INGENIERÍA DE SISTEMAS

Plataforma de seguridad basado en autenticidad de contenidos sobre conjunto de especificaciones SCORM

Carlos E. Montenegro-Marín[*], Elvis E. Gaona-García[*], Paulo A. Gaona-García[*§]

**Facultad de Ingeniería, Universidad Distrital, Bogotá, Colombia*
§ email: pagaonag@udistrital.edu.co

(Recibido: Octubre 28 de 2009- Aceptado: Noviembre 17 de 2010)

Resumen

Los mecanismos que se presentan en la mayoría de plataformas Learning Content Management Systems, (LCMS), no permiten evaluar el concepto de "autenticidad" en contenidos que se comparten en cada una de ellas con un buen grado de aceptación, por lo tanto, el siguiente artículo tiene como finalidad plantear un Modelo de seguridad informático sobre plataformas de aprendizaje virtual LCMS, mediante sus contenidos a través de las especificaciones dadas por Sharable Content Object Reference (SCORM), lo cual permita garantizar la autenticidad de contenidos mediante conceptos de firmas digitales e identificación de protocolos y mecanismos que garanticen este tipo de actividades. Para llevar a cabo esta actividad, se plantean alternativas de modelos de seguridad, partiendo por el análisis de los mecanismos de seguridad informáticos que se trabajan actualmente sobre la mayoría de plataformas LCMS, al igual que la identificación de componentes y variables desde el punto de vista del desarrollo de contenidos mediante las especificaciones SCORM. Finalmente se propone un modelo de seguridad para su implementación sobre el desarrollo de objetos de aprendizaje que permitan identificar niveles de confianza en los diferentes contenidos que se comparten dentro de una Plataforma LCMS.

Palabras Claves: Seguridad informática, Mecanismos de autenticidad, Plataformas virtuales de aprendizaje, Firma digital, Certificados de autenticación.

SYSTEMS ENGINEERING

Security Framework based on Authenticity Content over SCORM specification group

Abstract

The mechanism presents in most Learning Content Management Systems, (LCMS) platforms, do not allow to evaluate the concept of "authenticity" in content to be shared by each of them with a good degree of acceptance, therefore, the following paper look for to propose a security model for LCMS platforms through its content in the specifications given by Sharable Content Object Reference Model (SCORM), which will guarantee the authenticity of content through concepts of digital signatures and identification of protocols and mechanisms to ensure this type of activity. To carry out this activity, it is proposed different alternative of security models, starting with the analysis of computer security mechanisms currently working on most platforms LCMS, as well as the identification of components and variables from the point of view of the content development using the SCORM specifications. Finally, it is proposed a security model for implementation on the development of learning objects to identify levels of trust in the content that are shared within a platform LCMS.

Keywords: Informatics security, Authenticity mechanisms, Virtual learning platforms, Digital signatures, Vertificates of authentication.

1. Introducción

La palabra autenticidad encierra una serie de características dentro del área de seguridad, que a la luz de aplicaciones informáticas representa un concepto fundamental para lograr encausar con algún grado de confianza los datos que se comparten en un sistema de información. Por lo tanto dentro de los esquemas de representación de seguridad informática, la parte de autenticidad es uno de los principios que se proyecta dentro del área de certificados digitales como uno de los ejes fundamentales para garantizar la validez de documentos enviados a través de una Red de comunicaciones entre sistemas cliente-servidor y por ende sobre Internet.

Las plataformas LCMS, representan uno de los avances más significativos para llevar a cabo mecanismos de comunicación y servicios que se prestan entorno a un proceso de formación, siendo una herramienta clave para el manejo de procesos orientados hacia la publicación de contenidos y guías pedagógicas, como también centro de acopio de información, enviada tanto por estudiantes como por docentes de un centro de formación académica.

El concepto de contenidos que se publican sobre una LCMS ha evolucionado con el transcurrir de los tiempos, el cual ahora se resume en el desarrollo de objetos virtuales de aprendizaje Learning Object (LO), que permiten el uso de contenidos mediante el concepto de estructura jerárquica de datos para su identificación y parametrización de variables, los cuales se llevan a cabo a través de un conjunto de especificaciones como Sharable Content Object Reference Model (SCORM), Instructional Management System (IMS), Learning Object Metadata (LOM) entre otros.

Estas especificaciones deben regirse por lo menos bajo tres elementos: Adaptabilidad, reusabilidad y accesibilidad, aunque la adaptabilidad actualmente no es soportada completamente por muchos sistemas, de acuerdo a Kareal & Klema, 2006, la plataforma Moodle es uno de los LCMS mejores preparados para soportarlo (Santos, 2006), pero al igual que la mayoría de plataformas que se presentan en el mercado, carecen de mecanismos que logren garantizar la autenticidad de contenidos que se publican sobre cada una de ellas.

2. Seguridad y panorama de plataformas LCMS en mercado

Las plataformas LCMS en cierto sentido han sido la evolución de los sistemas gestores de contenidos Content Management System (CMS), los cuales han sido creados específicamente para la administración y control de información de usuarios a nivel corporativo. Desde su aparición ha sido producto de integración y creación de diferentes tipos de comités y grupos que a nivel mundial han permitido apoyar esta iniciativa para tratar de estandarizar los procesos de desarrollo de plataformas que se prestan para su uso en particular de formación y que por tanto según Boneu 2007, ha representado un factor determinante para facilitar metodologías de estudio diferente a las tradicionales basadas en entrenamiento Computer Based Training (CBT), Internet Based Training (IBT) y Web Based Training (WBT).

El panorama que se presenta a nivel de autenticidad de contenidos sobre las actuales plataformas LCMS, no es muy alentador, si bien es cierto que existen mecanismos que permiten llevar a cabo procesos de autenticación de usuarios, asignación de claves entre otros mecanismos de seguridad, el grado de confianza generado para identificar la procedencia y creación de contenidos académicos en este tipo de plataformas es un hecho que no ha sido controlado en su totalidad por ningún mecanismo informático y que a la luz de instituciones académicas representa un tema fundamental dentro de los procesos de formación y evaluación a nivel formativo.

Lo anterior podemos reforzarlo a partir de los resultados obtenidos sobre niveles de autenticación que se presentan en aplicaciones informáticas, en un estudio realizado a más de 300 empresas por el Computer Security Institute, (CSI) a sectores de salud, financiero y educativo (Richardson, 2008) , el cual se destaca, que el uso inadecuado de la información es uno de los factores más críticos en la mayoría de aplicaciones

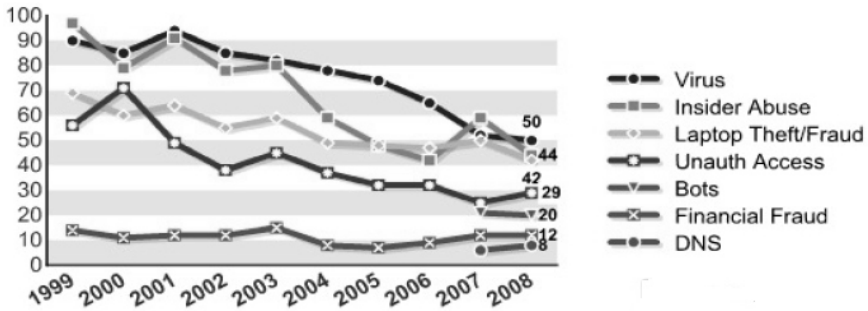

Figura 1.Número de incidentes ocurridos en los últimos 10 años en sectores gobierno, financiero, salud y académicos.

informáticas; y dentro del sector educativo representa el segundo sector más vulnerable de ataques mediante el uso de herramientas de comunicación y de aprendizaje, dentro de los cuales se resaltan a nivel del mal uso de plataformas virtuales de aprendizaje LCMS.

En la Figura 1 se puede identificar algunas incidencias de mayor representación e impacto en el mercado, una de las más representativas son los fraudes informáticos, los cuáles son incidentes que todavía las organizaciones no han logrado controlar del todo dentro de sus políticas de seguridad, ya que la mayoría se centra en definir aspectos entorno a la autenticación y controles de acceso, pero la parte autenticidad, representados en cierta medida sobre certificados, muestran cifras que no han sido abordados en su totalidad.

2.1 Servicios de autenticidad

El concepto de autenticidad se encuentra relacionado con el principio de confidencialidad, el cual permite llegar a otro concepto conocido como niveles de confianza y otro principio conocido como integridad de contenidos generados en un entorno de comunicación. La palabra "confidencialidad" en el mundo de la informática encierra muchos elementos que desde hace varios años hasta la fecha varios autores han tratado de darle un enfoque diferente a la hora de aplicarlo por lo que ha sido considerado junto a la autenticidad, integridad, no repudio y controles de acceso como componentes claves de la comunicación segura por mucho tiempo (McCumber 1991) . Desde el punto de vista académico, autores como JF Kurose, 2004, trabajan este concepto bajo la posibilidad de que "El emisor y receptor deben ser capaces de entender el contenido del mensaje" y por lo tanto se debe certificar la encripción y Desencripción del mensaje a través de una serie de claves que se utilizan dentro del proceso de comunicación entre dos entidades. Por otro lado Halsall, 2006, menciona la confidencialidad como parte primordial de la privacidad, el cual debe permitir en lo posible asegurar la procedencia de la información que se recibe en una red destino. Carracedo, 2004, afirma que la confidencialidad no se debe confundir con la privacidad, porque aunque sean palabras las cuáles a nivel de sinónimos mantienen cierto significado, su aplicación en el contexto de seguridad informática varia significativamente teniendo en cuenta "el uso coordinado de políticas y servicios de seguridad que se proporcionan". Para llevar a cabo la implementación de este concepto es necesario encerrarlo dentro de su base fundamental que se encuentra relacionado con los principios criptográficos.

3. Técnicas de comprobación de autenticidad

Dentro de las técnicas de comprobación existentes para verificar la autenticidad de documentos digitales existen muchos mecanismos y algoritmos que lo realizan sobre un ambiente de comunicaciones, en este apartado se tomaran en cuenta los más representativos a que nivel del mercado son los más aceptados por la mayoría de empresas que lo utilizan.

3.1 Certificados digitales

Los certificados digitales se conocen como una parte de la información que se asocia a un

documento digital. Para lograr obtener un certificado digital, esta debe funcionar bajo el concepto de "entidad" quien en la encargada de generar la pareja de claves pública y su correspondiente asignación de clave privada garantizando su validez durante un periodo determinado de tiempo. Este proceso genera lo que se conoce como "Certificado Digital", el cuál es distribuido por un agente externo conocido como Trusted Third Parties, (TTP) y generado a través de una Authority Certification, (CA) bajo el nombre de autoridad de certificación.

La presencia de una Autoridad de Certificación garantiza un escenario seguro de comunicaciones, los cuáles para cubrir todos estos procesos de gestión de certificados y distribución de las mismas mediante TTPs a través de una Autoridad de Certificación dentro de un modelo de seguridad compartida por varios usuarios, es necesario trabajar bajo una infraestructura conocida como Public Keys Infraestructure (PKI) también conocida como Infraestructura de Certificación.

3.2 Firma digital

De manera textual, Carracedo, 2004, la define como "una pieza de información añadida a una unidad de datos, que es el resultado de una transformación criptográfica de ésta en la que se ha usado una transformación privada del signatario, que permite a una entidad receptora probar la autenticidad del origen y la integridad de los datos recibidos". Por la tanto se considera que la firma que se genera es aplicada a una fracción reducida del mensaje original que se está enviando a un destinatario. Por su parte el destinatario, realiza unas operaciones básicas de comprobación para adquirir las garantías suficientes del autor intelectual del documento y la integridad del mismo mensaje.

Este concepto de firma digital en el ámbito telemático ha tenido gran aceptación, hasta el punto de generar una serie de especificaciones a través de la creación de mecanismos, técnicas y algoritmos que validen efectivamente su correcto funcionamiento y al mismo tiempo la generación de nuevas especificaciones que determinan la evolución de este concepto en ambientes informáticos, lo que logran posicionarlo como un mecanismo para acreditar la validez de un documento perteneciente a un autor (autenticación), verificar que no ha sido manipulado ni modificado (integridad), al igual que impide que el autor niegue su autoría (no repudio) mediante validación de la clave pública del autor, quedando de esta manera vinculado al documento de la firma.

3.2.1 Modelo y proceso de firma digital

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 gran valor agregado en el mundo de la informática y las telecomunicaciones. A continuación se realiza la representación gráfica de la firma digital conocida como genérica dentro de cualquier tipo de especificación, mecanismo y /o algoritmo criptográfico utilizado para tal fin, ejemplo de ello se presenta en la Figura 2.

Por lo tanto, la Firma digital representa una de las características claves para llevar a cabo la autenticidad de contenidos, el cual representa uno de los valores más importantes para trabajar un concepto sobre redes informáticas conocidas como Web of Trust, (WoT) que se menciona en el siguiente apartado.

4. Web of trust

El concepto de web of trust se ha venido desarrollando desde la creación del mecanismo Pretty Good Privacy, (PGP) para seguridad de correos electrónicos (Zimmermann, 1995), el cuál trata de plantear la idea de permitir y aceptar la identidad de un usuario en un sistema de comunicaciones siempre y cuando este sea reconocido por otro usuario perteneciente al Sistema que me garantice unas condiciones mínimas de confianza para aceptarlo dentro del esquema de comunicación de la plataforma que están compartiendo.

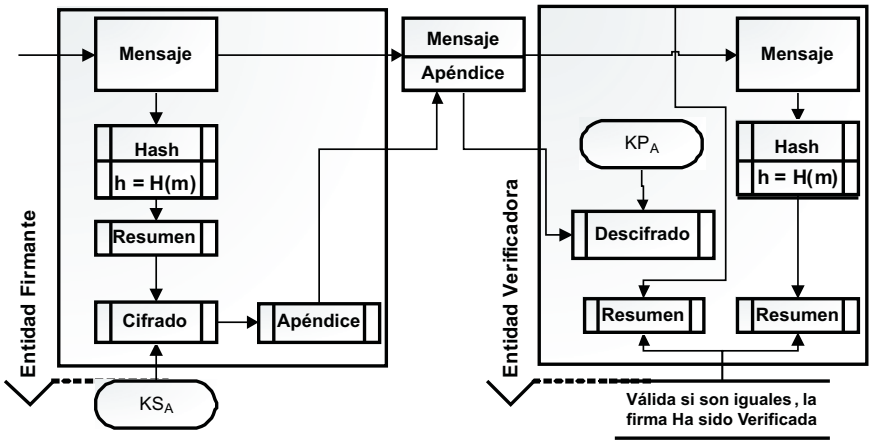

Figura 2. Esquema de Firma Digital. Fuente (SIGN, 2008)

De esta manera nace un concepto que permite la interacción de usuarios sobre redes sociales y el cual es relacionado mediante el proyecto Social Interaction Framework (SIF), trabajado en su momento por Schillo et al., 1999. En este *framework* un agente evalúa la reputación de otro agente basado directamente en observaciones de otros testigos participes del mismo sistema, mientras que los sistemas tradicionales electrónicos se deben fiar de mecanismos externos que sirvan de intermediarios entre las personas que desean comunicarse.

Algunos prototipos que han trabajado con este modelo de *Webs* de Confianza se pueden reflejar en el modelo de , construyendo una red de confianza y prototipos trabajados por Yu et al., 2003, los cuáles requieren que los usuarios den una calificación para sí mismos y de esta manera tener un organismo central (puntuaciones directa)

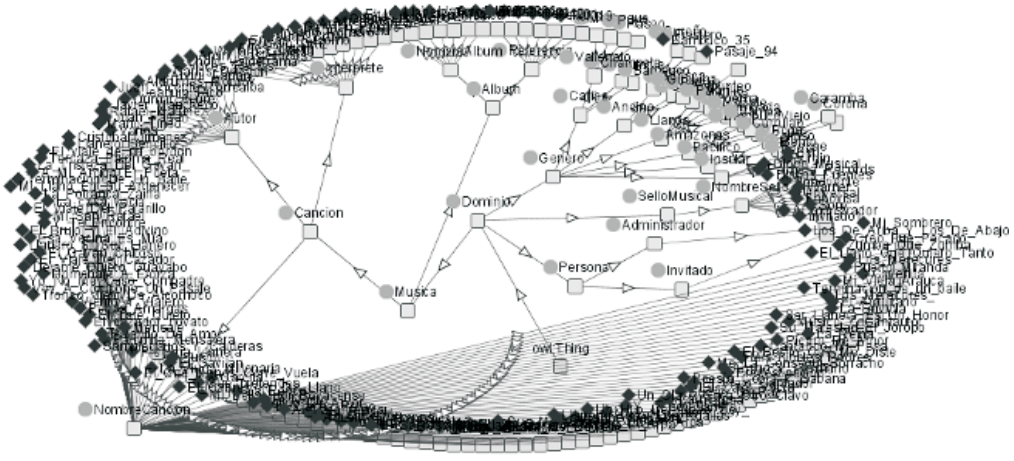

Figura 3. Ejemplo de web of trust.

a otros usuarios de confianza (puntuaciones colaborativas), un ejemplo se puede representar en la Figura 3.

A partir de este concepto un sistema central realiza un seguimiento de los usuarios que generan puntuaciones de cada uno, y utiliza esta puntuación para generar una reputación con respecto a un usuario específico.

Estos sistemas requieren de relaciones sociales preexistentes entre los usuarios de su comunidad electrónica, pero lo que no es claro es cómo se establecen esas relaciones y cómo se propagan las calificaciones a través de esta comunidad, lo que ha generado la formalización de algunos proyectos que para nuestro caso nos permite reforzar esta propuesta de trabajo para lograr implementar un sistema de confianza de contenidos digitales sobre una LCMS basado en una serie de especificaciones mediante SCORM, el cual se comentará con mayor detalle a continuación.

5. Modelos de representación objetos de aprendizaje

Cuando las plataformas virtuales de aprendizaje empezaron a tomar vuelo sobre la comunidad académica como una de las alternativas válidas de apoyo para seguimiento de actividades no presenciales, se presento de manera instantánea una corriente de estudio que permitió de cierta forma plantear unos lineamientos válidos para generación de contenidos y su funcionamiento independientemente de la plataforma de trabajo, fue así como surgieron grupos de interés a nivel internacional que han permitido determinado una serie de especificaciones para el manejo de contenidos, en este sentido podemos basarnos en trabajos realizados en especificaciones como (SCORM 2004), IMS Content Packaging (CP 2005)para definición de estructuras de contenidos, IMS Simple Sequencing, (SS 2003) para la estructuración de contenidos de aprendizaje y la evolución de estos mediante Learning Design (LD 2003) y modelándolos a través de IMS Model Data (MD 2006) con el fin de generar una estructura de datos dentro de una representación de diversos escenarios de aprendizaje para su aplicación dentro de diferentes enfoques pedagógicos, elementos propuestos en trabajos realizados por Burgos et al., 2007.

5.1 Objetos y representación de contenidos

Dentro del modelo de empaquetamiento de datos para contenidos sobre plataformas virtuales de aprendizaje LCMS existen referencias las cuáles sirven de base para determinar el funcionamiento de cada uno de ellos, por un lado autores como Burgos, 2006 define las especificaciones más importantes basados en IMS General Content (GC, 2009) y por SCORM, 2004. Por otro lado Marquez, 2007, presenta las características acordes a un modelo genérico para la definición de contenidos basados en estándares y especificaciones presentes en el mercado y los cuales han sido mencionados por Vélez and Fabregat, 2007, definiendo un concepto ligado al reuso de objetos de aprendizaje Reusable Learning Object, RLO y la definición de metadatos caracterizado por Wiley and Edwards, 2002.

5.2 Conjunto de especificaciones SCORM

Fue una iniciativa desarrollada por Advanced Distributed Learning, ADL, el cuál surgió cobijado del Departamento de Defensa de los Estados Unidos en el año de 1997. La propuesta fundamental de este organismo es apoyarse en las anteriores iniciativas para conformar su propio conjunto de especificaciones, el cual combina muchas especificaciones de IMS, IEEE mediante LOM, AICC entre otras.

5.2.1 Modelo operativo de SCORM

Actualmente se está trabajando la segunda versión de 2004 (SCORM, 2004), se representa mediante cambios significativos realizados de la primera versión lanzada al mercado.

• Content Aggregation Model (CAM). El Modelo de agregación de contenidos según su especificación (SCORM, 2004) define cómo hay que ensamblar, etiquetar y empaquetar el contenido. Como el objetivo de SCORM es orientados a objetos, se necesita de una descripción detallada sobre cómo se conectan estos objetos.

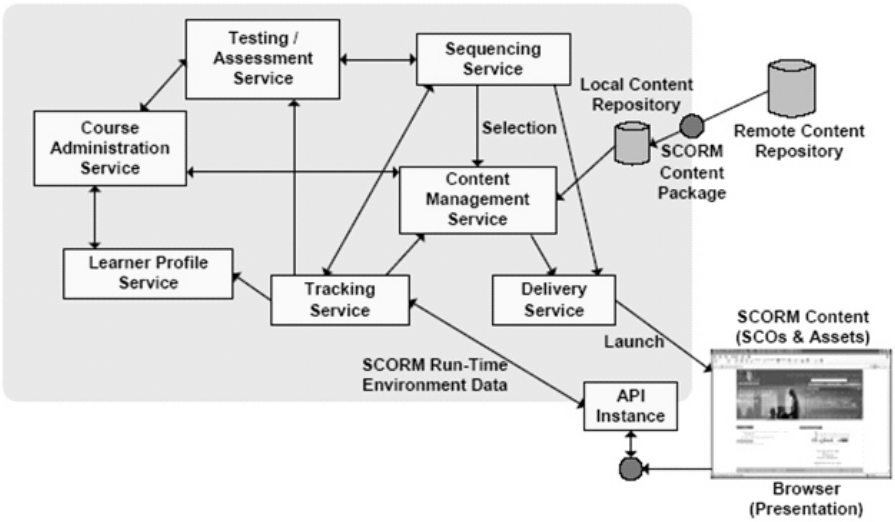

Figura 4. Modelo SCORM dentro de plataformas LCMS. Fuente: (SCORM, 2004)

• Run-Time Environment (RTE). RTE describe el proceso de ejecución que debe realizar un LCMS con un SCO, así como el proceso de comunicación entre ambos. Un estudiante sólo tiene un SCO activo en cada momento.

• Sequencing and Navegation (SN). El modelo SCORM describe cómo el secuenciamiento interactúa con el resto del RTE; sin embargo, la descripción del proceso, de secuenciamiento se hace usando la especificación Simple Sequencing, IMS, descrita en SS, 2003.

Por lo tanto, el modelo SS, 2003 está orientado a la relación e intencionalidad directa de los modelos pedagógicos utilizados y el uso de estrategias metodológicas de tipo instruccional, para que de manera guiada el proceso de aprendizaje se garantice al estudiante. El trabajo realizado por SCORM bajo plataformas LCMS, es servir de Repositorio Local para el empaquetamiento de Contenidos, con el ánimo de ser usado al interior de la plataforma como un administrador de servicios de contenidos dentro de un curso para que finalmente sea usado por un usuario en particular para visualización de los mismos como se representa en la Figura 4.

Dentro de las especificaciones trabajadas por SCORM a nivel de LCMS, básicamente se necesita parámetros para el manejo de contenidos para el aprendizaje correcto por parte de los usuarios, garantizando de esta manera una evolución paulatina de momentos de aprendizaje a través de la secuencia que SCORM maneja al interior de cada contenido realizado. Bajo estas características, la especificación define una serie de reglas para el manejo de los contenidos y momentos para la secuencialización de contenidos y seguimiento del proceso de aprendizaje de los estudiantes.

6. Modo de contemplar la seguridad en especificaciones y estándares

Otro de los factores que se tienen en cuenta para analizar la seguridad en plataformas LCMS son las especificaciones y estándares reflejadas en la reusabilidad y accesibilidad, los cuáles en términos de soporte de estándares autores como Santos, 2007, concluye que plataformas como dotLRN soporta un gran rango de estándares junto a nivel educativo tales como el modelo de referencia SCORM y las especificaciones de IMS, al igual que la plataforma Moodle; las cuáles se ven favorecidas para garantizar dentro de sus funcionalidades requerimientos de accesibilidad para sus recursos y contenidos.

Dentro del conjunto de especificaciones SCORM, hay elementos que sirven de partida para trabajar de manera estratégica y adaptar en este sentido a través del empaquetamiento de contenidos la parte de autenticidad de contenidos, el cuál será un parámetro de análisis que depende directamente del lenguaje que se maneje para trabajar autenticidad mediante firma digital, para este caso las definiciones dadas por XML que se comentará a continuación.

6.1 XML-Security

El proyecto XML-Security dispone de tres elementos representativos que permiten identificar los formatos aptos para el tratamiento de firmas digitales en un sistema de comunicaciones; por un lado las características dadas para la firma digital de documentos dadas por XML-Signature (SIGN, 2008), por otro lado a nivel de encripción de datos mediante XM-Encryption Syntax and Processing (ENC, 2002), y finalmente la distribución de claves mediante XML-Key Management (KEY, 2001).

6.1.1 XML- Encryption

XML-Encryption descrita en la W3 (ENC, 2002), describe la manera en que los datos firmados deben ir totalmente cifrados por la Web, con el propósito de no ser detectados fácilmente por agentes externos dentro del proceso de comunicación, como se define en el Código 1:

```
<EncryptedData Id? Type? MimeType? Encoding?>
  <EncryptionMethod/>?
  <ds:KeyInfo>
    <EncryptedKey>?
    <AgreementMethod>?
    <ds:KeyName>?
    <ds:RetrievalMethod>?
    <ds:*>?
  </ds:KeyInfo>?
  <CipherData>
    <CipherValue>?
    <CipherReference URI?>?
  </CipherData>
  <EncryptionProperties>?
</EncryptedData>
```

Código 1. Representación de XML-Encryption. Fuente (ENC, 2002)

En el Proceso de Encripción y Desencripción definida por la (ENC, 2002), se identifican los siguientes roles:

• Aplicación: La aplicación que realiza la petición de encriptación XML a través de la provisión de datos y parámetros necesarios para su procesamiento.

• Encriptación: Una implementación de la Encriptación XML con la función de encriptar los datos.

• Desencriptar: Una implementación de la Encriptación XML con la función de desencriptar los datos.

7. Metodología de trabajo.

Para llevar a cabo el planteamiento del modelo, se basara en la ISO/IEC 27002 para el tratamiento de la información, los cuales dentro de esta familia incluye estándares internacionales sobre requerimientos, gestión del riesgo, métricas y mediciones, al igual que lineamientos de implementación del sistema de gestión de seguridad informático, el cuál es el elemento que se pretende asegurar dentro de una plataforma LCMS mediante mecanismos de autenticidad.

7.1 Estándar internacional ISO/IEC 27002

El estándar enfoca sus lineamientos sobre la necesidad de determinar los requerimientos de seguridad dentro de cualquier ámbito de trabajo, dentro de los cuáles resalta la existencia de tres fuentes primarias para lograr identificar estos requerimientos: los riesgos, la estrategia general y los objetivos de Organización, los cuales se usaran para llevar a cabo la implementación del prototipo.

7.1.1 Riesgos

Para nuestros fines particulares, los riesgos que se han logrado identificar parten de la vulnerabilidad que tienen el conjunto de especificaciones para generación de contenidos al no contemplar mecanismos para autenticidad de información, lo que potencialmente representa una amenaza para el contenido generado al desconocer la procedencia y validez del mismo.

7.1.2 Estrategia general

La estrategia que se tiene previsto manejar es el uso de certificados digitales y la generación de (2) dos firmas digitales para lograr ubicar dentro de SCORM la creación de contenidos y el uso de los mismos por parte del estudiante o invitado; al mismo tiempo la generación de una firma a nivel administrativo, el cual se puede generar a partir de la misma plataforma quién genera los espacios virtuales de trabajo. En este sentido el estándar especifica la ubicación de requerimientos legales y regulatorios, para lo cual específicamente nos regiremos sobre la documentación del conjunto de especificaciones SCORM, al igual que los parámetros regidos por la Plataforma LCMS Moodle para la implementación del plugin, al igual que elementos propios del lenguaje mediante XML-Security.

7.1.3 Objetivos de organización

Para llevar a cabo este requerimiento, es necesario la generación firmas digitales para la creación de contenidos por parte de docentes, y el uso de los mismos por parte de los estudiantes y/o invitados, con el ánimo de garantizar la autenticidad y validez de los contenidos generados dentro de un ambiente virtual de aprendizaje LCMS.

7.2 Cómo asegurar información según ISO/IEC 27002 dentro del conjunto de especificaciones SCORM

Para plantear el modelo se tendrán en cuenta las consideraciones de la ISO/IEC 27002 en cuanto a clasificación de este activo desde el punto de vista legal mediante tres elementos:

7.3 Protección de data y privacidad de la información personal

Bajo los tres elementos representados anteriormente es importante dentro de la estrategia que va a plantear a nivel de autenticidad, que el mecanismo asegure protección de información y privacidad de los mismos mediante un conjunto de reglas que debe definirse mediante XML-Encryption logrando ubicar la protección de:

• Información de persona que crea el ambiente de trabajo.

• Información de persona que crea el recurso para el curso virtual

• Información de persona que hace uso del recurso compartido en un curso virtual.

7.4 Protección de los registros organizacionales

Para la protección de los registros organizacionales, para nuestros propósitos se tendrán en cuenta empresas del mercado que generan certificados digitales y que hacen mención particular a la Institución Académica que hace usa de ellas, con el ánimo de certificar la validez de los contenidos generados dentro de la Institución.

7.5 Derechos de propiedad intelectual

Para validar los datos de las personas participantes en el proceso de comunicación, es importante hacer referencia los derechos y la propiedad intelectual del contenido generado, para ello es importante el uso de XML-Signature para identificar la validez de los mismos. Los casos a evaluar son:

• Información de persona que crea el ambiente de trabajo.

• Información de persona que crea el recurso para el curso virtual

• Información de persona que hace uso del recurso compartido en un curso virtual.

8. Propuesta de seguridad sobre archivo manifiesto de SCORM

En este sentido para cumplir con estos tres elementos se implementara XML-Security mediante XML-Signature y XML-Encryption para tratar de contrarrestar estos problemas. Para lograr aplicar estas características es importante resaltar la idea que el archivo el cuál llevará mayor representación para realizar este proceso dentro del conjunto de especificaciones SCORM se conoce como Manifiesto mediante la siguiente representación en la Figura 5.

Figura 5. Propuesta archivo manifiesto con parámetros de seguridad a nivel de autenticidad de contenido

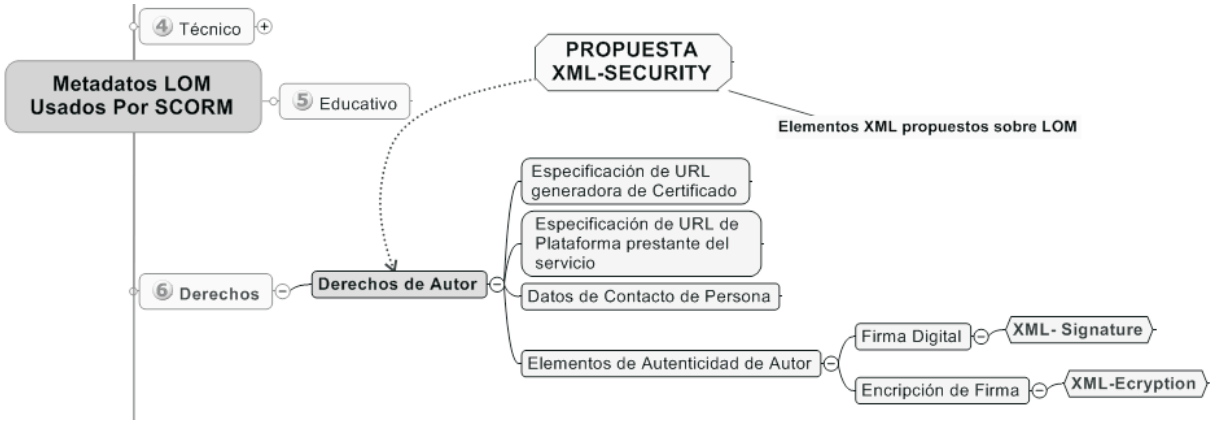

Figura 6. Propuesta de etiquetas de seguridad sobre elementos de derechos de autor en LOM

Este archivo manifiesto cumple una labor importante dentro del proceso de creación, apertura y búsqueda del objeto de aprendizaje creado dentro de una plataforma LCMS bajo especificación SCORM, ya que permite ser puente para abstraer todas las características dadas por el objeto de aprendizaje, el cual tiene como propósito resumir todas las características del mismo. Por lo tanto representa el elemento que permitirá identificar y etiquetar el contenido con seguridad apoyado del estándar LOM.

8.1 Propuesta de seguridad sobre LOM

El trabajo que realiza LOM en este sentido es ubicar dentro de la etiqueta Derechos las características del tipo de firma que se agrega al contenido, para ello la parte de XML-Security se apoyaría en gran sentido sobre esta parte del estándar el cuál es la propuesta que se pretende abordar para llevar a cabo esta implementación y se representa a continuación en la Figura 6.

En este sentido LOM apoyaría en gran medida el proceso de autenticidad de contenidos soportado por esta parte del estándar, el cuál como se abordaba en apartados anteriores solamente se menciona, mas no se agrega parámetros de seguridad que logren fortalecer la autenticidad del contenido que se genera por parte del autor.

9. Cláusulas ISO/IEC 27002 manejadas dentro del proyecto

El estándar de seguridad de información ISO/IEC 27002 propone 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridad principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

Según la ISO/IEC 27002 se define las siguientes cláusulas de trabajo, los números que hacen referencia en cada cláusula hacen mención a las categorías manejadas por la misma: (a) Política de Seguridad (1), (b) Organización de la Seguridad de la Información (2), (c) Gestión de Activos (2), (d) Seguridad de Recursos Humanos (3), (e) Seguridad Física y Ambiental (2), (f) Gestión de Comunicaciones y Operaciones (10), (g) Control de Acceso (7), (h) Adquisición, Desarrollo y Mantenimiento de Sistemas de Información (6), (i) Gestión de Incidentes de Seguridad de la Información (2), (j) Gestión de la Continuidad Comercial (1), (k) Conformidad (3).

Para nuestro caso en particular, solamente se tendrán en cuenta las cláusulas (a) y (g) para validar los procesos necesarios para la implementación de autenticidad dentro de los casos de pruebas identificados en el proyecto, el resto de cláusulas no se tienen en cuenta ya que tocan otros aspectos a nivel organizacional que no son válidos para nuestro propósito del proyecto.

9.1 Política de seguridad

Política a Trabajar: Determinar la autenticidad de contenidos dentro de un conjunto de especificaciones a través de SCORM para determinar:

•¿Quién genera espacios dentro de Plataforma?
• ¿Quién crea contenidos?
• ¿Quién usa contenidos?

Identificados estos elementos, a continuación se detallan las características de los procesos generados en cada instancia, con el ánimo de enmarcarlo dentro de las políticas de seguimiento para identificación de posibles fallas que pueda generarse en el momento de validación de autenticación.

9.2 Proceso de generación de curso

Para generar este proceso, se puede representar en la Figura 7, el cual se definen los parámetros y definición de elementos para crear un curso.

Esta plantilla representa una caracterización que se ha tomado como referencia para identificar las secuencias que se llevan a cabo con el proceso de creación de curso dentro de una plataforma LCMS.

Existen tres instancias primordiales dentro de este tipo de procesos, partiendo de la idea que el administrador o creador del curso previamente ha realizado el proceso de autenticación sobre la plataforma:

• La primera instancia se declara los elementos de entrada, para este caso el administrador decide crear el curso, para lo cual debe ubicarlo sobre una categoría.

• En la segunda instancia se declaran los procesos que se llevan a cabo a nivel de creación del recurso en el aula virtual bajo especificación SCORM, para lo cual se establecen parámetros de recursos y elementos de la plataforma virtual que permita realizar este proceso.

• En la tercera instancia se maneja procesos para la creación de la firma digital sobre los recursos creados, el cual se agrega automáticamente se guarde el recurso dentro de la plataforma LCMS.

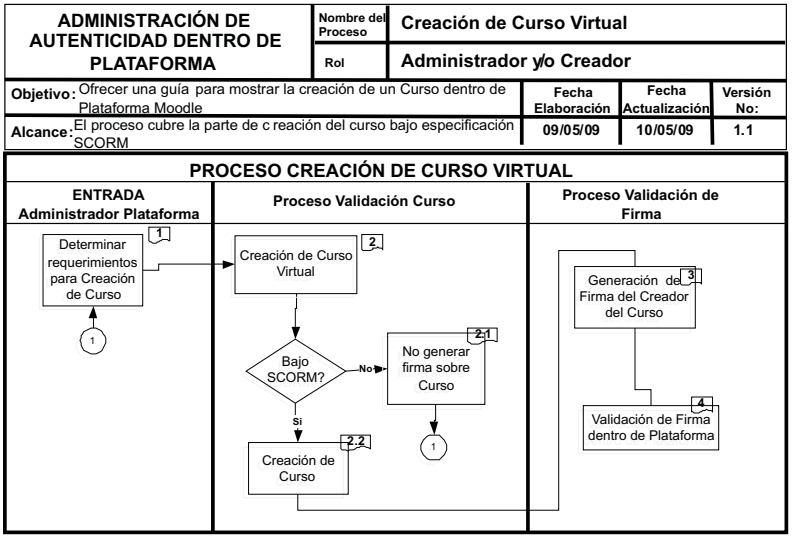

Figura 7. Propuesta formato de seguimiento a nivel de creación de curso por parte del administrador

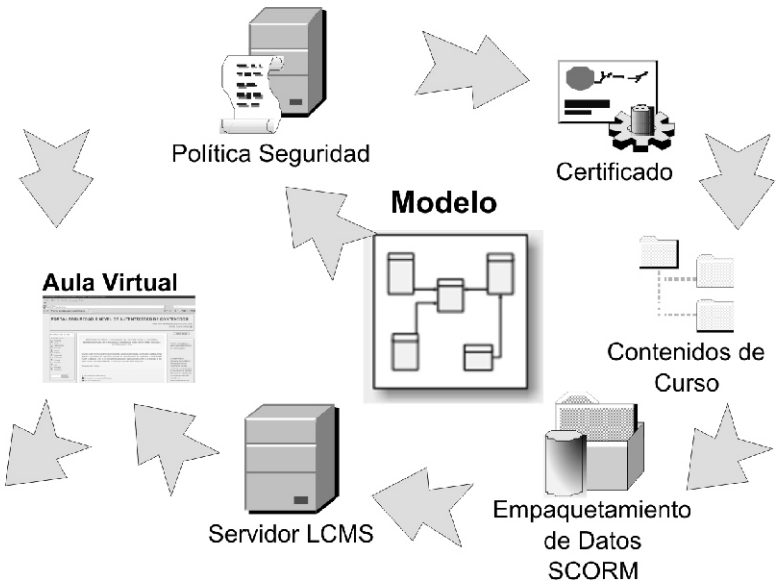

Figura 8. Modelo de seguridad de contenidos propuesto

10. Modelo de seguridad de contenidos propuesto y discusión.

El modelo propuesto parte de la representación funcional de las herramientas y elementos que se reflejan dentro del conjunto de especificaciones para contenidos definidos por SCORM. En este sentido a continuación se presenta un modelo genérico de la propuesta que se pretende abordar, los cuáles deben cumplir con los siguientes lineamientos representados en la Figura 8.

Es importante reconocer la idea de la generación del modelo que se presenta en la Figura 8, el cual está enmarcado dentro de una política de seguridad, para este caso mediante la

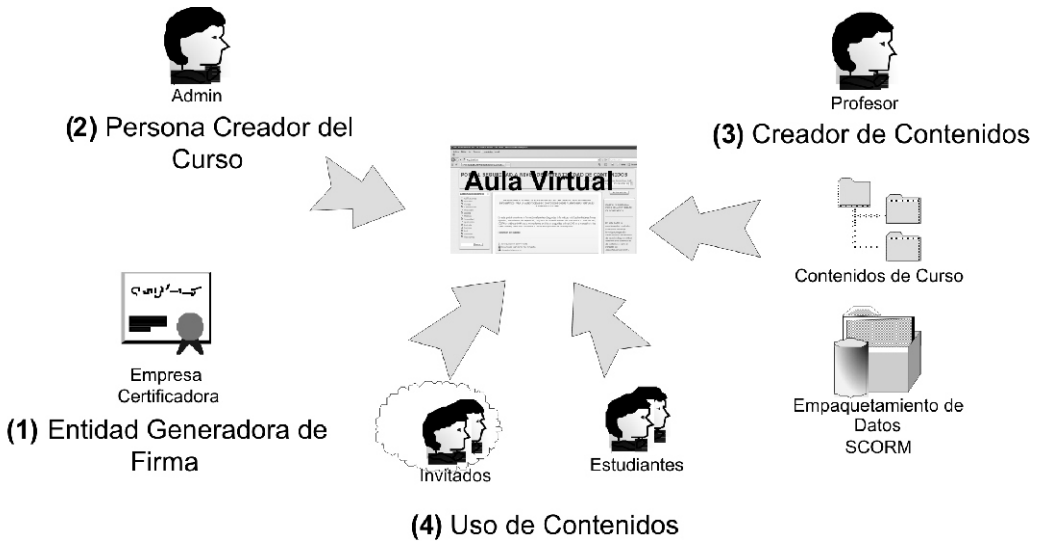

Figura 9. Tipos de firmas generados en plataforma LCMS

representación realizada a través del estándar ISO/IEC 27002 comentado anteriormente, al igual que debe basarse en mecanismos de seguridad, que para este caso se trabajará mediante certificados a través de una empresa para la generación de firmas realizadas sobre los contenidos que se encuentran regidos bajo un conjunto de especificaciones SCORM y que al mismo tiempo se encuentran sobre una Plataforma Virtual de Aprendizaje LCMS.

Para poder plantear la anterior propuesta, es necesario entender la generación del modelo a partir de la representación de cada uno de los roles identificados dentro del proceso de comunicación (administrador, docente, estudiante y/o invitado). De manera general podemos indicar que el modelo que se propone pretende abordar los siguientes Casos representados en la Figura 9.

Por lo tanto se pretende proponer un prototipo informático que permita plantear una arquitectura para la generación de certificados digitales mediante Infraestructuras PKI, el cuál permita que la misma plataformas virtual de aprendizaje LCMS sea la encargada de gestionar y administrar la autenticidad de contenidos a través de actividades generadas en la misma por parte de usuarios os administradores, docentes, estudiantes y/o invitados soportados sobre el conjunto de especificaciones SCORM.

11. Modelamiento del prototipo

Según el estudio realizado en el anterior apartado el estándar LOM presenta una etiqueta que permitiría agregar elementos de validación de contenidos y derechos intelectuales. Esta es conocida con el nombre de Right (Derecho) por lo tanto dentro de esta etiqueta Derechos se representan las características del tipo de firma que se agrega al contenido, el cuál será trabajada mediante XML-Security y los elementos de firma y encripción de la misma a través de XML-Signature y XML-Encryption.

11.1 Diagrama de despliegue

En la Figura 10 se presenta una caracterización del diagrama de despliegue propuesto para el prototipo.

La Figura 10 presenta la abstracción que se hace de la plataforma Moodle para lograr ubicar la parte de autenticación de usuarios para la identificación de

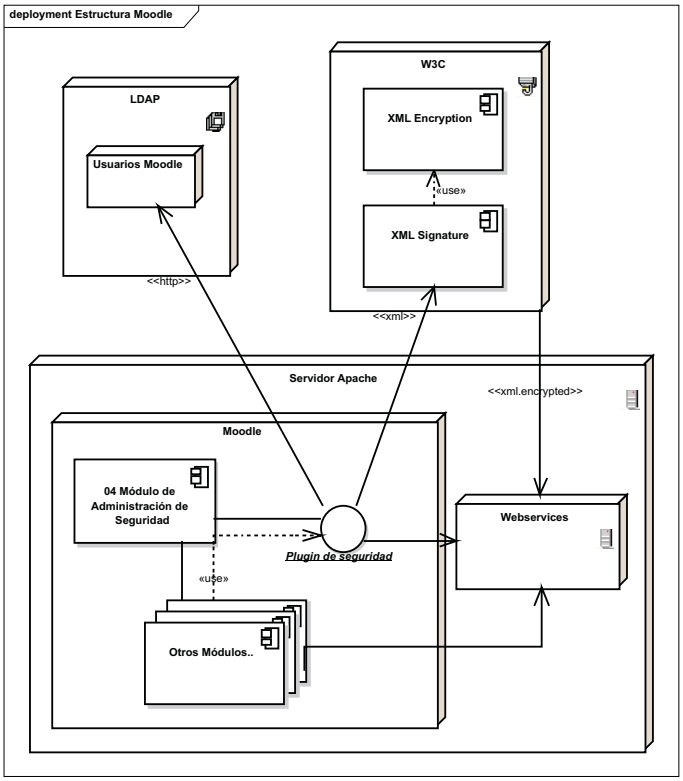

Figura 10. Diagrama de despliegue del prototipo

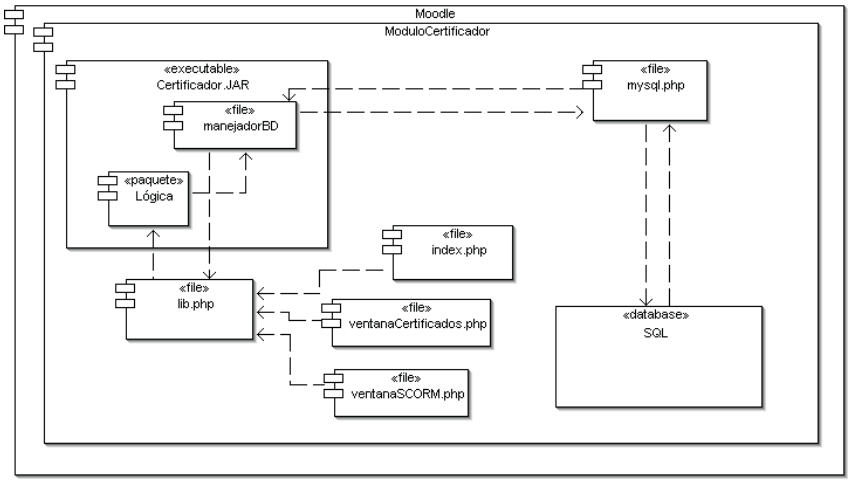

Figura 11. Diagrama de componentes del sistema

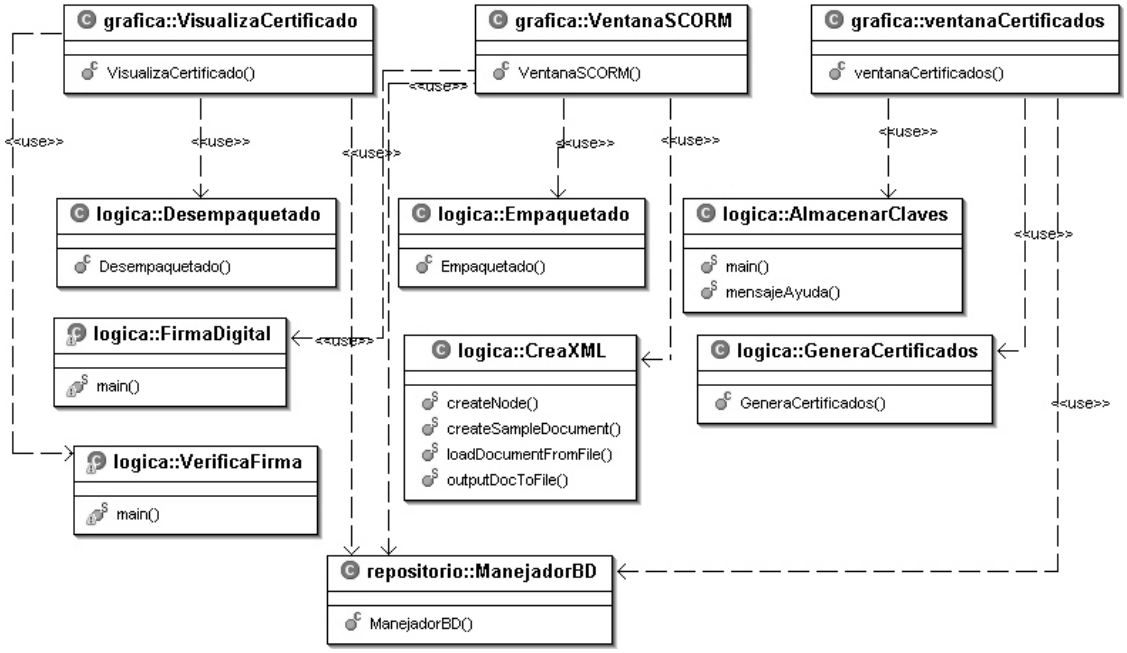

Figura 12. Diagrama de clases del sistema

roles y perfiles dentro del Sistema, la interacción de este módulo relacionado con otros módulos dentro de la plataforma para determinar el acceso a los mismos, y se observa la posible dependencia que tiene este módulo de seguridad con la parte de autenticidad de contenidos.

11.2 Arquitectura

Este diagrama muestra la arquitectura, ya no conceptual, sino de software que exhibirá el modulo, con los principales componentes de interés para el proyecto, ya que sería imposible listarlos a todos y sus relaciones, en vez de eso se presentan los componentes funcionales y las relaciones que les permitirán realizar sus tareas, el cual se puede visualizar en la Figura 11.

Bajo el anterior prototipo, podemos determinar que para el planteamiento de mecanismos de seguridad a nivel de autenticidad de contenidos sobre plataformas LCMS, dependen directamente del conjunto de especificaciones que hay en el mercado, pero actualmente no han madurado lo suficiente para poderlas plantear y así mejorar tipo de parámetros. Por tanto dentro de la propuesta realizada es importante determinar que se tendrán en cuenta no solamente una firma digital dentro de un ambiente LCMS, sino que se tendrán en cuenta la validación de contenidos de personas que crean el espacio virtual por parte del administrador, personas encargadas de crear contenidos por parte del profesor y finalmente se generará una firma por parte de la persona que utiliza el material, para este caso el estudiante y/o invitado, lo que genera un nivel de seguridad alto en la procedencia de los contenidos disponibles en un LCMS, logrando plantear en este sentido un concepto sobre este tipo de plataformas que a la fecha se vienen trabajando en las redes sociales conocidos como web of trust, WOT, el cual permitirá generar un ambiente de trabajo más confiable sobre el material disponible en estos ambientes de aprendizaje, representados en la Figura 12.

11.3 Diagrama de clases

Con este diagrama pretendemos mostrar el diseño conceptual del modulo, tal como se concibe en este momento, el cual como se puede observar es

consecuente con el diagrama de paquetes presentado anteriormente.

12. Conclusiones

Podemos determinar que en el mercado existen una gran cantidad de organizaciones apoyadas por grupos de investigación que se dedican a estandarizar componentes de uso sobre aplicaciones informáticas mediante arquitecturas de seguridad Web, los cuáles logran destacar la importancia del lenguaje XML, como uno de los elementos diferenciadores para garantizar todo proceso de comunicación que se logre gestar dentro de un entorno de trabajo orientado hacia la Web. Por lo tanto se resalta la importancia que grupos como Nadalin et al., 2007, la IETF, la W3C y aportes realizados por autores a nivel investigativo como Burgos, 2006, y Marquez, 2007 resaltan la idea de que mediante las facilidades que nos ofrece XML, podemos plantear un ambiente seguro de comunicaciones para garantizar los procesos de integridad de información, que de manera representativa se ajustan al conjunto de especificaciones trabajados por SCORM realizando una adaptación al modelo que trabaja para la creación de contenido sobre plataformas LCMS.

A nivel de seguridad en cuanto a generación de contenidos para garantizar autenticidad de los mismos, prácticamente ninguna especificación de las anteriormente analizadas no se contempla de manera directa esta característica, esto debido a que se enfocan netamente a los aspectos administrativos a nivel de etiquetar contenidos, generación de contenidos y desde el punto de vista pedagógico mediante el seguimiento de cada una de las actividades manejadas al interior de cada contenido.

El consorcio IMS también ha trabajado el tema de seguridad, pero solamente como propuestas poco profundas en aspectos relacionado a la autenticación de usuarios y mecanismos de acceso a diferentes tipos de plataformas LCMS bajo modelos de comunicaciones orientados a la Web mediante el apoyo de protocolos de comunicación y soportado por mecanismos como SSL, SLT, redes VPN entre otras alternativas mediante la especificación GWS, 2005, el cuál a nivel de comunicación entre plataformas solamente llega a proporcionar una propuesta de autenticación, aunque dentro de sus características se considera como una especificación poco madura para tratar temas relacionados con la seguridad de los contenidos a nivel de metadatos.

De manera particular LOM contiene una etiqueta donde hace referencia al uso de propiedad intelectual del objeto de aprendizaje, esta es conocida como Derechos, el cuál describe los derechos de propiedad intelectual y las condiciones de uso aplicables al objeto de aprendizaje que se esté trabajando, pero como lo indica el mismo estándar simplemente han sido propuestas en donde no se ha abordado mas el tema de seguridad sobre el objeto que se está trabajando, permitiendo en este sentido ser un fuerte candidato para la implementación de mecanismos de autenticidad.

Para nuestro caso en particular, SCORM parece tener ventajas significativas sobre el conjunto de especificaciones analizadas, puesto que maneja de manera estratégica dentro de su estructura modular el estándar LOM, el cuál como se comento anteriormente maneja un metadato conocido como Derechos y trata particularmente los derechos intelectuales del objeto de aprendizaje, aunque poco profundo, pero sirve de punto de partida para los propósitos de este proyecto, el cual solamente se podrá validar dentro del conjunto de especificaciones manejados por SCORM; donde encontramos elementos que sirven de partida para trabajar de manera estratégica y adaptar en este sentido a través del empaquetamiento de contenidos la parte de autenticidad de los objetos de aprendizaje, y al mismo tiempo será un parámetro de análisis que depende directamente del lenguaje que se maneje para trabajar autenticidad mediante Firma Digital, para este caso las definiciones dadas por XML-Security.

Dentro del modelo de seguridad informático planteado es importante resaltar su buen funcionamiento sobre una infraestructura de confianza mediante el concepto de WOT, al igual que el uso y distribución de claves mediante PKI bajo el apoyo de una entidad certificadora que permita y gestione la generación de cada uno de

los certificados para el ingreso de usuarios sobre la plataforma, lo que permite gestionar dentro del conjunto de especificaciones dado por SCORM la creación del espacio virtual y los contenidos por parte del Administrador y Docente, pero la Plataforma LCMS también debe tener mecanismos de seguridad externos que permita realizar el control sobre los perfiles de usuarios que se manejen en cada situación en particular. Lo que garantiza en este sentido plantear un modelo de seguridad a nivel de autenticidad de contenidos sobre especificaciones manejadas por SCORM, pero al mismo tiempo apoyadas por mecanismos externos que garanticen su buen funcionamiento mediante cada uno de los actores participantes dentro de un proceso de comunicación a saber: administrador, creadores, docentes, estudiante, invitados, personal administrativo, etc.

13. Referencias Bibilográficas

Boneu, J. (2007). Plataformas abiertas de e-learning para el soporte de contenidos educativos abiertos. *Revista de Universidad y Sociedad del Conocimiento,* RUSC, 4, 8.

Burgos, D. (2006). *The structure and behavior of virtual communities engaged in informal learning about e-learning standards (Estudio de la estructura y del comportamiento de las comunidades virtuales de aprendizaje no formal sobre estandarización del e-learning).* Doctoral dissertation, European University of Madrid, Villaviciosa de Odón, Madrid, Spain.

Burgos, D., Tattersall, C. & Koper, R. (2007). How to represent adaptation in e-learning with IMS learning design. *Interactive Learning Environments*, 15, 161-170.

Carracedo, J. (2004). *Seguridad en Redes Telemáticas*. 549. McGraw Hill.

CP, I. (2005). IMS *Content Package. Global Learning Consortium*. [Online]. Available: http://www.imsglobal.org/content/packaging/index.html [Accessed June 2010].

Encryption. XML Encryption Syntax and Processing [Online]. Available: http://www.w3.org/TR/xmlenc-core/ [Accessed June 2010].

Foner, L. (1997). Yenta: a multi-agent, referral-based matchmaking system. ACM, 301-307.

GC, I. (2009). *IMS General Content. Global Learning Consortium* [Online]. Available: http://www.imsglobal.org [Accessed June 2010].

GWS, I. (2005). *IMS General Web Service. Global Learning Consortium* [Online]. Available: http://www.imsglobal.org [Accessed June 2010].

Halsall, F. (2006). *Redes de Computadores e Internet*. Pearson – Addison Wesley, Quinta Edición, 858.

JF Kurose, K. R. (2004). *Redes de Computadores Un Enfoque Descendente Basado en Internet Addison Wesley*.

Kareal, F. & Klema, J. (2006). Adaptivity in e-learning. *A. Méndez-Vilas, A. Solano, J. Mesa and JA Mesa: Current Developments in Technology-Assisted Education,* 1, 260-264.

Key, W. C. (2001). *W3C Note Key. Key Management Specification* [Online]. Available: http://www.w3.org/2001/XKMS/ [Accessed June 2010].

LD, I. (2003). *IMS Learning Design. Global Learning Consortium*. [Online]. Available: http://www.imsglobal.org/learningdesign/index.cfm [Accessed June 2010].

Marquez, J. (2007). Estado *del arte del eLearning. Ideas para la definición de una plataforma universal*. Trabajo de investigación doctoral. Universidad de Sevilla. Departamento de lenguajes y sistemas informáticos.

McCumber, J. (1991). Information systems security: A comprehensive model.

MD, I. (2006). IMS *Meta Data. Global Learning Consortium* [Online]. Available: http://www.imsglobal.org/metadata/index.html [Accessed June 2010].
].

Nadalin, A., Goodner, M., Gudgin, M., BARBIR, A. & Granqvist, H. (2007). WS-Trust 1.3. *OASIS Standard, March.*

Richardson, R. (2008). 2008 CSI Computer Crime & Security Survey. *Computer Security Institute*.

Santos, G. (2007). *Secuenciamiento de actividades educativas orientado a la reutilización y la auto-organización en tutoría inteligente.*

Santos, O. (2006). Technology Enhanced Life Long eLearning for All. in *Technology Enhanced Learning*, 66.

Scorm, A. (2004). *Documentation* 2005 [Online]. Available: http://www.adlnet.org/Pages/Default.aspx [Accessed June 2010].

Schillo, M., Funk, P. & Rovatsos, M. (1999). *Who can you trust: Dealing with deception*. 95–106.

Sign, W. C. (2008). *W3C Recommendation Signature*. XML Signature Syntax and Processing [Online]. Available: http://www.w3.org/TR/xmldsig-core/ [Accessed June 2010].

SS, I. (2003). *IMS Simple Sequence. Global Learning Consortium*. [Online]. Available: http://www.imsglobal.org/simplesequencing/index.html [Accessed June 2010].

Vélez, J. & Fabregat, R. (2007). *Arquitectura para la Integración de las Dimensiones de Adaptación en un Sistema Hipermedia Adaptativo*. Published at Published at Proceedings of Research report Institut d'informàtica i aplicacions (IIiA 07-01-RR).

Wiley, D. & Edwards, E. (2002). Online Self-Organizing Social Systems: The Decentralized Future of Online Learning. *Quarterly Review of Distance Education*, 3, 33-46.

Yu, B., Venkatraman, M. & Singh, M. (2003). An adaptive social network for information access: Theoretical and experimental results. *Applied Artificial Intelligence*, 17, 21-38.

Zimmermann, P. (1995). *The official PGP user's guide*, 216, ISBN 13:978-0-262-74017-3. The MIT Press.