Aplicación de la firma dual para la corrección de exámenes en el entorno web

Application of the Dual Signature to the Evaluation of Exams on the Web Environment

O. Cánovas, F. J. García, A. F. Gómez y G. Martínez

Resumen

Existen aplicaciones orientadas al web que deben incorporar una prueba persistente de algún hecho realizado durante su ejecución. Esta prueba persistente puede ser la firma digital. La tarjeta inteligente se presenta como un soporte de almacenamiento seguro para la información secreta de cada firmante. Por tanto existe la necesidad de integrar en el entorno web la firma digital mediante el uso de la tarjeta inteligente. Microsoft Internet Explorer y Netscape Navigator son los navegadores con más usuarios, y por lo tanto se trata de conseguirlo mediante las tecnologías criptográficas que ambos navegadores nos proporcionan. Para conseguir integrar la firma digital en el navegador Navigator debemos hacerlo en base a un módulo criptográfico PKCS#11, mientras en el Explorer debemos hacerlo mediante un Cryptographic Service Provider (CSP).

Una utilidad de la firma digital en el entorno web es la corrección de exámenes. La implantación de un sistema de firma dual en los formularios web de los exámenes posibilita la ocultación de los datos. De tal forma que la firma dual posibilita el anonimato del opositor garantizando la imparcialidad del Tribunal en la corrección del examen.

Palabras clave: Firma dual, firma digital, CSP, PKCS#11, aplicación web.

Summary

Some web applications have to add a persistent proof of the information exchanged during its execution. This persistent proof can be a digital signed document. On the other hand, Smart cards are secure devices to store the signer private key. Therefore, it needed to achieve the digital signature support using smart cards on the web environment, in order to provide a High-security service. As Microsoft Internet Explorer and Netscape Navigator are the most widely used browsers, we have to achieve our goal through the cryptographic capabilities provided by these applications. Digital signature support can be added to Navigator with an PKCS#11 compliant implementation, whereas Internet Explorer requires a Cryptographic Service Provider (CSP).

An application of the digital signature on the web environment is the application of exams. Using dual signatures, it is possible to hide certain data to some participants, making feasible the anonymity and assuring the evaluators impartiality.

Keywords: Dual Signature, digital signature, CSP, PKCS#11, web application.

La implantación de un sistema de firma dual en los formularios web de los exámenes posibilita la ocultación de los datos

1.- Introducción

Existen aplicaciones orientadas al web que deben incorporar una prueba persistente de algún hecho realizado durante su ejecución, como por ejemplo la autorización de una transacción en una herramienta de comercio electrónico. Esta prueba persistente, duradera en el tiempo, puede ser la firma digital que nos garantiza la autenticidad, la integridad y el no repudio de los datos.

En la implantación de la firma digital es fundamental el desarrollo de una Infraestructura de Clave Pública (PKI). La PKI proporciona el conjunto de estándares y servicios que facilitan el uso de la criptografía de clave pública sobre la cual se sustentan los mecanismos de la firma digital. Los dispositivos portables tales como las tarjetas inteligentes, tarjetas PCMCIA, y discos inteligentes son herramientas ideales para implementar criptografía de clave pública, en tanto que proporcionan una forma segura de almacenar la clave privada, bajo el control de un único usuario. Actualmente la tarjeta inteligente se presenta como un soporte de almacenamiento seguro, de coste asequible y bien aceptado por los usuarios finales.

Netscape Communicator permite la instalación de un módulo criptográfico PKCS#11 en su librería de seguridad, de tal forma que integra el uso de dispositivos criptográficos, y por tanto de tarjetas inteligentes, desde sus aplicaciones

Para conseguir el uso de la tarjeta inteligente en una aplicación orientada a web es necesario integrar su acceso desde el navegador con el objetivo de leer la información secreta almacenada en ella y poder realizar la firma digital.

2.- La firma digital mediante tarjeta inteligente en el entorno web

Por tanto existe la necesidad de integrar en el entorno web unos servicios básicos de seguridad a través de la firma digital y mediante el uso de la tarjeta inteligente. Microsoft Internet Explorer y Netscape Navigator son los dos navegadores comerciales con más usuarios en el mundo, y por lo tanto se trata de conseguirlo mediante las tecnologías que ambos navegadores nos proporcionan a nivel criptográfico. Para conseguir integrar la firma digital en el navegador Netscape Navigator debemos hacerlo en base a un módulo criptográfico PKCS#11 que integre el uso de la Infraestructura de Clave Pública (PKI) con las tarjetas inteligentes, mientras en el Microsoft Internet Explorer debemos hacerlo mediante un Cryptographic Service Provider (CSP).

Módulo PKCS#11 en Netscape Communicator

PKCS #11, miembro de la familia de estándares de criptografía de clave pública (PKCS: Public Key Cryptography Standard)[1], especifica una API, llamada "Cryptoki", para dispositivos que poseen información criptográfica y realizan funciones criptográficas. Criptoki aisla a una aplicación de los detalles de los dispositivos criptográficos. La aplicación no tiene que cambiar de interface para un tipo diferente de dispositivo o para ejecutarse en un entorno diferente; es decir, la aplicación es portable.

Netscape Communicator permite la instalación de un módulo criptográfico PKCS#11 en su librería de seguridad (Netscape Security Library)[2], de tal forma que integra el uso de dispositivos criptográficos, y por tanto de tarjetas inteligentes, desde sus aplicaciones, como por ejemplo Netscape Navigator. Una vez instalado un módulo criptográfico PKCS#11, una aplicación web puede acceder a sus funcionalidades de forma muy limitada mediante el firmado de formularios (Netscape Form Signing).Una aplicación web que necesite unas funcionalidades criptográficas más amplias puede buscar una solución en la instalación de un plugin y en el uso de diversas tecnologías de Netscape (LiveConnect y SmartUpdate).

MODELO GENERAL DE CRYPTOKI

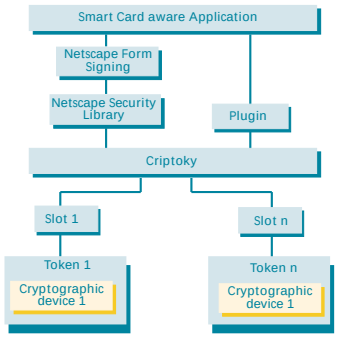

Figura 1

El modelo general de Cryptoki en Netscape Communicator es ilustrado en la Figura 1. El modelo comienza con una o más aplicaciones que necesitan realizar operaciones criptográficas sobre tarjetas inteligentes, y finaliza con un dispositivo criptográfico, sobre el cual alguna o todas las operaciones le son requeridas. La figura propone dos caminos de acceso a las funcionalidades criptográficas, mediante la librería de seguridad y mediante el desarrollo de un plugin que bien puede basar sus funcionalidades criptográficas en la API Cryptoki o en otras librerías externas.

CSP en Microsoft Internet Explorer

Los componentes básicos del subsistema de tarjetas inteligentes de Windows están basados

en el estándar PC/SC [3]. La especificación PC/SC abarca desde las características físicas requeridas por las tarjetas inteligentes y los lectores hasta los niveles de aplicación.

La arquitectura del subsistema de tarjetas inteligentes de Windows [4] desde la perspectiva del desarrollador de aplicaciones proporciona cuatro mecanismos para acceder a los servicios soportados por una tarjeta inteligente: CryptoAPI, Microsoft Win32 API, Scard COM y un interface de usuario. El mecanismo elegido depende del tipo de aplicación y las capacidades de la tarjeta inteligente. La Figura 2 muestra un esquema de la arquitectura PC/SC que presenta el subsistema de tarjetas inteligentes de Windows.

ESQUEMA DE LA ARQUITECTURA PC/SC

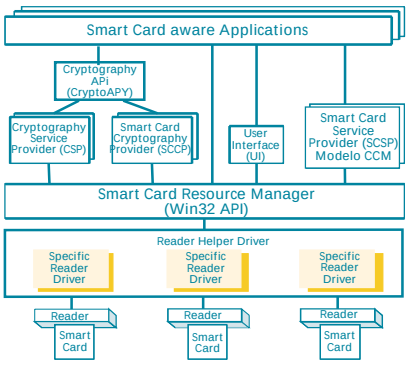

Figura 2

Desde el punto de vista de un desarrollador de una aplicación web el acceso idóneo sería mediante la CryptoAPI. Esta es la API de las funciones criptográficas (cifrado, firma digital,...). Toda aplicación que desee realizar una función criptográfica debe acudir a ella. El tipo de criptografía que ofrezca la CryptoAPI depende del CSP que selecciones para trabajar.

Los beneficios de usar la CryptoAPI son significativos porque el desarrollador puede tener la ventaja de las características criptográficas integradas dentro de la plataforma Windows sin tener que conocer la criptografía o como funciona un algoritmo en particular.

El acceso desde una aplicación web a la CryptoAPI no puede ser directo, ya que no se trata de un conjunto de objetos COM. Una solución inmediata es el desarrollo de un ActiveX COM que realice el puente y el filtrado de las funciones de la CryptoAPI necesarias en la aplicación web.

El acceso desde una aplicación web a la CryptoAPI no puede ser directo, ya que no se trata de un conjunto de objetos COM

3.- Aplicación de la firma dual en la corrección de exámenes

Tras mostrar los mecanismos para conseguir acceder a las funcionalidades criptográficas a través del navegador, Netscape Navigator o Internet Explorer, según el caso, a continuación se presenta una aplicación que muestra la utilidad de la firma digital en el entorno web. La aplicación consiste en la implantación de un sistema de firma dual (dual signature) en los formularios web de los exámenes.

Se denomina firma dual (Dual Signature) al firmado digital del resumen de la concatenación de los resúmenes de dos documentos. Los pasos para realizar la firma dual, dados dos documentos, son:

- Calcular el hash de ambos documentos, Hash 1 y Hash 2 respectivamente.
- Concatenar ambos resúmenes Hash 1 y Hash 2.
- Calcular el hash de la concatenación, este hash se denomina resumen dual.
- Cifrado del resumen dual con la clave privada del firmante obteniendo la firma dual.

Con la firma dual conseguimos un mecanismo que enlaza a un mismo firmante con dos documentos diferentes, manteniendo una relación permanente entre ambos documentos. El sistema de firma dual

La firma dual es la relación permanente entre los resultados y los datos personales, y es por tanto utilizada para enlazar los datos personales y la nota cuando el Tribunal envía a Secretaría su evaluación y la firma dual correspondiente a los resultados evaluados, y todo ello firmado digitalmente

es fácilmente ampliable, en cuanto al número de documentos implicados, aunque el análisis aquí planteado se centrará en el caso básico de dos documentos.

La utilidad de la firma dual se manifiesta en un escenario como el propuesto en la corrección de exámenes y que muestra en la Figura 3, donde un opositor envía al Tribunal uno de los documentos con las respuestas del examen y a la Secretaría el otro de los documentos con los datos personales del opositor. En ningún momento después del envío de ambos documentos, respuestas y datos personales, se vuelven a encontrar juntos en ninguna entidad, esto proporciona el anonimato del opositor ante el Tribunal. Una vez evaluado el examen por el Tribunal la nota es enviada a la Secretaria que establece formalmente la nota al opositor.

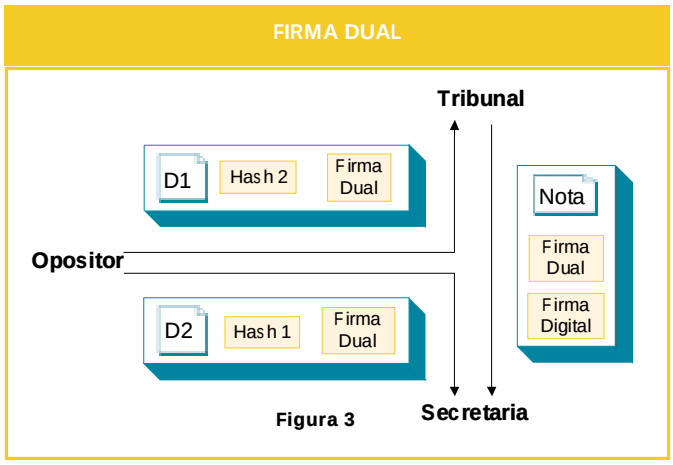

Figura 3

El opositor envía a cada receptor el documento de texto, el resumen del otro documento y la firma dual. El receptor consigue comprobar la autenticación, la integridad y la relación con el otro documento, verificando la firma dual siguiendo el siguiente proceso:

- Obtener el resumen del documento recibido.
- Concatenar el resumen del documento con el resumen recibido.
- Obtener el resumen dual de la concatena-ción anterior.
- Descifrar con la clave pública del emisor la firma dual.
- Comparar el resultado de los dos puntos anteriores, si coinciden, la firma dual queda verificada, en caso contrario no.

La firma dual es la relación permanente entre los resultados y los datos personales, y es por tanto utilizada para enlazar los datos personales y la nota cuando el Tribunal envía a Secretaría su evaluación y la firma dual correspondiente a los resultados evaluados, y todo ello firmado digitalmente.

4.- Conclusiones

Los navegadores Internet Explorer y Netscape Navigator proporcionan las tecnologías suficientes para desarrollar aplicaciones web que necesiten ciertas funcionalidades criptográficas. Si bien en Netscape

Navigator se debe desarrollar un plugin que amplíe las necesidades criptográficas y en Internet Explorer se debe introducir un objeto ActiveX COM que facilite el acceso a funciones de la CryptoAPI. Así es posible el desarrollo de aplicaciones como la corrección de exámenes donde el uso de la firma dual posibilita el anonimato del opositor ante un Tribunal de evaluación.

El uso de la firma dual posibilita el anonimato del opositor ante un Tribunal de evaluación

Este trabajo ha sido parcialmente financiado por el proyecto FEDER CICYT TEL-1FD97-1426

Referencias bibliográficas

[1] Public-Key Cryptography Standards, [www] http://www.rsa.com/rsalabs/pubs/PKCS/
[2] Netscape Security Developer Central, [www] http://developer.netscape.com/security/
[3] PC/SC workgroup, [www] http://www.pcscworkgroup.com
[4] Microsoft Security, [www] http://www.microsoft.com/security/devlink.asp

O. Cánovas
(ocanovas@ditec.um.es)
Dpto. Ingeniería y Tecnología de Computadores
F. J. García
(fgarcia@dif.um.es)
A. F. Gómez
(skarmeta@dif.um.es)
G. Martínez
(gremar@dif.um.es)
Dpto. Informática, Inteligencia Artificial y Electrónica
Universidad de Murcia