Aproximaciones a la seguridad en educación vía Web en entornos controlados: integridad, no repudio y sellado de tiempo en la tele-evaluación.

A. I. González-Tablas Ferreres, M. A. Fernández Vega,
J. M. Sierra Cámara, A. Orfila Díaz-Pabón

Resumen

La educación a distancia tiene graves deficiencias de seguridad. En este artículo se realiza un análisis del estado actual de la seguridad en la educación a distancia. Tras el estudio de este análisis, los autores extraen la necesidad de proponer una nueva arquitectura que enfoque globalmente la seguridad. La arquitectura propuesta incluye una PKI, una PMI y un servidor de Sellos de Tiempo, y se basa en la familia de estándares de seguridad sobre XML. Al apoyarse sobre XML, la arquitectura adopta las ventajas de esta tecnología consiguiendo una plena integración con la futura Web semántica. Como primera aproximación a esta arquitectura, se estudian los requisitos del proceso de tele-evaluación y se propone un protocolo que abarque los requisitos de integridad, no repudio y sellado de tiempo no contemplados en su totalidad en trabajos anteriores.

Palabras Clave: Educación a distancia, tele-evaluación, autenticación y firma digital, XML, seguridad en redes e Internet.

1 Introducción

La seguridad es un tema ampliamente considerado en todos los aspectos relacionados con Internet. La educación a distancia vía web (*e-learning*) no es la excepción. Muchos de los requisitos de seguridad en educación vía Web son los mismos que los requisitos de sistemas *e-business*, sin embargo no todas las tecnologías de seguridad actualmente disponibles se han aplicado. Los aspectos de seguridad que más se han desarrollado son los relativos a prevención de la manipulación de contenidos, autenticación de usuarios, confidencialidad, privacidad en el aprendizaje, y protección de la propiedad intelectual. Uno de los campos en el que la investigación se ha dejado en un segundo plano es la realización de exámenes y/o certificaciones finales de forma segura. De entre los escenarios posibles [11], nos centraremos en los exámenes realizados en entornos controlados, para asegurar en cualquier caso la autenticación del usuario ante una tercera persona y la realización del examen en condiciones de aislamiento.

Haciendo un análisis de las soluciones de seguridad que se han desarrollado para la educación vía Web y comparándolas con los requisitos de seguridad de un sistema de educación vía Web, encontramos que existen graves deficiencias. Las soluciones propuestas se han centrado en proteger la confidencialidad e integridad del material educativo y su distribución. La autenticación y control de acceso en estos sistemas muchas veces se obtiene simplemente con usuario más contraseña. Los requisitos de no repudio raramente se contemplan.

La mejor solución propuesta hasta ahora es la utilización de una Infraestructura de Clave Pública, aunque todavía no se ha desarrollado un entorno completo de educación vía Web. Ciertamente la PKI soluciona gran parte de los requisitos, pero se requiere un mayor detalle y especificación de los protocolos a utilizar.

Por otro lado, las características de acceso universal, multimedia e hipermedia de la Web hacen que éste sea el medio idóneo a través del cual va a desarrollarse la educación a distancia en el futuro. Y el futuro de la Web está ligado estrechamente a la familia de estándares XML (eXtensible Markup Language). Sobre ellos, la organización OASIS está desarrollando una serie de estándares que definen los mecanismos que permitan garantizar los requisitos de seguridad en el acceso, tratamiento e in-

tercambio de documentos XML.
En este artículo, se realiza una comparación de las soluciones en educación a distancia vía Web existentes en la actualidad con los requisitos de seguridad para estos sistemas. A continuación, en la sección 2, los autores plantean una arquitectura nueva que mejore las arquitecturas existentes. La sección 3 se centra en el proceso de tele-evaluación, analizando sus necesidades de seguridad y proponiendo un protocolo que afronta los requisitos de integridad, no repudio y sellado de tiempos. En la sección 4, se exponen las conclusiones y ampliaciones de este trabajo.

1.1 Requisitos de seguridad de un sistema de educación vía Web

Se pueden identificar una serie de requisitos de seguridad de un sistema de educación vía Web. En el proyecto SDLearn [4] se realiza una excelente recopilación de éstos, que se exponen a continuación:

(1) Privacidad y confidencialidad de los datos personales

(2) Seguridad en el uso de los servicios: autenticación y contabilidad; control de acceso al sistema central; sistema de detección de intrusos.

(3) Comunicaciones seguras entre el profesorado/ personal de administración y los alumnos.

(4) Seguridad en el pago: no repudio del pago; integridad; prevención del fraude.

(5) Seguridad de los trabajos enviados por los estudiantes: autenticación; confidencialidad; no repudio; integridad.

(6) Seguridad del material del curso: prevención de accesos no autorizado; prevención de distribución ilícita; control de las licencias de software.

(7) Certificados digitales de finalización de un curso: verificación del centro emisor; verificación de la integridad del certificado.

(8) Confidencialidad de las calificaciones de los estudiantes

(9) Fiabilidad y disponibilidad del sistema central

(10) Confidencialidad y realización segura de los exámenes

Algunos requisitos están más desarrollados que otros. La realización de exámenes de forma segura (10) es un tema complejo sin una solución clara todavía y al que dedicaremos nuestra atención.

1.2 Tecnologías asociadas

PKI. Las Infraestructuras de Clave Pública son organizaciones que utilizan criptografía de clave pública y certificados digitales para proporcionar seguridad en las comunicaciones. Cada entidad de la PKI posee un par de claves relacionadas, una pública y otra privada. El certificado digital es el documento digital que asegura que una clave pública pertenece a un sujeto determinado.
Control de acceso. En muchas ocasiones la tecnología de control de acceso más utilizada es usuario más contraseña. En otros casos se utilizan PKIs.
XML. XML es un metalenguaje que sirve para definir lenguajes propios de representación de la estructura de datos, el estándar ha sido desarrollado por *World Wide Web Consortium* (W3C). XML ya se está utilizando para todo tipo de aplicaciones tanto de almacenamiento y acceso a información como de comunicación de datos o establecimiento de transacciones en Internet.
Estándares de seguridad sobre XML. La organización OASIS está realizando un gran esfuerzo en desarrollar estándares que definen los mecanismos que permitan garantizar los requisitos de seguridad en el acceso, tratamiento e intercambio de documentos XML. Los estándares más desarrollados hasta el momento son *XML Signature Syntax and Processing*, *XML Access Control Language* y *Security Assertion Markup Language*.

1.3 Soluciones en la seguridad de la educación vía Web

A continuación realizaremos un breve repaso de las soluciones propuestas para educación vía Web, comparando con los requisitos de seguridad expuestos en la sección 1.1 y haciendo hincapié en la realización de exámenes.
Universitat Oberta de Catalunya UOC. Podemos considerar la Universidad Oberta de Catalunya [10] como un ejemplo de la Universidad a través de Internet. El usuario mediante un identificador y contraseña accede al Campus Virtual. El mecanismo de evaluación es continuado a través de la entrega periódica de ejercicios vía correo electrónico. Para aprobar la asignatura se debe realizar siempre un examen presencial.
Muchos de los requisitos no se contemplan. En estos sistemas existe un control de

acceso y autenticación mediante usuario y contraseña. El resto de requisitos no están contemplados.

Páginas Web dinámicas: WEBTEST, Hot Potatoes, TexToys, ... Otra de las soluciones ampliamente utilizada es la realización de pruebas de tipo objetivo mediante páginas HTML que incluyen código JavaScript con formularios. Los resultados son enviados a un servidor Web donde son procesados, o el resultado es procesado directamente por el código insertado en la página Web. Tres herramientas representativas son WEBTEST, Hot Potatoes y TextToys [2].

Estas tecnologías utilizadas sin complementar con otras son claramente inseguras y deberían utilizarse al menos con mecanismos de control de acceso y autenticación y cifrado de la comunicación.

Coimbra. En [11] se describe Coimbra, un sistema para distribución segura de contenidos digitales multimedia con el fin de prevenir el acceso no autorizado y simultáneamente la distribución ilícita de los contenidos. La información está cifrada al descargarla un cliente y para descifrar el contenido es necesario conectarse al servidor mediante usuario y contraseña. En [12] se realiza una propuesta para especificar sencillamente reglas de control de acceso de manera similar a cómo se especifican en el estándar XACML.

Estas soluciones empiezan a tener en cuenta los requisitos de seguridad como los requisitos (2) y (6), pero no se contemplan el resto, por ejemplo el (10).

Testing Open Framework - Cipress. En [5] se proponen dos soluciones para dos escenarios de sistemas de educación vía Web: Testing Open Framework y Cipress. La primera solución es una arquitectura para la realización de ejercicios diseñada para integrarse en un sistema de educación a distancia para entornos abiertos -como Internet- y, teniendo en cuenta la seguridad. Las funcionalidades que proporciona son la entrega segura del material del ejercicio, la evaluación segura de los resultados, control fiable del tiempo, reconocimiento y evaluación de las acciones del usuario, y, por último, creación y entrega de información de realimentación. La segunda solución es el sistema CIPRESS que asegura la confidencialidad del material educativo, y de esta manera proporciona protección de los derechos de autor frente a la copia y distribución ilegal. CIPRESS es una extensión del sistema operativo que utiliza técnicas de cifrado junto con técnicas de marcas de agua.

Cipress es similar a Coimbra y por tanto es una buena solución ante la seguridad del material del curso. Testing Open Framework se centra únicamente en la realización de ejercicios de forma segura, y la solución que propone es muy interesante y efectiva. Sin embargo, esta solución no debería ser utilizada en exámenes finales y necesita contrastar los resultados con ejercicios presenciales, ya que hay requisitos que no contempla como el no repudio. Hay que tener en cuenta además que no es una solución global para la seguridad de los entornos de educación vía Web.
PKI como necesidad en la Universidad Virtual (Podestá y Meinel). Podestá y Meinel [8] proponen el uso de la PKI como parte fundamental de una universidad virtual. Los certificados de una PKI proporcionarían autenticación de cada recurso de la universidad, firma digital de los documentos, cifrado de los datos y sellos de tiempo en los ficheros. Con esto se posibilitaría una solución *single sign-on* para el acceso a todos los recursos del campus; la confidencialidad y la autenticación en el intercambio de información; y, en el envío de ejercicios mediante el correo electrónico, el no repudio (del autor del ejercicio enviado por correo), la autenticación y la integridad. La implementación considera una Autoridad de Certificación, un Servidor de Directorio y un Servidor de Sellado de Tiempo. La firma digital sería el mecanismo para probar la autenticidad respecto al origen de los datos, verificar su integridad y asegurar no repudio en el envío. El sellado de tiempos garantizaría un control fiable de tiempos de las condiciones de entrega de enunciados y recepción de ejercicios contestados.
Esta aproximación nos parece que es la adecuada, aunque los autores no detallan los procedimientos necesarios para que todos los requisitos de [4] se contemplen. En la sección 3 se detallará el procedimiento de tele-evaluación que los autores proponen.

2 Arquitectura propuesta

Nosotros queremos avanzar un paso más proponiendo la utilización de Infraestructuras de Clave Pública sobre XML para resolver la seguridad de la educación vía Web. Desarrollar la educación vía Web sobre XML es una solución adecuada para satisfacer tanto los requisitos multimedia y de futuro desarrollo de la Web como para resolver los requisitos de seguridad necesarios, utilizando para ello los estándares de

seguridad sobre XML.
Una Infraestructura de Clave Pública proporciona los mecanismos para obtener confidencialidad, autenticación, integridad y no repudio. Esto afrontaría los requisitos (1), (3), (4), (5), (7), y (8) y parcialmente, si consideramos una solución *single sign-on*, los (2) y (6). El requisito (9) debe hacerse frente con otros métodos fuera del alcance de este trabajo, y el requisito (10) requiere, además de los mecanismos provistos por la PKI, de procedimientos especificados especialmente mediante un protocolo de tele-evaluación segura.
Por otro lado, consideramos que la solución de los requisitos (2) y (6) debería afrontarse con una nueva perspectiva. En lugar de considerar control de accesos, la arquitectura podría comprender tanto una PKI (Infraestructura de Clave Pública) como una PMI (Infraestructura de Gestión de Privilegios), más un servidor de Sellado de Tiempos. Esta PMI se ocuparía de autorizar las acciones de las entidades de la arquitectura y por tanto de controlar los accesos al sistema. Con esto obtendríamos una arquitectura global de seguridad para desarrollar la educación a distancia vía Web en entornos controlados. Para complementar esta arquitectura, sería necesario desarrollar una serie de protocolos que especifiquen cómo llevar a cabo los servicios del sistema.

La utilización de XML para implementar la PKI y la PMI nos proporcionaría las siguientes ventajas.

- Portabilidad de los datos de seguridad XML sobre cualquier plataforma
- La información de seguridad puede mantenerse como parte constituyente de los datos
- Flexibilidad y extensibilidad de los estándares de seguridad
- Flexibilidad proporcionada por el mismo XML
- Integración con la futura Web semántica [1]
- Redefinición de los estándares /mecanismos de seguridad existentes sobre la misma base (XML): mayor facilidad de diseño, desarrollo y mantenimiento de aplicaciones teniendo en cuenta la seguridad desde el principio
- Estándares no propietarios, con soporte de la comunidad internacional
- Integración con Java
- Consideración desde el principio de los conceptos de multimedia y web dinámica

3 Integridad, no repudio y sellado de tiempo

La realización de exámenes finales vía Web o tele-evaluación de forma segura es el aspecto que más falta por definir dentro del campo de la seguridad en educación vía Web. Este proceso necesita de los servicios de autenticación, autorización, integridad, confidencialidad, no repudio y sellado de tiempos. Por su complejidad, los autores pensamos que necesita que se defina un protocolo de tele-evaluación. Los requisitos de esta arquitectura de tele-evaluación y los servicios de seguridad asociados serían los de la tabla siguiente:

Servicios	**Requisitos profesor**	**Requisitos alumno**
Autenticación	Acceso al sistema	Acceso al sistema
	Firma del enunciado y condiciones y Firma de las calificaciones	Firma del enunciado contestado y condiciones
	Verificación de la autenticidad de los documentos enviados por el alumno	Verificación de la autenticidad de los documentos firmados por el profesor
Autorización	Poner enunciado del examen	Acceso al enunciado en las condiciones
	Establecer alumnos autorizados, fecha, hora de comienzo y duración	Contestación y envío del examen contestado
	Corrección y calificación de exámenes contestados	Acceso a su calificación
Confidencialidad	Enunciado, totalidad de enunciados contestados, calificaciones	Enunciado contestado
Integridad	Enunciado, condiciones de acceso y entrega	Enunciado contestado
	Verificación de documentos enviados por el alumno	Verificación documentos firmados por profesor
No repudio	Publicación de enunciado, condiciones y notas	Recepción del enunciado y condiciones
	Recepción del enunciado y condiciones	Envío del enunciado contestado
Notaría (sellado de tiempos)	Publicación del enunciado y notas	Acceso al enunciado
	Recepción del enunciado contestado	Envío del enunciado contestado

Precisamente la integridad y el no repudio debe establecerse todavía en el proceso completo de tele-evaluación, resultando fundamental para llevar a cabo un examen vía web adecuadamente. Tanto para el no repudio del origen como para el no repudio de la recepción, la firma digital más los sellos de tiempo son la solución. Continuando con el planteamiento expuesto en la sección 2, utilizaríamos el estándar de firma digital XML Signature Syntax and Processing [3].
Como ventajas de utilizar el estándar de firma digital XML sobre otros estándares de firma digital y a pesar de existir mecanismos como SSL (o HTTP-S) para proteger la transmisión de los datos [9] podemos destacar dos. La primera de ellas es la portabilidad de la firma digital, que en este caso va entrelazada con los mismos datos. De esta manera, la firma es parte constituyente de los datos, no es un fragmento extraído del flujo de red que se pierde al ir atravesando las distintas capas de protocolos. La segunda de ellas, es la flexibilidad de la firma digital XML que permite, entre otras variantes, varios firmantes en un mismo documento, la firma de distintas partes de un documento, y la firma de documentos distintos y partes de documentos distintos también, además de poder incluir sellos de tiempo.
A continuación nos centraremos en la descripción del protocolo de tele-evaluación que proponen los autores.

3.1 Protocolo de tele-evaluación

El profesor se autentica y es autorizado para poner un enunciado de examen y las condiciones de realización del mismo en el servidor. Este enunciado se mantendrá confidencial hasta el inicio del examen mediante cifrado y control de autorización en el acceso. Tanto el enunciado como las condiciones irán firmados utilizando la firma digital XML, ya que con ésta aseguramos el no repudio del contenido, la autenticidad y la integridad. Al almacenarse en el servidor las condiciones y el enunciado firmados, se emitirá un sello de tiempos para asegurar la publicación de éstos en una fecha concreta.
El examen se realizará en un entorno controlado (aula o centro remoto), para asegurar la autenticación física del alumno y el hecho de que éste realiza el examen sin la colaboración de terceras partes [13]. Una persona deberá identificar al alumno y

vigilar el proceso. Así mismo todas las comunicaciones entre las partes implicadas se realizarán cifradas.
En la fecha y hora acordada, el alumno accederá al sistema para obtener el enunciado. El servidor le autenticará y autorizará para ello. Una vez obtenido el enunciado del examen, el alumno podrá verificar la autenticidad e integridad del enunciado y las condiciones del examen, validando para ello la firma del profesor.
El alumno firmará el resumen del documento recibido y se emitirá un sello de tiempo sobre éste. El sello se enviará al servidor, obteniendo de esta manera la confirmación de la recepción del enunciado y la fecha en la que el alumno comienza el examen.
El alumno contesta el examen y una vez lo ha terminado, lo firma y se emite un sello de tiempo sobre el resumen del examen firmado. Este sello se envía al servidor junto con el examen firmado.
El servidor verificará la autenticidad e integridad del enunciado contestado, y del sello de tiempo. Además se comprobará que la entrega se ha realizado en el tiempo acordado. Los exámenes se almacenarán cifrados y sólo podrá acceder a ellos el profesor para su corrección.
Se verificará que todo el proceso ha sido correcto y el profesor calificará cada uno de los exámenes. Las notas de cada alumno firmadas por el profesor serán enviadas al mismo y se autorizará únicamente al alumno el acceso a su propia nota.

4 Conclusiones

Las soluciones actuales para la educación a distancia vía Web no abarcan todos los requisitos de seguridad necesarios. Sobre todo, en lo referente a tele-evaluación, ya que no se especifica la realización de exámenes finales que evalúen completamente los conocimientos adquiridos por el alumno, y no tan sólo la entrega de ejercicios parciales. Al haberse desarrollado únicamente soluciones parciales, no se han contemplado como debería los requisitos de integridad, no repudio y sellado de tiempo en el proceso completo de tele-evaluación.
La solución propuesta por los autores de este trabajo, no sólo realiza un estudio de cuáles son los requisitos del proceso de tele-evaluación sino que propone un protocolo que los aborda.

El protocolo de tele-evaluación se enmarca dentro de una arquitectura de educación vía Web que también proponen los autores. Esta arquitectura contempla la inclusión de una PKI, una PMI y un servidor de Sellos de Tiempo, y estará desarrollada completamente sobre los protocolos XML de seguridad. Esta arquitectura mejora las arquitecturas existentes hasta ahora dando un nuevo enfoque al control de accesos mediante la inclusión de la PMI para gestionar autorizaciones. El hecho de desarrollarse sobre XML provoca que la solución adopte las ventajas propias de esta familia de lenguajes, consiguiendo una arquitectura extensible e integrada plenamente en la Web futura.
Dentro de los futuros trabajos, los autores implementarán el protocolo propuesto y desarrollarán en más profundidad la arquitectura global de educación a distancia. Se integrarán los otros estándares de seguridad sobre XML en el proceso y mecanismos de autenticación que utilicen tarjetas inteligentes para transportar los certificados.
Las necesidades de seguridad en la educación a distancia vía Web son una cuestión abierta que hay que afrontar cuanto antes, puesto que cada vez son más las necesidades de la sociedad en esta materia.

Referencias

[1] T. Berners-Lee, J. Hendler, O. Lassila. *The Semantic Web. http://www.scientificamerican.com/2001/0501issue/0501berners-lee.html* (2001)

[2] WEBTEST *http://fpg.uwaterloo.ca/WEBTEST/WEBTEST_intro.html*, TexToys *http://www.cict.co.uk/software/textoys/*, Hot Potatoes *http://web.uvic.ca/hrd/halfbaked/*

[3] Eastlake, D., Reagle, J., Solo, D. (2002) Xml signature syntax and processing. IETF Internet-Draft. http://www.ietf.org/internet-drafts/draft-ietf-xmldsig-core-2-03.txt y *http://www.w3.org/TR/2001/PR-xmldsig-core-20010820/*

[4] Furnell, S. *A security framework for online distance learning.* Security in Online Learning environments Workshop, South Bank University, October 2000.

[5] Graf, F. *Secure ilearning.* IFIP TC6 / TC11 Fith Joint Conference on Communications and Multimedia Security (CMS'01) May 21-22, 2001, Darmstadt, Germany.

[6] Karlinger, G. (2001). *Xml electronic signatures. Application according to the international standard XML Signature Syntax and Proccessing.* IFIP TC6 / TC11 Fith Joint Conference on Communications and Multimedia Security (CMS'01) May 21-22, 2001, Darmstadt, Germany.

[7] Rolf Oppliger. *Security Technologies for the World Wide Web.* Artech House Inc. 2000. ISBN 1580530451

[8] M. Podestá, Ch. Meinel. *Integration of a Public Key Infrastructure in a Virtual University.* Proc. CACIC 2000, Ushuaia, (Argentinien),2000, pp. 1-8.

[9] Selkirk, A. *XML and Security.* BT Technology Journal. Vol. 19 No. 3 JULY 2001. *http://www.bt.com/bttj/vol19no3/selkirk1/selkirk1.pdf*

[10] Universitat Oberta de Catalunya *http://www.uco.es*

[11] Weippl, Edgar. *Security Models for elearning.* Vienna International Workshop on Distance Education & Learning, 2001

[12] Weippl, Edgar. *Coimbra: Secure Web Access to Multimedia Content.* Multimedia and Security Workshop at ACM Multimedia At the 8th ACM International Multimedia Conference November 4, 2000 Los Angeles, California.

[13] Kerstin Rönnberg. *User authentication in online assesment* Masther Thesis, May 2001. Umea University, Sweden. Department of Computer Science.

Ana Isabel González-Tablas Ferreres, María Ángeles Fernández Vega, José María Sierra Cámara, Agustín Orfila Díaz-Pabón
Departamento de Informática
Universidad Carlos III de Madrid
Calle Butarque 15
28911, Leganés.
E-mail: {aigonzal, mafvega, sierra, adiaz}@inf.uc3m.es