

## FORTALEZAS Y DEBILIDADES DEL DNI ELECTRÓNICO (eDNI)

Josefa García Mestanza.

### RESUMEN

La explosión y extensión de internet ha marcado la globalización mundial abriendo una serie de retos a la sociedad desde el punto de vista de la identificación de los ciudadanos. A fin de responder a estas nuevas necesidades de la población española el Gobierno decidió lanzar el eDNI. En este trabajo se presentan los acontecimientos más relevantes que antecedieron a esta trascendente decisión, así como el modelo de DNI electrónico propuesto, el cuál es analizado a través de sus muchas fortalezas y debilidades.

**PALABRAS CLAVES:** eDNI, DNI electrónico, identidad digital.

### ABSTRACT

The outbursts and spreading of internet has affected the world globalization opening a series of challenges to this society from the point of view of citizen's identification. In order to answer to these new needs of Spanish population, the Government decided to set up the DNI. On this task we are not only introduced to the outstanding events that preceded this transcendental decision, but also the proposed electronic DNI, which is analysed through its varied strength and weakness.

**KEY WORDS:** digital identification systems, electronic DNI, electronic identity.

---

La evolución de las posibilidades que ofrecen los avances telemáticos, hace necesaria buscar nuevas formas de ajustarse a los cambios en las necesidades de la población, a fin de lograr capturar sus beneficios fundamentales para ciudadanos y empresas, tanto en el ámbito económico (incremento de la productividad y de la competitividad)<sup>127</sup> como en el social (reduciendo las diferencias sociales para contribuir a un mayor bienestar)<sup>128</sup>.

En este proceso una medida emblemática es la implantación del DNI electrónico (eDNI), al permitir al ciudadano acreditar su identidad tanto por el canal tradicional (físico) como por los nuevos canales telemáticos. Máxime cuando en el contexto mundial, el pasado año reflejaba el fin de la crisis del sector de las tecnologías y de las comunicaciones que se inició en 2000, con la telefonía móvil y el uso de internet como los sectores más dinámicos.

---

<sup>127</sup> Los datos recientes indican una tendencia creciente en la difusión del uso de las TIC entre las empresas españolas, destacando, respecto a años anteriores, el mayor equipamiento de los empleados (entre el 75% y el 100%). Sin embargo, aún es necesario lograr una mayor asimilación de su uso, sobre todo por parte de las PYMES (eEspaña – Fundación Auna, 2004).

<sup>128</sup> El aprovechamiento de las posibilidades que nos ofrecen las nuevas tecnologías, permitiría aspirar a un nuevo modelo social, la denominada “Sociedad de la Información”. Ésta se define como el estadio de desarrollo social caracterizado por la capacidad de sus miembros (ciudadanos, empresas y Administraciones Públicas) para obtener, compartir y procesar cualquier información por medios telemáticos instantáneamente, desde cualquier lugar y en la forma que se prefiera.

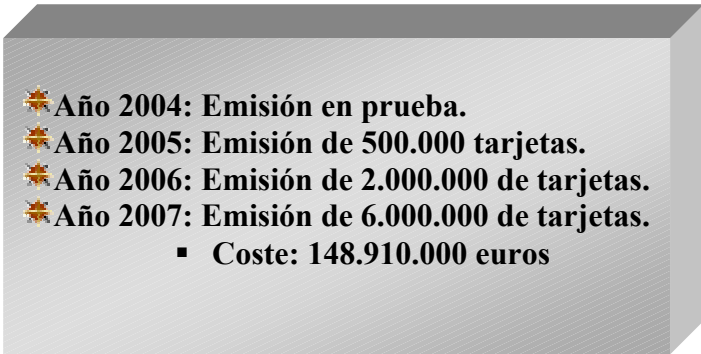
Concretamente en nuestro país, en el último cuatrimestre del año, el número de internautas ascendió a 9.789.000, con un volumen de transacciones en comercio electrónico, dirigidas al mercado final de consumo, de 143,6 millones de euros. Asimismo, la expansión del uso de internet en el ámbito de la banca y la prestación de servicios financieros *online* se ha consolidado a lo largo de los últimos tres años (eEspaña, 2004).

## 1.- ANTECEDENTES Y CONTEXTUALIZACIÓN DEL DNI ELECTRÓNICO ESPAÑOL

La globalización mundial, marcada por la irrupción de las nuevas tecnologías y, más concretamente, la explosión y extensión de internet ha abierto una serie de nuevos retos a la sociedad en general y a la española en particular desde el punto de vista de la identificación de los ciudadanos. Para responder a estas nuevas necesidades el Gobierno va a lanzar el eDNI.

De hecho, los estudios sobre identidad digital, en nuestro país, se remontan a los noventa, destacando, entre otros, el **Plan Info XXI**, tachado de ambicioso, y las Recomendaciones de la Comisión Especial de Estudios para el Desarrollo de la Sociedad de la Información<sup>129</sup>, la denominada Comisión Soto, quien en abril de 2003 para luchar contra las barreras que impedían el pleno desarrollo de la Sociedad de la Información proponía un “golpe de timón” en el que se enmarcaba el desarrollo del DNI electrónico, a fin de que éste diese soporte al conjunto de transacciones electrónicas, ya que mejoraría la seguridad en las transacciones e impulsaría el desarrollo de los servicios *online* de la Administración.

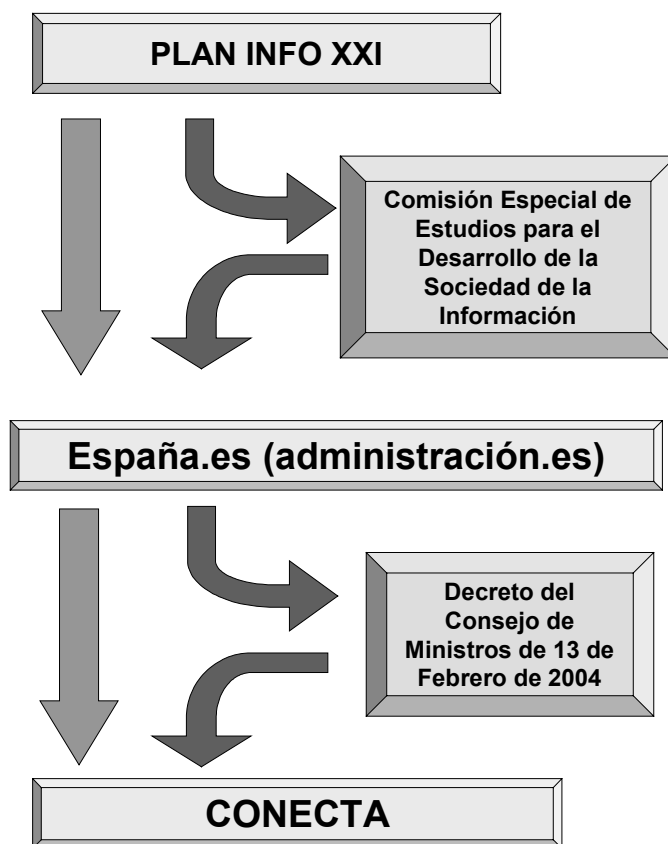
Siguiendo sus directrices estratégicas, en julio de 2003, se diseñó un Plan de Choque para el impulso de la Administración Electrónica, **administración.es**, dentro del Plan de Actuaciones para el desarrollo de la Sociedad de la Información en España, **España.es**.

- 
- ✦ **Año 2004: Emisión en prueba.**
  - ✦ **Año 2005: Emisión de 500.000 tarjetas.**
  - ✦ **Año 2006: Emisión de 2.000.000 de tarjetas.**
  - ✦ **Año 2007: Emisión de 6.000.000 de tarjetas.**
    - **Coste: 148.910.000 euros**

<sup>129</sup> A propuesta del Ministerio de Ciencia y Tecnología, con la finalidad de analizar la implantación de la Sociedad de la Información en nuestro país y proponer medidas para su desarrollo, el Consejo de Ministros creó la Comisión Especial de Estudio para el Desarrollo de la Sociedad de la Información en España (CDSI) formada por representantes del ámbito profesional, tecnológico, empresarial y académico, que inició sus esfuerzos el 27 de noviembre de 2002.

Las recomendaciones efectuadas fueron: definir un nuevo Plan General de actuaciones para el desarrollo de la Sociedad de la Información; asegurar el liderazgo político; institucionalizar la gestión “empresarial” del Plan; desarrollar un plan de comunicación que informe e ilusiones a la sociedad con el Plan definido; potenciar decididamente las iniciativas de formación para motivar y facilitar el uso de las TIC; reforzar la apuesta por la administración electrónica avanzando en servicios que creen valor y en la mejora de su eficiencia; avanzar en la equiparación del “mundo de internet” al “mundo físico” abriendo la legislación a las posibilidades que ofrecen las nuevas tecnologías; acelerar la entrada de ciudadanos en internet potenciando el acceso a equipos y conectividad; impulsar la integración de las TIC en los procesos de las empresas; y, contribuir a la integración social.

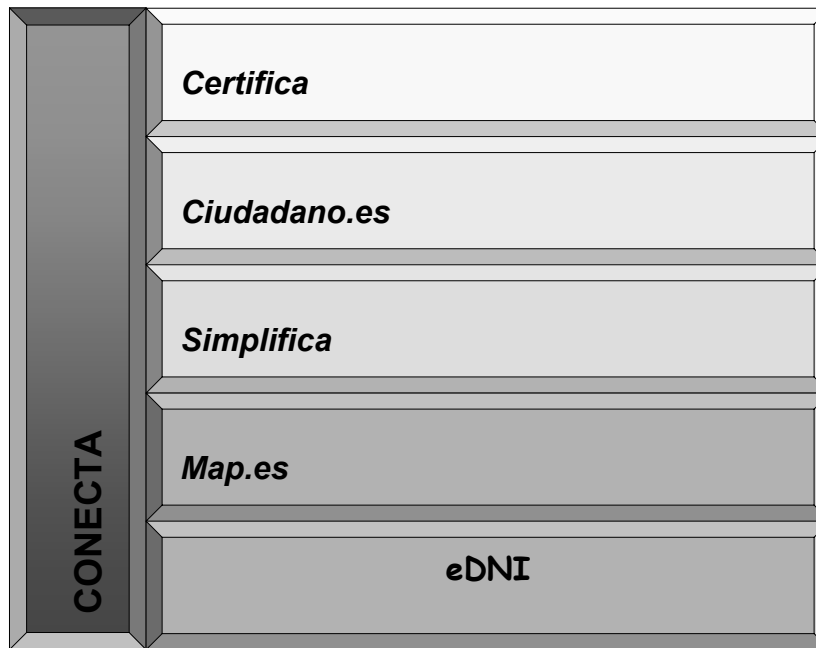
A raíz de este Plan, administración.es, el 13 de febrero de este año, el Consejo de Ministros aprobó un Decreto en el que se estableció que se comenzara a expedir el DNI electrónico en prueba y se completara la iniciativa de renovación total para el 2007<sup>130</sup>, pero este proyecto se retrasó por problemas técnicos de compatibilidad entre los certificados digitales de la Fabrica Nacional de Moneda y Timbre (FNMT) y la Seguridad Social.



Solucionados los problemas técnicos, el nuevo Documento se distribuirá en enero de 2005, coincidiendo con el inicio del **Plan Conecta**, que sustituye a España.es. Conecta cuenta con cinco grandes líneas de actuación, desglosadas en 43 planes concretos que se desarrollarán hasta 2007:

<sup>130</sup> Para el 2007 este proyecto estaría totalmente consolidado ya que el promedio de renovación natural de documentos es de seis millones año.

## CITIES IN COMPETITION



- **Certifica**: para el desarrollo de sistemas de interacción de datos entre las Administraciones Públicas y el ciudadano.
- **Ciudadano.es**: para acercar la Administración al ciudadano.



### **Proyectos Ciudadano.es:**

- ◆ 01 Agente inteligente buscador.
- ◆ 02 Catálogo de publicaciones.
- ◆ 03 Información pública electrónica.
- ◆ 04 Red de registros.
- ◆ 05 Red de atención e información al ciudadano.
- ◆ 06 Centros de gestión unificada.
- ◆ 07 Ciudadano.es.
- ◆ 08 Gestión integrada de ayudas y subvenciones.
- ◆ 09 Pasarela de pago.
- ◆ 10 Teléfono unificado de atención.
- ◆ 11 Desarrollo de espacios en el Portal del empleado público.
  - Plazo: años 2004 - 2007
  - Coste: 10.030.000 euros

- **Simplifica:** en búsqueda de una gestión pública, racional y eficiente, reduciendo costes y tiempos de respuesta.

### **Proyectos Simplifica:**

- ◆ 01 Impulso a la imagen institucional.
- ◆ 02 Revisión del marco normativo para la implantación de la AE.
- ◆ 03 Herramientas de apoyo al rediseño de procedimientos.
- ◆ 04 Licitaciones electrónicas.
- ◆ 05 Georreferenciación.
- ◆ 06 Enriquecimiento del sistema de información de RR.HH.
- ◆ 07 Mejora de la nómina estándar NEDAES.
- ◆ 08 Gestión de recursos humanos.
- ◆ 09 Completar la Intranet Administrativa con CC.AA y EE.LL.
- ◆ 10 Tramitación telemática expedientes de compras TIC.
- ◆ 11 Observatorio de la Administración Electrónica.
- ◆ 12 Reforma del Consejo Superior de Informática y creación del Comité técnico de la Conferencia Sectorial.
  - Plazo: años 2004 - 2005
  - Coste: 12.497.000 euros

### **Proyectos Map.es:**

- ◆ 01 Red corporativa y multiservicio del MAP.
- ◆ 02 Correo electrónico y directorio.
- ◆ 03 Publicación de contenidos. INTRAMAP.
- ◆ 04 Gestión automatizada de expedientes.
- ◆ 05 Aplicaciones departamentales extranjería.
- ◆ 06 Videoconferencia.
- ◆ 07 Formación virtual.
- ◆ 08 Centro de atención a usuarios.
- ◆ 09 Web de información y servicios del MAP.
- ◆ 10 Firma electrónica para la gestión interna del MAP.
- ◆ 11 Cooperación económica del Estado con los Entes locales.
  - Plazo: años 2004 - 2007
  - Coste: 55.334.782 euros

- **MAP.es:** para la actualización y mejora tecnológica del MAP, unificando y potenciando las páginas web de la Administración del Estado.

### **Proyectos eDNI:**

- ◆ 01 Plataforma común de validación de firma electrónica.
- ◆ 02 Difusión eDNI.
- ◆ 03 Reconocimiento de autoridades de certificación.
- ◆ 04 Política de firma electrónica.
- ◆ 05 Identificación única (SSO).
- ◆ 06 Sellado de tiempo (Time stamping).
  - Plazo: años 2004 - 2007
  - Coste: 2.577.000 euros

- **eDNI:** para la implantación del DNI electrónico, que sustituirá paulatinamente al actual<sup>131</sup>.

<sup>131</sup> Actualmente, el número total de Documentos es de 29 millones, aproximadamente, por lo que las autoridades estiman que los documentos actuales serán reemplazados hacia el 2010.

## 2.- EL DNI ELECTRÓNICO ESPAÑOL

El modelo de DNI propuesto acreditará la identidad personal de su titular y permitirá la firma electrónica de documentos, por lo que posee las mismas funciones que el actual, con la firma física, pero ampliándolas a la red.



El soporte de este Documento será una tarjeta de policarbonato, semejante a una tarjeta de crédito, con el mismo tamaño y color que el DNI actual, aunque la foto se desplaza hacia la derecha, la firma pasa a la parte inferior e incluirá un chip informático en la parte izquierda.

Este chip tendrá una parte pública que reflejará los datos personales básicos del individuo (la huella, la fotografía digitalizada y la imagen digitalizada de la firma manuscrita) y una parte privada que incluirá un certificado que garantizará digitalmente la identidad del ciudadano y le dará capacidad para firmar con una clave criptográfica personal, y el Pin, que sólo conocerá él.



La expedición del nuevo Documento se hará en el momento de su solicitud. Frente a los plazos de espera actuales (entorno a una semana) el eDNI se podrá expedir y entregar en el acto, facilitándose de este modo, que las solicitudes de obtención y renovación puedan efectuarse electrónicamente.

Este Documento incorpora mecanismos de seguridad tanto físicos como administrativos o electrónicos para evitar su falsificación, e, incluso, algunos requieren un análisis de laboratorio.

### Seguridad Administrativa:

El Ministerio del Interior creará en la Dirección General de la Policía una Autoridad de Certificación electrónica propia, que acreditará, con carácter exclusivo, los dos certificados del DNI digital: el de autenticación del ciudadano y el de firma digital. De este modo con el nuevo Documento las Fuerzas de Seguridad del Estado tendrán mayor certeza sobre la identidad de los individuos en sitios como aeropuertos u oficinas de la Administración.

Además, por razones de seguridad, el ciudadano, de modo voluntario, podrá activar el certificado de firma electrónica en las Oficinas de Expedición. En caso de sustracción o pérdida del DNI y hasta que no se proceda a la denuncia del hecho, se podría utilizar para firmar electrónicamente en su nombre; aunque a la zona privada de información del chip sólo podrá acceder el propietario del Documento tecleando su propia clave o PIN. En caso de haberlo olvidado, accederá con su huella.

## CITIES IN COMPETITION



### **Seguridad Física:**

El material elegido para su confección, el policarbonato, es más duro que el empleado a día de hoy, con una duración estimada superior a los diez años, el cual no permite combustión alguna por debajo de los 200 grados centígrados y, además, no puede dividirse en láminas, sin provocar su destrucción.

Asimismo, para garantizar la plena seguridad del Documento, se utilizará en su confección tinta ópticamente variable. con un hilo de seguridad embebido en el panel. relieves en el plástico v la

### **Seguridad Electrónica:**

Está previsto utilizar métodos criptográficos y códigos de barra bidimensionales, con un dispositivo de encriptación/desencriptación de memoria para la RAM, ROM y EEPROM. Según reza en la página web de la FNMT las tarjetas inteligentes estarán fabricadas en torno al chip SLE66CX320P de la empresa alemana Infineon Technologies, empresa relacionada con Siemens. Este chip que tiene un coste aproximado de 12 euros para tarjeta fabricada, cuenta con el certificado de evaluación de "alta seguridad" para el nivel E4 del "Information Technology Security Evaluation Criteria" (ITSEC) y está clasificado como de altas características. Pero según el fabricante este chip ha sido sustituido por otro más moderno, con la denominación SLE66CX322P que tiene unas prestaciones similares.

Este chip pertenece a la familia 66Plus de Infineon. Se trata de un procesador de 16 bits fabricado con tecnología de 0,25 micrones, especializado en tareas criptográficas, por lo que puede procesar los algoritmos RSA con claves de hasta 2048 bits, en menos de 290 segundos, o trabajar con DES, triple DES y con criptografía de curvas elípticas. En su interior integra una gran cantidad de dispositivos, como un generador de números aleatorios por hardware, lógica de seguridad antimonitorización de datos y claves, una unidad de manejo de memoria (MMU), un generador de frecuencia (PLL), cifrado/descifrado DES/triple DES por hardware, dos temporizadores de 16 bits, un circuito de comprobación de redundancia cíclica (CRC) y la lógica de interrupciones del dispositivo.

Entre sus medidas de seguridad destacan: un número de identificación único para cada chip, un generador de números aleatorios por hardware verificable internamente, una disposición de elementos optimizada para dificultar el acceso a los componentes, contramedidas para el análisis de fallos diferencial, alimentación diferencial o de análisis simple de potencia y un blindaje activo con detección de ataques.

Para operar con el nuevo DNI a través de la red se deberá introducir en un lector de tarjetas, previamente conectado al PC. Una vez recopilada la información a enviar, se inicia la comunicación para su transmisión. En ese momento se requerirá la identificación del usuario, que facilitará el número Pin. El sistema de autenticación verifica la validez de los certificados digitales. Una vez identificado, la información viaja encriptada hasta su destinatario.



De este modo, para autenticarse el usuario o firmar digitalmente documentos electrónicos se requerirá un lector de tarjeta y un software, que puede descargarse en cada ordenador, vía internet. De hecho, en la FNMT ya están disponibles las unidades de la Tarjeta Criptográfica, el Cryptokit, que es el embrión del DNI digital. De aspecto prácticamente igual al de una tarjeta de crédito de un banco, se distribuye junto con un lector que permite conectar la tarjeta con el ordenador personal, y certificar así la identidad del usuario cuando esté navegando y realice operaciones *online*.

### 3.- FORTALEZAS Y DEBILIDADES DEL eDNI

El nuevo Documento de identidad, además de la utilidad convencional tradicional, va a permitir actuar en las redes de comunicación públicas y privadas, respaldando a su propietario al garantizar la integridad del documento firmado, el no repudio de éste y la autenticidad de origen, mientras que al receptor de un correo electrónico o de un pedido en una tienda de internet le permitirá saber quién está realmente al otro lado. Aunque, en ningún caso garantiza que se tengan fondos en el banco y tampoco contiene aplicaciones de monedero electrónico.

Una persona con este DNI podrá renovar, sin salir de casa, el pasaporte, presentar y pagar impuestos, tasas o multas, solicitar licencias de importación o exportación, certificados de empadronamiento o de la Seguridad Social, presentar reclamaciones, compra-venta de valores, votar, matricularse o solicitar becas en centros públicos o privados, firmar contratos y documentos notariales, efectuar transacciones bancarias *online* o de comercio electrónico, etc.

Además, gracias a su chip, la policía podrá reconocer a sus usuarios desde un simple teléfono móvil o PC de bolsillo y determinar su autenticidad sin tener que llamar a la central. Incluso, este documento podría sustituir a las tarjetas de identificación electrónica que llevan los empleados en algunas empresas.

Y en lo relativo a lo Judicial, hasta ahora, el principal problema en las comunicaciones a través de la red ha sido la identidad de las partes que interactuaban. Con la emisión del nuevo Documento digital y la creación y aprobación de los “Terceros de Confianza”, se podrá solventar este problema. El DNI digital permitirá asegurar que la persona es realmente quien dice ser, y la entidad certificadora, podrá actuar a modo de “notario virtual”.

En principio los beneficios derivados de su uso son muchos e importantes. Este proyecto ha sido valorado positivamente por la Asociación Nacional de Empresas de Internet y el Consejo Superior de las Cámaras de Comercio, Industria y Navegación a través de su Foro de Firma Electrónica al estimar que favorecerá el comercio al incrementar la seguridad y la confianza en las transacciones *online*.

No obstante, las críticas tampoco se han hecho esperar. Por ejemplo, la Asociación de Internautas y la Comisión de Libertades Informáticas manifestaron que no se debía despachar la regulación del DNI electrónico en dos artículos de la Ley 29/2003 de firma electrónica<sup>132</sup>, cuando se requeriría una Ley Orgánica específica por afectar directamente a derechos fundamentales, además de criticar la imposición por decreto de su puesta en marcha sin ningún tipo de debate político ni social previo. Esta realidad se puso de manifiesto en las enmiendas formuladas a esta Ley en el Congreso (casi 250) y en el Senado (289).

De otro lado, la seguridad del nuevo Documento se convierte en una cuestión clave. Mientras que la pérdida o sustracción del DNI tradicional no supone un riesgo grave para el usuario, ya que normalmente requiere su presencia al ser autenticado mediante la firma y la fotografía, en el DNI electrónico la seguridad se ve comprometida al poder usarse por un tercero sin consentimiento o conocimiento del titular.

Incluso, la seguridad basada en el oscurantismo del hardware tecnológico no es una garantía absoluta, puesto que las tarjetas se pueden criptoanalizar teniendo los recursos adecuados, y cada día aparecen medios más sofisticados. Y es que, las firmas manuscritas son complicadas de falsificar, mientras que una clave de 8 cifras, una vez conocida, puede ser introducida por cualquiera.

O también, puede que se filtre la información y a partir de ahí manipular o crear circuitos que emulen el funcionamiento de estos dispositivos. Si se lograra clonar los DNI o se rompieran los sellos criptográficos, no sería necesario disponer de las tarjetas originales, lo que dificultaría la detección del fraude.

El hecho de que no se informen o conozcan fallos de seguridad no significa que no existan, e incluso, que no se estén explotando con éxito por los delincuentes.

Además, los chips de estas tarjetas deberían estar fabricados con tecnología nacional propia o licenciada, que sea perfectamente conocida y auditada, que evite la inclusión inadvertida o premeditada de vulnerabilidades y que permita modificaciones en caso necesario, a fin de tener continuidad en el tiempo, ya que su paralización o sustitución masiva implicaría un enorme perjuicio, de todo tipo.

También, cuando se da de alta el uso de su utilización en la red, se da como un “todo”, y no por servicios. Si el usuario pudiera activar o desactivar en el tiempo las operaciones que desea, o establecer un límite en la cuantía de las mismas, se minimizarían los posibles ataques, y en el supuesto caso de fallo de seguridad, su uso estaría limitado a una serie de acciones previamente definidas por su usuario.

Por ello, al tener más usos y funciones que el DNI actual, se aumentarían considerablemente los ámbitos de aplicación, el interés por el producto y sus funcionalidades y, paralelamente, las áreas con un riesgo potencial para los usuarios.

Otro punto débil indirecto puede derivar del lugar desde el que se realicen las operaciones. En ocasiones, estas tarjetas se usarán en ámbitos no controlados, como el hogar o en instalaciones no vigiladas, en los que cabe la posibilidad de coacción o amenaza. Si no se garantiza algún tipo de seguridad al respecto, pueden ser bastantes

---

<sup>132</sup> Artículos 15 y 16 de la citada Ley (BOE nº 304, de 20 de diciembre, título II, capítulo III). La base legal para la construcción de la presente Ley es la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica.

los casos en los que se obligue al titular a hacer un uso del DNI mediante intimidación, máxime con el aumento de los casos de malos tratos que existen.

Además, se ha de tener en cuenta las limitaciones de los usuarios a la hora de establecer y recordar las contraseñas de seguridad.

Otro problema que puede afectar a su extensión y uso es el hecho de que no sea universal. Cuando se pretendía que este documento fuese crucial para actuar en las redes de comunicaciones públicas y privadas, acreditando la identidad del usuario y posibilitándole para firmar digitalmente, no se contemplaba que su uso estuviese limitado al estado de español.

En este terreno se está avanzando bastante. Por ejemplo, en el Plan de Acción eEuropa 2005, el programa IDABC, para el periodo 2005-2009, trabajará en el intercambio electrónico de datos entre Administraciones en la Unión Europea, la interoperabilidad de los mismos y su normalización.

De otro lado, a finales de septiembre se presentó en Murcia el modelo español definitivo<sup>133</sup>, en Bélgica ya se expide de manera oficial el DNI electrónico y en Finlandia se dispone de este sistema desde diciembre de 1999. No obstante, a pesar de que su Documento sirve para realizar gestiones con la Administración, como documento de viaje y desde junio de este año como identificación para la Seguridad Social, no ha sido todo lo exitoso que se esperaba.

De hecho, el éxito de este Documento electrónico no dependerá sólo de la creación de un sistema que garantice la seguridad de las comunicaciones electrónicas sino también de que este sistema vaya acompañado de las facilidades de uso que permitan su aplicación generalizada.

Incluso, siempre que se establezca un sistema de gestión basado en el Documento electrónico debe haber un procedimiento alternativo tradicional, para que su uso mayoritario no suponga un problema a los usuarios que tengan menos recursos, una reducida capacitación técnica o simplemente, no lo quieran utilizar en su faceta electrónica.

#### 4.- CONCLUSIONES

Estos datos obligan a pensar que la implantación del DNI electrónico en España será una realidad en enero de 2005, aunque a corto plazo es difícil que se extienda su uso, sobre todo en el ámbito privado, donde se mezclan intereses económicos nacionales e internacionales que pueden implicar la coexistencia de otros medios para efectuar operaciones que impliquen identificación y firma electrónica.

Además, la Sociedad de la Información en nuestro país sigue presentando un avance muy desigual entre ciudadanos, empresas y Administraciones en los distintos elementos de la cadena de valor, tanto en infraestructura, como en conectividad, servicios y uso de los mismos. De hecho, el último estudio de World

---

<sup>133</sup> Bajo el lema “e-Cooperación en la Administración Pública” se celebró la VIII edición de Tecnimap en Murcia, entre los días 28 de septiembre y 1 de octubre, presentándose el prototipo de DNI electrónico. Como anunció el secretario general para la Administración Pública, el MAP está elaborando un proyecto de Real Decreto sobre las tecnologías de la información por el que las administraciones tramitarán en soporte informático todos sus documentos. El objetivo de los responsables de la Administración Pública es reducir al máximo el uso del papel. En palabras de su secretario general, la intención del MAP es que en “el futuro no se tramite nada que no venga en soporte electrónico”.

Economic Forum (febrero de 2004) sitúa a España en el puesto número 17 del ranking de países de la Unión Europea en cuanto a desarrollo general de la Sociedad de la Información.

## 5.- BIBLIOGRAFÍA

**Aprovechar la Oportunidad de la Sociedad de la Información en España. Recomendaciones de la Comisión Especial de Estudios para el Desarrollo de la Sociedad de la Información**, de 1 de abril de 2003.

**Borrador del Anteproyecto de Ley de Firma Electrónica**, Ministerio de Ciencia y Tecnología, Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, Dirección General para el Desarrollo de la Sociedad de la Información, <http://www.mcyt.es>, [www.tecnoley.es](http://www.tecnoley.es).

**Directiva 1999/93/CE**, del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica, Diario Oficial de las Comunidades Europeas, de 19 de enero de 2000.

<http://informativos.net/notampliada.asp?idNoticia=41861> ("Valoración de la Ley de Firma Electrónica", *Informativos.net*).

<http://kalysis.com/content/index.php?newlang=spa> (KALYSIS. Nuevo carnet electrónico español permitirá transacciones a través de la red).

<http://www.camerfirma.com> ("Foro de Firma Electrónica", *Camerfirma*).

<http://www.cert.fnmt.es> (FNMT).

[http://www.consumer.es/web/es/especiales/2004/02/23/96094\\_2.php](http://www.consumer.es/web/es/especiales/2004/02/23/96094_2.php) (CONSUMER. Nuevo DNI electrónico).

<http://www.csi.map.es/csi/pg5c10.htm> (Criterios de seguridad, normalización y de conservación de las aplicaciones utilizadas para el ejercicio de potestades).

<http://www.directoriodeestado.com.ar/contenido.php?pais=Espa%F1a&nota=158> ("El proyecto de DNI electrónico se incentivará después de las elecciones de marzo").

<http://www.eepoch.net/> (eEurope Smart Card Charte Prof. of concept and holistic solution. eEpoch Projet, proyectos de cooperación europeo de interoperabilidad y seguridad en los sistemas de identidad digital. e-ID and the Information Society in Europe).

<http://www.fundacionauna.org> (Fundación Auna eEspaña 2004).

[http://www.fundacionauna.org/comunicados/comu\\_02.asp?ID=48](http://www.fundacionauna.org/comunicados/comu_02.asp?ID=48) (Informe eEspaña 2004 IV Informe Anual sobre el desarrollo de la sociedad de la información en España).

<http://www.hispalinux.es/docs/dni.html>

<http://www.ictsb.org/ToR.htm> (Group of organisations concerned with standardization and related activities in information and communications technologies).

<http://www.id.ee/porvoo5/?show=1> (Provoo 5 – Interoperable European Electronic Identities).

<http://www.ing.ucsg.edu.ec/paginas/seminario/modulo6.htm> (DEMOCRACIA ELECTRÓNICA. DNI digital).

<http://www.iniciativasnet.com/101iniciativas.htm> (INICIATIVAS.NET. El nuevo DNI electrónico).

<http://www.laflecha.net/canales/e-administracion/200409142/> (LAFLECHA: Bélgica es el primer país en adoptar el DNI electrónico).

<http://www.madridpress.com/home/DetailNews.jsp?id=19590&static=0> ("Según la Comisión de Libertades e Informática la Ley de Firma Electrónica tiene importantes defectos técnicos", *Madridpress.com*).

[http://www.map.es/gabinete\\_de\\_prensa/notas\\_de\\_prensa/20040930\\_0003-ides-idweb.html](http://www.map.es/gabinete_de_prensa/notas_de_prensa/20040930_0003-ides-idweb.html) (El Gobierno presenta el Plan Conecta, para el desarrollo de la Administración Electrónica de los cuatro próximos años).

[http://www.mcyt.es/asp/ministerio\\_informa/prensa/np13-02-04.htm](http://www.mcyt.es/asp/ministerio_informa/prensa/np13-02-04.htm) (MINISTERIO DE CIENCIA Y TECNOLOGÍA. El Gobierno aprueba la puesta en marcha del DNI Electrónico).

[http://www.mcyt.es/dgdsi/nota\\_informativa.htm](http://www.mcyt.es/dgdsi/nota_informativa.htm) ("Proyecto de Ley de Firma Electrónica", *Ministerio de Ciencia y Tecnología*).

<http://www.mir.es/oris/notapres/year04/np021301.htm>

[http://www.opinionvirtual.com/firm\\_electronica/firma\\_digital\\_futuro\\_dni\\_digital.php](http://www.opinionvirtual.com/firm_electronica/firma_digital_futuro_dni_digital.php) ("El futuro DNI electrónico en España", *opiniónvirtual.com*).

[http://www.pc-actual.com/Actualidad/Noticias/Inform%C3%A1tica\\_profesional/Infomercado/20040630033](http://www.pc-actual.com/Actualidad/Noticias/Inform%C3%A1tica_profesional/Infomercado/20040630033) (España pierde tres puesto en cuanto a desarrollo de la sociedad de la información en la UE).

[http://www.red.es/OpenMarket-Xcelerate-Reder\\_argitPagActual-1067345388248](http://www.red.es/OpenMarket-Xcelerate-Reder_argitPagActual-1067345388248) ("El Gobierno presenta un Plan de Choque para impulsar la Administración Electrónica").

<http://www.setsi.mcyt.es/eventos/firmaele/jornadadiv.htm> ("Jornada divulgativa sobre normalización técnica en firma electrónica", *Ministerio de Ciencia y Tecnología*).

<http://www.vnunet.es/Actualidad/Noticias/Comunicaciones/Internet/20040211030> ("El DNI Electrónico será una realidad el próximo viernes", *vnunet.es*).

<http://www.vnunet.es/Actualidad/Noticias/Comunicaciones/Internet/20031120023> ("El DNI Electrónico potenciará la seguridad de las redes", *vnunet.es*).

<http://www.vnunet.es/Actualidad/Noticias/Comunicaciones/Internet/2003121078> ("Las Cámaras de Comercio dudan de la efectividad de la Ley de Firma Electrónica", *vnunet.es*).

## CITIES IN COMPETITION

<http://www.vnunet.es/Actualidad/Noticias/Comunicaciones/Internet/20031201090> ("Las críticas a la futura Ley de Firma Electrónica no se hacen esperar", *vnunet.es*)

<http://www.votobit.org/articulos/dni.html> (VOTOBIT. El DNI electrónico y la e-firma).

Informe eEspaña 2004 IV Informe anual sobre el desarrollo de la Sociedad de la Información en España. Fundación Auna, 2004.

**Ley 59/2003**, de 19 de diciembre, de firma electrónica. BOE nº 304, de 20 de diciembre de 2003, <http://www.setsi.mcyt.es/legisla/internet.htm> (SETSI-LEY 59/2003).

**Plan de Choque para el impulso de la Administración Electrónica**, Ministerio de Ciencia y Tecnología y Ministerio de Administraciones Públicas, 8 de mayo de 2003.

**Propuesta de Directiva del Parlamento Europeo y del Consejo**, de 13 de mayo de 1998 por la que se establece un marco común para la firma electrónica, Comisión de las Comunidades Europeas COM(1998) 297 final, 98/0191 (COD).

**Proyecto de Ley 121/000158** Firma Electrónica, Boletín Oficial de las Cortes Generales nº 158-1, de 20 de junio de 2003.

**Real Decreto Ley 14/1999**, de 17 de septiembre, sobre firma electrónica.

**World Economic Forum** (febrero de 2004) en Informe eEspaña 2004 IV Informe anual sobre el desarrollo de la Sociedad de la Información en España. Fundación Auna, 2004.