

Autoría y confianza
DNle, Firma electrónica y certificación electrónica
Phishing

Raúl Jiménez Ortega - www.rauljimenez.info



Reconocimiento - NoComercial - CompartirIgual (by-nc-sa):

No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

Índice de contenido

Autoría y confianza.....	3
El DNI electrónico.....	4
¿Qué es y para qué sirve el DNI electrónico?.....	4
¿Qué contiene el chip?.....	4
Certificado de la Autoridad de Certificación expedidora.....	4
Certificado de componente.....	4
Certificado de autenticación.....	5
Certificado de firma electrónica reconocida.....	5
¿Qué ventajas ofrece?.....	5
La firma electrónica.....	6
¿Qué es la firma electrónica?.....	6
¿Cómo funciona la firma digital?	7
Cifrado.....	7
Comprobación de una firma digital.....	8
Certificado digital.....	8
¿Qué es un certificado digital?.....	8
¿Qué contiene un certificado digital?.....	8
¿Cuántos tipos de certificados existen?.....	9
¿Cuántos certificados puedo poseer?.....	10
El phishing.....	10
Fuentes:.....	11

Caperucita roja y el lobo feroz

La niña se acercó a la cama y vio que su abuela estaba muy cambiada.

- *Abuelita, abuelita, ¡qué ojos más grandes tienes!*

- Son para verte mejor- dijo el lobo tratando de imitar la voz de la abuela.

- *Abuelita, abuelita, ¡qué orejas más grandes tienes!*

- Son para oírte mejor- siguió diciendo el lobo.

- *Abuelita, abuelita, ¡qué dientes más grandes tienes!*

- Son para...¡comerte mejooooor!- y diciendo esto, el lobo

malvado se abalanzó sobre la niña y la devoró, lo mismo que había hecho con la abuelita.



Imagen y texto extraído de: www.conciencia-animal.cl

Este famoso cuento de hadas popular ha sido utilizado durante con el objetivo de enseñarle a los niños a desconfiar de los extraños, y que en el mundo de las comunicaciones telemáticas se podría traducir por: “*hay que tener los ojos bien abiertos cuando navegamos por la red*”. No podemos ser tan inocentes de creernos todo lo que vemos y tenemos que mantener siempre los ojos bien abiertos, cuestionándonos si quien se comunica con nosotros es quien dice ser, y si lo que dice es verdad.

Autoría y confianza

Internet a pasado a formar parte de nuestras vidas en un corto plazo de tiempo, apareció de la nada y sin darnos cuenta se ha establecido como uno de los medios líderes en las comunicaciones, ocio y negocios.

Es por ello que todo o casi todo lo que hacemos en el mundo físico también se puede hacer en Internet; hablar, escribir, intercambiar información, cotillear, comprar, vender, jugar, “viajar”, ... pero también se ha abierto una puerta a los delincuentes, conocidos como ciber-delincuentes para: robar, engañar, atacar, suplantar, falsificar, etc. debido a que en las relaciones por Internet las personas no se encuentran físicamente en el mismo sitio, se ha propiciado que aumenten este tipo de actos dolosos¹.

Pero sin duda alguna, Internet también ha aportado cosas buenas, a hecho añicos las fronteras que nos impedían compartir públicamente conocimientos, sentimientos, ideas,

1 Dolo implica la voluntad maliciosa de engañar a alguien o de incumplir una obligación contraída

etc. lo que ha permitido el desarrollo de una forma de relacionarse y a la forma de hacer negocios, etc. En definitiva un desarrollo global hasta entonces inimaginable.

Por tanto, y para evitar que esta herramienta que ha sido puesta en manos de millones de personas pierda su eficacia debido al miedo y a la falta de confianza, los gobiernos, empresas e instituciones están tomando medidas que nos permitan saber, con total garantía, qué hacemos en cada momento y con quien lo hacemos.

El DNI electrónico

¿Qué es y para qué sirve el DNI electrónico?

Concretamente en España desde 2006 se comienza a expedir el Documento Nacional de Identidad electrónico (DNLe) para aumentar la confianza de los ciudadanos en las comunicaciones telemáticas.

El DNLe permite otorgar identidad personal a los ciudadanos para su uso en la nueva Sociedad de la Información, siendo la adaptación del tradicional DNI a la nueva realidad de una sociedad interconectada por redes de computadores.

De modo que nos permite acreditar nuestra identidad, además de asegurar la procedencia y la integridad de los mensajes intercambiados en las comunicaciones electrónicas.

¿Qué contiene el chip?

Dentro del chip del DNLe se encuentran 4 certificados que son el principal objetivo de nuestro estudio; además contiene otros datos como: apellidos, nombre, sexo, nacionalidad, fecha de nacimiento, fecha de validez, NIF, etc.

El DNI electrónico no contiene información relativa a datos personales distintos a los que aparecen impresos en la superficie de la tarjeta.

Certificado de la Autoridad de Certificación expedidora

En caso del DNI electrónico encontraremos el certificado con la clave pública de la Dirección General de la Policía. Se encuentra en la zona pública de chip que será accesible sin restricciones.

Certificado de componente

Certificado X.509 que permite la autenticación (*ContentCommitment o clave RSA pública y privada de no repudio*) de la tarjeta de DNI electrónico. Lo que permite el

establecimiento de un canal de comunicación seguro (cifrado y autenticado) entre la tarjeta del DNIe y el ordenador. También se encuentra en la zona pública de chip

Certificado de autenticación

El certificado X.509 de ciudadano de autenticación o *Digital Signature*, permite al titular acreditar su identidad frente a cualquiera, demostrando la posesión y el acceso a la clave privada asociada a dicho certificado y que acredita su identidad.

Tanto las claves RSA privada como pública de autenticación se encuentran dentro del certificado.

Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos .

Este certificado **no está habilitado en operaciones que requieran no repudio** de origen(para ello se requiere el certificado de firma electrónica reconocida) y por tanto los prestadores de servicios no tendrán garantía del compromiso del titular del DNI con el contenido firmado.

Este certificado se encuentra en la zona privada y es accesible en lectura por el ciudadano, mediante la utilización de la clave personal de acceso o PIN.

Certificado de firma electrónica reconocida

Este certificado también se encuentra en la zona privada y garantiza la integridad del documento firmado y el **no repudio** de origen.

Igual que en el caso anterior, este certificado también contiene las claves RSA privada y pública del mismo.

¿Qué ventajas ofrece?

- En las relaciones entre ciudadanos:
 - Garantizar la identidad de la persona que realiza una gestión, así como la integridad del contenido.
 - Proporciona el máximo grado de confidencialidad y seguridad en Internet.
 - Identifica unívocamente a las partes que se conectan telemáticamente.
- En las relaciones con las Administraciones públicas
 - Posibilidad de realizar trámites telemáticamente y que antes requerían presencia física con la Administración Pública.

- En las relaciones con las empresas
 - Realizar trámites al máximo nivel de seguridad.

La firma electrónica

¿Qué es la firma electrónica?

La firma electrónica es un término de naturaleza fundamentalmente legal que a través de la firma digital (serie de métodos criptográficos) permite establecer **un mecanismo de no repudio** para documentos electrónicos, aunque también podremos usarla para firmar un documento electrónico usando la clave pública de otro usuario para cifrar el documento garantizando que tan solo éste pueda leerlo.

De este modo la firma electrónica no es más que un conjunto de datos en forma electrónica que permiten identificar al firmante, teniendo el mismo valor que la firma manuscrita. Que un emisor y un receptor se comuniquen puedan identificarse mutuamente con la certeza de que son ellos los que están interactuando. Esto evita que terceras personas alteren los contenidos durante la comunicación.

Existen tres tipos de firmas²:

- **Firma electrónica (simple)**: Datos que puedan ser usados para identificar al firmante (autenticidad). Puede ser desde una firma gráfica digitalizada (escaneada) hasta el PIN de las tarjetas de crédito. No tiene por qué garantizar la autenticidad del firmante ni la integridad del contenido.
- **Firma electrónica avanzada**: permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados. Debe cumplir que sea creada por medios que el firmante puede mantener bajo su exclusivo control y aquí es donde se utiliza la criptografía de clave pública con el respaldo de un certificado electrónico
- **Firma electrónica reconocida (o cualificada³)**: es una firma electrónica avanzada pero a diferencia de la anterior, en este caso la firma se realizará usando un certificado reconocido (certificado que se otorga tras la verificación presencia de la entidad del firmante) y generada mediante un dispositivo seguro de creación de

² Solo los dos últimos tipos de firmas son reconocidas por la Ley 59/2003, de 19 de diciembre.

³ Por traducción del término inglés qualified que aparece en la Directiva Europea de Firma electrónica.

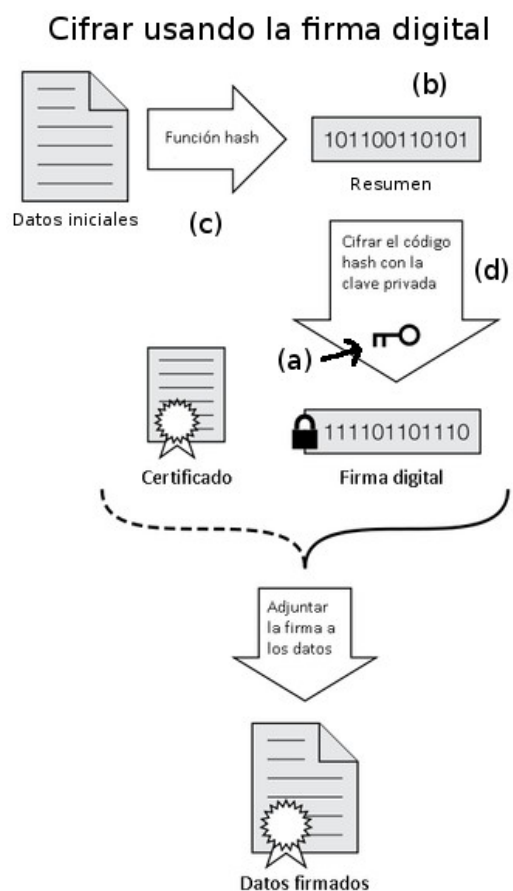
firma. Por tanto cualquier documento electrónico con una firma electrónica reconocida tendrá mismo valor que un documento en papel con una firma manuscrita.

¿Cómo funciona la firma digital?

Cifrado

Usaremos el certificado de firma reconocida para realizar la firma digital que nos permite garantizar que el documento no ha sido manipulado durante la comunicación.

- Cada parte tiene un par de claves, una se usa para cifrar (a) y la otra para descifrar.
- El emisor obtiene un resumen del mensaje (b) a firmar aplicando una función llamada “hash”⁴ (c) sobre los datos iniciales. El resumen es otro conjunto de datos de tamaño fijo, independientemente del tamaño original de los datos a resumir, 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 (d) el resumen del mensaje con la clave privada (a) que permitirá garantizar el origen y el no repudio del mensaje original.



El siguiente paso en la comunicación es adjuntar junto con los datos iniciales la firma digital. Para enviar el mensaje cifrado se puede utilizar la clave pública del certificado del emisor, garantizando que solo así este podrá descifrarlo usando su clave privada.

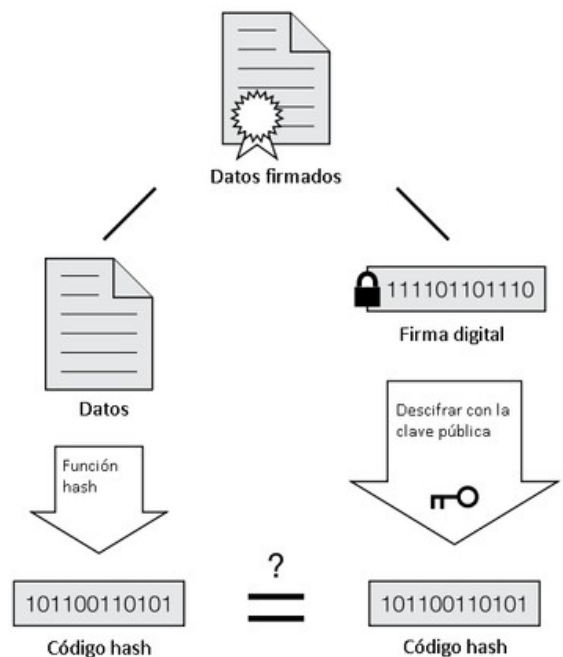
4 SHA y MD5 son los dos ejemplos más usados para aplicar generar este resumen.

Comprobación de una firma digital

Suponemos que hemos recibido los datos firmados (firma digital+datos iniciales) sin el certificado electrónico y que están sin cifrar.

El siguiente paso que tendrá que realizar el receptor, del mensaje, es generar un nuevo resumen mediante la función "hash". A continuación descifra la firma recibida 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.

Comprobación de una Firma



Si los códigos hash coinciden, la firma es válida

Certificado digital

¿Qué es un certificado digital?

Un certificado electrónico o digital es un documento generado y firmado electrónicamente por una "tercera parte de confianza"⁵ o también llamado "Prestador de Servicios de Certificación(PSC)"⁶ que garantizan la vinculación entre la identidad de una persona o entidad y su clave pública⁷, dándole a conocer como firmante en el ámbito telemático. Los PSC son las responsables de emitir y revocar los certificados electrónicos utilizados para realizar la firma electrónica. Esta denominación se origina por las propias funciones que realizan, y que está dirigida a que los usuarios de esta infraestructura tengan la seguridad de que el sujeto con el que se contacta es quién dice ser sin posibilidad de error.

¿Qué contiene un certificado digital?

Un certificado digital contiene usualmente:

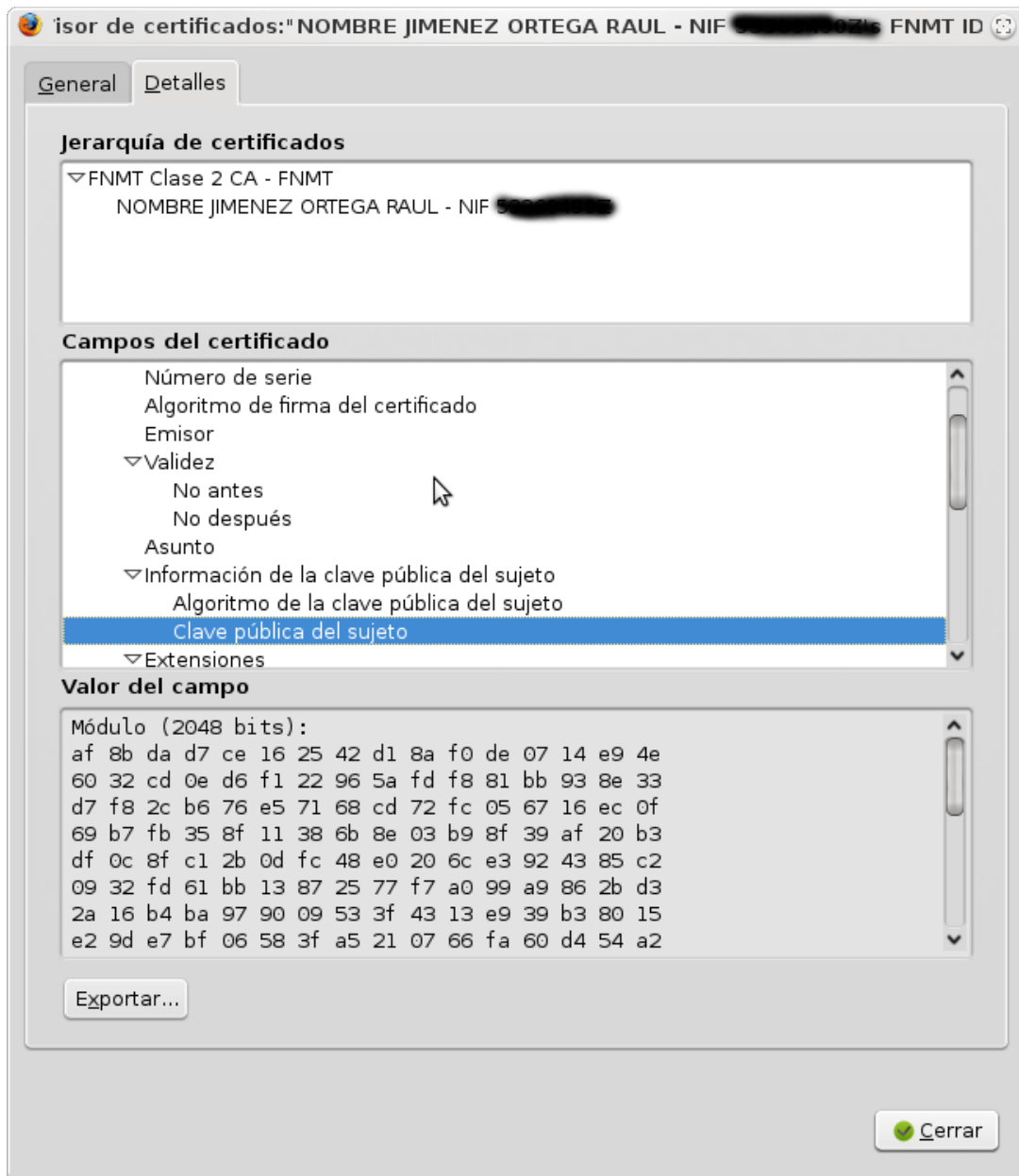
- el nombre de la persona o entidad certificada

5 Autoridades de Certificación: <https://www11.mityc.es/prestadores/busquedaPrestadores.jsp>

6 Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

7 Método de cifrado que garantiza la confidencialidad del envío del mensaje

- un número de serie
- fecha de espiración
- **una copia de la clave pública del titular del certificado** (utilizada para la verificación de su firma digital)
- firma digital de la autoridad emisora del certificado de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.



¿Cuántos tipos de certificados existen?

Existen diferentes tipos de certificados, que según el la entidad aportan un valor añadido diferentes a los certificados que los diferencia de los demás.

Podemos encontrar diferentes clasificaciones según la comprobación de datos que realizan o al uso al que se destina el certificado. Por ejemplo, según el uso se pueden clasificar como: “Certificados personales”, “Certificados de Servidor para SSL”, “Certificados de Infraestructura”, “Certificados de dispositivo” y “Certificados para Servicios de Sellado Digital de Tiempos”.

Algunos certificados de ejemplo son:

- Los certificados de persona física (o ciudadano) emitidos por la Fábrica Nacional de Moneda y timbre son gratuitos y van enfocados principalmente a su utilización ante las distintas Administraciones Públicas, aunque también se puede utilizar con otro tipo de entidades⁸ permiten realizar todo tipo de trámites de forma que queda garantizada la autoría y también realizar firmas electrónicas reconocidas..
- El certificado incluido en el DNI electrónico, gratuito también, permite trabajar con todas las Administraciones Públicas del Estado, tanto las de ámbito estatales, como a nivel Autonómico y Local.
- Otros como lo expedidos por Camerfirma, pueden utilizarse con las Cámaras de Comercio para realizar trámites como, por ejemplo, la gestión de certificados de origen para las exportaciones, etc.

¿Cuántos certificados puedo poseer?

Cualquier persona puede obtener diferentes certificados electrónicos siempre que estos sean de entidades de certificación diferentes. Además, una persona física puede disponer de varios certificados correspondientes a un mismo Prestador de Servicios de Certificación siempre que éstos sean: uno de ellos de persona física, y otro de persona jurídica, en el cual figure como representante legal o voluntario de dicha entidad.

El phishing

“El phishing es un delito de estafa cometido a través de una transferencia no consentida por el perjudicado mediante manipulación informática”

Sentencia de la Sala 2ª de 12 de Junio de 2007

A principios del año 2000 varios servidores ISP de Irlanda fueron atacados por un joven alicantino menor de edad utilizando pharming, consiguiendo redirigir a los usuarios que

⁸ Servicios a los que se puede acceder con el certificado de usuario:

<http://www.cert.fnmt.es/index.php?o=cert>

visitaban unos dominios a otras máquinas que se hacían pasar por la originales pero donde el atacante capturaba información privada de los usuarios sin su consentimiento ya que estaban siendo engañados.

El phishing se basa principalmente en entender la inteligencia humana y usar la ingeniería social para adquirir información confidencial de forma fraudulenta. Son conocidos cientos de casos donde los ciber-delincuentes tratan de aprovecharse de la inexperiencia de los usuarios normalmente suplantando la identidad de una persona o entidad con la que la víctima tiene algún tipo de acuerdo. Algunos de los ejemplos de las entidades por las que se hacen pasar son: compañía telefónicas, bancos, servidores de correo, servidores de mensajería instantánea, etc.

Intentando evitar este tipo de delitos se creó SSL (Secure Sockets Layer), un protocolo de comunicación que proporciona autenticación y privacidad en las comunicaciones telemáticas entre dos personas o entidades.

A día de hoy lo habitual es que solo el servidor sea quien garantice su identidad ya que la autenticación mutua requiere que el servidor conozca la clave pública del cliente, y esto supondría una barrera ya que no es frecuente que un usuario medio sepa usar su certificado digital.

Con este método se evitan las escuchas, la suplantación del remitente y se mantiene la integridad de los mensajes,

De modo que llegado a un punto del proceso de comunicación, tanto el cliente como el servidor intercambian las claves públicas para poder comunicarse. De este modo el cliente puede comprobar que el servidor es quien dice ser.

Para aumentar la seguridad en la red también han surgido otros mecanismos para cifrar todas las comunicaciones de datos entre dos entidades, por ejemplo el Protocolo Seguro de Transferencia de Hipertexto (HTTPS),

Fuentes:

Departamento de Certificación Española de la FNMT: <http://www.ceres.fnmt.es>

Portal Oficial sobre el DNI electrónico: <http://www.dnielectronico.es>

Wikipedia: <http://es.wikipedia.org>

Procedimientos Telemáticos y Electrónicos: <http://www.bartolomeborrego.com>

Transmisión de Datos y Redes de Computadores: Pearson Prentice Hall