Memoria de la acción AYUDAS DE LA UNIVERSIDAD DE SALAMANCA PARA LA INNOVACIÓN DOCENTE

Técnicas de buenas prácticas y desarrollo de sistemas seguros de comunicación Profesor-Estudiante en el EEES mediante firmas y certificados digitales: Caso de estudio aplicable a cualquier asignatura impartida en el marco del EEES

Código del Proyecto: ID9-017.

En la actualidad, en mayor o menor grado, todos hacemos uso de la informática tanto para almacenar como para transmitir información. En el marco de la convergencia de la enseñanza en el **espacio europeo de educación superior**, la necesidad de la utilización de las tecnologías de la información y de la comunicación se verá reforzada y ello conlleva que tengamos que planificar un **almacenamiento** y **una comunicación segura**.

Las metodologías docentes en las titulaciones dentro del marco del Espacio Europeo de Educación Superior (EEES) están sufriendo un proceso de transformación importante, debido a diferentes factores. Entre ellos no se puede dejar de lado el menor grado de presencialidad en las aulas y mayor comunicación telemática profesor-estudiante; por lo tanto este factor va a afectar a estudiantes y docentes. Con este proyecto hemos pretendido fomentar la utilización de las tecnologías de la información de forma segura haciendo uso de la firma digital.

En todas las asignaturas impartidas por los profesores que hemos llevado a cabo este proyecto correspondiente al "Máster en Sistemas Inteligentes", parte de la evaluación es continua y hasta ahora nos fiábamos de todos los correos que nos llegan en nombre de los estudiantes, así como de todas las cuestiones que nos plantean por correo electrónico. Por ello, Para el Máster en sistemas Inteligentes, ya adaptado EEES hemos llevado a cabo metodologías innovadoras en la comunicación segura profesor-alumno permitiendo realizar evaluación continua on-line.

La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de

identificación del firmante. **La firma electrónica permite que tanto el receptor como el emisor de un contenido puedan identificarse mutuamente con la certeza de que son ellos los que están interactuando, evita que terceras personas intercepten esos contenidos y que los mismos puedan ser alterados, así como que alguna de las partes pueda "repudiar" la información que recibió de la otra y que inicialmente fue aceptada.**

La **Firma electrónica** es un sistema de acreditación que permite verificar la identidad de las personas con el mismo valor que la firma manuscrita, autentificando las comunicaciones generadas por el firmante.

Por otra parte la Ley 59/2003, de 19 de diciembre, de firma electrónica define la firma electrónica de la siguiente manera:

- (Art. 3.1) La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Asimismo la Ley distingue entre "firma electrónica avanzada" y "firma electrónica reconocida":

- (Art. 3.2) La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- (Art. 3.3) Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
- (Art. 3.4) La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

El modo de funcionamiento de la firma electrónica basado en clave pública es el siguiente:

- Cada parte tiene un par de claves, una se usa para cifrar y la otra para descifrar.
- Cada parte mantiene en secreto una de las claves (clave privada) y pone a disposición del público la otra (clave pública).
- El emisor obtiene un resumen del mensaje a firmar con una función llamada "hash" (resumen). El resumen es una operación que se realiza sobre un conjunto de datos, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es

imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la función "hash".

- El emisor cifra el resumen del mensaje con la clave privada. Ésta es la firma electrónica que se añade al mensaje original.
- El receptor, al recibir el mensaje, obtiene de nuevo su resumen mediante la función "hash". Además descifra la firma utilizando la clave pública del emisor obteniendo el resumen que el emisor calculó. Si ambos coinciden la firma es válida por lo que cumple los criterios ya vistos de autenticidad e integridad además del de **no repudio** ya que el emisor no puede negar haber enviado el mensaje que lleva su firma.

Son muchas las Autoridades de Certificación que emiten la firma digital. La más ambiciosa de estas iniciativas, puestas en marcha por la Administración, es el denominado proyecto **CERES** (Certificación ESpañola) que lidera la Fábrica Nacional de Moneda y Timbre, y que en líneas generales, consiste en establecer una Entidad Pública de Certificación, que permita autentificar y garantizar la confidencialidad de las comunicaciones entre ciudadanos, empresas u otras instituciones y administraciones públicas a través de las redes abiertas de comunicación.

El objetivo principal de CERES es la securización de las comunicaciones electrónicas con la Administración, siendo un intermediario transparente al usuario que garantizará a ciudadanos y Administraciones la identidad de ambos partícipes en una comunicación, así como la confidencialidad e integridad del mensaje enviado. Para ello, CERES utiliza técnicas y sistemas criptográficos basados en lo que se conoce como sistema de clave pública, con dos características básicas:

- La identidad del usuario, al igual que su capacidad de firma, se encuentra, en el caso de máxima seguridad, almacenada en una tarjeta inteligente, que no puede ser accesible salvo por su propietario cuando introduzca el número de identificación personal, similar a la clave de una tarjeta de crédito. En caso de no utilizar tarjeta, el perfil criptográfico queda almacenado en un fichero, siendo necesario también un PIN de acceso.
- El sistema es completamente transparente al usuario, es decir, no es necesario conocer ninguna técnica criptográfica para realizar o verificar una firma electrónica o cifrar o descifrar un mensaje.

Por otra parte, el nacimiento del Documento Nacional de Identidad electrónico (DNIe), responde, a la **necesidad de otorgar identidad personal a los ciudadanos para su uso en la nueva Sociedad de la Información**, además de servir de impulsor de la misma. Así, el DNIe es la adaptación del tradicional documento de identidad a la nueva realidad de una sociedad interconectada por redes de comunicaciones. El DNI electrónico, además de la capacidad de identificación física de su titular, posee la capacidad de identificación en medios telemáticos y de firmar electrónicamente como si

de una forma manuscrita se tratase. De esta forma garantiza que la personalidad del firmante no es suplantada. Asimismo la firma electrónica permite proteger la información enviada a través de un medio telemático.

Ante esta situación valoramos si deberíamos trabajar con certificado en formato digital, el de la FNMT (CERES) o con certificado en tarjeta criptográfica como el DNIe y consideramos que los profesores deberíamos tener los dos, pero los alumnos al ser muchos extranjeros mejor era proponerles el de la FNMT.

Las ventajas e inconvenientes de los mismos son:

- El de la FNMT lo puede obtener cualquier ciudadano, de cualquier nacionalidad, además es por software y no necesitamos hardware adicional para utilizarlo, pero el inconveniente es instalarlo y almacenarlo de forma segura.

- El DNIe la ventaja es que al ser en tarjeta criptográfica es mucho más seguro, pero necesitamos un lector de tarjeta y si es cierto que compramos uno para cada profesor tuvimos problemas para conseguirlo y más al intentar localizar teclados con lector de tarjetas. Y además, en cada ordenador desde el cual lo queríamos utilizar teníamos que instalar los drivers.

A la hora de utilizarlo el problema con el que nos encontramos es que cada profesor y alumno tiene un software diferente y que en concreto a la hora de enviar correos firmados muchos de los implicados sólo trabajaban con el correo por página web y al no estar desarrollado el envío de correos firmados y cifrados desde la web tuvimos que configurar un gestor de correo para poder hacerlo (Outlook Express, Microsoft Outlook, mozilla thunderbind, etc.)

La plataforma que utilizamos para la formación on-line, Studium, tampoco permite identificar a los participantes de forma segura y tampoco la firma de los documentos desde la plataforma y en este caso lo resolvimos firmando previamente los ficheros Word, open-office, pdf, …

Por otra parte, los alumnos eran conscientes de que llevaban parte de sus trabajos en memoras USB y que los profesores llevábamos no sólo material de las materias sino también exámenes, notas de alumnos, … , hicimos un estudio de quien llevaba la información protegida y llegamos a la conclusión que ni un 10%. Por ello decidimos estudiar que software era el más adecuado y llegamos a la siguiente conclusión:

- Debemos proteger de forma individual cada uno de los documentos.
- Debemos comprar memorias USB que traigan incorporado software de seguridad. El que tiene la mayoría de las que encontramos en el mercado fue uno que se llama U3 y que es muy cómodo de utilizar.
- De no tenerlo preinstalado aconsejamos bajarnos uno de la red y que fue mejor valorado por nosotros es el llamado REMORA.

La mayor dificultad la hemos tenido en el proceso administrativo, a la hora de intentar hacer la gestión on-line, La universidad tiene el registro telemático pero en determinadas ocasiones que lo hemos intentado utilizar nos ha dado problemas y además la Orden reguladora del mismo no permite hacer todas las gestiones deseadas, en concreto sólo permite:

- Presentación de documentos ante órganos colegiados.
- Comunicación entre órganos (colegiados y unipersonales) de la Universidad.
- Escritos y reclamaciones ante la Junta Electoral.
- Comunicaciones entre las Juntas Electorales de los Centros y la Junta Electoral de la Universidad.
- Presentación de solicitudes de ayudas, becas.
- Presentación de informes.
- Presentación de preinscripciones en estudios de postgrado.
- Presentación de recursos ante el órgano competente de la Universidad.
- Solicitudes en concursos.

Hay que destacar que sí permitió hacer la preinscripción a los alumnos por Internet, con la gran ventaja que supone para nuestros alumnos, que como decíamos la mayoría son extranjeros, y en concreto de Latinoamérica.

También nos encontramos con que los alumnos tuvieron que hacer un Trabajo de Fin de Máster que en muchas ocasiones trabajaron con el tutor de forma on-line y con el certificado digital lo pudieron hacer de forma segura. Ahora bien se planteó la entrega de la documentación, firmada digitalmente y en exclusiva por Internet pero no se pudo llevar a cabo por la normativa existente de Trabajos Fin de Máster.

Como conclusiones consideramos que se puede trabajar de forma segura en la comunicación:

- Sistemas de evaluación continua de competencias
- Nuevas modalidades de tutorización adaptadas al EEES
- Trabajos de Fin de Grado/Máster y su evaluación

Después de todo este estudio, consideramos que las conclusiones de este proyecto, permitirán mejorar la implantación de las materias prácticas del Máster y los grados en informática, poner a disposición del profesorado de la titulación nuevas metodologías activas de enseñanza y aprendizaje, así como modalidad de seguimiento y autorización trabajando de forma segura.

NOMBRE GONZALEZ ARRIETA MARIA ANGELICA - NIF 06555917C

Firmado digitalmente por NOMBRE GONZALEZ ARRIETA MARIA ANGELICA - NIF 06555917C
Nombre de reconocimiento (DN): CN = NOMBRE GONZALEZ ARRIETA MARIA ANGELICA - NIF 06555917C, C = ES, O = FNMT, OU = FNMT Clase 2 CA
Fecha: 2010.05.29 23:58:05 +02'00'