SISTEMA DE AUTENTICACIÓN UNIVERSITARIO BASADO EN JAVA CARD Y CERTIFICADO DIGITAL X.509

María T. Ortega
Universidad Tecnológica de Panamá
Ciudad de Panamá, Panamá

Sergio Sánchez
Universidad Politécnica de Madrid
Madrid, España

RESUMEN

Este artículo presenta una solución al problema de autenticación segura, portable y expandible realizando una combinación de la tecnología Java y el almacenamiento del certificado digital X.509 en las tarjetas Java para acceder a los servicios ofrecidos por una institución, en este caso concreto la Universidad Tecnológica de Panamá, garantizando la autenticidad, confidencialidad, integridad y no repudio.

PALABRAS CLAVES

Autenticación, Tarjetas inteligentes, Tarjetas Java, PKI, Certificado X.509

1. INTRODUCCIÓN

Con los avances tecnológicos y el mayor poder de proceso de los computadores 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 (Diaz et al., 2001; Watts et al., 2010; Harn and Ren, 2011).

En el caso de 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.

2. METODOLOGÍA DE TRABAJO

Consta de varias fases. La primera es la de análisis. Se ha realizado un estudio de la situación actual del problema, tomando en cuenta el caso de estudio concreto de la UTP. En la fase de diseño se ha realizado un diagrama de componentes que muestra el conjunto de entidades presentes en la arquitectura propuesta como

solución y la relación que existe entre ellas. También se presenta un diagrama de secuencia que muestra el acceso seguro y con garantías a los servicios ofrecidos. En la fase de implementación se desarrolla un pequeño demostrador de la arquitectura para comprobar la funcionalidad de lo diseñado. Sobre este demostrador se realizarán pruebas individuales y, en base a los resultados obtenidos, se volverá a incidir en la fase de diseño para realimentar y mejorar la solución.

3. RESULTADOS

A partir de lo expuesto en los párrafos anteriores se han identificado los distintos componentes involucrados en el escenario. Tenemos al *usuario*, persona que va a hacer uso de algún servicio ofrecido por la UTP puede ser administrativo, profesor o estudiante. Por otra parte, tenemos al *proveedor de servicios*, Institución que proveerá los servicios para los usuarios, es la UTP. También, tenemos al *PC*, dispositivo desde el que el usuario va acceder al servicio desde la institución o desde la comodidad de su hogar. El *lector de tarjeta Java*, es otro componente, que estará conectado al PC y se comunicará con él para leer la tarjeta Java. Por supuesto que la *tarjeta Java*, es un componente, que almacena las claves y certificados de identidad del usuario, a través del lector se comunica con las aplicaciones necesarias y gestiona el control de acceso al usuario y el uso del certificado para acceder a las aplicaciones o servicios ofrecidos por la institución. Y por último, pero no menos importante, tenemos a la *PKI*, infraestructura de clave pública que estará asociada a la UTP y que será encargada de entregar los certificados a los usuarios. Constará de una Autoridad de Registro (RA) para validar el registro de usuario y de una CA para emitir y consultar el estado del certificado X.509 de un usuario.

Con todas estas entidades, se presenta a continuación la arquitectura lógica de la solución, recogida en la figura 1.

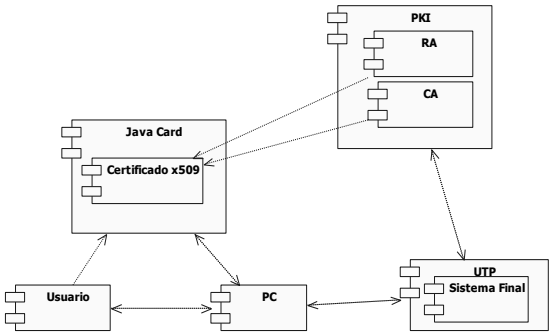

Figura 1. Arquitectura lógica y relaciones

El usuario dispone de una tarjeta Java, ingresa el Número de Identificación Personal (PIN). Luego, se autentica mediante el certificado que está almacenado en la tarjeta Java y accede al sistema final. En la figura 2 se presenta la arquitectura de la comunicación de la tarjeta Java con el lector de tarjetas o CAD (Card Accepting Device). El intercambio de información y comandos entre la tarjeta y el CAD se realiza a través de Unidades de APDUs (Application Protocol Data Units).

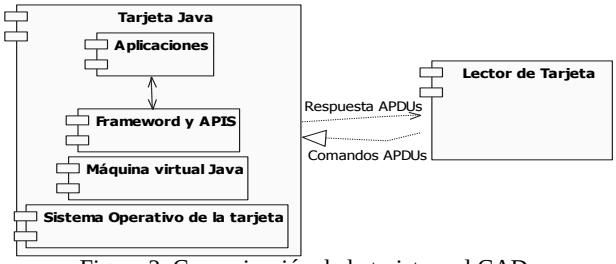

Figura 2. Comunicación de la tarjeta y el CAD

Por otra parte, se ha realizado el diagrama de secuencia de acceso a un servicio. En él se muestra cómo el usuario accede a los servicios autenticándose y utilizando la seguridad del certificado digital X.509 almacenado en su tarjeta inteligente (ver Figura 3).

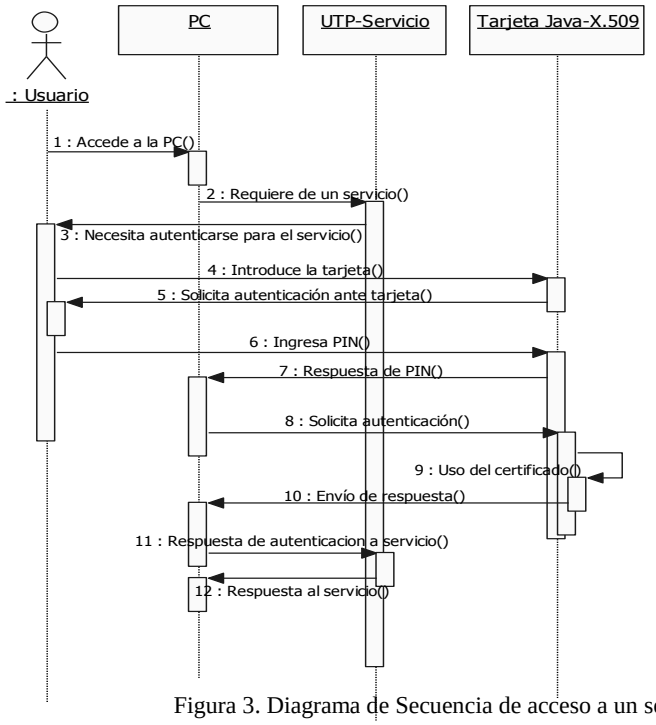

Figura 3. Diagrama de Secuencia de acceso a un servicio

4. CONCLUSION

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 y 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 demostrador de usuario/servidor. Este 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.

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

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.

Elfadil, N. A. and Al-raisi, Y. J., 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.

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.

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

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.