Universidad de Burgos
CENTRO DE ATENCIÓN A USUARIOS
SERVICIO DE INFORMÁTICA Y COMUNICACIONES
Septiembre de 2009

El DNI Electrónico

¿Qué es?

Todos sabemos que el DNI se utiliza para acreditar nuestra identidad ante "personas" que dan validez al mismo observándolo. Con el DNI también podremos acreditar la identidad frente a terceros pero de forma electrónica.

Mediante este tipo de acreditación podremos realizar acciones electrónicas con plena validez legal evitando posibles fraudes de suplantación de identidad, que cada vez con más frecuencia estamos viendo en Internet.

No tenemos que tener miedo y estar preparados ante las nuevas tecnologías, que no nos pase como a nuestros mayores que incrédulos observaban como un cajón sin llamas ni calor calentaba los alimentos.

¿Para qué sirve?

El DNI contiene un certificado electrónico y una firma electrónica, que es la que te permite realizar operaciones con garantías a través de Internet. La aplicación más destacada es la que te permite realizar trámites con las administraciones públicas sin tener que esperar colas, ya que lo puedes hacer desde casa: completar la declaración de la renta, consultar los datos de tu vida laboral en la Seguridad Social, comprobar el saldo de puntos de tu carnet de conducir o inscribirte en concursos y oposiciones, y con el tiempo cientos de cosas.

Y.. ¿Qué necesito en mi ordenador?

Para la utilización del DNI electrónico es necesario contar con determinados elementos hardware y software que nos van a permitir el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

Equipamiento físico:

- Un lector de tarjetas inteligentes que cumpla el estándar ISO-7816. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados vía USB) o bien a través de una interfaz PCMCIA.

Software:

- Navegadores: el DNI electrónico es compatible con Microsoft Internet Explorer (versión 6.0 o superior), Mozilla Firefox (versión 1.5 ó superior) y Netscape (versión 4.78 o superior)
- Controladores / Módulos criptográficos para hacer uso del DNIe.

Cómo podemos conseguir un lector de DNI electrónico

El Ministerio de Industria, en colaboración con Tractis, Jazztel y Red.es ha anunciado una campaña por la que repartirá 300.000 lectores del nuevo DNI electrónico o DNIe. Toda empresa o particular que esté interesado en uno de estos dispositivos tendrán que cursar su solicitud en la correspondiente web del Ministerio del Interior. Una vez aceptada recibirán el gadget por sólo 2 euros de gastos de envío.

La campaña empieza el 1 de octubre y termina el 31 de diciembre o hasta fin de existencias. El Ministerio pretende, con este reparto masivo, potenciar el uso del nuevo documento del que, aunque se han expedido ya más de 12 millones de unidades, sólo se han registrado 2,5 millones de operaciones electrónicas.

Si deseas solicitar uno de estos lectores de DNI puedes acceder a:.

https://www.tractis.com/red-es/lectores

Red.es asumirá el coste de los lectores que se repartan en Galicia, Asturias, Castilla y León, Castilla La Mancha, Extremadura, Andalucía, Comunidad Valenciana, Murcia, Canarias, Ceuta y Melilla. Por otro, los patrocinadores abonarán los equipos que se distribuyan en el resto de comunidades que engloban a Aragón, Baleares, Cantabria, Cataluña, Comunidad de Madrid, La Rioja, Navarra y País Vasco.

DNI-Electrónico, Firma digital de documentos, Transacciones electrónicas, etc.

El Ministerio de Industria repartirá en una campaña que se inicia el día 1 de octubre 300.000 lectores del nuevo DNI electrónico.

Contenido:

¿Cómo funciona eso del cifrado?

Intentaremos explicarlo de la forma más sencilla.

Cifrado Simétrico

Cuando era pequeño jugaba con mis amigos a intentar enviarnos mensajes de forma que otros no nos entendieran. Algunos métodos eran tan sencillos como agregar a cada sílaba otra previamente compartida:

"tiestite ties timi tiseticretito" intentábamos decir lo más rápido que podíamos.

En otros casos colocábamos el abecedario asignando un número a cada letra (a=1, b=2, etc.) convertíamos ese mensaje en números, le incrementábamos en una cantidad conocida por el emisor y el receptor y lo convertíamos en las letras que formaban el mensaje cifrado.

Estos tipos de cifrado forman parte de una clasificación denominada "Sistemas de cifrado simétrico" en los que existe una única clave utilizada para cifrar y descifrar el mensaje, y que por lo tanto debe de ser conocida de antemano por todos los interlocutores.

La criptografía simétrica garantiza rapidez en los cálculos pero sólo es aconsejable en grupos reducidos.

NOTA: los sistemas de cifrado incluidos son "infantiles" se utilizan para ilustrar un proceso. Los sistemas de cifrado simétrico actuales utilizan unos algoritmos mucho más complejos.

Cifrado Asimétrico

La criptografía de clave pública o asimétrica está basada en el uso de **un par de claves** que cumplen, entre otros requisitos, que lo que somos capaces de cifrar con una de ellas, somos capaces de descifrarlo con la otra y sólo con ella.

En los sistemas de Criptografía Asimétrica cada usuario tiene un par de claves, **pública** (que conoce o puede conocer todo el mundo, incluidos los enemigos) **y privada** (que solamente guarda y conoce el propio usuario).

Para que dos usuarios puedan intercambiar información sin conocerse previamente, lo único que tienen que hacer es intercambiar sus claves públicas, incluso a través de un medio inseguro como Internet.

Además, los métodos de cifrado asimétrico garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si un usuario A quiere enviar un mensaje cifrado a otro usuario B, lo primero que ha de hacer es coger la clave pública del usuario B y aplicarla al mensaje.

Una vez recibido el mensaje, B le aplica su clave privada, recuperando el mensaje original.

EN LA CRIPTOGRAFÍA ASIMÉTRICA UN USUARIO SIEMPRE USA SU PROPIA CLAVE PRIVADA O BIEN LA CLAVE PÚBLICA DEL USUARIO CON EL QUE SE QUIERE COMUNICAR

Desde el 1 de octubre se pueden solicitar estos lectores de DNIe a través de la web

www.tractis.com/red-es

Confidencialidad, integridad, no repudio y resumen.

La confidencialidad, integridad y el no repudio son tres características con las que podemos dotar a la información.

Confidencialidad es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. Por tanto, dicha información está oculta (cifrada).

El término **integridad** de datos se refiere a la corrección y completitud de los datos en una transmisión, transferencia o almacenamiento de datos. Es decir, que la información no sufre modificación durante el intercambio o almacenamiento.

El **no repudio** o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Es decir, que una vez enviados los datos no podremos posteriormente negar que vienen de nosotros.

Firma digital es: **datos agregados a o una transformación criptográfica** de una unidad de datos que **permite al receptor** de esa unidad de datos **probar el origen** de la unidad de datos **y protegerla frente a la falsificación**, p. e. por el receptor.

Es, por tanto, un mecanismo para garantizar y validar el origen y la integridad de datos en formato electrónico.

El receptor de los datos no es necesariamente un ser humano. Puede ser un dispositivo hardware, un programa de ordenador o cualquier otro objeto.

El resumen de un documento o "Hash" consiste en obtener mediante una función o método una cadena que representen de manera casi unívoca a un documento, registro, archivo, etc..

Si modificamos cualquier parte del documento el resultado de la función de resumen será distinto.

Descripción del proceso

Cifrar un documento

Para asegurarnos de la confidencialidad de un mensaje o documento remitido a otro usuario debemos buscar su clave pública.

El sistema buscará la clave pública en la entidad de seguridad y cifrará el contenido mediante el principio del cifrado asimétrico. Si recordamos un poco nos daremos cuenta que el contenido únicamente podrá ser descifrado por aquella persona que disponga de la clave privada asociada, es decir: su destinatario.

Debemos hacer hincapié en que el documento permanece cifrado durante la trasmisión pero no podemos asegurar quién es el emisor del mismo dado que cualquier persona puede hacer uso de la clave pública del destinatario.

Firmar un documento

Este proceso es un poco más complicado.

Mediante una función de hash obtenemos una cadena resumen del documento que se cifra mediante la clave privada del usuario que desea estampar la firma.

Este resumen cifrado se anexa al documento original. Este proceso se puede repetir por cuantas personas deseen firmar el documento pero para nuestro ejemplo sólo hemos incluido una firma.

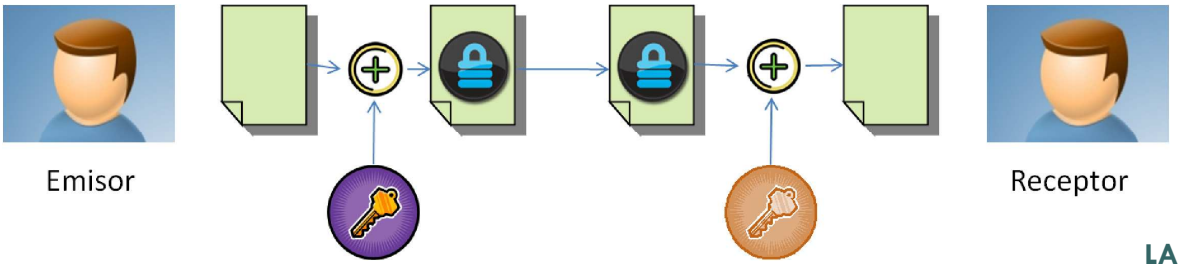
El documento y el resumen firmado son trasmitidos hacia el receptor, el cual para comprobar la información separa el documento original de la firma (o resumen cifrado con la clave privada del emisor).

El destinatario aplica el mismo algoritmo de hash que el emisor y obtiene el resumen del documento.

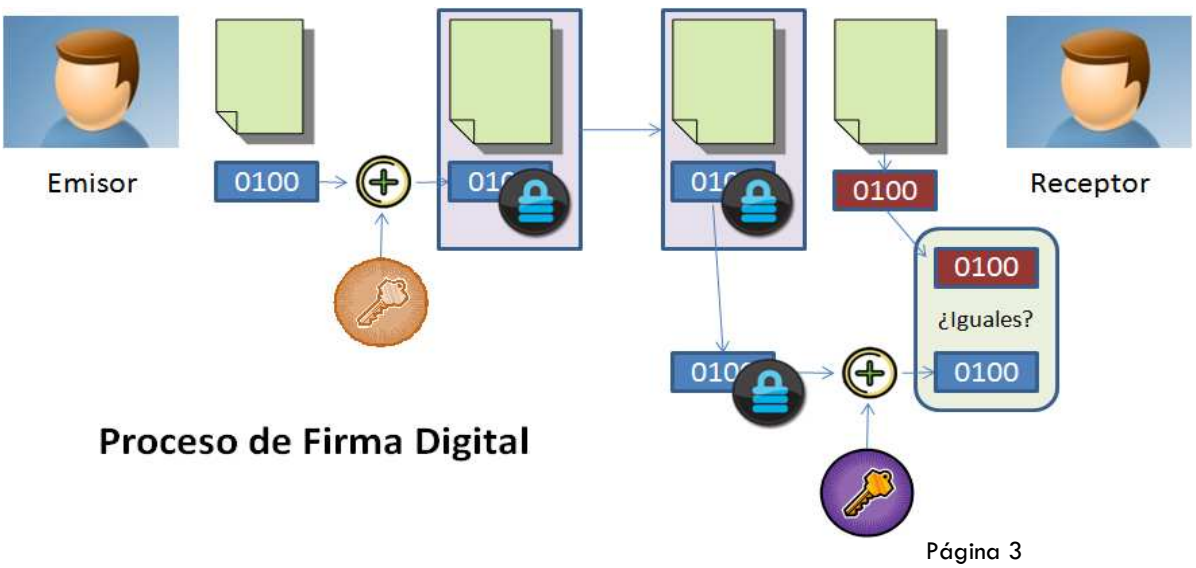
Por otro lado, utiliza la clave pública del emisor para desencriptar la firma que acompañaba al documento.

Como consecuencia de esta última acción obtiene un resumen teórico que debe de concordar con el que ha obtenido anteriormente.

Si son iguales el documento no ha sufrido alteración alguna dado que el resumen es el mismo en su origen que el obtenido en destino. Además, como hemos utilizado la clave pública del usuario para descifrar la firma y el resultado concuerda, estamos seguros de que fue cifrado con la clave privada del emisor con lo que se está dotando al documento de integridad y no repudio por parte del emisor.



LA FIRMA DIGITAL CONSISTE EN UNA SERIE DE DATOS QUE SE AGREGAN AL DOCUMENTO Y QUE PERMITEN PROBAR SU ORIGEN Y PROTEGERLO DE LA FALSIFICACIÓN



Proceso de Firma Digital

Centro de Atención al Usuario
Facultad de CCEE y Empresariales
C/ Parralillos s/n
09001 BURGOS

Teléfono: 947 25 95 05

Estamos en:
www.ubu.es/sic

La Ley 11/2007 de 22 de Junio, de acceso electrónico de los ciudadanos a los servicios públicos o de Administración Electrónica y la Identificación electrónica

Esta ley prevé que los ciudadanos podrán realizar todas sus gestiones administrativas por medios electrónicos, con la consecuente obligación de la Administración de ofrecer sus servicios por cualquier canal que facilite esta relación (Internet, móviles, etc).

Y en cuanto a la Identificación electrónica

Se entiende por identificación electrónica el conjunto de medios y procedimientos tecnológicos que permiten asegurar jurídicamente, en las relaciones telemáticas entabladas entre los ciudadanos y las Administraciones Públicas, que cada una de las partes es quien dice ser.

La Ley 11/ 2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos incluye expresamente entre los derechos de los ciudadanos enumerados en su Título I, artículo 6, el de la obtención de los medios de identificación necesarios, que no son otros que los sistemas de firma electrónica o digital así como el expreso derecho de las personas físicas a utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública. Este derecho, subrayado más adelante en la misma Ley, artículo 13.2.a y artículo 14, tiene su correlato en la obligación de todas las Administraciones Públicas de admitir los certificados incluidos en el DNI electrónico, por lo que cualquier plataforma de firma debe incluirlo.

Os presentamos un ENIGMA

LA IMPORTANCIA DE LA CRIPTOGRAFÍA EN LA HISTORIA DE LA HUMANIDAD

"Cuando el acorazado alemán Scharnhorsf zarpó de Noruega en diciembre de 1943 en una misión secreta, ya estaba echada su suerte. Dos días después los ingleses hundieron la nave, una de las tres más grandes de Alemania, gracias a la precisa información que tenían de los movimientos navales enemigos.

Muchos submarinos alemanes corrieron una suerte similar: 287 en 1943, más que los hundidos en los tres años anteriores. Falló totalmente el intento de Alemania de cortar la vital línea de suministro de los EUA hacia su aliada Inglaterra. La victoria aliada en el Atlántico norte fue un triunfo del servicio de inteligencia británico.

Antes de que estallara la guerra, los ingleses ya sabían de Enigma, una máquina construida en 1923 por el ingeniero alemán Arthur Scherbius para codificar mensajes por medios electromecánicos. Aunque recibieron dos de estas máquinas de sus aliados polacos, los ingleses no pudieron descifrar las claves hasta 1941, cuando capturaron a un submarino alemán que contaba con una máquina codificadora Enigma y los libros de claves para usarla. Los alemanes no supieron de la captura y actuaron con la confianza de poseer las claves más sofisticadas y seguras en existencia. El inesperado botín permitió a Inglaterra descifrar las radiocomunicaciones alemanas.

Según algunas estimaciones, el conocimiento preciso de los aliados acerca de las posiciones de los submarinos enemigos cobró 28 mil muertos de los 39 mil tripulantes de submarinos alemanes durante la crucial batalla por el control de la importante zona estratégica del Atlántico norte".

Recomendamos artículos sobre enigma:

http://2gmblog.blogspot.com/2008/06/salvemos-bletchley-park.html

http://www.portierramaryaire.com/arts/enigma_1.php

Este artículo ha sido extraído de 2GMBlog autor "cero91" enlace http://2gmblog.blogspot.com/2009/03/sabias-que-enigma.html

SU OPINIÓN ES MUY IMPORTANTE PARA NOSOTROS, SI DESEA REALIZAR CUALQUIER SUGERENCIA SOBRE TEMÁTICAS A TRATAR ASÍ COMO DE CUALQUIER OTRA ÍNDOLE NO DUDE EN HACERLO EN NUESTRO BUZÓN DE SUGERENCIAS LOCALIZADO EN LA WEB WWW.UBU.ES/SIC