Hacia una nueva identificación electrónica del ciudadano: el DNI-e

J. Crespo Sánchez[1], J. Espinosa García[2], L. Hernández Encinas[3], H. Rifà Pous[2], M. Torres Hernández[2]

[1] Área de Informática, Dirección General de la Policía, Ctra. M-505 km. 5.5, E-28280-El Escorial,Madrid, España
certificacion.identidad@dni.es
[2] Safelayer Secure Communications S.A., http://www.safelayer.com
C/ Basauri 17, Edif. Valrealty, Edif. B, Pl. Baja Izq., E-28023-Madrid, España
{javier.espinosa, helena.rifa, manuel.torres}@safelayer.com
[3] Dpto. Tratamiento de la Información y Codificación
Instituto de Física Aplicada, Consejo Superior de Investigaciones Científicas
C/ Serrano 144, E-28006-Madrid, España
luis@iec.csic.es

Resumen El Documento Nacional de Identidad electrónico (DNI-e) pretende proporcionar un mecanismo de identificación al ciudadano español, permitir la firma electrónica de documentos y fomentar la confianza de los españoles en la Sociedad de la Información. Se presentan en este trabajo las principales características del DNI-e, tanto desde el punto de vista de su soporte físico (tarjeta y chip), como desde el punto de vista lógico (certificados digitales, firmas electrónicas, claves, etc.). Se hará especial hincapié en la infraestructura de clave pública (PKI) en la que se apoya su desarrollo y uso futuro.

Palabras clave: Autenticación de ciudadanos, Certificados digitales, Criptografía de clave pública, DNI-e, Identificación electrónica.

1. Introducción

El rápido desarrollo de las Tecnologías de la Información en nuestra sociedad hace necesario que éstas respondan a nuevos retos, cada vez más solicitados por los usuarios. Uno de estos retos es el de dotar y garantizar a todos los ciudadanos de mecanismos adecuados que aseguren su privacidad, libertad y derechos, en el actual marco democrático.

Para dar respuesta al reto de la identificación electrónica personal, el Ministerio del Interior, mediante el organismo afiliado de la Dirección General de la Policía (DGP), proporcionará a todos los ciudadanos del Estado Español un nuevo mecanismo de identificación basado en el actual Documento Nacional de Identidad (DNI). Este nuevo mecanismo permitirá al ciudadano establecer sus relaciones de confianza con terceros.

Como es sabido, desde hace más de 50 años, el DNI es el documento público que acredita la auténtica personalidad de su titular y es, a la vez, el justificante de su identidad. Este documento es imprescindible, desde su creación, en el territorio español para justificar por sí mismo y de manera oficial la personalidad de su titular. Además, sirve para acreditar la nacionalidad española del titular y los datos personales que en él se consignan.

El DNI electrónico (DNI-e) garantizará la identidad de cada individuo (rasgos y propiedades que le diferencian de los demás) mediante mecanismos y procesos electrónicos y no sólo físicos, como hasta ahora. Los principales objetivos que la DGP pretende poner en marcha con el nuevo DNI-e son los siguientes:

1. Proporcionar un mecanismo de identificación al ciudadano, de manera que tanto física como electrónicamente, se pueda acreditar la identidad del titular del DNI-e.
2. Posibilitar que se lleve a cabo la firma digital de documentos mediante protocolos de identificación, autenticación y firma electrónica[1].
3. Fomentar, en todo el Estado Español, la confianza en la Sociedad de la Información y en los nuevos medios electrónicos, proporcionando un mecanismo adecuado que garantice la identidad, privacidad y derechos fundamentales de los ciudadanos.
4. Cooperar con los diferentes proyectos europeos relacionados con la identificación digital.
5. Mantener su funcionalidad y características como documento de viaje (futuro pasaporte), teniendo en cuenta al Reconocedor Óptico de Caracteres de la Organización Internacional de Aviación Civil[2].

Para ello, la DGP tiene previsto implantar una infraestructura de clave pública (PKI) que dotará al nuevo DNI-e de los mecanismos necesarios para cumplir con los objetivos anteriores.

El resto del presente trabajo se distribuye de la siguiente manera: en la sección 2 se presenta el soporte físico del nuevo DNI-e, es decir, las características de la tarjeta y del chip que constituyen la parte física del DNI-e. Las características criptográficas en las que se fundamenta la seguridad lógica del DNI-e, es decir, la PKI a emplear se describe en la sección 3. En la sección 4 se presentan las conclusiones. En las referencias se incluye la legislación en vigor que regula los diferentes aspectos que afectan al DNI y al DNI-e ([15], [16],[17]).

2. Soporte físico

En primer lugar, se puede apreciar que la apariencia del DNI-e apenas difiere de la del actual (véase la Figura 1). La diferencia más notable es la de la aparición del chip insertado en la tarjeta (por razones de seguridad, la mayoría las figuras de este trabajo han sido reducidas y tienen una resolución de 72 ppp).

[1] IAS: Identification, Authentication and Electronic Signature.

[2] OCR-ICAO: Optical Character Recognition-International Civil Aviation Organization.

Figura 1. Aspecto del nuevo DNI electrónico

A continuación se describen las principales características físicas del DNI-e, que hacen referencia a las propiedades de la tarjeta y a las del chip que ésta llevará.

2.1. Tarjeta

La tarjeta del DNI-e consiste en un soporte de policarbonato, con una durabilidad estimada de unos 10 años. Dicha tarjeta es similar a cualquier otra tarjeta de crédito, tarjeta monedero o tarjeta con chip que se puede encontrar actualmente.

Con el fin de dotar de una alta seguridad física a la tarjeta base del DNI-e, ésta se personaliza mediante un dispositivo láser de grabación destructiva. Esta operación tiene tres niveles:

1. Nivel 1, formado por los elementos perceptibles a simple vista:
   - Holograma[3] o Kinegrama[4] protegido por un overlay[5] de 100 nm., diseñado artísticamente.
   - Tintas Ópticamente Variables[6], es decir, tintas de impresión con cambio de color (ver Figura 2).

[3] Estructura de difracción microscópica fina, mediante la que se generan imágenes tridimensionales.

[4] Estructura de difracción microscópica por la que se generan imágenes no tridimensionales, pero que al moverlas muestran animaciones gráficas.

[5] Imagen digitalizada que se superpone a los datos impresos de la misma forma que lo hace el pre-impreso en una impresora de impacto.

[6] OVI: Optically Variable Ink.

Figura 2. Tintas ópticamente variables

- Imagen Láser Cambiante[7], esto es, elementos de información diferentes y específicos combinados en una estructura grabada a láser (ver Figura 3), junto con una fotografía láser múltiple[8].

Figura 3. Imágenes láseres cambiantes

- Letras detectables al tacto.
- Estructuras superficiales en relieve.

2. Nivel 2, caracterizado por marcas que sólo resultan perceptibles mediante equipos mecánicos y electrónicos:
   - Fondo de seguridad: constituido por unas gráficos de guilloches[9] que pueden incorporar logotipos, junto con una impresión irisada (ver Figura 4).
   - Tintas visibles únicamente con luz ultravioleta o infrarroja, así como tintas fluorescentes (ver Figura 5).

[7] CLI: Changing Laser Image.
[8] MLI: Multiple Laser Image.
[9] Patrones complejos formados por líneas curvadas trazadas según principios matemáticos.

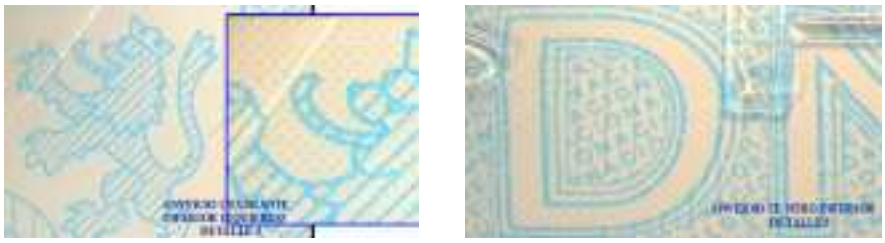

Figura 4. Ejemplos de guilloches

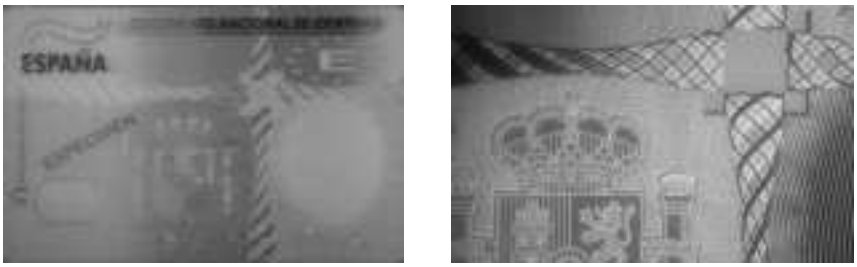

Figura 5. Tintas visibles con luz ultravioleta o infrarroja

- La fotografía del individuo grabada con tecnología láser en el fondo de la tarjeta y protegida contra la falsificación. Dicha fotografía presentará un borde del retrato superpuesto junto con un fondo de seguridad (véase Figura 6).

Figura 6. Fotografía del titular del DNI-e

3. Nivel 3, compuesto por elementos que sólo son perceptibles en laboratorio:
   - Medidas criptográficas.
   - Medidas biométricas.

2.2. Chip

La exigencias relacionadas con el nivel de seguridad del chip a utilizar son las siguientes:

- Certificación Common Criteria con un nivel de seguridad CC EAL 4+ ó superior ([1]).
- Dispositivo seguro de creación de firma CWA 14890-3 ([2]).
- Las aplicaciones que se ejecuten en la tarjeta tendrán, al menos, el nivel de certificación EAL4+.
- Los chips provendrán de, al menos, dos suministradores.

La información contenida en el chip estará firmada electrónicamente por la autoridad de certificación del DNI-e, con el fin de garantizar su autenticidad e integridad y será la siguiente:

- Los datos de filiación del ciudadano.
- Imagen digitalizada de la fotografía.
- Imagen digitalizada de la firma manuscrita.
- Plantilla de la impresión dactilar.
- Datos criptgráficos.
- Datos biométricos.
- Una aplicación de Match On Card.
- Un procesador con capacidad criptográfica para garantizar que la clave privada del ciudadano no sale nunca del soporte físico.
- Un certificado de autenticación, X509v3.
- Un certificado de firma (no repudio), X509v3.
- El certificado de la autoridad de certificación emisora.

Dicho contenido estará estructurado en tres zonas o áreas:

- Primera zona, que será de acceso libre a voluntad del titular (vía PKCS#11) y será empleada en el proceso de autenticación. En ella se almacenarán los certificados.
- Segunda zona, en la que se guardará la huella dactilar del individuo. Esta zona sólo será accesible por personal autorizado de las FCSE[10] y se empleará en aplicaciones Match On Card, necesarias para procesos como borrado de certificados en la tarjeta, renovación de certificados, etc. Además, esta huella servirá para la autenticación inmediata de cualquier individuo a través del dispositivo oportuno, sin más que validar la huella de éste con la que se encuentra almacenada en el DNI-e. Los certificados de ciudadano que se almacenan en el DNI-e no disponen del habitual número de desbloqueo PUK[11]. En esta situación, caso de llegar a bloquearse la tarjeta, ésta sólo se podrá volver a ser habilitada mediante el empleo de la huella dactilar del propio individuo.
- Tercera zona, en la que irán todos los datos de filiación. Estos datos, al igual que la huella dactilar, sólo estarán disponibles para las personas autorizadas (FCSE).

[10] FCSE: Fuerzas y Cuerpos de Seguridad del Estado.
[11] PUK: Personal Unblocking Key.

3. Soporte lógico

En esta sección se presenta el soporte lógico en el que se basa la seguridad del DNI-e. En primer lugar se comentan los protocolos de firma digital y de certificación (para más información véanse, por ejemplo, [5], [6], [8], [14]), para desarrollar, posteriormente y con mayor detalle, la infraestructura de clave pública en la que se fundamenta la puesta en marcha del DNI-e.

3.1. Firma electrónica y Certificados digitales

La legislación española contempla tres tipos diferentes de firma electrónica:

1. Firma electrónica: conjunto de datos, en forma electrónica, consignados junto a otros o asociados con ellos, con los que se identifica al firmante.
2. Firma electrónica avanzada: es la firma electrónica que permite la identificación del firmante y ha sido creada por medios que éste puede mantener bajo su exclusivo control.
3. Firma electrónica reconocida: es la firma electrónica avanzada basada en un certificado reconocido y generada mediante dispositivos seguros de creación de firma.

Para poder implementar cualquiera de ellas, hace falta tener instalados los certificados correspondientes. Por otra parte, los ejes en los que se fundamenta la puesta en marcha del DNI-e son los siguientes: Confidencialidad (capacidad de intercambiar información de forma segura y secreta), Integridad (garantía de que la información no ha sido modificada ni alterada), Autenticación (prueba de la identidad de emisor) y No repudio (garantía que tiene el receptor de que el emisor ha realizado una transacción). Estos ejes quedarán garantizados por la DGP con la incorporación al DNI-e de los siguientes certificados digitales.

- Certificado X509 de autenticación del ciudadano, que permitirá acreditar y garantizar electrónicamente la identidad del ciudadano frente a terceras partes.
- Certificado X509 de firma (o de no repudio) del ciudadano para garantizar que un documento firmado electrónicamente por el titular no ha sido alterado, y para acreditar la procedencia del documento firmado y la identidad del firmante. La firma de documentos electrónicos se llevará a cabo mediante el protocolo estándar de firma digital ([4], [6], [8], [13]), es decir, la firma electrónica de un ciudadano para un documento digital será el resultado de cifrar con su clave privada un resumen (hash, véanse [7], [11], [12]) del documento. La verificación de la firma se realizará mediante el acceso al servicio de validación, que publicará la DGP, con el fin de comprobar que el certificado de firma no ha sido revocado o anulado.
- Certificado X509 de la Autoridad Raíz.

3.2. Pre-personalización del DNI-e

El proceso de emisión de un DNI-e requiere de varias fases, de modo que quede garantizada la seguridad de cada una de las partes que intervienen en el proceso de emisión (autoridades de certificación, puestos de expedición, etc.).

La primera fase es la de pre-personalización de la tarjeta.

Como se puede apreciar en el modelo esquematizado en la Figura 7, la Fábrica Nacional de Moneda y Timbre (FNMT) será la encargada de proporcionar lotes de tarjetas para su utilización como soporte para el DNI-e a los distintos Puestos de Expedición (Comisarías de policía), así como de las tarjetas para la identificación de estos puestos (TIP: Tarjeta de Identificación de Puesto).

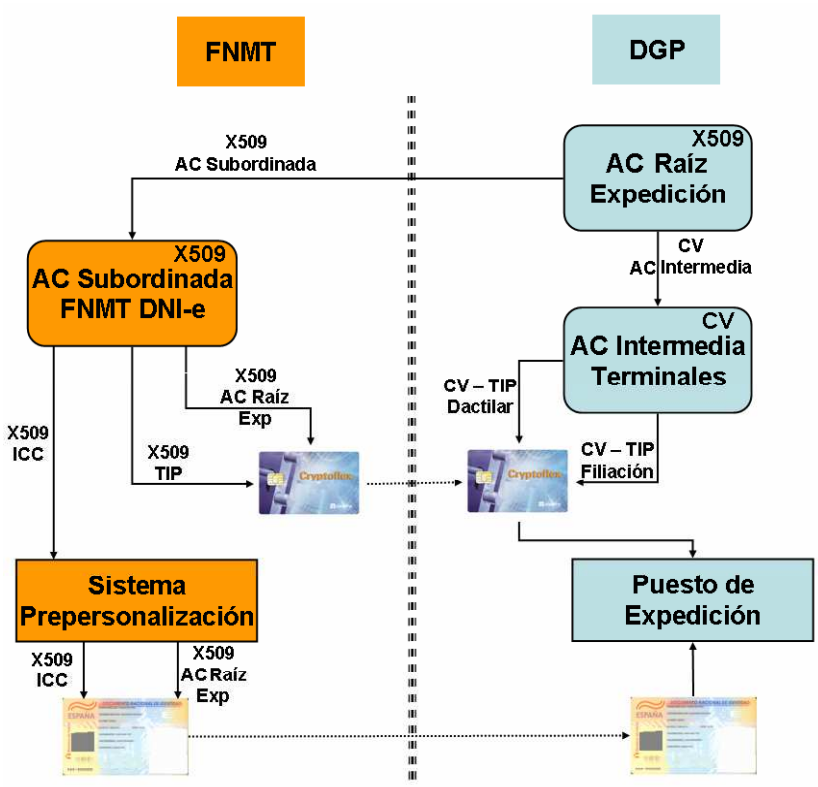

Figura 7. Modelo de Referencia del proceso de pre-personalización

Para que la FNMT lleve a cabo esta tarea, una Autoridad de Certificación Raíz de Expedición, ubicada en dependencias de la DGP, generará dos certificados: un certificado X509 para la AC Subordinada de la FNMT dedicada al DNI-e, y otro certificado tipo Card Verificable (CV) para la AC Subordinada

Intermedia de Terminales de la DGP. Este certificado CV está definido acorde con el formato expuesto en el capítulo 14 de CWA 14890-1 (véase [2]).

Por su parte, la AC Subordinada de la FNMT dedicada al DNI-e generará dos certificados X509: uno de identificación de componente para tarjetas TIP y otro de identificación para la tarjeta del DNI-e (ICC). Ambos certificados se guardan en las correspondientes tarjetas, junto con el certificado X509 de la AC Raíz de Expedición. Las tarjetas del DNI-e, una vez pre-personalizadas tanto eléctrica (chip) como físicamente (plástico), son trasladadas a los distintos puestos de expedición, dispuestas para ser personalizadas.

Por otra parte, las tarjetas TIP tienen que ser personalizadas antes de comenzar con la emisión de un DNI-e. Dicha personalización se realiza por parte del personal de la DGP utilizando la consola de administración de una autoridad de certificación (con tecnología Safelayer) del dominio de certificación responsable de la emisión de certificados de componente y de certificados CV (dominio diferente al correspondiente a los certificados de ciudadano). Para ello, la AC Subordinada Intermedia de Terminales de la DGP generará dos certificados CV que se almacenarán en la TIP: uno para la firma de información dactilar y otro para la firma de datos de filiación, incluyendo fotografía y firma manuscrita.

Nótese que la AC Intermedia de Terminales no puede generar una lista de revocación de certificados, dado el carácter de la misma. Sin embargo, mediante una asociación entre el certificado CV de la AC Intermedia de Terminales y un certificado X509 "ficticio" de la misma, sí se puede conseguir una lista de revocación de certificados.

Una vez concluidos los pasos anteriores, la tarjeta del DNI-e estará pre-personalizada tanto física como electrónicamente (un certificado X509 y su cadena de confianza); mientras que la tarjeta TIP estará personalizada (un certificado X509 de identificación, dos certificados CV y las cadenas de confianza). Todo ello permitirá que el puesto de expedición se encuentre en condiciones de emitir el DNI-e a los ciudadanos que lo soliciten.

3.3. Expedición del DNI-e

Una vez que un puesto de expedición dispone de su tarjeta TIP personalizada y de tarjetas pre-personalizadas del DNI-e, ambos se habrán de autenticar mutuamente. Por ello se hizo se necesario el proceso de pre-personalización. La validación se lleva a cabo como sigue: la tarjeta del DNI-e validará el certificado X509 TIP del puesto de expedición, mientras que el puesto de expedición, a su vez, validará el X509 de la tarjeta del DNI-e. Ambos procesos de autenticación son posibles gracias a que se dispone de la cadena de confianza. De esta manera se asegura que un puesto de expedición sólo personalizará aquellas tarjetas que hayan sido emitidas por la FNMT, al igual que las tarjetas del DNI-e sólo podrán ser personalizadas por los puestos de expedición autorizados.

Una vez que se hayan verificado tanto la tarjeta como el puesto de expedición, se procede a la personalización de la tarjeta, es decir, a expedir DNI-e a los ciudadanos que lo soliciten. El proceso de emisión de un DNI-e se puede observar en la Figura 8.

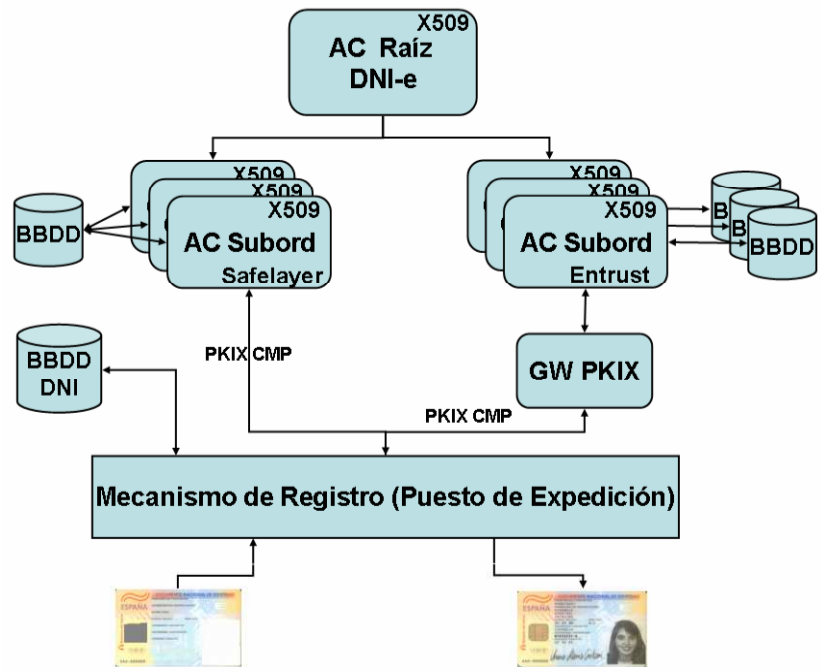

Figura 8. Proceso de Expedición del DNI-e

Cuando un usuario acuda a un puesto de expedición para obtener su DNI-e, rellenará o modificará, según el caso, un formulario con sus datos de filiación. Adicionalmente, será escaneada una fotografía del individuo junto con su firma manuscrita. Una vez se disponga de estos datos, serán enviados, vía protocolo PKIX-CMP (véase [9]), a una de las posibles autoridades de certificación, la cual se encargará de emitir los correspondientes certificados.

Es de destacar en este modelo PKI para la expedición del DNI-e, la presencia de dos tecnologías completamente distintas en la generación de los certificados: Safelayer y Entrust. Para asegurar la operatividad con ambas, se ha optado por el protocolo PKIX-CMP, si bien la autoridad de certificación de Entrust utilizará un gateway para compatibilizarlo, existiendo un protocolo propietario de Entrust entre dicho gateway y la autoridad de certificación. Otra diferencia entre ambas tecnologías radica en el aspecto de las bases de datos: la de Safelayer, aún en el caso de alta disponibilidad, siempre es única, mientras que en el caso de Entrust, habrá tantas bases de datos como autoridades de certificación.

Los certificados que irán incluidos en el DNI-e se han señalado en **S**3.1. El resto de información necesaria para completar la personalización del DNI-e se introducirá también en la tarjeta, para lo que se emplearán los certificados CV de la tarjeta TIP. Toda la información dactilar, así como la de filiación, fotografía

y firma manuscrita, viajará firmada hasta la propia tarjeta. En ese momento la tarjeta tendrá que validar la firma de los dos certificados CV que dispone la tarjeta TIP para proceder a la grabación de los datos. Al finalizar este proceso, el DNI-e estará completamente personalizado y el ciudadano podrá disponer del mismo.

La validez de estos certificados incluidos en el DNI-e será de 36 meses, mientras que la del DNI-e será similar a la actual, es decir, 5 años para los ciudadanos menores de 30 años y 10 para los mayores. Por tal motivo, los certificados del ciudadano deberán renovarse. Para ello se dispondrán unos Dispositivos Autónomos Autorizados (DAA) que se encargarán de realizar la renovación de los certificados. En el proceso de renovación, el ciudadano deberá autenticarse, para lo que será necesaria su huella dactilar.

3.4. Revocación de certificados

Una importante novedad que se presenta en este modelo de PKI, es la relacionada con la revocación de los certificados.

En el modelo de referencia de la Figura 9, se ha introducido una entidad, denominada Autoridad de Revocación de Certificados (CRA), que es quien centraliza este proceso y que responde a las siguientes necesidades:

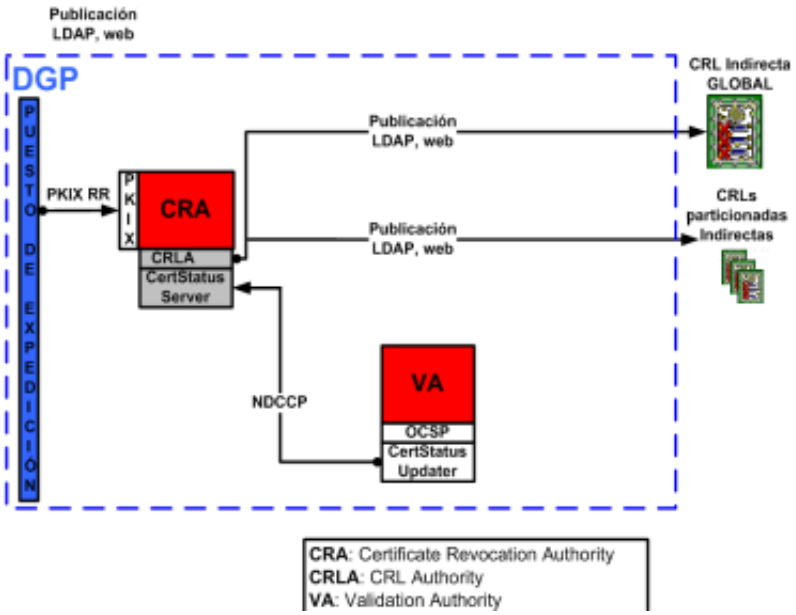

Figura 9. Proceso de Revocación del DNI-e

1. Disponibilidad. En general, la misma AC que emite un certificado es la que tiene que revocarlo, en caso necesario. Sin embargo, este proceso supone un obstáculo en el sistema presentado anteriormente, por lo que para solventarlo, el proceso de revocación se centraliza en una entidad aislada de la AC emisora.
2. Multitecnología. Dado que en el modelo de PKI presentado se emplean dos tecnologías diferentes, si la misma AC que emitió un certificado fuera la responsable de revocarlo, surgiría el problema de determinar cuál de las dos tecnologías es la emisora.
3. Vigencia. El uso de una Lista de Certificados Revocados (CRL[12]) supone que una aplicación no refrescará la CRL de que actualmente dispone hasta que la vigencia de la misma haya expirado. Este hecho repercute de forma directa en la en la inmediatez del proceso de revocación y propagación del estado del certificado a las aplicaciones usuarias de los mismos.

Teniendo en cuenta que la RFC 3280 (véase [10]) señala que los procesos de revocación de certificados pueden no estar vinculados a la propia AC emisora y que se pueden utilizar mecanismos no basados en CRLs, se ha optado por mecanismos de validación en línea. Además, como la generación de CRLs en el sistema sigue siendo necesaria y dado que no es objetivo de la DGP el dimensionamiento de un sistema para una autoridad de validación nacional con 80 millones de certificados vigentes en un entorno de uso del DNI-e, diferente del de procesos propios de la DGP, es necesario un mecanismo de alimentación del estado de los certificados para con el exterior. Este mecanismo se puede conseguir de dos formas diferentes:

- Procesos batch: Para lo que se requiere una CRL global. Dado que hay diferentes AC y un único punto de revocación, se ha optado por la CRL indirecta.
- Procesos de validación externos. Para ello, el DNI-e incorpora en el propio certificado la extensión AIA OCSP[13] con una URL[14] nacional que podrá ser trasladada según diferentes criterios (DNS, aplicación, etc.). El mecanismo más apropiado para ello es dividir la CRL en otras más pequeñas, de modo que éstas puedan ser actualizadas por las instituciones o Proveedores de Servicios de Certificación Nacionales que se establezcan, con una frecuencia mayor a su propia vigencia. Estos proveedores podrán ofrecer servicios de validación del DNI-e, bien basándose en el certificado presentado por el ciudadano (OCSP, SCVP[15]), bien validando las firmas realizadas por éstos en sus procesos de autenticación/no repudio (DSS[16]).

[12] CRL: Certificate Revocation List.
[13] AIA OCSP: Online Certificate Status Protocol.
[14] URL: Uniform Resource Locator.
[15] SVCP: Simple Certificate Validation Protocol.
[16] DSS: Digital Signature Standard.

La CRL es, por tanto, un subproducto utilizado como mecanismo de transporte de la información del estado de los certificados del DNI-e, entre la DGP y las instituciones.

4. Conclusiones

Desde que la ley 59/2003, de 19 de Diciembre, de firma electrónica atribuyera al documento nacional de identidad la capacidad de acreditar electrónicamente la identidad de su titular y reconociera a éste la facultad de firmar electrónicamente documentos, se inició un proceso de cambio tecnológico del que somos testigos y que no ha hecho más que comenzar.

El hito de salida de este proceso fue efectuado durante la ceremonia de generación de claves de la AC raíz, acto presidido por el entonces ilustre Ministro del Interior D. José Antonio Alonso. La colocación de esta primera piedra ha venido seguida por sucesivos progresos, como la expedición inicial de documentos en la provincia de Burgos o la puesta en marcha de un portal de información al ciudadano acerca de las bondades del nuevo documento (véase [3]).

Sin embargo, lo más importante y destacable del proyecto, no es en sí el propio documento, cuyo ciclo de vida ha sido descrito en el presente artículo. Lo verdaderamente destacable son las implicaciones sociales que acarrea y que desde ya, todos los ciudadanos pueden disfrutar. Debe tenerse en cuenta que, conjuntamente con la aparición del DNI-e, la Administración Pública, en su conjunto, está implantando proyectos que la acerquen a la sociedad y permitan a sus ciudadanos agilizar tediosos trámites burocráticos que exigían acreditar su identidad, lo que ahora ya se puede hacer de forma electrónica. Sólo por ofrecer una muestra, en los dos primeros meses desde de la emisión del primer DNI-e existen más de 40 servicios administrativos DNIe-Ready y otros tantos en preparación.

El DNI ha sido durante más de 50 años una enseña española de identidad, ahora lo seguirá siendo, pero además electrónicamente.

Una gestación del proyecto de más de cinco años, con intervención en diferentes proyectos internacionales, ha servido para que hoy se disponga de un Documento con capacidad de ofrecer servicios en el presente y con una clara orientación de futuro. No se debe olvidar que España es una de las pioneras en este tipo de tecnología y que actualmente en el resto del mundo, y de forma más cercana y quizás más pragmática, se está trabajando en el desarrollo de estándares de identidad electrónica. El DNIe no puede y no debe cerrarse a la interoperabilidad futura. Ha sido diseñado atendiendo a las diferentes líneas de estandarización y debe continuar dicha línea, adaptarse a nuevos cambios y sobre todo por su experiencia, liderarlos.

Agradecimientos

Este trabajo ha sido parcialmente subvencionado por el Ministerio de Educación y Ciencia bajo el Proyecto SEG2004-02418. Los autores agradecen a la

Dirección General de la Policía, así como a la Unión Temporal de Empresas formada por Telefónica, Indra y Software AG, por su colaboración prestada para la realización de este trabajo.

Referencias

1. CC EAL 4+, `http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1$\&$dis-playPage=13`
2. CWA 14890, *Application Interface for smart cards used as Secure Signature Creation Devices-Part 1: Basic requirements*, `ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf`; *Application Interface for smart cards used as Secure Signature Creation Devices-Part 2: Additional Services*, `ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eSign/cwa14890-01-2004-Mar.pdf`
3. `http://www.dnielectronico.es`
4. R. Durán Díaz, L. Hernández Encinas y J. Muñoz Masqué, *El criptosistema RSA*, RA-MA, Madrid, 2005.
5. W. Feghhi, J. Feghhi and P. Williams, *Digital certificates*, Applied Internet Security, Addison-Wesley, Reading, MS, 1999.
6. A. Fúster Sabater, D. Guía Martínez, L. Hernández Encinas, F. Montoya Vitini y J. Muñoz Masqué, *Técnicas criptográficas de protección de datos*, RA-MA, Madrid, 3^a ed., 2004.
7. National Institute of Standards and Technology, Secure hash standard, *FIPS PUB*, 180-1 (1995).
8. A.J. Menezes, P.C. van Oorschot and S. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.
9. PKIX-CMP, `http://www.entrust.com/resources/docs/protocols_pki.htm`
10. RFC 3280, `http://www.faqs.org/rfcs/rfc3280.html`
11. R.L. Rivest, The MD4 message digest algorithm, *Proc. Crypto'90, LNCS* **741** (1991), 303–321.
12. R.L. Rivest, RFC 1321: The MD5 message-digest algorithm, *Internet Activity Board*, 1992.
13. R. Rivest, A. Shamir and L. Adelman, A method for obtaining digital signatures and public key cryptosystems, *Comm. ACM* **21** (1978), 120–126.
14. W. Stallings, *Cryptography and network security*, 2nd. ed., Prentice Hall, 1999.
15. Legislación sobre Firma electrónica: *Directiva 1999/93/CE* y *Ley 59/2003*.
16. Legislación sobre Protección de Datos Personales: *Directivas 1995/46/CE, 97/66/EC, 2002/58/CE*, *Reglamento (EC) 45/2001*, *L.O. 15/1999*, *Real Decreto 994/1999*, *Leyes 34/2002 y 32/2003*.
17. Legislación del DNI y del DNI-e: *Decreto 196/1976 regulación del DNI*, *Parcialmente modificado por R.D. 1189/1978, 2002/1979, 2091/1982, 1245/1985*, *L.O. 1/1992, de Protección de la Seguridad Ciudadana*, *Orden del Ministerio del Interior de 12/7/1990 26/4/1996*, *R.D. 896/2003 de Regulación del Pasaporte*.