Autenticación basada en Java card y en certificado X.509 para ambientes universitarios

María Ortega[1], Sergio Sánchez [2]
[1] Universidad Tecnológica de Panamá
[2] Universidad Politécnica de Madrid
maria.ortega2@utp.ac.pa, sergio@diatel.upm.es

Resumen

Este artículo presenta la tecnología Java Card y los certificados X.509 como métodos de autenticación en aplicaciones web en ambientes universitarios, en el caso concreto la Universidad Tecnológica de Panamá (UTP). La solución consiste en mejorar el escenario de acceso a los servicios de la UTP tratando de extender el uso de la Infraestructura de Clave Pública, llevando a cabo la integración de estas tecnologías que aporten mayor seguridad a todos los usuarios y que gocen de un acceso a los servicios ofrecidos de manera flexible, segura y garantizando la autenticidad, confidencialidad, integridad y no repudio.

Palabras claves:

Autenticación, certificados X.509, tarjeta java.

Abstract

This paper presents the Java Card technology and X.509 certificates as authentication method in web applications in university settings in the specific case the Technological University of Panama (UTP). The solution is to improve the access scenario UTP services trying to extend the use of public key infrastructure, carrying out the integration of these technologies to provide greater certainty for all users and an access services offered in a flexible, secure, ensuring the authenticity, confidentiality, integrity and non repudiation.

Keywords:

Authentication, X.509 certificates, java card.

Introducción

Existen diversos mecanismos de protección de la información que aseguran el cumplimiento de las medidas de seguridad establecidas para el acceso y la utilización de dicha información [Bauer, 2010; Hurtado, 2009]. La autenticación es uno de esos mecanismos y se basa en la identificación de usuarios, es decir, en el proceso mediante el cual se comprueba la identidad de una persona o entidad en base a un conjunto de características [Chávez, 2006].

Atendiendo a qué tipo de características utilizan los sistemas de autenticación para identificar al usuario, se pueden clasificar, de forma genérica, en cuatro tipos: los basados en algo que la entidad sabe, los basados en algo que la entidad hace, los basados en algo que la entidad posee y los basados en algo que la entidad es [Hildebrandt et al. 2005; Carracedo, 2004]. Por lo tanto, los sistemas de autenticación comprenden procesos tan simples como el empleo de parejas usuario/contraseña o tan complejos como el análisis de patrones biométricos.

Con los avances tecnológicos y el mayor poder de proceso de los ordenadores actuales, se da la necesidad de incrementar la seguridad en los procesos de autenticación e incorporar nuevas tecnologías que aumenten y proporcionen un mayor nivel de seguridad. Diversas instituciones cuentan con sistemas de autenticación para el acceso a datos y aplicaciones de autenticación caracterizadas por el uso de usuario/contraseña [Vatra, 2010], denominado acceso clásico, que presentan el problema de que pueden ser fácilmente vulnerados con la tecnología actual, reduciendo la seguridad de las aplicaciones. Sin embargo, existen otras instituciones que han decidido contar con tecnología más segura a la hora de proteger el acceso a las aplicaciones e información [Díaz et al., 2001; Watts et al., 2010; Harn and Ren, 2011; Watts, J. et al., 2010].

En el caso del estudio concreto abordado en este artículo, el de la Universidad Tecnológica de Panamá (UTP), ésta cuenta con una Infraestructura de Clave Pública (PKI) [Vatra, 2010] utilizada solo por profesores para el registro de calificaciones y por administrativos para la evaluación anual, pero que no está disponible, actualmente, a todos los miembros de la comunidad universitaria.

El objetivo de este trabajo es tratar de mejorar el escenario de acceso a los servicios en la UTP tratando de extender el uso de la PKI [Elfadil and Al-raisi, 2008] y llevando a cabo una integración de tecnologías que aporten mayor seguridad a todos los usuarios (profesores, administrativos y estudiantes) y que garanticen un acceso a los servicios ofrecidos, flexible, seguro y con garantías.

En un entorno de uso de clave pública, resulta vital asegurarse de que la clave pública que se está utilizando, ya sea para cifrar o firmar datos, es en realidad la clave pública adecuada y no una falsificación. Se requiere, por lo tanto, de un intercambio de información que garantice o demuestre que la clave pública le pertenece al propietario. El mecanismo para garantizar esto es el certificado digital.

El certificado digital es un documento electrónico que demuestra la identidad de un usuario [Network Associates, Inc., 2004] y contiene otros atributos, por ejemplo, las fechas de inicio y fin de la validez del certificado. El certificado digital asocia una clave pública a un usuario y garantiza que la clave es válida y que pertenece al usuario que dice que es quien dice ser. Para ello se designan una o más entidades denominadas Autoridades de Certificación (CA), cuya función es generar los certificados de clave pública de la organización y luego darlos por buenos. El certificado está firmado por la clave privada (Ks) de la CA y cualquier usuario u organización que pertenece a una red puede verificar con la CA la validez de la clave pública certificada. Las CA y la administración de certificados digitales utilizan los sistemas de criptografía asimétrica ofreciendo un modelo de confianza que permite construir aplicaciones de alto nivel [Díaz, 2001].

La utilización de criptografía asimétrica [Ramió, 2006] ofrece ventajas como la confidencialidad para asegurar que ha sido esa persona y no otra la que ha leído o enviado un mensaje; la integridad, para asegurar que el mensaje no podrá ser modificado o alterado, y el no repudio de origen, que imposibilita al usuario negar su participación en una transacción si ha utilizado su firma electrónica, puesto que nadie más que él puede haber generado esa firma. Además, la firma permite asegurar la integridad de un documento.

Otro mecanismo de securización que ha tenido una gran aceptación en el mercado actual y está siendo ampliamente utilizado son las tarjetas inteligentes (Smart Cards) [S. C. Allience, 2006]. Ejemplos de uso de este tipo de tarjetas en diferentes ámbitos los encontramos en las tarjetas bancarias de pago seguro o las tarjetas de identificación utilizadas en la administración pública –por ejemplo, el Documento Nacional de Identidad electrónico en España (DNI electrónico, 2010)–.

Las tarjetas inteligentes son aquellas que almacenan y procesan información a través de circuitos electrónicos mediante un microordenador formado por un único chip que se encuentra situado en una tarjeta de plástico típicamente del tamaño de una tarjeta de crédito [Chen, 2000].

Existen diversos tipos de tarjetas inteligentes, pero las más interesantes, fundamentalmente por su flexibilidad y fácil adaptación a distintos entornos de utilización, son las tarjetas Java (Java Card). Se trata de tarjetas que utilizan la tecnología Java como base de programación para sus aplicaciones. Se trabaja en Java aplicado a entornos en los que existen ciertas limitaciones en los recursos de memoria, lo que permite la ejecución de pequeñas aplicaciones (applets) escritas en Java dentro del propio microprocesador de la tarjeta, haciendo uso de una máquina virtual Java reducida [Chen, 2000]. Cabe destacar que esta tecnología es compatible con los estándares de tarjetas inteligentes ISO 7816 [ORSI, 2010; Chen, Z. and Di Giorgio, R., 1998].

El resto de este trabajo está organizado de la siguiente manera. En la sección 2, se muestra los Trabajos Previos. La sección 3 describe la metodología utilizada en el desarrollo del proyecto. Los resultados y discusión se encuentran en la sección 4 y, finalmente, las conclusiones en la sección 5.

Conclusiones

Para el desarrollo de este trabajo, se ha utilizado una metodología basada en varias fases, comenzando con el análisis de requisitos y llegando hasta la implementación y pruebas de parte de lo diseñado.

Como se ha visto a lo largo del texto, se parte del estudio del caso concreto de la UTP, donde la autenticación para algunos usuarios se basa en certificados digitales de identidad almacenados en forma centralizada y para otros en el sistema clásico de usuario y contraseña. El cual, por su propia constitución resulta un poco inapropiado, ya que se requiere mayor seguridad en la institución.

De igual manera, se hace necesario involucrar a todo el personal en general que requiere de los servicios ofrecidos por la institución, pero manteniendo una comunicación segura. En este artículo, se propuso la utilización de la criptografía asimétrica que proporciona medios para asegurar la comunicación y el uso de la tecnología Java.

La solución se basa en el uso de PKI para el acceso a los servicios ofrecidos por la institución, utilizando algoritmos asimétricos para la creación de las claves del usuario. Se ha creado una infraestructura de seguridad que está compuesta por CA y RA que son las entidades encargadas de la generación y registro de los certificados digitales utilizados por los usuarios de acuerdo con su papel. Además, se ha incluido el uso de tarjetas Java para el almacenamiento del certificado y autenticación del usuario. La flexibilidad, practicidad y comodidad son algunas de las ventajas que ofrece esta tecnología.

Para comprobar la funcionalidad de lo diseñado, se ha desarrollado un pequeño demostrador de usuario/servidor o implementación de referencia. Se hace mención que es a pequeña escala para futuras ampliaciones. Éste consiste en el almacenamiento del certificado X.509 en la tarjeta Java y de una aplicación para acceder al recurso mediante la autenticación de la tarjeta y luego del certificado del usuario.

Con la integración de las dos tecnologías, se ha obtenido los beneficios de cada una como mayor escalabilidad, portabilidad, interoperabilidad y seguridad de la información en las aplicaciones.

Esto ha permitido una comunicación más segura que garantiza la autenticidad, la confidencialidad, la integridad y el no repudio de origen que es un punto importante porque es un servicio de seguridad que permite probar la participación de un usuario o entidad en una comunicación.

Como trabajo futuro, se pretende mejorar el acceso a la tarjeta Java mediante identificación biométrica, la cual dará mayor seguridad al momento de autenticarse.

Referencias

[1] [Bauer, 2010] Bauer, L., et al., (2010). Constraining Credential Usage in Logic-Based Access Control. Proceding of the 2010 23rd IEEE Computer Security Foundations Symposium (CSF), Edimburgo, Escocia, pp. 154-168.

[2] [Carracedo, 2004] Carracedo, J. (2004). Seguridad en redes telemáticas. McGraw-Hill, Madrid, España.

[3] [Chávez, 2006] Chávez, P. (2006). Autenticación y Control de Acceso. http://lsc.fie.umich.mx/~pedro/autenticacion_ac.pdf

[4] [Chen, 2000] Chen, Z. (2000). Java Card™ Technology for Smart Cards: Architecture and Programmer's Guide. Addison-Wesley, California, USA.

[5] [Chen, 1998] Chen, Z. and Di Giorgio, R., InfoWorld JavaWorld, Solutions for java Developers, Understanding Java Card 2.0. http://www.javaworld.com/javaworld/jw-03-1998/jw-03-javadev.html

[6] [Díaz, 2001] Díaz, I. et al. (2001). Autenticación en la Red: ACerO y JCCM*: Java Card Certicate Management. III Jornadas de Ingeniería Telemática. JITEL. Barcelona, España, pp. 405-412.

[7] [DNI electrónico, 2010] DNI electrónico, Guía de Referencia Básica, v1.3, 2010. http://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_v1_3.pdf

[8] [Elfadil, 2008] Elfadil, N. A. et al. (2008). An Approach for Multi Factor Authentication for Securing Smart Cards' Applications. Proceedings of the International Conference on Computer and Communication Engineering IEEE. Kuala Lumpur, Malasia, pp. 368-372.

[9] [Harn, 2011] Harn, L. and Ren, J., 2011. Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications. IEEE Transactions on Wireless Communications. Vol. 10, No. 7, pp. 2372 – 2379.

[10] [Henniger, 2006] Henniger, O. et al. Verifying X.509 Certificates on Smart Cards. In proceeding World Academy of Science, Engineering and Technology 22 2006.

[11] [Hilderbart, 2005] Hildebrandt, M. Et al. (2005). Future of Identity in the Information Society. FIDIS Inventory of Topics and Clusters, Deliverable 2.1, pp 38-39 [online] Disponible en: http://www.cosic.esat.kuleuven.be/publications/article-829.pdf

[12] [Hurtado, 2009] Hurtado, D. et al., 2009. Modelado de la seguridad de objetos de aprendizaje. Generación Digital, Vol. 8, No. 1. pp. 38-42.

[13] [ISO, 2011] International Organization for Standardization (ISO). International Standard. Identification Cards-Integrated circuit cards. ISO/IEC 7816-1:2011(E). http://webstore.iec.ch/preview/info_isoiec7816-1%7Bed2.0%7Den.pdf

[14] [Network Associates, 2004] Network Associates, Inc. and its Affiliated Companies, 2004. An Introduction to Cryptography. Network Associates, Inc. California, USA.

[15] [Ramió, 2006] Ramió, J., 2006. Libro Electrónico de Seguridad Informática y Criptografía. http://www.criptored.upm.es/descarga/SegInfoCrip_v41.zip

[16] [S.C.Alliance, 2006] S. C. Allience, 2006, Uso de tarjetas inteligentes para un control de acceso físico seguro, Informe de la Smart Card Alliance Latin America (SCALA). http://www.smartcardalliance.org/latinamerica/translations/Secure_Physical_Access_Spanish.pdf

[17] [ORSI, 2010] Observatorio Regional de la Sociedad de la Información de Castilla y León (ORSI), Tarjeta ciudadana, una visión de las tarjetas inteligentes y su aplicación en los ayuntamientos, 2010. http://www.jcyl.es/web/jcyl/binarios/910/900/TARJETA_CIUDADANA.pdf?blobheader=application%2Fpdf%3Bcharset%3DUTF-8

[18] [Vatra, 2010] Vatra N. (2010). Public Key Infrastructure for Public Administration in Romania. Communications (COMM), 2010 8th International Conference, IEEE. Bucarest, Rumania, pp. 481-484.

[19] [Vossaert, 2010] Vossaert, J. (2010). Developing secure Java Card applications.

[20] [Watts, 2010] Watts, J.et al., 2010. Case Study: Using Smart Cards with PKI to Implement Data Access Control for Health Information Systems. Proceding of the IEEE SoutheastCon 2010 (SoutheastCon). Concord, NC, USA, pp. 163-167.