

INFORME

## Detectan vulnerabilidades en las implementaciones del DNI electrónico

El [DNI electrónico](#) es el nuevo carnet de identidad de los españoles. Una de las grandes novedades es la incorporación de un chip que permite realizar operaciones de firma electrónica e identificar a los ciudadanos a través de Internet. El DNI-e sitúa a España en la vanguardia mundial en cuanto a firma digital y permitirá agilizar enormemente muchos de los trámites administrativos que hasta hace bien poco solo podían ser realizados en persona o bien requerían de engorrosos trámites técnico-burocráticos -obtención de un certificado, etc-.

En el interior del chip del nuevo DNI, se encuentra un certificado, que teóricamente no puede ser extraído de él. Además, todas las operaciones críticas -firmas- se realizan dentro del propio DNI. En eso radica su seguridad. Sin embargo, a pesar de que el diseño del DNIE es bastante seguro, no se puede decir lo mismo de su aplicación en el mundo real.

Si un ciudadano ha obtenido el nuevo carnet de identidad y lo ha activado en el kiosko de las dependencias donde lo expidieron, podrá realizar operaciones por Internet, como la declaración de la renta, el acceso a banca electrónica, acceso a la seguridad social, y en general a muchos servicios de la administración pública. Para ello solo tiene que introducir el DNI en un lector de tarjetas, acceder a la página web del sitio e introducir su PIN -contraseña- cuando su ordenador se lo solicite. Este único documento le da acceso a un infinidad de información vital y absolutamente privada. Esto no debería ser un problema, siempre que el usuario sea el propietario del DNI...

Las operaciones -firmas electrónicas- realizadas mediante DNI-e tienen plena validez legal. ¿Qué sucederá entonces cuando un delincuente suplante la identidad de un usuario y realice operaciones en su nombre? Pues que las operaciones realizadas por el delincuente no podrán ser refutadas por el usuario lícito -la víctima-. Y es que el sistema bajo el cual se ha desarrollado el DNI-e le otorga tanta "confianza" a este dispositivo, que no contempla la posibilidad de que pueda ser comprometido.

En Pentest comenzamos un trabajo de investigación en Febrero del 2008 y después de realizar numerosos análisis, comprobamos que, si bien el diseño del propio DNI aparenta robustez, **su implantación y su uso cotidiano no permiten afirmar que se pueda confiar totalmente en su uso**, y que a pesar de lo que organismos, promotores y desarrolladores de este proyecto defiendan, existen numerosas y sencillas maneras de comprometer la integridad de una operación realizada mediante DNI-e.

Si partimos de la base de que la mayoría de operaciones de DNIE se realizarán desde ordenadores convencionales -de usuarios domésticos- y que éstos pueden estar infectado con troyanos o con virus, ya tenemos un escenario que para nada inspira confianza. Y es que resulta que un virus puede capturar el número PIN cuando el usuario lo introduce y luego realizar una operación de firma electrónica sin que el usuario se percate de nada. Si no es un virus o un troyano, un atacante puede sencillamente emplear un programa de control remoto para operar como si estuviera sentado delante del ordenador de la víctima... En este caso, ¿Cómo diferenciar entre una acción realizada por el usuario lícito y otra realizada por el atacante?

Si nos vamos a escenarios menos concretos y de impacto masivo, podemos pensar en que muy pronto los desarrolladores de virus "adiestrarán" a sus especímenes para que obtengan información del DNI-e... Sí, porque aunque es cierto que cierta información que aparece en el certificado del DNI es "pública" -puede ser accedida sin necesidad de introducir PIN- lo que mucha gente no sabe es que dicha información puede quedar en algunos procesos del sistema operativo, incluso después de haber retirado el DNI del lector. De manera que el riesgo en el uso del DNI en un ordenador, ya no queda reducido a una ventana de tiempo determinada -mientras el DNI-e está en el lector- sino que muchos datos: Nombre, Apellidos, N° DNI, fecha de nacimiento, pueden quedar dispersos por el sistema y ser capturados por un oportunista.

Por último es interesante hacer notar que la sensación de seguridad que nos han intentado transmitir con el uso del DNI-e está algo distorsionada. Por ejemplo, cuando un usuario accede a su banco con el DNI-e, y además usa una conexión cifrada con SSL -el famoso candadito- puede pensar que está del todo seguro. Nada más falso. Algunos de los ataques que se podían realizar hace diez años, siguen siendo válidos. Por ejemplo, en todos los casos, un atacante siempre puede acceder a la memoria del sistema -en concreto la empleada por los navegadores- y obtener de ella, lo que desee: números de cuentas y tarjetas, saldo y en definitiva todo lo que la víctima haya visualizado en su navegador. También se pueden llevar a cabo ataques algo más complejos, si el intruso extrae los identificadores de sesión HTTP de la memoria, con lo cual, en muchos casos podrá acceder directamente a la web de la víctima en un ataque similar a lo que sería un secuestro de sesión.

El resultado de nuestro trabajo [se puede leer en un informe que se ha publicado](#) así como en varias demostraciones prácticas -vídeos y programas educativos- donde se pone de manifiesto que los recursos protegidos por el DNI-e no son, ni mucho menos, invulnerables.

Es importante terminar diciendo que desde Pentest Consultores apoyamos y creemos en el proyecto DNI electrónico, por su ambición y por lo que puede suponer en un futuro. Pero también creemos que se ha desarrollado una campaña de marketing alrededor de esta iniciativa que impide que los usuarios conozcan la realidad del uso del DNI-e sus limitaciones, sus riesgos legales, el poder que le otorga al gobierno sobre la intimidad de los ciudadanos, etc.

## **INFORME TÉCNICO SOBRE DNI ELECTRÓNICO: "ANÁLISIS DE VULNERABILIDADES E IMPLEMENTACIÓN"**

**[Vídeo ejemplo de un fallo de implementación mencionado en el informe](#)**

**Para más info:**

**[Pentest Consultores](#)**

**Fecha artículo: 2009-08-24 19:07:18 - url artículo: <http://www.internautas.org/html/5689.html>**

**Logos y marcas propiedad de sus respectivos autores.**

**Los comentarios son propiedad y responsabilidad de cada autor.**

**© 1998-2010 Asociación de Internautas - <http://www.internautas.org>**

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: [asociacion@internautas.org](mailto:asociacion@internautas.org)