarjeta inteligente. Permitiendo la conectividad entre estas últimas y los servicios web. SConnect incluye un sistema de medidas de seguridad para mitigar ciertos riesgos, proteger a los usuarios y sitios web conectados. Dichas medidas incluyen una extensión con firma digital de SConnect, un HTTPS reforzado, llave de conexión, validación de servidor y alarma a usuario.

Otra de las soluciones de Gemalto es Coesys eGov 2.0, producto que tiene como objetivo autenticar a los usuarios a través de la Web para que tengan acceso a los servicios en línea de gobierno electrónico. Permite un servicio de identificación electrónica mediante tarjetas

ISBN: XXX-XXX-XX-XXXX-X

inteligentes basado en la Web, en vez de un software basado en un cliente de autenticación de instalación local.

Por su parte la empresa I-Card Software ofrece la solución Control Paterno, producto que hace referencia a ciertas funcionalidades de un determinado dispositivo o software que permite a los padres filtrar o aplicar restricciones sobre toda la navegación que hacen sus hijos en la Web. Por otro lado la empresa Firma Profesional ofrece la solución WebLogon, producto que hace de la sencillez y velocidad de instalación su punto fuerte. Esta funciona como una pasarela intermedia, interceptando las peticiones de autenticación tradicional y modificándolas para realizar una verificación del certificado del usuario, que se encuentra en su tarjeta inteligente. Permite integrar en la red corporativa el acceso a cualquier página, propia o externa, con tarjeta inteligente y certificado, reforzando la seguridad.

Otra de las empresas dedicadas a dar soporte al trabajo con las tarjetas inteligentes es MacroSeguridad, esta da a conocer la solución Payment Card que ofrece transacciones online seguras, que ayuda a disminuir los peligros de fraude y phishing4 bancarios, por la incorporación de funciones lógicas de identificación y autenticación de usuarios.

Por su parte la empresa Athena SmartCard brinda el producto Payment and PKI, esta herramienta permite a una audiencia global ver y comprar desde cualquier lugar bienes y servicios. Por el auge del comercio minorista en línea, Athena proporciona una generación de herramientas para proteger a los emisores y continuar el crecimiento minorista en línea. Ofreciendo una solución de pago que cumpla con todos los estándares relevantes de la industria.

No obstante todas estas soluciones por su forma tradicional de interactuar con las tarjetas traen consigo algunas restricciones como son: el dominio que deben tener los usuarios para efectuar las actualizaciones en la tarjeta, así como la necesidad de poseer una serie de permisos en el manejo de los recursos de la computadora para poder instalarlas. Además las llaves simétricas necesarias para trabajar dentro de la tarjeta, se encuentran en el cliente.

ISBN: XXX-XXX-XX-XXXX-X

Al planificar el desarrollo de esta aplicación se tomaron en cuenta varios puntos esenciales como fueron la implementación del estándar de GlobalPlatform en su version 2.1.1, ya que este lidera mundialmente el desarrollo en temas de infraestructura de tarjetas inteligentes. Sus descripciones técnicas probadas para las tarjetas, dispositivos y sistemas son consideradas como las normas de la industria para lograr implementaciones interoperables, flexibles y sostenibles por tarjetas que soportan multi-aplicación y multi-actor e implementaciones multi-modelo de negocio. Además comprende la instalación y borrado de las aplicaciones y la administración de otras tareas de las tarjetas. El emisor de la tarjeta tiene el control total sobre el contenido de esta, pero puede permitir a otras instituciones administrar sus propias aplicaciones, esto se logra aplicando protocolos criptográficos, permitiendo a cada institución tener su propia área segura en la tarjeta.

Al escoger dicha tecnología se definen los lenguajes que serán utilizados en el desarrollo de la aplicación, destacando entre ellos Java como lenguaje en el servidor y JavaScript en el lado del cliente.

La aplicación utiliza como marco de trabajo JWebsocket, ya que este brinda una total flexibilidad, además se ejecuta fácilmente desde una línea de comandos o se integra a la biblioteca de una aplicación existente de Java. JWebSocket como servidor web proporciona un conjunto importante de funcionalidades y su arquitectura extensible permite añadir fácilmente características adicionales a un sistema independiente. Es el marco de trabajo y a la vez el servidor de aplicaciones con licencia libre más robusto y flexible para la plataforma Java. Está respaldado por excelentes resultados en cuanto a rendimiento y escalabilidad.

Después de darle solución a estos problemas se procede a definir las principales funcionalidades del software de acuerdo a los requisitos del cliente. Se define que se tendrán como funcionalidades principales obtener el estado de la aplicación, instalar aplicación, eliminar aplicación, entre otras. Además permitirá inserter llaves a la plicación.

Posteriormente se realiza un diseño de las interfaces basado en los requisitos previamente expuestos, el equipo define que se tendrán 6 interfaces que mostrarán los principales tipos de datos. Cada una de estas interfaces tendrá 4 columnas que desplegaran los datos

ISBN: XXX-XXX-XX-XXXX-X

esenciales de la tarjeta y permitirá al presionar cualquier elemento acceder a los detalles del mismo En el caso de las llaves específicamente esta interfaz contendrá tanto las generadas por el algoritmo 3DES, como por el RSA.

Una vez concluido el diseño de esta aplicación se procedió al proceso de desarrollo que fue de aproximadamente 3 meses, luego se le ralizaron pruebas funcionales arrojando como resultado final luego de 3 iteraciones cero no conformidades, lo que indica que la aplicación web para administrar tarjetas inteligentes con GlobalPlatform 2.1.1 cumple con los requerimientos definidos.

Conclusiones

Con el desarrollo de este trabajo se ha podido demostrar cómo se han cumplido los objetivos principales definidos para la creación de una aplicación web que permita la administración de tarjetas inteligentes, con la utilización del estándar GlobalPlatform. Algunas de las conclusiones arribadas luego de terminado este producto son:

- El análisis de las principales soluciones que utilizan tarjetas inteligentes en la Web posibilitó conocer el funcionamiento de las aplicaciones web, siendo de gran utilidad para la definición de los requisitos de la aplicación.
- El análisis de diferentes herramientas, tecnologías, lenguajes y metodologías ha permitido definir cuáles utilizar en el desarrollo del sistema.
- El desarrollo de la aplicación web para la administración de tarjetas inteligentes que implementen el estándar GlobalPlatform ha permitido aumentar los niveles de seguridad requeridos, ya que se utiliza como protocolo de comunicación WebSocket, permitiendo que el middleware se encuentre en el servidor.
- La ejecución de las pruebas ha posibilitado validar el correcto funcionamiento del sistema.

ISBN: XXX-XXX-XX-XXXX-X

Referencias Bibliográficas

1. Effing, Wolfgang and Rankl, Wolfgang. 2002. Smart Card Handbook Third Edition: John Wiley & SonsLtd. 2002.

2. GlobalPlatform. 2003. Card Specification Versión 2.1.1. 2003.

3. ERLICH, J. Especificación Formal de la Máquina Virtual Java Card Disponible en:. [Online].www.fing.edu.uy/.../informacion/.../documentacion_especificacionjavacard .doc.

4 .SOTOLONGO DAYRON ALMEIDA Solución para el control de acceso a la información de las entidades externas, en la cédula de identificación electrónica de la República Bolivariana de Venezuela. 2008.

5. ORTEGA, M. Implementación de Tarjeta Inteligente Java Card para el Control de Acceso a Instalaciones. Disponible en: http://www.eatis.org/eatis2010/portal/paper/memoria/html/files/sistemas/Maria%20Ortega.pdf.

6. VIÑOLO, K. P. y SANTANA, V. F. Plataforma para el desarrollo de servicios en línea utilizando tarjetas inteligentes. 2010.

7. Perovich, Daniel, Rodríguez, Leonardo and Martín, Varela.Proyecto de Taller V Programación de JavaCards.

8. PLATFORM, J. JavaTM 2 Platform Standard Ed. 5.0. Disponible en: http://download.oracle.com/. [Online].

9. http://sconnect.software.informer.com/. [Online].

10. Gemalto. 2007. Coesys Issuance Solutions for the Public Sector.

11. http://www.icard.net/web/icard/controlparental. [Online].

12.https://www.firmaprofesional.com/index.php/esp/ca/suport/certificats-arrel/114-ca-sin-categoria/263-certificats-ca-arrel-informacio-per-usuaris-finals. [Online].

13.http://www.macroseguridad.net/productos/smartcards/payment_card/especificaciones.php. [Online].

14. http://www.athena-scs.com/.../athena-smartcard. [Online].

ISBN: XXX-XXX-XX-XXXX-X

15. http://www.rfidpoint.com/fundamentos/middleware/. [Online].

16. Castells, M. La galaxia Internet – Reflexiones sobre Internet, empresa y sociedad. Barcelona (Plaza & Janés). [Online]. 2006.

17. http://www.masadelante.com/faqs/que-significa-http. [Online].

18. Masó, Rolando Santamaría. EventsPlugIn Developer Guide,Reference Documentation Version 1.0.

19. http://www.slideshare.net/rtorres462003/metologa-agiles-desarrollo-software-xp-1709082. [Online].

20. http://www.cad.com.mx/historia_del_lenguaje_java.htm. [Online].

21. Paradigmas de la Programación: JavaScript y PythonAgosto 2010.

22. https://jwebsocket.org. [Online].

23. http://www.programacionweb.net/cursos/curso.php?num=2. [Online].

24. Rankl, Wolfgang y Effing, Wolfgang. Smart Card Handbook Third Edition. West Sussex : John Wiley & Sons Ltd, 2003.

25. http://www.altova.com/umodel.html. [Online].

26. http://netbeans.org/index_es.html. [Online].

27. http://www.gemalto.com/products/jcardmanager/. [Online].

28. Pressman, Roger S. Ingeniería del Software. Un enfoque práctico. 2002. proyectos Ágiles. Qué es SCRUM | proyectos Ágiles. [Online].2002. http://www.proyectosagiles.org/que-es-scrum.

29. Sommerville, Ian. Ingeniería del software. Madrid : Pearson Educación, 2005.

30. PATRONES GRASP (Patrones de Software para la asignación General de Responsabilidad). [Online].[Citado el: 11 de marzo de 2013.] http://jorgesaavedra.wordpress.com/2007/05/08/patrones-grasp-patrones-de-software-para-la-asignacion-general-de-responsabilidadparte-ii.

31. http//:www.dcc.uchile.cl/~psalinas/uml/modelo.html. [Online]

32.Modelo de implementación. Diagramas de componentes y Despliegue. [Online]. [Citado el: 25 de marzo de 2013.] http://www.dsi.uclm.es/asignaturas/42530/pdf/M2tema12.pdf.

ISBN: XXX-XXX-XX-XXXX-X

33. http://www.slideshare.net/rinconsete/pruebas-de-caja-blanca-y-negra. [Online]

34. http://www.globetesting.com/2012/08/pruebas-de-caja-negra/. [Online]

ISBN: XXX-XXX-XX-XXXX-X