# Certificados digitales. Implantación en centros educativos

Autor: Juan Luis Vicente Carro
Centro Trabajo:Profesor Informática IES Gerardo Diego , Pozuelo de Alarcón, Madrid
Correo: juanluvica@gmail.com

## Resumen

El presente artículo describe de una forma sencilla y clara que son los certificados digitales y la función que realizan estos dentro de las diferentes transacciones de información que realizamos en la red. Una vez explicado su funcionamiento y ventajas trasladamos su posible aplicación a un centro educativo con el objetivo de ir mejorando la gestión del mismo mediante las diferentes oportunidades que nos proporcionan las TIC.

Actualmente con el incremento del uso de las nuevas tecnologías de la información, internet como máximo exponente, se han incrementado los riesgos relativos a la seguridad de la información y en especial la reciente problemática existente en la identificación con garantías de todos los interlocutores en una conversación, transacción económica etc…ya que han aumentado considerablemente el uso de chats, redes sociales etc. hasta el punto de ser algo cotidiano.

Uno de los grandes inconvenientes que presentan las redes de información es la dificultad de poder asegurar que quien está al otro lado es realmente quien dice ser. Sin embargo, hay que destacar el hecho de que muchos usuarios de internet buscan precisamente el anonimato que este proporciona, Internet únicamente se preocupa de conectar dos máquinas identificadas por direcciones IP la información de las personas que están detrás de dichas máquinas es indiferente para su funcionamiento.

Para la realización de ciertas tareas, estas deben ser realizadas en un contexto en el que debemos estar seguros de la identidad de todos los interlocutores, en la mayoría de las operaciones de la vida real nuestra identificación la realizamos mediante DNI o pasaporte pero ¿cómo poder trasladar este elemento dentro los sistemas informáticos? la forma de hacerlo es mediante los certificados digitales englobados dentro de las infraestructuras de clave pública (PKI).

Un certificado digital es un documento electrónico mediante el cual un tercero de confianza, identificada como autoridad de certificación, acredita electrónicamente la autenticidad de la identidad de una persona física, persona jurídica u otro tipo de identidad como lo puede ser, por ejemplo, una URL de un sitio Web. Como emisor y receptor confiarán en esa AC, el usuario que tenga un certificado expedido por ella se autenticará ante el otro, en tanto que su clave pública está firmada por dicha autoridad.

En definitiva se trata de un medio electrónico de acreditación equivalente a los existentes en el mundo del papel, de hecho, la propiedad más característica del DNI electrónico o DNIe es precisamente la incorporación de este tipo de certificados.

Simplificando los términos en cuanto a la función de una Autoridad de Certificación, esta actúa como un notario, acredita a aquellos certificados que tengan su firma al igual

que un notario da fe de alguna operación compra venta de una vivienda por poner un ejemplo, dando validez legal a la operación.

## Características

Los certificados digitales poseen variados formatos, los más comúnmente empleados se rigen por el estándar UIT-T X.509, el cual está basado en criptografía asimétrica y firma digital.

El certificado contiene usualmente

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado

Además, respecto a la Autoridad de Certificación

- El certificado se cifra con la clave privada de la Autoridad de Certificación.
- Todos los usuarios poseen la clave pública de la Autoridad de Certificación.

❖ Principales tipos de certificados
- *Certificados de servidor*
- *Certificados personales*
- *Certificados Aplicación de software*

❖ Principales extensiones de archivos
- *.CER*
- *.DER*
- *.PEM*
- *.P7B*
- *.P7C*
- *.PFX*
- *.P12*

## Funcionamiento

El usuario A enviará al usuario B su certificado (la clave pública firmada por AC) y éste comprobará con esa autoridad su autenticidad. Lo mismo en sentido contrario. Durante dicha comprobación se chequearán las listas de certificados revocados si alguno de los certificados implicados estuviera en dicha lista no se confiaría en él.


Figura 1.Proceso validación de certificados

Uno de los certificados de mayor presencia o conocimiento por parte de los usuarios, en España, es el certificado clase 2CA proporcionado por la fábrica nacional de moneda y timbre (FNMT) popularizado principalmente por la posibilidad de presentar de forma telemática la declaración de la renta o solicitar la vida laboral. Dicha gestión sobre los certificados a cargo de la FNMT se encuentra englobada dentro del proyecto CERES. Si bien el usuario medio desconoce la verdadera función de la FNMT en la emisión del certificado, así como la existencias de otros certificados proporcionados por otras entidades igualmente válidos para las operaciones anteriormente descritas.

## ¿Quién puede ser una autoridad de certificación?

Cualquier individuo o institución puede generar un certificado digital, desde un punto de vista técnico cualquiera puede erigirse en AC (sólo es necesario disponer de un par de claves pública-privada para firmar y verificar la firma, y todo aquel que desee obtener un certificado las tiene), pero si éste emisor no es reconocido por quienes interactúen con el propietario del certificado, el valor del mismo es prácticamente nulo.

Por ello los emisores deben acreditarse: así se denomina al proceso por el cuál entidades reconocidas, generalmente públicas, otorgan validez a la institución certificadora, de forma que su firma pueda ser reconocida como fiable, transmitiendo esa fiabilidad a los certificados emitidos por la citada institución. La gran mayoría de los emisores tienen fines comerciales, y otros, gracias al sistema de anillo de confianza, pueden otorgar gratuitamente certificados en todo el mundo.

Si el certificado digital X.509 de un servidor no pertenece a una Autoridad de Certificación reconocida o instalada en su programa/equipo, aparecerá una pantalla similar a la que se muestra a continuación en la que se expone dicha situación y se pregunta al usuario si confía en el certificado recibido y en la autoridad de certificación que lo emite.(Lo datos relativos al certificado pueden ser consultados pulsando en el botón "*Ver certificado*" )

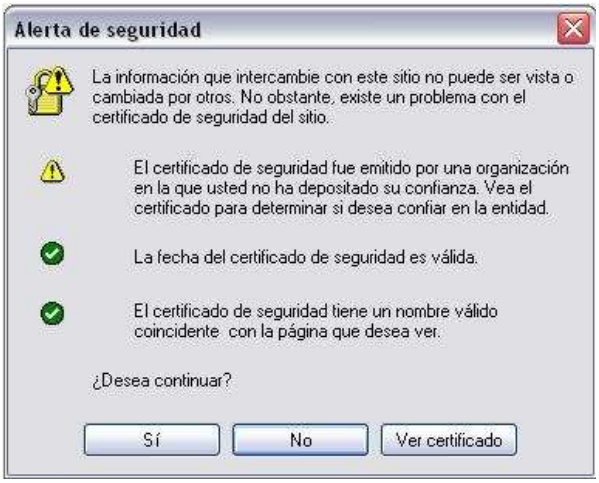


Figura 2.Pantalla informativa autoridades de certificación no registradas

Una Autoridad de Certificación, además de emitir certificados, debería ofrecer los servicios siguientes:

- Búsqueda de certificados: Una persona puede querer buscar el certificado referente a otra persona o entidad.
- Revocación: Si un certificado se pierde, el titular debe poder informar a la Autoridad de Certificación para que lo anule y emita otro. También si la clave privada ha quedado comprometida debe ser posible su revocación. Si ha quedado vulnerada la confidencialidad de la clave privada se aplica tanto para la clave privada del usuario como de la Autoridad de Certificación.
- Suspensión: La Autoridad de Certificación debe suspender la validez de un certificado si se hace un uso anormal de él.
- Estado del certificado: Las personas a las que se les presenta un certificado deben de poder comprobar que no ha sido revocado o suspendido. Una autoridad de Certificación dispone de una lista de certificados revocados, si un certificado determinado aparece en dicha lista se considera que no se puede confiar en él.

## Aplicación certificados digitales en centros educativos

Una vez vistas las características de los certificados digitales y la funcionalidad que estos aportan, sería muy interesante trasladar su aplicación a los centros educativos, estos podrían ser englobados dentro de alguno de los diferentes proyectos de innovación TIC.

A pesar de las limitaciones en cuanto a la escasez de los presupuestos en los centros para invertir en IT o la existencia de infraestructuras deficientes, reducidas casi en exclusiva a las aulas informáticas, la implantación de un sistema de certificados sería totalmente viable. Este sistema no necesita ninguna inversión o al menos esta sería mí-

nima ya que se puede apoyar en inversiones destinadas a otros proyectos como pueden ser una nueva dotación de equipos informáticos, la implantación de portales educativos, intranets, plataformas digitales con recursos educativos etc. Respecto al software necesario se podría utilizar tanto un sistema operativo con licencia como puede ser Windows Server 2003 o posterior, o bien su alternativa dentro del software libre OpenSSL disponible en las distribuciones Linux.

Basándonos en esto, cada centro educativo podría convertirse en autoridad de certificación, generando de esta forma sus propios certificados. Además de la posibilidad de crear un anillo de confianza con otros centros u organismos públicos. Cada certificado podría tener un periodo de validez equivalente al curso académico. El empleo de estos certificados podría combinarse con otros proyectos,

- Sustituir el envío de mensajes sms a los padres notificando las faltas de asistencia o incidencias graves con la posibilidad de consultarlas de forma autónoma vía web con el consiguiente ahorro económico, (esta opción obligaría a tener una conexión a internet con lo que la sustitución sería solamente para aquellas personas con disponibilidad de la misma en sus hogares)
- Empleo de la plataforma moodle. Se podría gestionar el acceso a los recursos mediante los certificados en lugar de cuentas de usuario ahorrando el trabajo añadido que generan estas en su mantenimiento
- Emplear uso de foros, wikies limitando su acceso solamente a los alumnos del centro, o de una clase/curso concreto. Para ello debería ser el propio centro quien proporcionara la infraestructura adecuada para dar cabida a la creación de dichos recursos web apoyándose en el uso de certificados como mecanismo de seguridad.
- Fomento del uso de las nuevas TI entre los alumnos y educándolos en el uso correcto seguro de internet.
- Matriculación online de los alumnos
- Enseñar al alumno el uso de la firma digital y sus características.
- El sistema de certificados vendría a complementar el sistema actual gestión de cuentas de usuario pero no a sustituirlo ya que existirán casos en los que se añadiría una mayor complejidad en lugar de facilitar las cosas.

La implantación de un sistema de certificados, al igual que el resto de innovaciones en el plano de las TI involucrará dos fases, la primera de "Introducción" donde se asimilan los conceptos o hasta que existe un dominio instrumental de la materia y la fase 2 de "Aplicación" donde se descubren sus aplicaciones pedagógicas o de gestión para mejorar los aspectos docentes o administrativos del centro. Quizás la primera fase sea la más complicada necesitándose cierta formación para el profesorado involucrado. La segunda evolucionaría a medida surgieran necesidades o se encontrarán sinergias positivas con el resto de aplicaciones

## Bibliografía

Juan de Pablo Pons, Pilar Colás Bravo,Teresa Gonzalez Ramirez. "Factores facilitadores de la innovación TIC en los centros escolares.Un análisis comparativo entre diferentes políticas educativas autonómicas".*Revista de Educacion Nº 352 Mayo/Agosto 2010.*

Arturo Ribagorda Garnacho ."Sistema de Certificación:la firma y el certificado digital".*Parte de la obra Régimen jurídico de internet, 2001* .ISBN 84-9725-147-4

Jose Luis Morant Ramon ,Justo Sancho Rodriguez, Arturo Ribagorda Garnacho .”Seguridad y protección de la información“.*Ed Centro de Estudios Ramon Areces,1994.ISBN 84-8004-098-x*

SOCIEDAD DE LA INFORMACION

www.sociedadelainformacion.com

Edita:

Director: José Ángel Ruiz Felipe
Jefe de publicaciones: Antero Soria Luján
D.L.: AB 293-2001
ISSN: 1578-326x

1