FACULTAD
DE CIENCIAS
ECONÓMICAS

UNC Universidad
Nacional
de Córdoba

REPOSITORIO DIGITAL UNIVERSITARIO (RDU-UNC)

Criptografía y firma electrónica/digital en el aula

Marcelo Emilio Rocha Vargas, Ricardo Justo Castello,
Daniel Enrique Bollo

Ponencia presentada en IX Jornadas DUTI (Docentes Universitarios de Sistemas y Tecnologías de Información en Ciencias Económicas) realizado en 2014 en Facultad de Ciencias Económicas-Universidad Nacional de Catamarca. Catamarca, Argentina

Esta obra está bajo una Licencia Creative Commons Atribución – No Comercial – Sin Obra Derivada 4.0 Internacional

Título: Criptografía y Firma Electrónica/Digital en el Aula

Autores: Cr. Marcelo Emilio Rocha Vargas
Dr. Ricardo J. Castello
Cr. Daniel E. Bollo

Correos:mrocha@eco.unc.edu.ar
castello@eco.unc.edu.ar
dbollo@eco.unc.edu.ar

Institución: Facultad de Ciencias Económicas
Universidad Nacional de Córdoba

Categoría: Propuestas didácticas

Modalidad depresentación: Exposición

Palabras Clave: SEGURIDAD - PKI – CRIPTOGRAFIA - FIRMA DIGITAL

Universidad Nacional de Catamarca – Secretaría de Ciencia y Tecnología
Editorial Científica Universitaria
ISBN: 978-987-661-170-1

RESUMEN:

Por lo general, en las asignaturas relacionadas con TI, y dentro del amplio abanico de los temas relacionados a la Seguridad de la Información, se incluye el tratamiento/estudio de los sistemas de criptografía de clave pública y su relación con los conceptos de firma electrónica y sus diferencias con la firma digital, tal como se plantea en la Ley de Firma Digital Argentina.

La problemática es: ¿Cómo lograr que los alumnos aprendan estos temas avanzados? ¿Cómo lograr que entiendan su utilidad? ¿Cómo evitar que el tratamiento del tema sea puramente "teórico"?

La respuesta más sencilla es llevar los conceptos a la práctica, por ello el objetivo del presente trabajo, es compartir las metodologías, estrategias e ideas que hemos implementado para que los alumnos de la asignatura Tecnología de Información I, como complemento al desarrollo teórico de los temas de firma electrónica y digital, realicen el proceso de:

- Solicitud de certificado digital al docente que oficia las veces de "Oficial de Registro"
- Generación del par de claves publica/privada
- Recepción del Certificado Digital emitido por la PKI de la Facultad de Ciencias Económicas
- Utilización del Certificado Digital para "FIRMAR ELECTRONICAMENTE" el trabajo final que es requisito de acreditación para regularizar la asignatura.

ISBN: 978-987-661-170-1

Criptografía y Firma Electrónica/Digital en el Aula

Área temática: Pedagogía

1. Introducción

El objetivo del presente trabajo es contribuir con el estudio y utilización de herramientas que permitan una mejor aproximación y comprensión de los conceptos de SI/T.I que se desarrollan en las carreras de Ciencias Económicas.

Abordaremos dentro del marco de la Seguridad de la Información, el tema Criptografía y su interrelación con los conceptos de firma electrónica y sus diferencias con la firma digital, tal como se plantea en la Ley de Firma Digital Argentina, haciendo especial énfasis en las técnicas y herramientas que permitirán hacer menos abstracto y más asequibles los conceptos que conforman esta problemática, tanto a alumnos como a los mismos docentes encargados de los prácticos de la asignatura

2. Antecedentes

Dentro del tema “Administración de Recursos Informáticos”, el tratamiento de la Seguridad Informática va adquiriendo paulatinamente cada vez mayor relevancia, la realidad de las operaciones cotidianas en un entorno organizacional/corporativo cada vez más conectado, hacen que este tema deba ser analizado cada vez con mayor detalle.

Las necesidades de proteger los activos de información, de asegurar la trazabilidad de las operaciones, y auditabilidad de los sistemas de información, requieren que el Profesional de Ciencias Económicas, esté adecuadamente formado en conceptos y técnicas relativos a la seguridad de la información, es por esa razón que en el presente trabajo pretendemos compartir las herramientas y técnicas que se han implementado en la cátedra para el abordaje de algunos de estos temas.

Si bien desde hace tiempo, la Seguridad Informática y de la Información, han sido receptados como temas relevantes en la bibliografía de la Cátedra, es solo recientemente que fueron incorporándose por la vía de anexos, los temas de Criptografía, y Firma Digital, manteniéndonos en el plano “teórico”, con la consecuente problemática de lo abstracto de los temas.

Más recientemente y gracias a la participación de los autores del presente trabajo en sendos proyectos de investigación relacionados con la Auditoría de Autoridades Certificantes de la Infraestructura de Firma Digital de la RA, y la Aplicación de la Firma Digital en nuestra Universidad, es que se adquirieron las habilidades y conocimientos necesarios para poner en funcionamiento una PKI (Public Key Infrastructure)que se utiliza con fines didácticos para mostrar el funcionamiento de un esquema completo de firma digital.

3. Los desafíos

Los desafíos que enfrentamos pueden resumirse en un interrogante: ¿Cómo hacer operativa una infraestructura, que teniendo en cuenta lo establecido en la Ley 25.506/2001 de Firma Digital y su Decreto Reglamentario, permita tanto a alumnos

ISBN: 978-987-661-170-1

como a los mismos docentes, asimilar conceptos de seguridad avanzados relativos a la criptografía de clave pública?

Entonces, cuales son los interrogantes que debemos resolver?

- Qué es la Firma Digital?
- Qué es la Firma Electrónica?
- Cómo funcionan?
- Qué son y cómo funcionan las claves simétricas?
- Qué son las claves públicas y las claves privadas?
- Qué son y para qué sirven las funciones de “hash” o resumen?
- Qué son los certificados digitales? Se ajustan a algún estándar?
- Cuál es el contenido de un certificado digital?
- Qué valor legal tiene la Firma Digital?
- Cuáles son los elementos necesarios para construir una Infraestructura de Clave Pública (PKI)?
- Existen las herramientas de software que permitan implementar una infraestructura de PKI funcional?
- Con qué criterios se hará la selección?
- ETC-

4. Consideraciones generales

Una firma digital (o el esquema de firma digital) es un sistema matemático para demostrar la autenticidad e integridad de un mensaje o documento digital. Una firma digital válida da una razón al destinatario a creer que el mensaje fue creado por un remitente conocido, y que no fue alterado durante la transmisión. [1]

Cuando hablamos de firma digital en realidad nos estamos refiriendo a muchos conceptosrelacionados, entre los cuales figuran documentos electrónicos, claves criptográficas,certificados digitales, funciones matemáticas, funciones de hash, autoridades certificantes, autoridades de registro, infraestructuras de clave pública y muchos otros conceptos que pueden resultarnos desconocidos o complicados, en especial para aquellos que recién se aproximan al tema. [2]

Por lo expuesto comenzaremos poniendo en claro aquellos conceptos fundamentales que luego nos permitirán comprender y poner en práctica lo que establece la legislación de nuestro país en relación a la “firma digital” y la infraestructura de clave pública.

5. Algunos conceptos criptográficos básicos

Desde antaño ha existido la necesidad de proteger y ocultar la información de aquellos que no están autorizados a acceder a la misma.

Así entre otras, podemos citar a las comunicaciones militares, diplomáticas, comerciales y tantos otros ejemplos que la lista sería interminable.

ISBN: 978-987-661-170-1

La necesidad de “obscurecer” el contenido de un mensaje a los ojos de un extraño, la de garantizar que el mensaje no fue alterado en el camino, o tan simple como garantizar que el mensaje proviene de donde “dice provenir”, es decir que el remitente del mensaje sea quien realmente dice ser, dieron origen a un conjunto de técnicas de fuerte base matemática que han permitido ir resolviendo, cada vez con mayor grado de éxito, las necesidades de proteger un mensaje.

Es así que tradicionalmente se ha definido a la “Criptografía” como el arte y la ciencia deocultar el contenido de un mensaje de forma tal que sólo puedan acceder a élobservadores autorizados.

El mensaje o texto a ocultar por lo general se denomina texto claro.

El proceso por el cual se lo oculta es el “cifrado”, y el resultado que se obtiene esel texto cifrado.

El proceso de transformar nuevamente el texto cifrado en textoclaro se llama “descifrado”.

Si consideramos que existen aplicaciones de la criptografía que no implican ocultamiento de un mensaje, tales como las funciones de hash o los mecanismos de firma digital podemos redefinir la “Criptografía” como el estudio de las técnicas matemáticas relacionadas con aspectos de seguridad de la información tales como la confidencialidad, integridad y autenticación, tanto de entidades como de origen de los datos. [3]

En resumen, mediante la criptografía o mejor dicho, gracias a sus técnicas podremos proteger las siguientes propiedades de la información:

- Confidencialidad: es decir que la información/mensaje sólo es accesible por quien está autorizado a verlo.
- Integridad: esta propiedad, garantiza que la información/mensaje no ha sido alterado, es decir garantiza la exactitud y completitud de la información.
- Autenticación: esta propiedad permite verificar la identidad del emisor del mensaje.

Y cuando la aplicación de estas técnicas y procedimientos se hacen de acuerdo a lo establecido en nuestra legislación de firma digital, podemos agregar:

- No repudio: esta propiedad significa que cuando un mensaje se encuentra firmado digitalmente, el “firmante” NO puede desconocerlo (repudiarlo).

Al plantearse la necesidad de cifrar un determinado mensaje, implica que existe alguien no autorizado que desea acceder a su contenido, y que por lo tanto puede tratar de violar o “romper” el cifrado. El arte de romper el cifrado, se denomina “Criptoanálisis”, y a sus practicantes se los conoce como “criptoanalistas”[4]

5.1Algoritmos de cifrado

Primeramente dejaremos en claro, que no pretendemos extendernos en el desarrollo del tema, ya que la complejidad del mismo excede con mucho el alcance no sólo de este trabajo, si no el de los conceptos que deseamos transmitir, que son los mínimos necesarios para comprender las bases conceptuales de la firma digital.

ISBN: 978-987-661-170-1

Así decíamos que el cifrado es el proceso de convertir un mensaje, o texto claro, en un texto cifrado, y que el descifrado es el proceso inverso.

Un aspecto muy importante a tener en cuenta, es que un buen sistema de cifrado debería basar su seguridad en la clave, y no en el algoritmo en sí mismo, es decir que para un potencial atacante, no debería ser de ninguna ayuda conocer el algoritmo de cifrado, esta información sólo sería relevante para el caso de conocer la clave.

Veamos algo de notación, si con M representamos el texto claro, o mensaje, y con C al texto cifrado. Entonces una función de cifrado E, operando sobre M produce C.

$$E(M) = C$$

Si sobre C aplicamos la función de descifrado D, obtenemos nuevamente M.

$$D(C) = M$$

Es decir, se debe verificar que

$$D(E(M)) = M$$

La función matemática que se utiliza para el cifrado y descifrado (a veces es una misma función, y a veces se trata de dos funciones relacionadas) se denomina algoritmo de cifrado, o simplemente cifrado.

Ahora bien, contar con un algoritmo de cifrado no es suficiente para resolver el problema, por lo general es necesario asociarlo a alguna “clave” que podremos denotar como “K”, y cuyos valores pueden variar dentro de un amplio rango, que comúnmente se denomina “espacio de claves”.

Así, si la clave de cifrado/descifrado es la misma, podemos completar la notación como sigue:

$$E_K(M) = C$$
$$D_K(C) = M$$
$$D_K(E_K(M)) = M$$

Y para el caso de que la clave de cifrado fuera diferente a la de descifrado, denotaríamos:

$$E_{KA}(M) = C$$
$$D_{KB}(C) = M$$
$$D_{KB}(E_{KA}(M)) = M$$

ISBN: 978-987-661-170-1

5.2 Clasificación de los algoritmos de cifrado

Es posible clasificar los algoritmos de cifrado de acuerdo a distintos criterios:

- Según la clave:
  - De clave simétrica
  - De clave asimétrica
- Según la operación:
  - Sustitución
  - Transposición
  - Producto
- Según la unidad sobre la que se aplican:
  - De bloque
  - De flujo

A nuestros fines, nos interesan particularmente los **algoritmos según la clave**.

5.2.1Algoritmos de clave simétrica

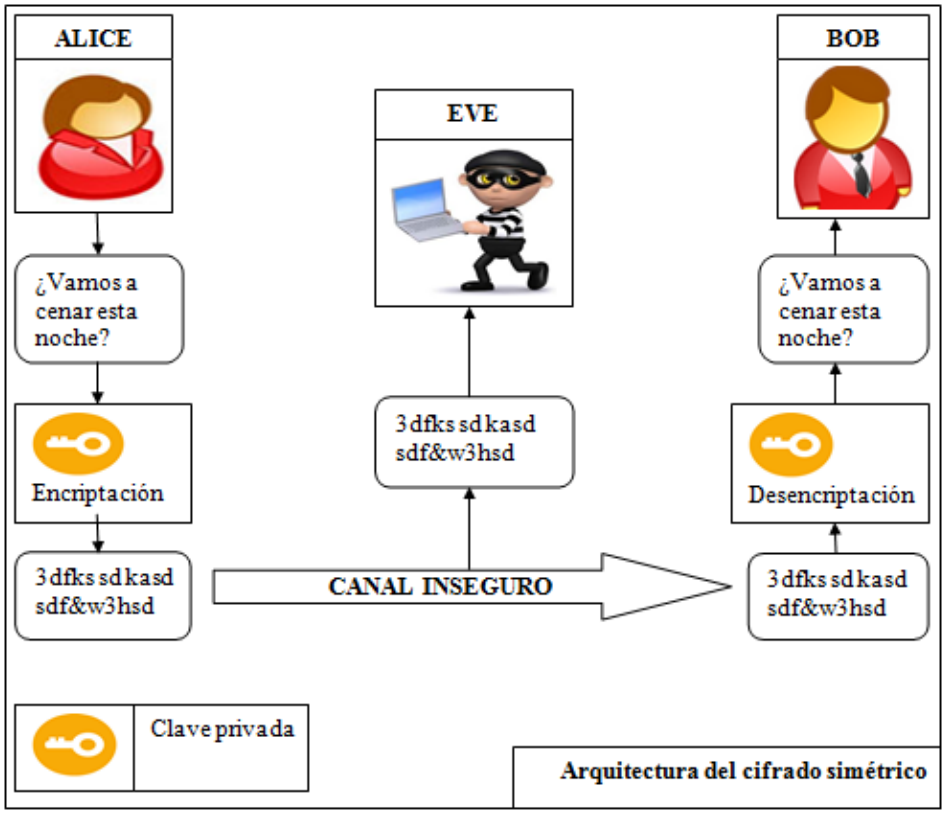
Los algoritmos simétricos, también llamados convencionales, de clave única o de clave secreta son algoritmos en los que la clave de descifrado puede ser deducida de la clave de cifrado, y viceversa. La seguridad de estos algoritmos se basa en el carácter secreto de la clave, que debe ser conocida solo por el emisor y el receptor.

Para ilustrar, algunos ejemplos de algoritmos de clave simétrica:

- AES
- DES
- IDEA
- 3DES
- Blowfish

Sin ahondar en los detalles técnicos, diremos que si bien los mecanismos que utilizan claves simétricas, son rápidos y seguros, presentan una debilidad y es que al utilizarse una única clave para las operaciones de cifrado/descifrado, la misma debe ser conocida por quienes se comunican, esto significa que en algún momento la clave, que debe ser secreta, debe ser intercambiada (comunicada) y eso la hace pasible de intercepción, con lo que un potencial atacante (en la figura sería EVE) que lograra apoderarse de la clave, podría además de leer los mensajes que intercambian BOB y ALICE, alterar el contenido del mismo, ya que conoce la clave, y solo le resta conocer que algoritmo se utilizó.

ISBN: 978-987-661-170-1



5.2.2 Algoritmos de clave asimétrica

En los algoritmos de clave **asimétrica**, a diferencia de los anteriores, se utilizan claves de cifrado y descifrado diferentes, y tienen la característica de que no puede calcularse o derivarse una clave de la otra, y que conforman un par fuertemente vinculado.

Esta característica, hace posible que la clave de cifrado se difunda, es decir se haga pública, de allí que estos algoritmos también se conozcan como de "clave pública", como ya se puede advertir, también se elimina la necesidad de intercambiar claves "secretas", que como hemos visto, era necesario cuando se utilizan mecanismos de clave simétrica.

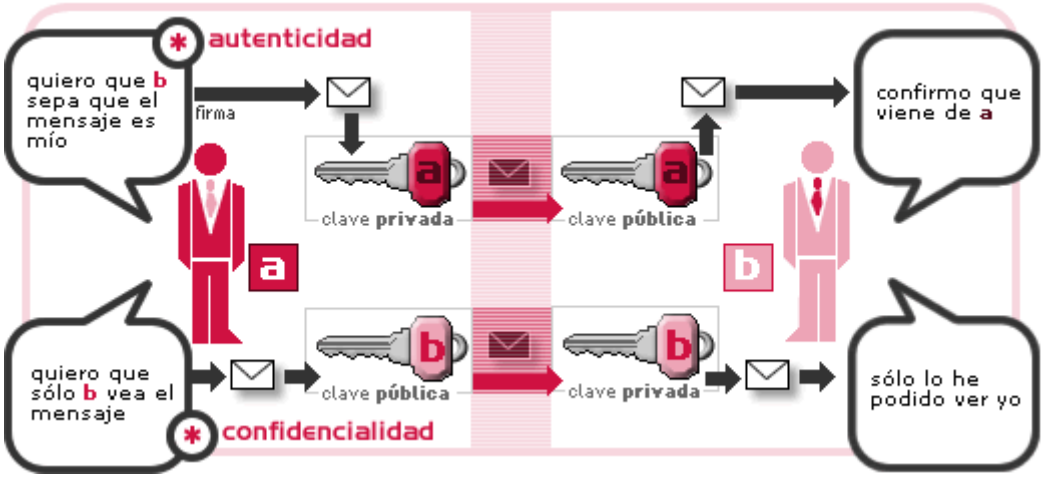
Entonces, cuando alguien desea enviar un mensaje en forma confidencial, lo cifra con la clave pública del destinatario teniendo la seguridad que sólo este último será capaz de descifrarlo ya que solo él conoce la clave privada asociada con la clave pública que se utilizó para cifrar el mensaje.

Estos algoritmos, tienen la propiedad de que lo que se cifra utilizando la clave privada, se descifra con la correspondiente clave pública, y viceversa, entonces cabe preguntarnos…¿qué utilidad tiene este mecanismo si cualquiera puede descifrar ?

La respuesta a este interrogante es de particular utilidad, ya que los mensajes así cifrados, sólo pudieron haber sido generados por aquel que posee la clave privada asociada a la clave pública, así…casi sin darnos cuenta, hemos logrado un mecanismo de "autenticación", ya que cualquier persona que posea la clave pública podrá verificar la identidad del emisor, por otra parte como sólo el emisor posee la

ISBN: 978-987-661-170-1

clave privada, no puede negarhaber emitido el mensaje, es decir que también estamos consiguiendo un mecanismo de "**no repudio**".



Fuente: http://www.geocities.ws/daniel.infante/fase3/llave.gif

Como vemos, paso a paso, valiéndonos de las funcionalidades que nos proveen estos mecanismos, vamos consiguiendo las diferentes propiedades que son requeridas para implementar "firma digital".

Entonces para lograr las propiedades de "**confidencialidad**", "**autenticidad**" y "**no repudio**", el emisor debe cifrar el mensaje con su clave privada y con la clave pública del destinatario.

De esta forma, se sabe que sólo el verdadero destinatario puede leerlo, y éste sabe que sólo el emisor pudo haberlo generado.

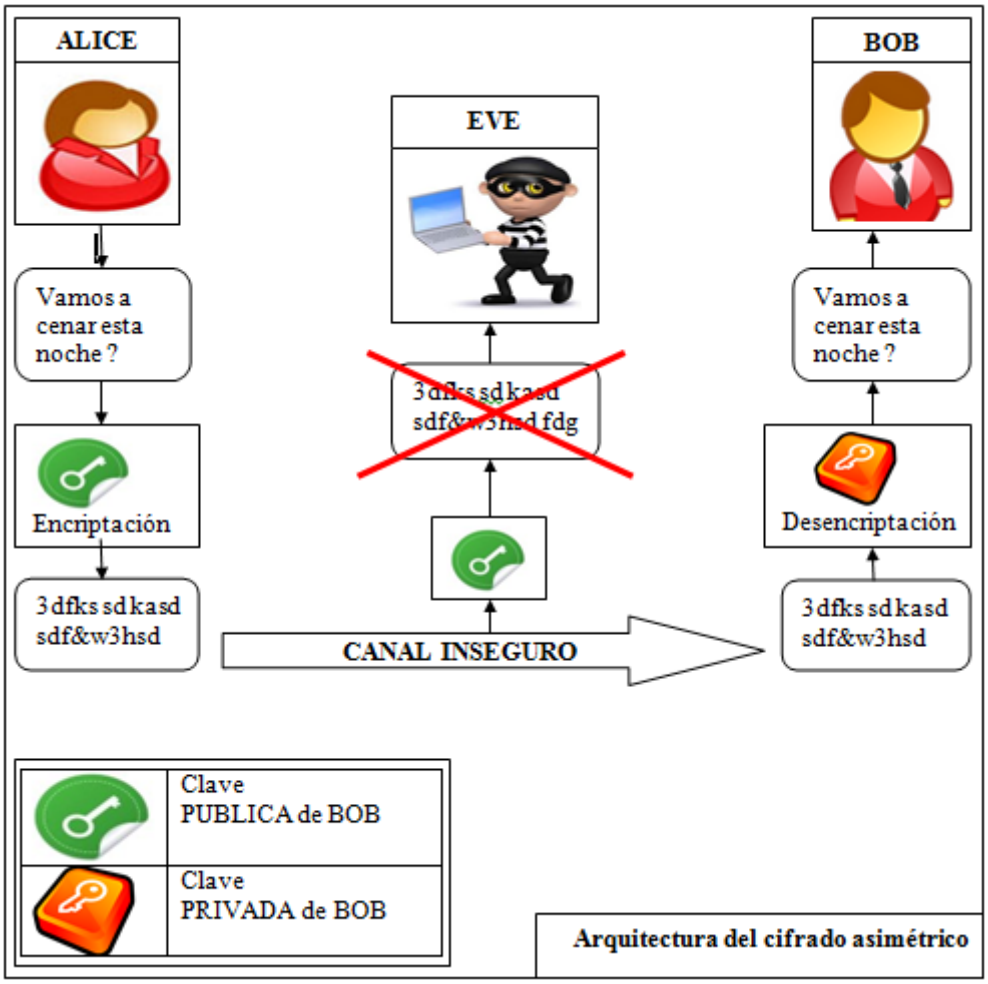
Los ejemplos más típicos de cifrados de clave pública son:

- RSA
- ElGamal
- DSA (Digital Signature Algorithms)

Veamos un ejemplo en el gráfico siguiente:

ALICE desea enviar un mensaje a BOB, y que el mismo permanezca confidencial, para ello utiliza la clave pública de BOB para encriptar el mensaje y poder transmitirlo por un canal inseguro, EVE captura el mensaje pero NO puede descifrarlo, ya que el único que posee la clave capaz de desencriptar el mensaje es BOB, que tiene la clave privada asociada a la clave pública utilizada por ALICE para cifrar el mensaje.

ISBN: 978-987-661-170-1



6. FUNCIONES DE HASH

Una función de hash H(M) también llamada función resumen, es una funciónque opera sobre un mensaje M de longitud arbitraria, y produce una salida hde longitud fija.

$$h = H(M)$$

Una buena función de hash, en general reúne una serie de propiedades, a modo de ejemplo citaremos algunas:

- Las funciones de hash, no tienen “inversa”, es decir que dado un hash no existe forma de poder recuperar algo del texto claro original, es decir la función de hash no es reversible
- Dado un mensaje M, es muy difícil encontrar otro mensaje M’, tal que H(M) = H(M’)
- No es factible encontrar o descubrir texto claro, que verifique un valor de hash específico.
  Es decir dado h, es difícil encontrar un M tal que H(M) = h
- Un cambio en un bit del texto claro, debería traducirse en un cambio de al menos el 50% en el hash resultante.

ISBN: 978-987-661-170-1

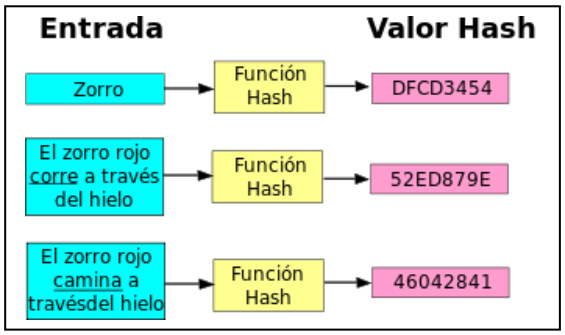
- ETC.

Ahora bien, en que me ayuda conocer sobre las funciones de hash y sus propiedades?

La respuesta podemos encontrarla en las propiedades mismas de una buena función de hash, las que me van a permitir garantizar la "**integridad"** de un mensaje, con lo que al combinar funciones de hash y cifrados asimétricos, estamos conformando el escenario necesario para poder "firmar digitalmente" un mensaje.

Algunos ejemplos de funciones de hash:

- MD5
- SHA1
- MD4



Fuente : http://commons.wikimedia.org/wiki/File:Hash_function2-es.svg

7. FIRMA DIGITAL Y FIRMA ELECTRONICA

En la República Argentina la Ley Nº 25.506 y sus normas reglamentarias, el Decreto Nº2628/02 y la Decisión Administrativa N° 06/2007, regulan la aplicación de la Firma Digital.

De acuerdo al artículo 2° de la LFD

"*Se entiende por **firma digital** al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.*

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes."

A su vez, respecto de la firma electrónica, el artículo 5° de la citada ley, nos dice:

"*Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez*."

ISBN: 978-987-661-170-1

De estos textos se desprende el valor legal de la Firma Digital vs F.Electrónica:

- La firma digital, tiene una presunción “iuris tantum” a su favor, ya que si el firmante pretende desconocerla, la prueba corre a su cargo
- La falta u omisión de alguno de los requisitos que establece la ley tiene como inmediata implicancia la inversión de la carga de la prueba, ya que se trata de firma electrónica.

Actualmente la infraestructura de Firma Digital de la República Argentina dispone de tres Autoridades Certificantes (AC) estatales autorizadas (ANSES, AFIP y la Oficina Nacional de Tecnologías de Información-ONTI) y una privada (Encode). Las primeras están autorizadas a emitir certificados digitales para agentes y funcionarios del Sector Público. La segunda está autorizada a emitir certificados para entidades privadas. Dichas Autoridades Certificantes, en especial ONTI, tienen como misión vincularse con distintos organismos de la Administración Central y organismos descentralizados así como Gobiernos y Poderes Judiciales de las Provincias, para difundir la aplicación de la Firma Digital en la Tramitación Electrónica de Expedientes. Esta acción es llevada a cabo por la AC ONTI a través de la creación de Autoridades de Registro (AR) en los distintos organismos que pretenden comenzar a usar su infraestructura de firma digital.

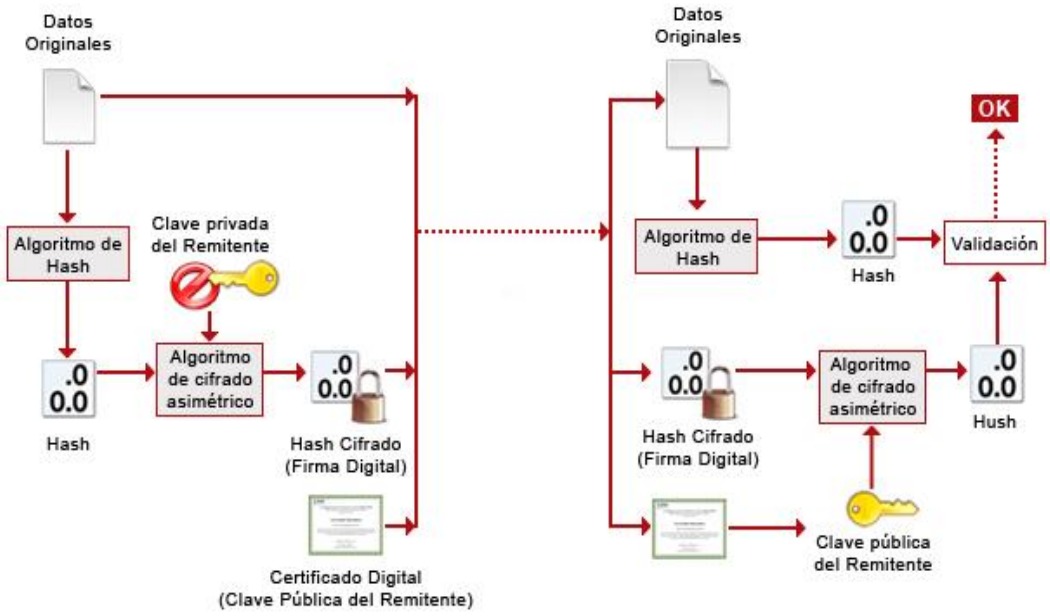
7.1¿Cómo funciona?

La firma digital funciona utilizando procedimientos matemáticos que relacionan el documentofirmado con información propia del firmante, y permiten que terceras partes puedan reconocerla identidad del firmante y asegurarse de que los contenidos no han sido modificados.

El firmante genera, mediante una función matemática, una “huella digital” del mensaje, la cualse cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, quese enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento unamarca que es única para dicho documento y que sólo él es capaz de producir.

Para realizar la verificación del mensaje, en primer término el receptor generará la huella digitaldel mensaje recibido, luego descifrará la firma digital del mensaje utilizando la clave pública delfirmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellasdigitales coinciden, significa que no hubo alteración y que el firmante es quien dice serlo.

ISBN: 978-987-661-170-1



Fuente: http://www.inteco.es/extfrontinteco/img/dnie/contenido_esquema1.jpg

8. ¿Qué son y qué contienen los certificados digitales?

Los certificados digitales son documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

En su forma más simple, el certificado contiene una clave pública y un nombre. Habitualmente, también contiene una fecha de expiración, el nombre de la Autoridad Certificante que la emitió, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del mismo. Su formato está definido por el estándar internacional ITU-T X.509. De esta forma, puede ser leído o escrito por cualquier aplicación que cumpla con el mencionado estándar.

Estructura de un Certificado X.509

CERTIFICADO DIGITAL
Versión del Certificado
N° de Serie
Id. Algoritmo de la firma
Autoridad Certificante (AC)
Período de validez
Usuario
Clave pública del usuario
Id de la CA
Extensiones

La firma se genera aplicando la función de cifrado a estos parámetros

Reseña (Hash) encriptada utilizando la clave privada de la CA

Firma digital de la AC

ISBN: 978-987-661-170-1

9. La implementación

De acuerdo a lo desarrollado, vemos que es necesario montar una PKI, que emule las funciones básicas de una infraestructura de firma digital, con el objetivo de que los alumnos firmen “digitalmente” el trabajo final que es uno de los requisitos de acreditación de la asignatura.

¿Existe software que permita hacerlo? ¿Son productos propietarios o de Software Libre? ¿Cómo evaluarlos?

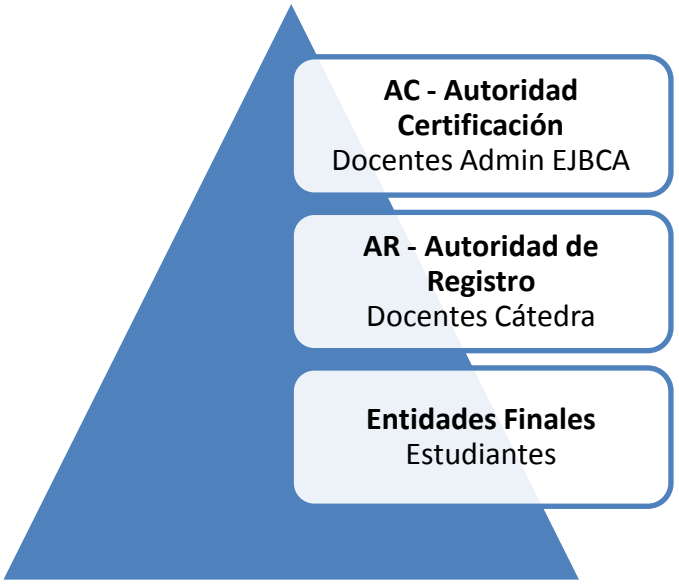
Bien, en nuestro caso, las respuestas a estos interrogantes se resolvieron gracias al aporte técnico de los ingenieros que participaron en los proyectos de investigación relacionados a firma digital que estamos llevando adelante. El carácter interdisciplinar de los mismos, nos ha permitido incorporar conocimientos técnicos avanzados que nos posibilitan brindar a nuestros alumnos una PKI de uso académico adaptada a nuestras necesidades.

El producto seleccionado fue EJBCA PKI BY PRIMEKEY, es software libre y de su larga lista de prestaciones, podemos destacar:

- Sigue el X509 y PKIX (RFC5280)
- Soporte de algoritmos RSA , y DSA entre otros
- Funciones de hash SHA-1, SHA-2, etc.
- Soporte de HSM (Hardware Security Modules)
- Gestión de Listas de Revocación de Certificados
- Administración y acceso Web diferenciado entre funciones de usuario y administradores.

El mismo se encuentra disponible en: http://www.ejbca.org/, con manuales de uso y guías de instalación detalladas, además de profusa documentación.

Solucionado el aspecto técnico de nuestra PKI, la estructura administrativa de la misma sería:

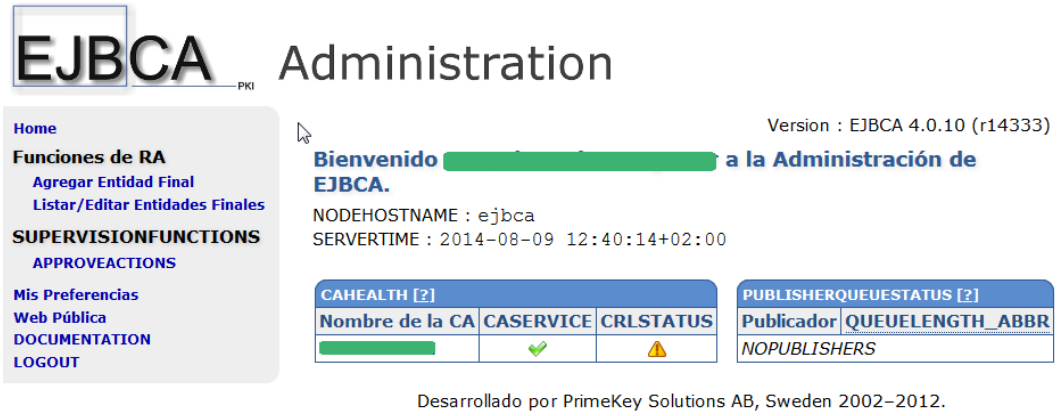


ISBN: 978-987-661-170-1

Ahora bien, como puede observarse, todos los integrantes de la jerarquía deben tener un certificado digital que les permita desempeñar su rol específico:

- En el nivel superior, los docentes administradores de la AC deben poseer un certificado digital que les permita emitir un certificado a aquellos docentes que desempeñarán el rol de Autoridad de Registro.
- Los docentes que ofician el rol de Autoridad de Registro deben a su vez emitir certificados digitales a los alumnos, para su rol de entidades finales.
- Las entidades finales, en este caso los alumnos, utilizarán los certificados digitales para firmar "digitalmente" los trabajos y monografías que solicita la Cátedra.

Aquí podemos ver la entrada administrativa a la PKI, para el rol de Autoridad de Registro:

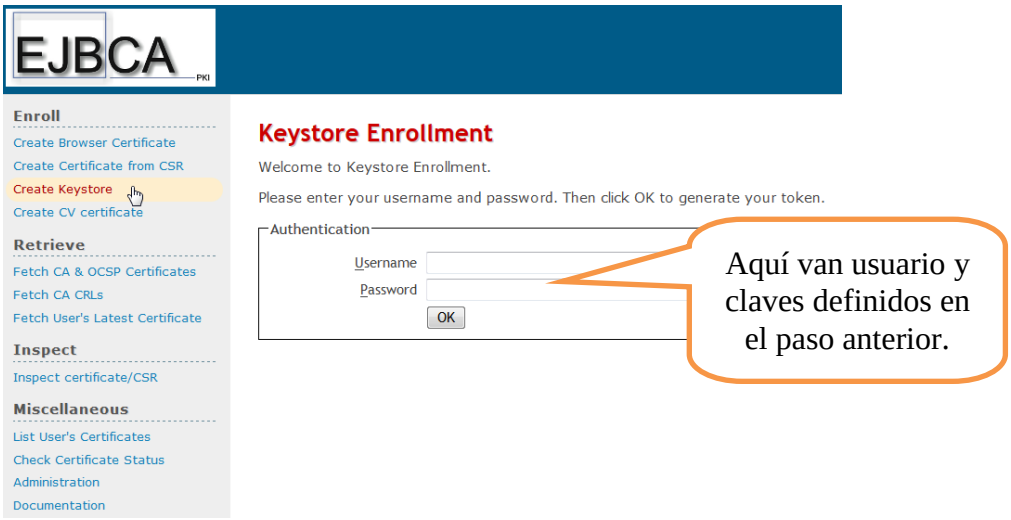


Y así luce al momento en que el docente, registra a un alumno como entidad final, que es el primer paso en el proceso de emisión del certificado.

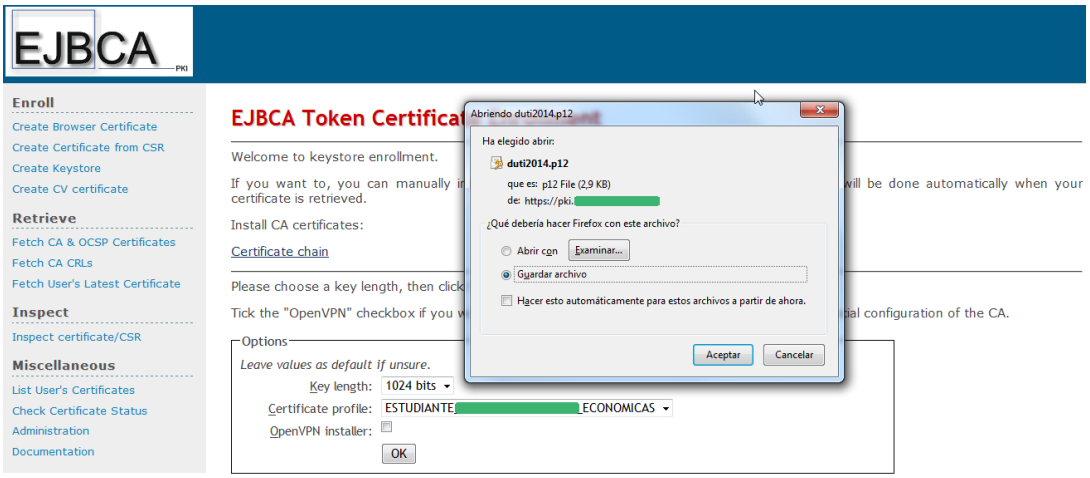
ISBN: 978-987-661-170-1

En el paso anterior, el Docente explica al alumno que en un caso “real” el “Oficial de Registro”, verifica los datos y documentación para asegurarse de la identidad y cargos del solicitante del certificado digital.

Falta ahora, que la “entidad final” en este caso el Alumno, “retire” su certificado, esto puede verse en la siguiente pantalla:



Y a continuación, el sistema PKI emite el certificado, en nuestro caso hemos configurado que se emita en formato .P12 para facilitar su utilización en un “token” simulado.



Como se observa, el sistema nos ofrece guardar el certificado generado. La pregunta a responder es donde lo guardamos? y luego como lo usamos? En este paso el docente explica que según lo establecido por la ONTI, para almacenar el certificado es necesario contar con un dispositivo criptográfico denominado “TOKEN”, el cual debe cumplir con avanzados estándares de seguridad (FIPS-140).

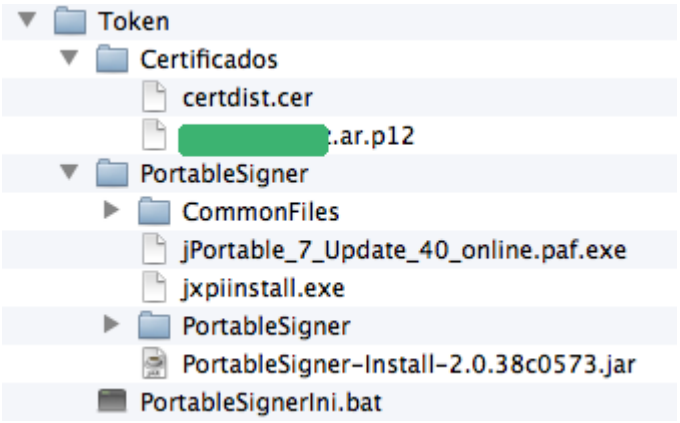
Ya que no es práctico proveer de tokens criptográficos a los alumnos, y mucho menos requerir que estos los adquieran, es que la Cátedra implementó la idea de “token virtual”, basado en la utilización de un pendrive, se almacenará en el mismo,

ISBN: 978-987-661-170-1

además del certificado del alumno, el certificado correspondiente a la AC, que luego permitirá verificar la firma digital y verificar la cadena de confianza correspondiente, también se almacenarán los programas necesarios para firmar archivos pdf.

10. Token Virtual, firma de archivos PDF

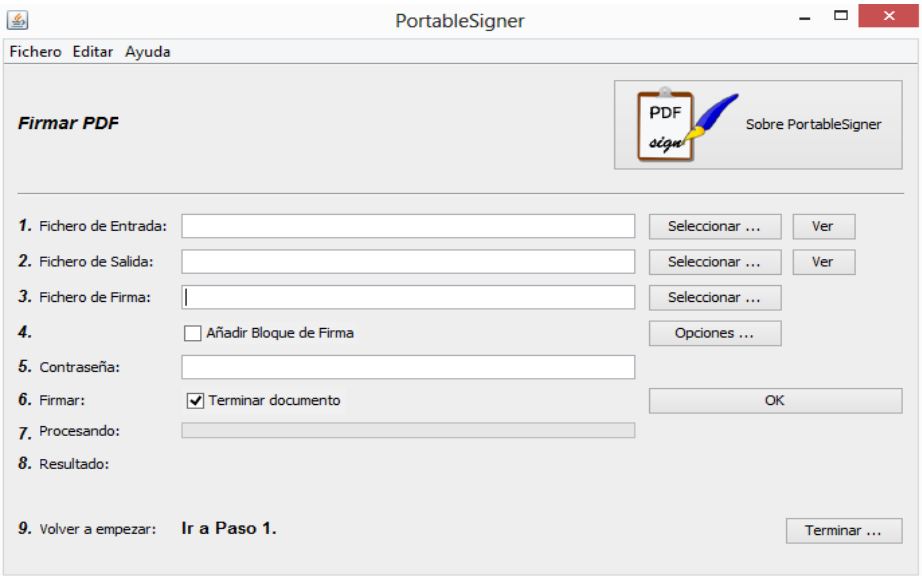
En el pendrive que posee el alumno, se graba el siguiente contenido:



Como se observa, se utiliza el software "PortableSigner" en su versión portable,y al lanzarlo mediante la ejecución del archivo de proceso por lotes: PortableSigerini.bat, cuyo contenido es:

```
@echo off
PortableSigner\CommonFiles\Java\bin\java -jar  PortableSigner\PortableSigner\PortableSigner.jar
```

Tenemos la posibilidad de firmar digitalmente documentos PDF, aquí una muestra del software en acción:



ISBN: 978-987-661-170-1

Los pasos a seguir:

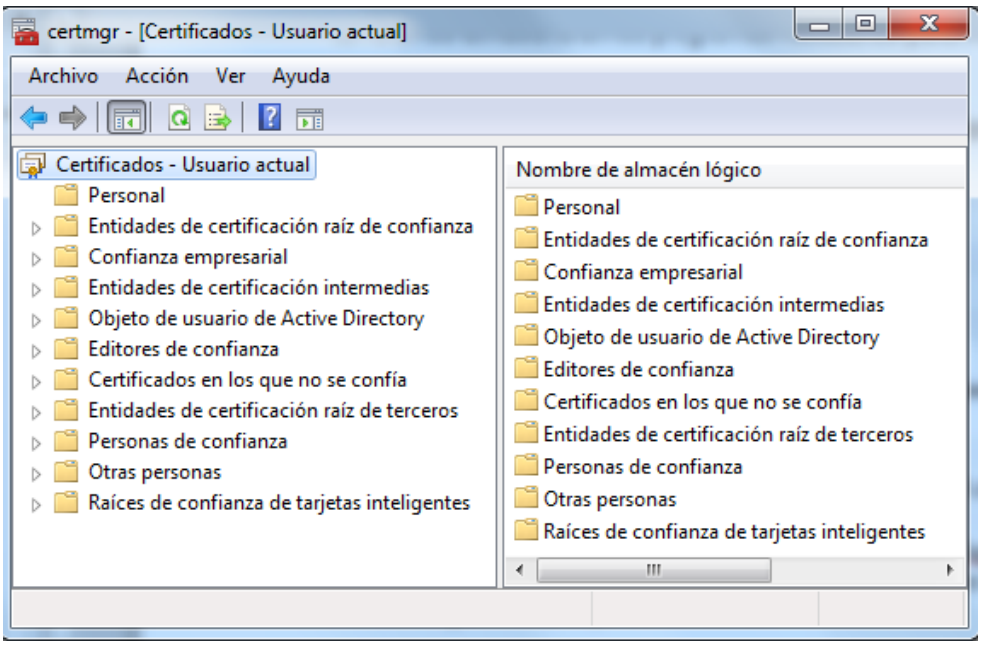
a. Fichero de entrada: Seleccionar archivo a firmar
b. Fichero de salida: Por defecto, creará un archivo firmado en la misma carpeta
c. Fichero de firma: Seleccionar el certificado digital personal
d. Marcar “Añadir bloque de firma”
e. Contraseña: Ingresar el password del certificado
f. Firmar: Clic en OK.

Cabe aclarar que si bien existe una gran variedad de aplicaciones que permiten firmar digitalmente documentos, se eligió PortableSigner en virtud que al almacenarlo en un pendrive junto a los certificados digitales, permite emular la utilización de un token criptográfico.

10.1 Verificación de la firma digital

Esta operación merece un párrafo aparte, ya que el proceso depende de las características de la herramienta que se utilice.

Sin pretender extendernos sobre el tema, diremos que algunas aplicaciones leen el almacén de certificados digitales de Windows, los que se gestionan con la herramienta “certmgr.msc”.

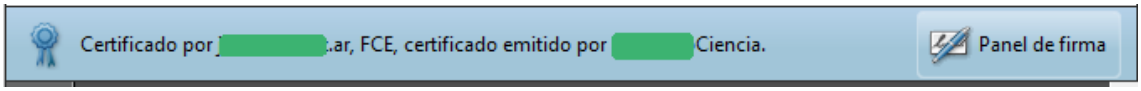


Otros, por el contrario utilizan su propio almacén de certificados digitales, un caso típico de estas últimas es Acrobat Reader.

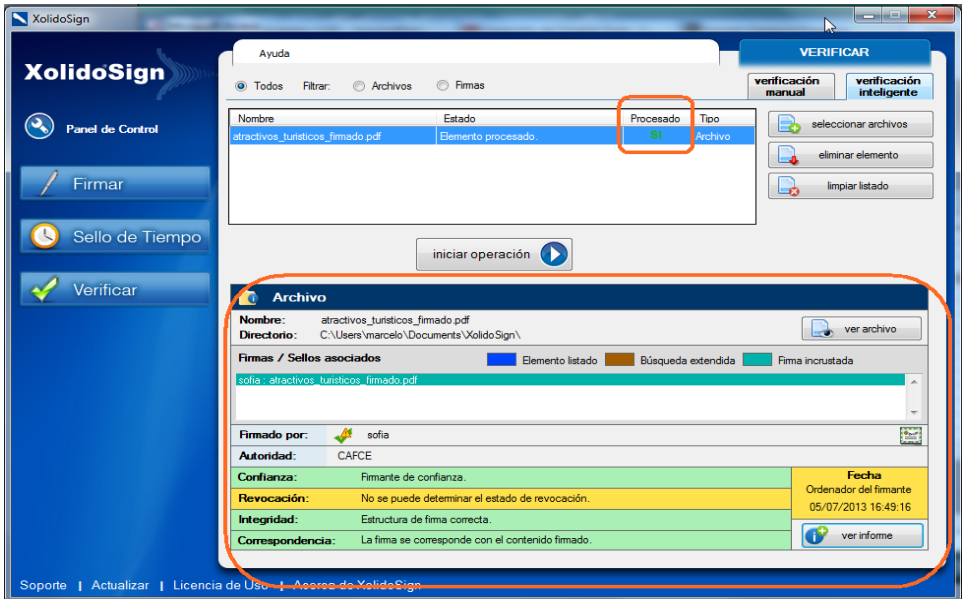
La importancia de conocer estos detalles, radica en que de la adecuada gestión de los certificados, dependerá que se verifiquen correctamente las cadenas de confianza de toda la PKI.

ISBN: 978-987-661-170-1

A modo de ejemplo, un documento PDF con firma digital verificada, al ser leído con Acrobat Reader luciría debajo de la barra de herramientas, un aviso como el siguiente:



Ejemplo de validación con la aplicación XolidoSign:



11. Conclusiones

Teniendo en cuenta la complejidad de los conceptos necesarios para comprender el tema de “Firma Digital”, entendemos que al haber logrado poner en producción una PKI académica cuyo funcionamiento nos ha permitido que tanto docentes, como alumnos participen desempeñando los diferentes roles que involucra el funcionamiento de una infraestructura de firma digital, constituye un importante logro toda vez que los conceptos dejan de ser abstractos y pasan a ponerse en práctica, lo que favorece su apropiación por parte de los alumnos, las definiciones plasmadas en la Ley de Firma Digital, dejan de ser solo letra que se olvida fácilmente, pasan a ser conceptos incorporados fuertemente gracias a haberlos puesto en práctica, en definitiva, tal vez el alumno pueda olvidar “los detalles”, pero los conceptos fundamentales perdurarán.

12. Referencias Bibliográficas

[1] http://en.wikipedia.org.es.mk.gd/wiki/Digital_signature 11/08/2011
[2] http://www.mpd.gov.ar/articulo/index/articulo/firma-digital-280 11/08/2011
[3] Alfred J. Menezes, Paul C. van Oorschot, y Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, http://www.cacr.math.uwaterloo.ca/hac/, 1996.
[4] Bruce Schneier. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition. John Wiley & Sons, Inc., 1996.

ISBN: 978-987-661-170-1