Artículo de Reflexión

Citación: Gaona P., Montenegro C. y Wiesner H. "Hacia una propuesta de mecanismos para la autenticidad de objetos de aprendizaje en plataformas LCMS," *Ingeniería, vol. 19, no. 1, pp. 50-64, 2014.*

Hacia una propuesta de mecanismos para la autenticidad de objetos de aprendizaje en plataformas Learning Content Management Systems

Mechanisms for Authenticity of Learning Objects in Learning Content Management Systems Platforms: Issues and Proposals

Paulo Alonso Gaona García
Universidad Distrital F.J.C
y Universidad de Alcalá
pagaonag@udistrital.edu.co

Carlos Enrique Montenegro Marín
Universidad Distrital F.J.C
cemontenegro@udistrital.edu.co

Helvert Wiesner González
Universidad Distrital F.J.C
helvertw@gmail.com

Resumen

Los actuales mecanismos de seguridad, dentro de una plataforma Learning Content Management Systems (LCMS), carecen de principios para llevar a cabo procesos de confidencialidad, integridad y privacidad de contenidos. Específicamente, la autenticidad de contenidos, es uno de los temas que dentro del área de seguridad informática requiere el establecimiento de una serie de normas y procesos para la veracidad de la información en cualquier entorno de trabajo. Por lo tanto, el presente artículo presenta una propuesta para la definición de un mecanismo de seguridad informático, que permita suplir algunas de estas necesidades dentro de una plataforma LCMS; para este caso, asociadas a la seguridad de los LCMS usando el concepto de firmas digitales bajo una Infraestructura PKI (Public Key Infrastructure).

La propuesta contempla definir aspectos para que cualquier entidad educativa pueda gestionar certificados digitales. El objetivo es ofrecer una serie de lineamientos y consideraciones para la gestión e integración de certificados digitales, con el propósito de facilitar el funcionamiento de un mecanismo de seguridad para validar la autenticidad de recursos digitales dentro de una plataforma LCMS.

Palabras clave: certificados digitales, firmas digitales, infraestructura de clave pública, LCMS, seguridad de la información

Abstract

The current security mechanisms of Learning Content Management Systems (LCMS) platforms, do not contemplate aspects related to confidentiality, integrity and privacy of contents in learning objects. In particular,

Fecha recibido: 12/12/2013
Fecha modificado: 14/06/2014
Fecha aceptado: 16/06/2014

the authenticity of content is one of the topics in the field of information security that requires principles and processes to carry out the veracity of information in any collaborative work environment. Within this context, this paper presents a proposal for the definition of a computer security mechanism to improve protection levels of LCMS platforms, through the concept of digital signatures and PKI (Public Key Infrastructure).

The approach considers the definition of aspects so that educational institutions can improve the digital certificate management or become a certification authority. The goal is to provide a set of guidelines and considerations for the management and integration of digital certificates, in order to facilitate the operation of a security mechanism to validate the authenticity of digital resources within a LCMS platform.

Key words: digital certificates, information security, learning content management system, public key infrastructure.

1. Introducción

El concepto de autenticidad de contenidos y recursos digitales presentes en internet no ha sido implementado de manera amplia sobre las diferentes plataformas, servicios o páginas disponibles en la web. Este concepto, orientado a respetar la autoría y la integridad de la información, parece no tener una mayor relevancia cuando se comparte y se gestiona por toda la web, mediante distintas entidades e infraestructuras informáticas. Por un lado, este comportamiento se presenta, en gran medida, por desconocimiento de los usuarios y, por otro, se relaciona con la falta de mecanismos informáticos que le faciliten a los usuarios tener un control de sus contenidos que circulan a través de Internet de manera insegura. A partir de estas perspectivas, diferentes iniciativas se han estado desarrollando como un intento de abordar parte de la problemática, aunque, en cierta manera, la abordan para generar soluciones parciales sobre casos particulares. Un ejemplo de ello, podemos relacionarlo con el proyecto denominado Plan Avanza [1] de la sociedad española. Proyecto que dentro de sus múltiples objetivos se encargó de implementar un sistema de autenticación denominado DNI electrónico, con el fin de crear una herramienta de identificación personal que acreditara la identificación de cada ciudadano de manera física y electrónica. Esta herramienta ha venido evolucionando en servicios de identificación y autenticación de diferentes documentos digitales utilizados por empresas en España.

Diferentes servicios y herramientas web tienen como eje principal el intercambio de contenidos a través de la red, y en este campo los LCMS se destacan como una de las herramientas de valor agregado para el apoyo académico y administrativo en la gestión de contenidos y recursos digitales, entre otras funcionalidades.

Los LCMS nacieron como evolución de los LMS (Learning Management System) para el manejo de contenidos generados alrededor de un sistema de enseñanza y aprendizaje mediante herramientas Web [2, 3]. Su popularidad se debe a que posibilitan el desa-

rrollo colaborativo del aprendizaje y enriquecen este proceso mediante la administración de los usuarios alrededor de este, permitiendo así gestionar estudiantes, profesores, administradores, entre otras actividades, y enfocando todo el contenido generado en llevar a cabo un proceso de aprendizaje [4]. A pesar del uso y la expansión de los LCMS, la seguridad que se registra en algunos de ellos no es lo suficientemente robusta como para asegurar los contenidos [5-7].

Trabajos previos han definido algunos lineamientos para la definición de un *framework* que facilite la distribución de contenidos fiables dentro de plataformas virtuales a partir de estándares como SCORM [8], y estrategias mediante el concepto web de confianza [9]. Gualberto y Zorro [10] presentaron el caso de estudio para la certificación de contenidos emitidos por dos usuarios en plataformas Sakai [11] y Moodle [12] mediante Web Service; sin embargo, solo se enfocan en la autenticidad de usuarios, dejando a un lado los contenidos. Otro trabajo para resaltar es la iniciativa presentada por el proyecto PERMIS (Privilege and Role Management Infrastructure Standards Validation) [13], que integra universidades de España, Italia y Reino Unido, y cuyo propósito es el uso de certificados digitales para llevar a cabo controles de acceso de usuarios en plataformas LCMS mediante el uso de una infraestructura de clave pública. De igual forma, se han realizado estudios mediante análisis de minería de datos [14], donde se identificaron algunas de las plataformas LCMS más comunes, las cuales presentaron un mayor número de mecanismos de seguridad. Como resultado de este análisis, se identificó la herramienta Moodle como una de las plataformas LCMS con mayor número de mecanismos de seguridad implementados. Dentro de estos mecanismos se cuenta con módulos de autenticación mediante LDAP, PAM, Kerberos y correo electrónico, y se da la posibilidad de generar certificados mediante SSL y TS, al igual que el uso de protocolos HTTPS, para manejar listas de control de acceso, entre otros. Cabe señalar que la autenticidad de contenidos asociados dentro de objetos de aprendizaje es un campo que todavía no ha sido explorado en su totalidad [8].

A partir de este marco de referencia, una de las motivaciones que dio lugar a este estudio es proporcionar estrategias que logren abordar estas necesidades, mediante el planteamiento de una serie de consideraciones para la integración de una herramienta informática que le facilite a una institución académica la autenticación de contenidos dentro de una plataforma LCMS. El estudio se centrará, de manera especial, en los objetos de aprendizaje desarrollados por profesores o creadores de materiales educativos y, de manera general, abordará la validación de información presente en este tipo de herramientas.

Para llevar a cabo este estudio, el presente artículo se encuentra organizado de la siguiente manera: la sección 2 presenta un panorama del tema relacionado con la autenticación de contenidos y la seguridad en la web. La sección 3 aborda el tema de autoridades certificadoras o AC encargadas de la administración de los certificados digitales y de cómo un LCMS puede convertirse en esta función. La sección 4 aborda las consideraciones para llevar a cabo una propuesta de desarrollo y su implementación sobre la

plataforma Moodle. Esta sección también define algunas de las recomendaciones más representativas para la integración de certificados digitales. Finalmente, se describen las conclusiones de la propuesta planteada, para la implementación de este tipo de mecanismos sobre una entidad académica.

2. Seguridad y autenticación de contenidos Web

El concepto de seguridad en documentos informáticos, contenidos web y en general sobre cualquier recurso digital presente en internet presenta varios enfoques. Carracedo [15] los define a partir de cuatro pilares básicos: 1) La *privacidad*, que hace referencia a proteger la información para que solo esté disponible para los usuarios a los cuales les esté permitida dicha información; 2) la i*ntegridad*, bajo la cual se debe garantizar que la información no es alterada durante el proceso de transmisión en un sistema de comunicaciones; 3) *la autenticidad*, que tiende a garantizar la autoría del mensaje y, finalmente, 4) el *no rechazo o no repudio*, enfocado a que el autor no pueda rechazar el contenido que fue emitido por él mismo. Diferentes técnicas han ido evolucionando para intentar solventar estas necesidades, partiendo de los principios de la criptografía moderna [16] y gracias al impulso de grandes esfuerzos para el desarrollo de herramientas criptográficas conocidas e implementadas en la actualidad. Una de las técnicas más difundidas y utilizadas para asegurar la información en internet se conoce como las firmas digitales. Este concepto surge como evolución electrónica de las firmas manuscritas sobre la base de la criptografía y el área de seguridad informática.

2.1 Firmas digitales

En medio de la evolución de la seguridad informática, en los años setenta Rivest, Shamir y Adelman [17] diseñaron un sistema criptográfico conocido como RSA. El sistema funciona con la generación de dos pares de números ligados matemáticamente, conocidos en el léxico de la criptografía como clave privada y clave pública [18, 19]. Esta relación matemática entre los números garantiza que dada una clave pública, sea imposible deducir la clave privada. De la misma manera que para dos claves públicas diferentes no existe una misma clave privada. Este esquema hoy en día se conoce como criptografía de clave pública [18] y es ampliamente utilizado, ya que con el par de claves permite un proceso de encripción de la información y de la firma digital. Para el proceso de encriptación de la información en un sistema de comunicaciones, utilizando algoritmos de clave pública, es necesario que el emisor y el receptor hayan generado su correspondiente par de claves. La clave pública de cada usuario es enviada entre todos los miembros del sistema, o debe estar disponible en el momento en que cualquier usuario la necesite. El proceso que normalmente se lleva a cabo se presenta en la figura 1, donde un usuario que emite un mensaje debe tener la clave pública del receptor, con la cual encripta el mensaje. Esto garantiza que el único que puede desencriptar el mensaje es el receptor, quien tiene la correspondiente clave privada.

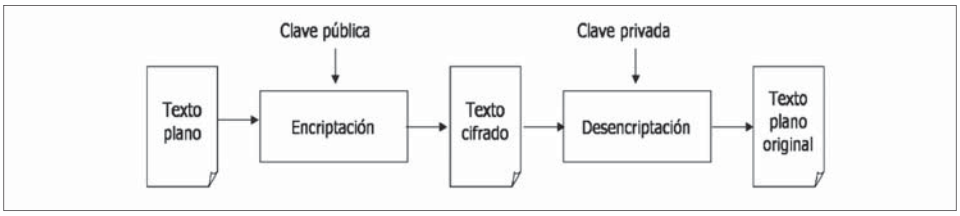

Figura 1. Proceso de encriptación con clave pública.
Fuente: [20]

Ahora bien, para generar una firma digital se usa la clave privada de quien firma el mensaje. Una vez se tiene el documento a firmar y la clave privada, por medio de funciones Hash, se genera lo que se conoce como huella digital. Tanto la huella digital como el documento son enviados al receptor, el cual, utilizando la clave pública del emisor, obtiene un Hash del documento y este se compara con un *Hash* del documento original; en consecuencia, si estos dos coinciden la firma digital es válida.

A continuación, en la figura 2, se realiza la representación gráfica de la firma digital dentro de cualquier tipo de especificación, mecanismo o algoritmo criptográfico.

La función *Hash* es parte fundamental en la estructura de los algoritmos de firma digital al utilizar funciones unidireccionales en la autenticación de los mensajes, lo que garantiza que una vez ha sido cifrado el mensaje no se puede descifrar. Esta función garantiza la "huella dactilar" del documento, por lo tanto, este tipo de funciones genera un valor agregado en el área informática y de las telecomunicaciones. A continuación, se presentan los pasos para firmar digitalmente un documento:

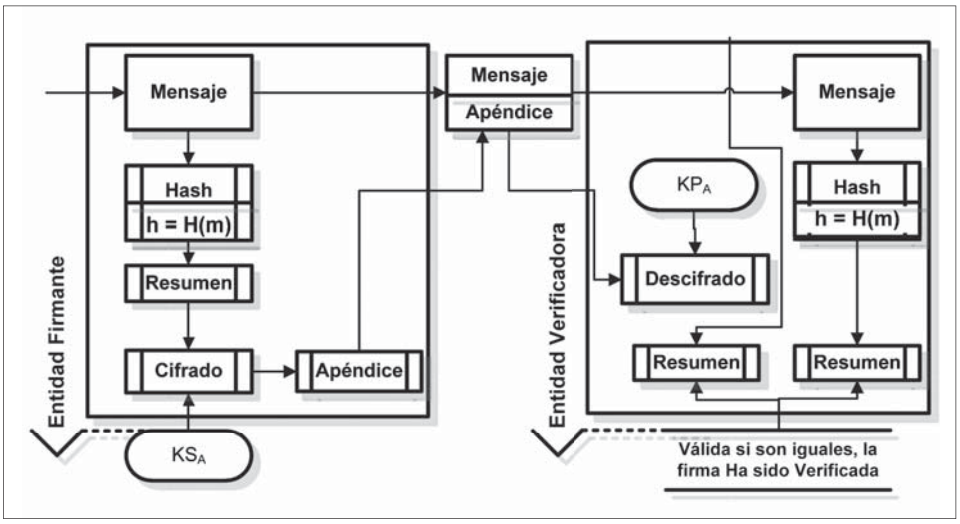

Figura 2. Adaptación de un esquema de firma digital genérico.
Fuente: el autor.

1. El valor *Hash* (*H*) es conocido también como resumen de (*m*) (longitud del mensaje original), y logra obtener la siguiente función para su cálculo de acuerdo a la ecuación 1:

$$\text{Función Hash} \quad h = H(m) \tag{1}$$

Este proceso genera una firma que se trabaja mediante un resumen del mensaje.

2. El resumen sufre un proceso de cifrado junto con su clave privada KSA, la cual se envía junto con el mensaje original al receptor. Para cifrar se utiliza un algoritmo criptográfico (clave pública o privada), el cual garantiza la autenticación del mensaje mediante la generación de una firma digital.

3. El proceso de verificación de la firma se consigue descifrando el valor del apéndice enviado por el emisor, utilizando para ello la clave pública. Este proceso debe generar la firma del resumen, la cuál debe ser comparada con la firma original generada por el emisor para identificar la validez de esta.

2.2 Certificados digitales

Un certificado digital es un documento electrónico por medio del cual se puede dar fe de que una determinada clave pública pertenece a un determinado usuario. La institución que garantiza esta relación entre usuario y clave pública es denominada autoridad de confianza (CA). Para garantizar que el certificado digital no ha sido alterado, este documento va firmado con la clave privada de una CA, de manera tal que cualquier usuario del sistema puede verificar la validez del certificado con la clave pública de la CA. La misión de las CA es generar el par de claves de los usuarios y mantener un registro de claves públicas [21], para que cualquier usuario pueda verificar la firma de otro usuario con ayuda de la CA.

Existen varios tipos de certificados según su uso; los certificados personales, usados primordialmente para el cifrado personal, cifrado de email, firma de formularios, etc; los certificados de servidor, utilizados para el protocolo SSL, VPN, entre otros, y los certificados de firma de código, para garantizar la autenticidad del software. La estructura de los certificados está, en su mayoría, definida por el estandar X509. La primera versión del estándar X509 surgió en 1988 y en la actualidad está en su versión 3. Su estructura se muestra en la figura 3:

Figura 3. Estructura de un certificado X.509. Fuente: [22].

2.3 Autoridad certificadora

Tambien conocidas como autoridades de confianza, son las encargadas de emitir los certificados digitales de los usuarios de un sistema de seguridad que implemente infraestructura PKI. Para este proceso las AC o autoridades de certificación almacenan las claves públicas de los clientes y la correspondiente información que identifica al usuario. En el momento en que cualquier usuario necesite verificar una firma digital dentro del sistema de comunicaciones requiere la clave pública de quien emitió el mensaje. La función de la CA es garantizar la relación existente entre la clave pública y los datos de usuario inscritos dentro de un certificado digital. Este proceso es posible ya que cuando una CA emite un certificado lo firma digitalmente con su clave privada; de manera tal que si el certificado es alterado en cualquier momento este no puede ser verificado por la CA y, por tanto, el certificado es revocado.

3. Consideraciones para el modelo trabajo de certificados digitales en Moodle

Para llevar a cabo una implementación sobre plataformas digitales como Moodle, es necesario extender las funcionalidades de la plataforma para brindarle capacidades de emisión, revocación y validación de certificados digitales. Adicionalmente, es importante proveer de un mecanismo para la firma de contenidos gestionados por un LCMS, esto se realiza a través de los certificados generados. Por citar un ejemplo, la plataforma Moodle en su núcleo no provee estas características, y el uso de certificados se restringe a su caracteristica de *Red* Moodle; aunque, esta se usa para cifrar la autenticación de usuarios entre servidores de Moodle y no para la gestión de certificados. Por tanto, es necesario contar con entornos de trabajo que faciliten una integración de este tipo de procesos. Para este caso se considera el uso de OpenSSL [23], dado que es un API que proporciona un entorno de trabajo para encriptar datos de manera eficiente.

En consecuencia, en el esquema planteado en la figura 4 se presenta el entorno de trabajo OpenSSL como una herramienta para la creación y gestión de certificados del lado del servidor, que, en conjunto con una capa de persistencia definida mediante un lenguaje tipo servidor, como es el caso de PHP, permite no solo garantizar la integridad de los contenidos subidos, sino también almacenar la información referida a la certificación de los contenidos para su posterior manejo.

El mecanismo en el lado cliente se orienta, primordialmente, para la firma de los documentos usando los certificados generados con OpenSSL para los usuarios del LCMS. Este componente de firmado de archivos y solicitud de certificados se define como un *applet* para el navegador de java y es diseñado para comunicarse con el servidor de Moodle. Esto facilita la firma de archivos en entornos multiplataforma, cuyo funcionamiento es independiente del navegador usado por el usuario (figura 5).

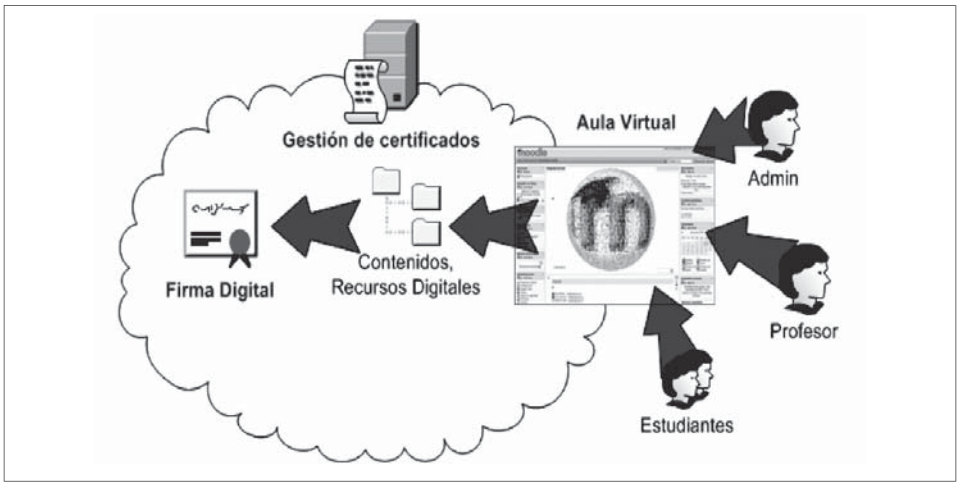

Figura 4. Modelo propuesto de trabajo.
Fuente: el autor

3.1 Modelo de capas planteado

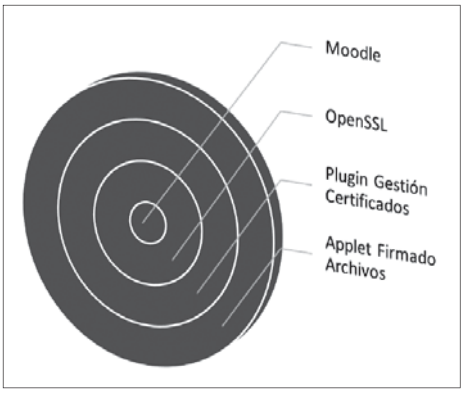

Figura 5. Diagrama del esquema propuesto de autenticación de contenidos sobre Moodle.
Fuente: el autor

La figura 5 presenta de forma esquemática los componentes usados para llevar a cabo el desarrollo del modelo planteado. Como base se encuentra Moodle, que provee toda la funcionalidad de LCMS y, además, alimenta al prototipo con los registros de usuarios existentes en la plataforma. En un segundo nivel se encuentra OpenSSL, que provee de toda la infraestructura para la generación de certificados digitales y su posterior administración. En el tercer nivel se ubica el plugin de gestión de certificados que modifica a Moodle, facilitando la comunicación con OpenSSL y agregando los cambios en la interfaz de Moodle para el acceso a las nuevas funciones. Finalmente, en el nivel más externo tenemos el *applet* de firmado digital, que se encarga de firmar del lado del cliente los contenidos educativos antes de subirlos a Moodle y las solicitudes de generación de certificados y validación de estos.

3.2 Generación de certificados digitales

Para la generación de los certificados digitales se debe estructurar un esquema cliente-servidor, que permita el manejo de información y entrega de los certificados a los usuarios de manera segura. Para establecer la comunicación de modo seguro se utiliza una

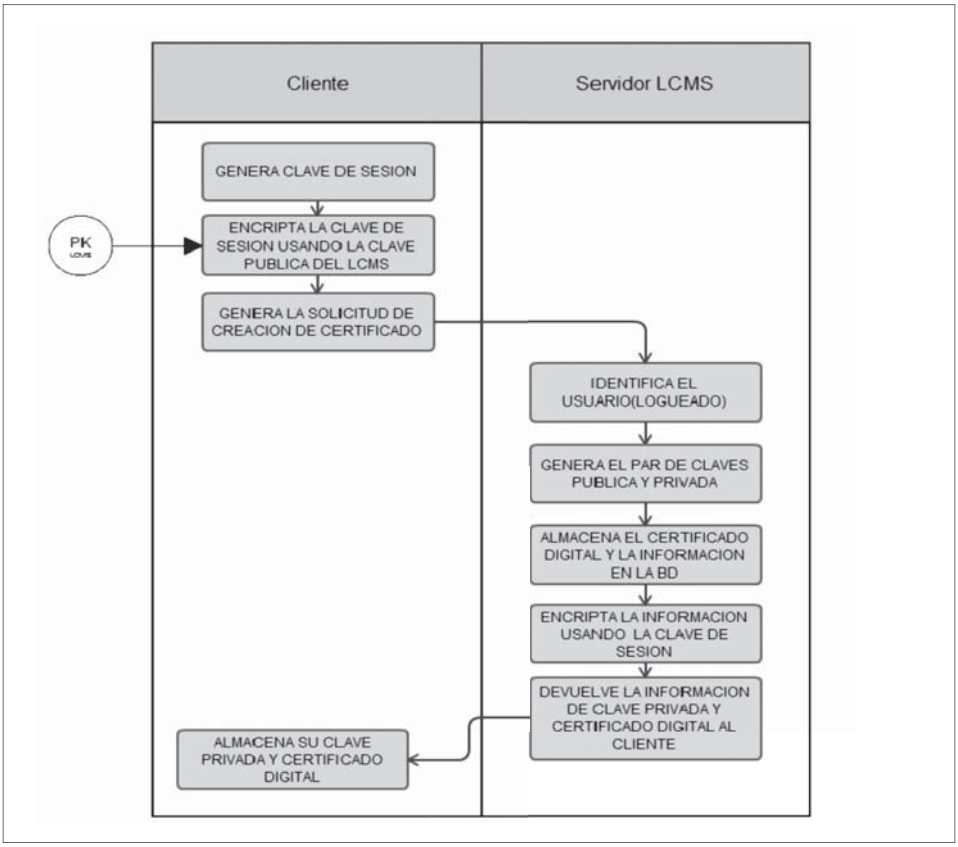

Figura 6. Proceso de firma digital planteado.

clave de sesión. La clave de sesión es una clave que el usuario genera antes de hacer la solicitud de creación del certificado y sirve para encriptar la información que el servidor devuelve al cliente como respuesta a la solicitud. El concepto de la clave de sesión se basa en la criptografía simétrica o de clave privada [24]. El proceso de generación de los certificados de esta forma se presenta en la figura 6.

A continuación, se describe cada una de las etapas definidas en la figura 6:

1. Una vez que el usuario ha realizado el proceso de autenticación en la plataforma LCMS se genera una clave de sesión aleatoria por medio del mecanismo.

2. El mecanismo del lado del cliente encripta la clave de sesión con la clave pública del LCMS, con el fin de que solamente sea conocido por el mecanismo de seguridad del LCMS.

3. El usuario hace la solicitud de generación del certificado y envía los datos encriptados al servidor por medio de una solicitud POST.

4. El mecanismo del lado del servidor valida los datos del usuario (autenticado en la plataforma) y genera la clave pública y privada del usuario.

5. El mecanismo del lado del servidor almacena el certificado público del usuario y su correspondiente par de claves en la base de datos.

6. El mecanismo del lado del servidor encripta los datos a retornar al usuario por medio de la clave de sesión y le devuelve la información al usuario.

7. El mecanismo del lado del usuario desencripta la información con la clave de sesión y guarda la clave privada y el certificado digital de manera segura.

La siguiente sección presenta algunas de las consideraciones más representativas para llevar a cabo la implementación de este tipo de soluciones.

4. Consideraciones para la integración de certificados digitales

Para llevar a cabo el diseño y desarrollo de un mecanismo, se evalúan a continuación dos escenarios para la firma de contenidos (tomando como caso de estudio la plataforma Moodle). El primero es la transmisión de los contenidos como funciona actualmente la plataforma Moodle, para su posterior firma en el servidor. Si bien esto tiene la ventaja de que se podría usar OpenSSL para el cifrado de los archivos mediante de la función *openssl_encrypt*, presenta el inconveniente de que los archivos recibidos pueden ser potencialmente diferentes de los que el usuario desea subir, por problemas de transmisión o por algún atacante en el medio del canal de comunicaciones. El segundo escenario plantea, por el contrario, la firma de los archivos en el cliente para su posterior transmisión al servidor, puesto que durante la firma se valida el certificado utilizado por el usuario, con lo cual es posible verificar en cualquier momento si el archivo recibido coincide con el firmado del lado del cliente, solucionando el problema que surge en el primer escenario.

A fin de lograr que el prototipo ofrezca seguridad desde su diseño se toma como referencia el segundo escenario. Esto plantea, por supuesto, un reto en la implementación del firmado del lado del cliente ya que actualmente no existe un estándar abierto y de facto para el firmado con certificados digitales en ambientes Web. Como propuestas existen Javascript Crypto [25] de Mozilla, CAPICOM y Certenroll [25] de Microsoft, que funcionan con ActiveX, y, finalmente, Web Cryptography API de la W3C. Esta última es una de las propuestas firmes para ser el estándar a implementar en todos los navegadores que soporten de forma completa HTML5, pero que aún no se encuentra desarrollado en su totalidad [25].

Las propuestas de Mozilla y de Microsoft se encuentran implementadas actualmente, pero solo están disponibles para los navegadores Firefox e Internet Explorer, respectivamente. La propuesta de la W3C aún se encuentra lejos de publicar su documento final y

Figura 7. Consideraciones para proceso de firmado digital.
Fuente: el autor

se requeriría un tiempo mayor para que los navegadores terminen sus implementaciones. Por lo tanto, no puede ser considerada como parte del desarrollo de nuestra propuesta. En consecuencia, el prototipo de este desarrollo se basa en Java, el cual permite que el componente de firma digital funcione en los sistemas operativos soportados por la máquina de ejecución de Java (JRE) y en diferentes navegadores a través de la implementación en forma de Applet, tal como se presenta en la figura 7.

5. Recomendaciones para LCMS como autoridades certificadoras

Basados en las consideraciones de la sección anterior y en estudios previos para la gestión de contenidos dentro de una plataforma LCMS [26], a continuación se presentan una serie de lineamientos para implementar un sistema de seguridad basado en certificados digitales.

1. *Proceso de generación de certificados digitales*. Este proceso contempla la generación de una clave pública y privada a petición del usuario. El LCMS debe gestionar el almacenamiento de los certificados digitales emitidos a los usuarios además de la información correspondiente al certificado en la base de datos del LCMS.

2. *Sistema de almacenamiento de claves privadas*. La AC debe almacenar la clave privada de cada usuario en una base de datos, no vinculada dentro del sistema de gestión de recursos digitales. Esto permitirá crear un modelo de autenticación de usuarios fiable dentro de la plataforma.

3. *Mecanismo de verificación de certificados digitales*. Luego del proceso de creación de los certificados digitales, estos son firmados por la LCMS. Esta firma permite garantizar que el certificado es válido en todo momento y que ninguna tercera parte en el sistema lo puede alterar en algún momento. De la misma manera, el LCMS debe contener un mecanismo que permita validar un certificado digital en cualquier momento por parte de otro usuario del sistema, y una vez verificado lo pueda usar en las diferentes herramientas del mecanismo.

4. *Lista de revocación de certificados o CRL*. Dentro de las herramientas con las que cuenta la LCMS para poder expedir certificados, se debe generar una lista que contenga los certificados que han sido revocados antes de su expiración y, por tanto, se invalide cualquier proceso que se haga con los mismos dentro del sistema. Cada entidad puede resolver las causales de revocación de los certificados; sin embargo, dentro de las más comunes se puede presentar que la clave privada del usuario se vea comprometida o la pérdida de estatus de un usuario dentro del sistema, por ejemplo, un estudiante que es expulsado.

5. *Validación del certificado*. Para poder validar un certificado, el usuario debe descargar la CRL que debe estar firmada con la clave privada de la AC, para garantizar su integridad. Si el identificador del certificado está contenido dentro de la lista, el certificado no es valido.

6. Conclusiones

La aplicación e integración de tecnologías estándar son de gran soporte para la seguridad en la web, pero su implementación está aún lejos de su adopción. Por lo tanto, actividades como la firma digital de archivos de lado del cliente necesitan aún del uso de tecnologías propietarias que no están diseñadas para funcionar en distintos entornos. Por este motivo, las consideraciones que se definen dentro de este artículo son un buen punto de partida para llevar a cabo el desarrollo de certificados digitales para la autenticidad de contenidos dentro de una plataforma LCMS, para este caso en particular, sobre la plataforma Moodle.

El estudio realizado evidencia la falta de mecanismos implementados dentro de las diferentes plataformas LCMS que, en principio, se encuentren orientadas a garantizar la confidencialidad de los contenidos gestionados dentro de ellas. En consecuencia, se pueden desarrollar herramientas y plantear soluciones que de manera particular ayuden a reducir el problema; sin embargo, cada LCMS tiene diferentes técnicas y estructuras de desarrollo, y cada uno define sus propias reglas para la implementación de extensiones,

por lo que aunque la solución planteada se pueda extender a cualquier LCMS, el prototipo desarrollado es una solución particular enfocada sobre la plataforma Moodle.

Por lo anterior es importante el establecimiento y divulgación de normas técnicas y legales para proteger el desarrollo de recursos digitales o la definición de pautas para la reutilización de las mismas dentro de un entorno académico. Por lo tanto, el desarrollo de este tipo de propuestas definen un nivel de confianza sobre el uso de materiales y recursos digitales dentro de un entorno académico, aunque existen otras vías legales que favorecerían el uso de materiales educativos, bajo el soporte de normas que amparan los derechos de autor.

Como trabajo futuro se prevé el desarrollo de un prototipo informático mediante la aplicación de los lineamientos definidos en el presente artículo, con el fin de llevar a cabo estudios que permitan evaluar el desempeño del mecanismo dentro de un entorno de trabajo real. Para ello, se llevarán a cabo varios casos de estudio mediante la definición de escenarios que faciliten la identificación de problemas o desafíos para la integración en plataformas LCMS.

Finalmente, es claro que los certificados digitales y firmas digitales no son una solución completamente fiable y segura dentro de un entorno abierto como lo es Internet. Por tal razón, es importante reconocer este tipo de mecanismos como alternativas de mayor aceptación dentro del área informática. Sin embargo, el tratamiento de información requerirá a futuro plantear estrategias más robustas para definir mayores niveles de confianza, donde las entidades y empresas en particular sobre cualquier área de conocimiento, necesitarán de la vinculación de información cada vez más fiable y veraz, a través de estrategias como Linked Data y Open Data.

Referencias bibliográficas

[1] S. Muriel, "Las TIC y la identificación personal: el DNI electrónico," *Física y Sociedad,* p. 28, 2009.

[2] L. Greenberg, "LMS and LCMS: What's the Difference," *Learning Circuits,* vol. 31, 2002.

[3] K. Harman and A. Koohang. *Learning Objects: Standards, Metadata, Repositories, and LCMS*. Santa Rosa: Informing Science, 2007.

[4] S. Irlbeck and J. Mowat, "Learning Content Management System (LCMS)," in *Learning Objects: Standards, Metadata, Repositories, and LCMS.* Santa Rosa: Informing Science, 2007, pp. 157-184.

[5] D. C. Luminita, "Information Security in E-learning Platforms," *Procedia-Social and Behavioral Sciences,* vol. 15, pp. 2689-2693, 2011.

[6] S. Kumar and K. Dutta, "Investigation on Security in LMS moodle," *International Journal of Information Technology and Knowledge Management,* vol. 4, pp. 233-238, 2011.

[7] L. M. R. Moreno, "La seguridad informática en el trabajo con la plataforma" Moodle," *Revista de Humanidades,* pp. 169-190, 2010.

[8] P. Gaona*, et al.*, "Plataforma de seguridad basado en autenticidad de contenidos sobre conjunto de especificaciones SCORM," *Revista Ingeniería y Competitividad,* vol. 12, pp. 51-68, 2011.

[9] P. Gaona*, et al.*, "Trust Levels Definition on Virtual Learning Platforms Through Semantic Languages," *International Journal of Interactive Multimedia and Artificial Intelligence,* vol. 1, 2010.

[10] T. M. Gualberto and S. D. Zorzo, "Incorporating Flexible, Configurable and Scalable Security to the Education Collaborative Environments," in *Frontiers in Education Conference, 2009. FIE'09. 39th IEEE*, 2009, pp. 1-6.

[11] Sakai, "Sakaiproject.org," [Online]. sakaiproject.org. Disponible en: http://www.sakaiproject.org. Consultado: junio 10 de 2014.

[12] Moodle, "Proyecto Moodle". [Online]. moodle.org. Disponible en: http://moodle.org. Consultado: junio 10 de 2014.

[13] D. W. Chadwick and A. Otenko, "The PERMIS X. 509 Role Based Privilege Management Infrastructure," *Future Generation Computer Systems,* vol. 19, pp. 277-289, 2003.

[14] D. Castañeda*, et al.*, "Análisis de reportes de seguridad sobre plataformas LCMS de tipo open source aplicando minería de datos," in *LACCEI - Latin American and Caribbean Consortium of Engineering Institutions*, Peru: 2010.

[15] J. Carracedo Gallardo. *Seguridad en redes telemáticas*. España: *Mc Graw Hill,* 2004.

[16] W. Mao, "Modern Cryptography," in *Selected Areas in Cryptography VIII (SAC'01)*, 2001.

[17] A. Shamir, "On the Generation of Cryptographically Strong Pseudorandom Sequences," *ACM Transactions on Computer Systems (TOCS),* vol. 1, pp. 38-44, 1983.

[18] S. Halevi and H. Krawczyk, "Public-key cryptography and password protocols," *ACM Transactions on Information and System Security (TISSEC),* vol. 2, pp. 230-268, 1999.

[19] J. L. G. Pardo, "Private-Key Encryption," in *Introduction to Cryptography with Maple*, New York: Springer, 2013, pp. 131-179.

[20] F. L. Hernandéz, *Seguridad, criptografía y comercio electrónico con Java*, febrero de 2007. favor aclarar qué tipo de publicación es

[21] C. García Figuerola Paniagua*, et al.*, "Preservación digital," *Ibersid: revista de sistemas de información y documentación,* vol. 3, pp. 265-274, 2009.

[22] A. Arsenault and S. Turner, "Internet X. 509 Public Key Infrastructure: Roadmap," *draft-ietf-pkix-roadmap-09 (work in progress),* 2002.

[23] J. Viega*, et al. Network Security with OpenSSL: Cryptography for Secure Communications*. Sebastopol: O'Reilly Media, Inc., 2002.

[24] R. Canetti and H. Krawczyk, "Universally Composable Notions of Key Exchange and Secure Channels," in *Advances in Cryptology—EUROCRYPT 2002*, 2002, pp. 337-351.

[25] Mazumdar and Subrata, "Key Manager Tool – Extension of Mozilla Certificate Manager for Key Generation and Certificate Enrollment," *Avaya LAbs Research,* 2006.

[26] P. Lara and J. M. Duart, "Gestión de contenidos en el e-learning: acceso y uso de objetos de información como recurso estratégico," 2005. establecer datos de en dónde se encuentra publicado el artículo

Paulo Alonso Gaona-García

Candidato a doctor en Ingeniería de la Información y del Conocimiento en la Universidad de Alcalá (España). Magíster en Ciencias de la Información y de las Comunicaciones de la Universidad Distrital Francisco José de Caldas. Profesor de tiempo completo adscrito a la Facultad de Ingeniería de la Universidad Distrital Francisco José de Caldas. Sus áreas de interés se encuentran enfocadas en redes y comunicaciones, seguridad informática, *e-learning*, visualización de información y Web semántica.

Correo electrónico: *pagaonag@udistrital.edu.co*

Carlos Enrique Montenegro Marín

Doctor en Ingeniería Informática de la Universidad Oviedo (España). Magíster en Ciencias de la Información y de las Comunicaciones de la Universidad Distrital Francisco José de Caldas. Profesor de tiempo completo de la Facultad de Ingeniería en la Universidad Distrital Francisco José de Caldas. Sus áreas de interés de investigación están orientadas hacia la virtualización y computación en la nube, y la ingeniería dirigida por modelos y servicios Web en ingeniería de software.

Correo electrónico: *cemontenegro@udistrital.edu.co*

Helvert Wiesner González

Estudiante de último semestre de Ingeniería de Sistemas de la Universidad Distrital Francisco José de Caldas. Sus áreas de interés son la ingeniería de software, la telemática y la seguridad informática.

Correo electrónico: *helvertw@gmail.com*