

F.14. DNI electrónico (DNle)

Por Tomàs Baiget

Baiget, Tomàs. "DNI electrónico (DNle)".
En: *Anuario ThinkEPI*, 2007, pp. 203-204.



EL 16 DE MARZO DE 2006 se puso en marcha el *Documento Nacional de Identidad* electrónico español (DNle).

El primero se expidió en Burgos y a lo largo de los próximos dos años se irá extendiendo a las trescientas comisarías de todo el Estado. Este nuevo documento posibilitará identificarse y firmar electrónicamente para realizar transacciones telemáticas con todas las garantías técnicas y jurídicas que tenemos al alcance.

Los trámites que efectuaremos con el DNle serán siempre como ciudadanos, puesto que los datos que constan en el mismo son estrictamente: nombre, apellidos, fecha de nacimiento y número de DNI. No se incluyen datos sobre la profesión.

Para responder a las necesidades profesionales existe un cierto número de servicios de certificación que proveen a los diferentes colectivos (empresas, trabajadores públicos...) certificados digitales con otros atributos.

El hecho que todos los ciudadanos disfruten de certificados digitales impulsará que se efectúen más trámites telemáticos comerciales y a través de las administraciones públicas, haciendo realidad la e-administración.

Funcionamiento

Se necesita un ordenador convencional conectado a internet, un navegador (Explorer, Netscape, etc.), y descargarse desde la página web del DNle un programa, sólo la primera vez, que facilita el entendimiento entre el sistema operativo y la tarjeta. Si el ordenador carece de lector de tarjetas deberá comprarse uno.

El chip del DNle contiene los datos indicados (registrados también en el soporte físico de la tarjeta) y dos certificados expedidos según la ley de Firma Electrónica. Uno de ellos sirve para autenticarse (acreditar ante terceros nuestra identidad) y el otro, para firmar electrónicamente. No todos los trámites telemáticos exigen firma electrónica. Además alberga un tercer certificado del propio DNI (que se ha constituido en autoridad de certificación) que firma los certificados del



Fuente: Resumen de prensa y webs.

ciudadano, y un patrón de la impresión dactilar (que no es una fotocopia de la misma sino los vectores que la identifican) y tiene la finalidad de identificarse en caso de problemas –hace las funciones de PUK (clave personal de desbloqueo)–.

Al ciudadano se le entrega un pin personal que es una garantía de acceso, mientras que los certificados son una garantía para la tramitación. Es importante tener en cuenta que el pin es la contraseña que protege sus claves privadas y permite activarlas en las aplicaciones que generan firma electrónica y, por tanto, es confidencial, personal e intransferible.

Como se ha dicho, el DNIE tiene un certificado de autenticación y otro de firma digital, cada uno de ellos con un par de claves (una pública y otra privada). Estas claves (de 2.048 bits) se generan en el DNI automáticamente y cuando se inicia una sesión para un trámite en que necesita demostrar su identidad, el DNI envía su clave pública al peticionario. Si necesita firmar electrónicamente el

trámite, el peticionario se lo enviará con la clave pública del ciudadano de tal manera que sólo el certificado, el del titular del DNI, que tenga la clave privada aparejada a la pública podrá firmarlo. La clave privada nunca abandona la tarjeta. Hay otra cautela de seguridad. Si necesita firmar electrónicamente un trámite o documento, antes de hacerlo, aparecerá una ventana que advierte del inicio del proceso y pide nuevamente el pin. El pin no se puede cachear (almacenarlo en el ordenador para no tener que teclearlo nuevamente). Hay que tener claro que todo ello funciona para asegurar la identidad y el trámite. El DNI no cifra el contenido de los mensajes. Si alguien quiere enviar documentos cifrados debe acudir a los programas ya existentes.

Todo el proceso del DNI, tanto la tarjeta como los protocolos de empleo, está auditado por la *Agencia de Protección de Datos* y el *Centro Criptológico Nacional*.
<http://www.dnielectronico.es/>