Towards a new electronic identification of citizens: the DNI-e

Published at the RECSI 2006 conference proceedings
(Spanish Conference on Cryptography and Information Society).
Editors J. Borrell and J. Herrera.

By J. Crespo (Spanish DGP), J. Espinosa (Safelayer), L. Hernández (CSIC),
H. Rifà (Safelayer), M. Torres (Safelayer)

Summary: The electronic Spanish Identity Card (DNI-e) aims to provide Spanish citizens with an identification mechanism that enables them to electronically sign documents and improve the level of trust of the Spanish population in the Information Society. This work presents the main features of the DNI-e, in terms of its physical support (card and chip) and from a logical viewpoint (digital certificates, electronic signatures, keys, etc). Particular emphasis is placed on Public Key Infrastructure (PKI), the basis of its development and future use.

Keywords: Citizen Authentication, Digital Certificates, Public Key Cryptography, DNI-e, Electronic Identification.

1. Introduction

The rapid development of Information Technologies in our society makes it necessary for them to respond to emerging challenges, a request that is on the rise among users. One such challenge is to guarantee and provide citizens with the appropriate mechanisms to ensure their privacy, freedom and rights in today's democratic framework.

In order to respond to the challenge of personal digital identification, the Spanish Ministry of Interior, via the Spanish Directorate General of Police (DGP) affiliated organisation, will provide Spanish citizens with a new identification mechanism based on the current Spanish Identity Card (DNI). The new mechanism will allow citizens to establish trusted relationships with third parties.

For over fifty years, the DNI has been the public document used to prove the genuine personality of its holder while providing evidence of the person's identity. From the outset, it has been compulsory in Spain as proof in itself and officially of the bearer's personality, and serves to ascertain the bearer's Spanish nationality and the personal information contained therein.

The electronic ID Card (DNI-e) will guarantee the identity of each individual (the features and properties that set the person apart from others) using mechanisms and processes that are electronic rather than merely physical, as has been the case to date. With the new DNI-e, the DGP aims to:

1. Provide citizens with an identification mechanism that can accredit the identity of the DNI-e holder both physically and electronically.

2. Enable documents to be digitally signed using identification, authentication and electronic signature protocols[1].
3. Build trust, throughout Spain, in the Information Society and new electronic media, providing a mechanism that is able to guarantee the identity, privacy and fundamental rights of citizens.
4. Cooperate with European projects related to digital identification.
5. Maintain its functionality and features as a travel document (future passport), taking into account the Optical Character Recognition of the International Civil Aviation Organization[2].

The DGP plans to introduce a Public Key Infrastructure (PKI) that will provide the new DNI-e with the mechanisms needed to comply with these objectives.

The remainder of this paper is distributed as follows: section 2 presents the new DNI-e's physical support, that is, the features of the card and chip that constitute the physical part of the DNI-e. The cryptographic features on which the logical security of the DNI-e is based (its PKI) are described in section 3. The conclusions are presented in Section 4. References include the current legislation regulating different aspects that affect the DNI and DNI-e ([14], [15], [16]).

2. Physical support

The appearance of the DNI-e is very similar to the one used at present (see Figure 1). The most remarkable difference is the security chip embedded in the card.

The main physical features of the DNI-e, including the properties of the card and its chip, are described below.

2.1. Card

The DNI-e card consists of a polycarbonate support, with an estimated durability of approximately ten years. The card is similar to any other credit card, electronic wallet or card with a chip that can be found today.

[1] IAS: Identification, Authentication and Electronic Signature.
[2] OCR-ICAO: Optical Character Recognition-International Civil Aviation Organization.

Figure 1. Appearance of the new DNI-e

In order to achieve a high level of physical security in the DNI-e base card, it is customised using a destructive recording laser device. The operation has three levels:

1. Level 1, made up of the elements that are visible to the naked eye:

- Hologram[3] or Kinegram[4] protected with an artistically designed 100-nm overlay[5].
- Optically Variable Ink[6], that is, printing ink that changes colour (see Figure 2).
- Changing Laser Image[7], i.e., specific informative elements combined in a laser printed structure (see Figure 3), together with a Multiple Laser Image[8].
- Letters detected by touch.
- Embossed superficial structures.

2. Level 2, characterised by marks that can only be perceived using mechanical and electronic equipment:

Figure 2. Optically Variable Ink

[3] Thin microscopic diffraction structure that generates three-dimensional images.
[4] Microscopic diffraction structure that generates non-three-dimensional images that show graphic animations when moved.
[5] Digital image superimposed on printed data the same way an impact printer does a preprint.
[6] OVI Optically Variable Ink.
[7] CLI: Changing Laser Image.
[8] MLI: Multiple Laser Image.

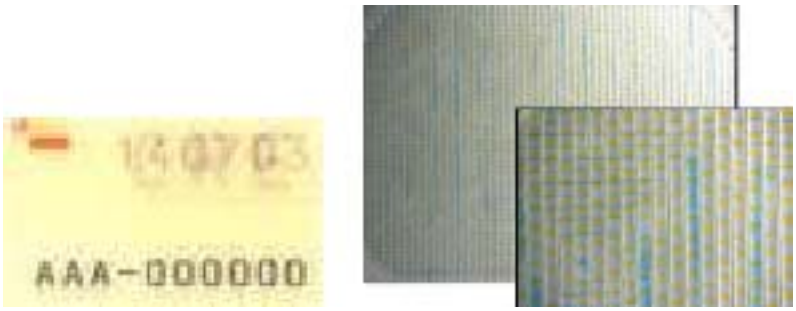

Figure 3. Changing laser images

- Security background: made up of Guilloché patterns[9] that can incorporate logos, together with an iridescent print (see figure 4).


Figure 4. Examples of Guilloché patterns

- Inks that are only visible with ultraviolet and infrared light, as well as fluorescent inks (see Figure 5).

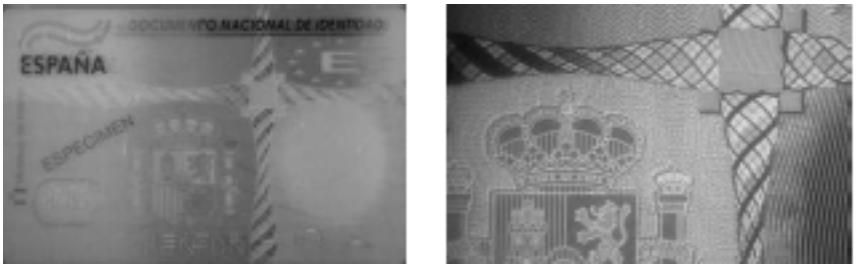

Figure 5. Inks visible with ultraviolet and infrared light

- The photograph of the individual printed with laser technology on the background of the card and protected against forgery. The photograph will feature a rim of the portrait superimposed alongside the security background (see Figure 6).


Figure 6. Photograph of the DNI-e holder

3. Level 3, comprising elements that can only be perceived in a laboratory:

[9] Complex patterns formed by curved lines traced according to mathematical principles.

- Cryptographic measures.
- Biometric measures.

2.2. Chip

The requirements related to the chip's level of security are:

- Common Criteria certification with a CC EAL 4+ level of security or higher ([1]).
- Secure signature creation device CWA 14890-3 ([2]).
- The minimum certification level of applications executed in the card will be EAL4+.
- The chips will come from a minimum of two suppliers.

The information contained in the chip will be electronically signed by the DNI-e certification authority in order to guarantee its authenticity and integrity, and it will comprise:

- The individual's personal details.
- Digital image of the photograph.
- Digital image of the hand-written signature.
- Fingerprint template.
- Cryptographic data.
- Biometric data.
- A Match-On-Card application.
- Processor with cryptographic capacity to guarantee that the citizen's private key never leaves the physical device.
- X.509v3 authentication certificate.
- X.509v3 signature certificate (non-repudiation).
- The certificate of the issuing certification authority.

This content will be structured in three zones or areas:

- First zone, with free access at the holder's discretion (via PKCS #11) will be used during the authentication process. The certificates will be stored here.
- Second zone, where the individual's fingerprint is stored. This zone will only be accessible for authorised personnel belonging to the State Security Forces and Agencies (FCSE) and will be used in Match-On-Card applications, necessary for processes such as removing certificates from the card, renewing certificates, etc. The fingerprint will also serve to instantly authenticate any individual using the appropriate device simply by validating the person's fingerprint against the one stored in the DNI-e. Citizen certificates stored in the DNI-e do not include the usual PUK[10]. If the card becomes blocked, it will only be authorised again by means of the fingerprint of the same individual.
- Third zone, containing the personal data, which, like the fingerprint, will only be available to authorised parties (FCSE).

[10] PUK: Personal Unblocking Key.

3. Logical support

This section presents the logical support on which DNI-e security is based. The digital signature and certification protocols are explained first (for further information see [4], [5], [7], [13]), then a detailed description is given of the public key infrastructure on which the DNI-e start-up is based.

3.1. Electronic signature and Digital certificates

Spanish law provides for three types of electronic signature:

1. Electronic signature: set of electronic data consigned or associated with other data used to identify the signer.
2. Advanced electronic signature: electronic signature used to identify the signer created by means that the latter can keep under his/her exclusive control.
3. Recognised electronic signature: advanced electronic signature based on the recognised certificate and generated using secure signature creation devices.

To implement any of the above signatures, the corresponding certificates have to be installed. Moreover, the DNI-e start-up is based on: Confidentiality (ability to exchange information in a secure and secret manner), Integrity (guarantee that the information has not been modified or altered), Authentication (issuer's proof of identity) and Non-repudiation (the receiver's guarantee that the issuer has carried out a transaction). These axes will be guaranteed by the DGP by incorporating the following digital certificates in the DNI-e:

- X.509 Citizen authentication X.509 certificate for electronically accrediting and guaranteeing the citizen's identity to third parties.
- X.509 Citizen signature (or non-repudiation) X.509 certificate for guaranteeing that a document digitally signed by the holder has not been altered and accrediting the origin of the signed document and the signer's identity. Electronic documents will be signed by means of the standard digital signature protocol ([3], [5], [7], [12]), that is, a citizen's electronic signature for a digital document will be the result of ciphering a digest (hash, see [6], [10], [11]) of the document with his/her private key. The signature will be verified by accessing the validation service published by the DGP to verify that the signature certificate has not been revoked or cancelled.
- X.509 certificate of the Root Authority.

3.2. Pre-personalisation of the DNI-e

The DNI-e issuing process involves a number of stages to guarantee the security of each of the parts that intervene in the issuing process (certification authorities, issuing places, etc).

The first stage is the pre-personalisation of the card.

As illustrated in the schematic model in Figure 7, the Spanish Royal Mint (FNMT) will be in charge of providing batches of cards to be used as the DNI-e support

to the Issuing places (Police stations), as well as cards for identifying these posts (Post identification card).

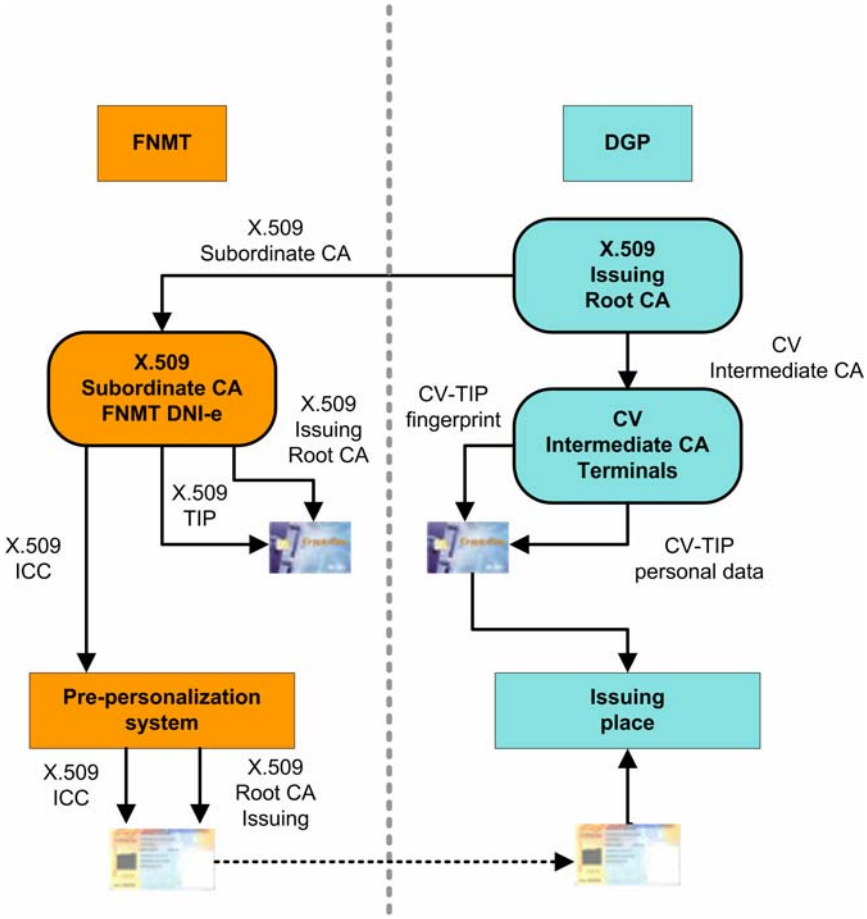

Figure 7. Reference model of the pre-personalisation process

For the FNMT to carry out the task, an Issuing Root Certification Authority located in the DGP offices will generate two certificates: an X.509 certificate for the FNMT's Subordinate CA dedicated to the DNI-e, and another Card Verifiable (CV) certificate for the DGP's Intermediate Subordinate CA for Terminals. This CV certificate is defined according to the format described in chapter 14 of the 14890-1 CWA (see [2]).

Meanwhile, the FNMT's Subordinate CA dedicated to the DNI-e will generate two X.509 certificates: a component identification certificate for TIP cards and an identification certificate for the DNI-e card (ICC). Both certificates are stored in the corresponding cards together with the X.509 certificate of the Issuing Root CA. The DNI-e cards, once they are both electronically (chip) and physically (plastic) pre-personalised, are moved to the various issuing places, ready to be personalised.

TIP cards have to be personalised before issuing any DNI-e. DGP personnel are in charge of personalisation using a certification authority's administration console (with Safelayer technology) of the certification domain responsible for issuing component certificates and CV certificates (a different domain to the one used for citizens' certificates). To do so, the DGP's Intermediate Subordinate CA for Terminals

will generate two CV certificates that will be stored in the TIP: one for signing fingerprint information and the other for signing personal data, including the photograph and hand-written signature.

It is worth noting that, given its nature, the Intermediate CA for Terminals cannot generate a certificate revocation list. However, a certificate revocation list can be achieved by associating the CV certificate of the Intermediate CA for Terminals and a "fictitious" X.509 certificate of the same authority.

Once the previous steps are taken, the DNI-e card will be both physically and electronically pre-personalised (a X.509 certificate and its chain of trust), and the TIP card will be personalised (an identification X.509 certificate, two CV certificates and their chains of trust). All of this will enable the issuing place to deliver the DNI-e to those citizens that request it.

3.3. Issuing the DNI-e

Once the issuing place has its personalised TIP card and pre-personalised DNI-e cards, both will need to be mutually authenticated, that is the reason to require a pre-personalisation process. Validation is completed as follows: the DNI-e card validates the issuing place's TIP X.509 certificate, whilst the issuing place validates the DNI-e card's X.509. Both authentication processes are possible thanks to the chain of trust. This ensures that the issuing place will only be personalised by cards issued by the FNMT and that DNI-e cards can only be personalised by authorised issuing places.

Once the card and the issuing place have been verified, the card is personalised, that is, the DNI-e is issued to the citizens requesting it. The DNI-e issuing process is described in Figure 8.

When users go to an issuing place to get their DNI-e, they are asked to either fill in or modify a form with their personal data. In addition, a photograph of the individual is scanned together with his/her hand-written signature. Once the data has been collected, it is sent via PKIX-CMP protocol (see [8]) to one of the certification authorities, which will be responsible for issuing the certificates.

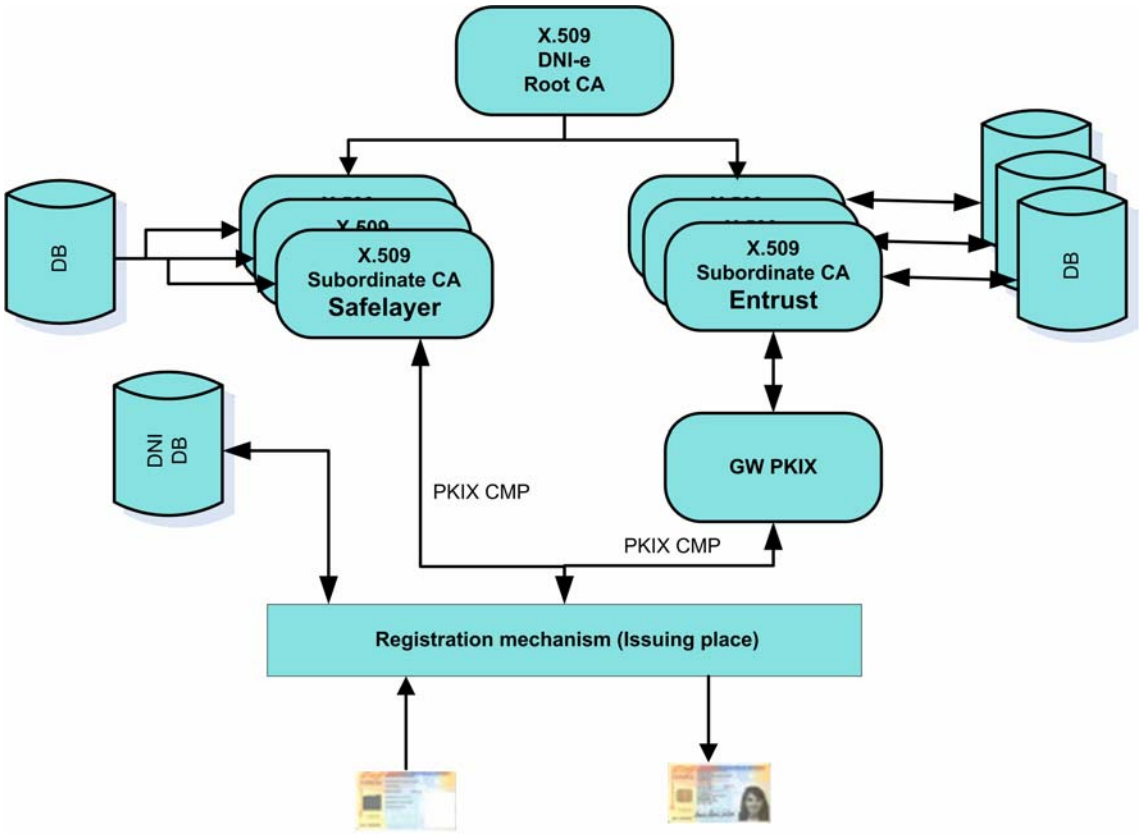

Figure 8. DNI-e Issuing Process

Attention must be paid to the fact that in the PKI model for issuing the DNI-e there are two completely different technologies for generating certificates: Safelayer and Entrust. The PKIX-CMP protocol has been chosen to ensure their interoperability , although the Entrust certification authority will use a gateway to make it compatible, with a protocol owned by Entrust between the gateway and certification authority. Another difference between both technologies lies in the databases: even in the event of high availability, Safelayer technology is always unique, whilst Entrust's will have as many databases as there are Certification Authorities.

Certificates included in the DNI-e are specified in section 3.1. The remaining information needed to complete the personalisation of the DNI-e will also be recorded in the card using the TIP card's CV certificates. The fingerprint information, personal details, photograph and hand-written signature will be signed before being transferred to the card. The card will then have to validate the signature of both CV certificates of the TIP card to proceed to store the data. At the end of this process, the DNI-e will be completely personalised and the citizen will be able to use it.

The certificates included in the DNI-e will be valid for 36 months. Even so, the DNI-e will last for as long as the traditional DNI: five years for people under the age of thirty and ten years for those over thirty. Therefore, citizens' certificates will have to be renewed by means of Authorised Autonomous Devices (AAD). During the renewal process, citizens' fingerprints will be used to authenticate them.

3.4. Certificate revocation

An important new feature of this PKI model has to do with certificate revocation.

The reference model in Figure 9 shows an entity called a Certificate Revocation Authority (CRA) that centralises this process and responds to the following requirements:

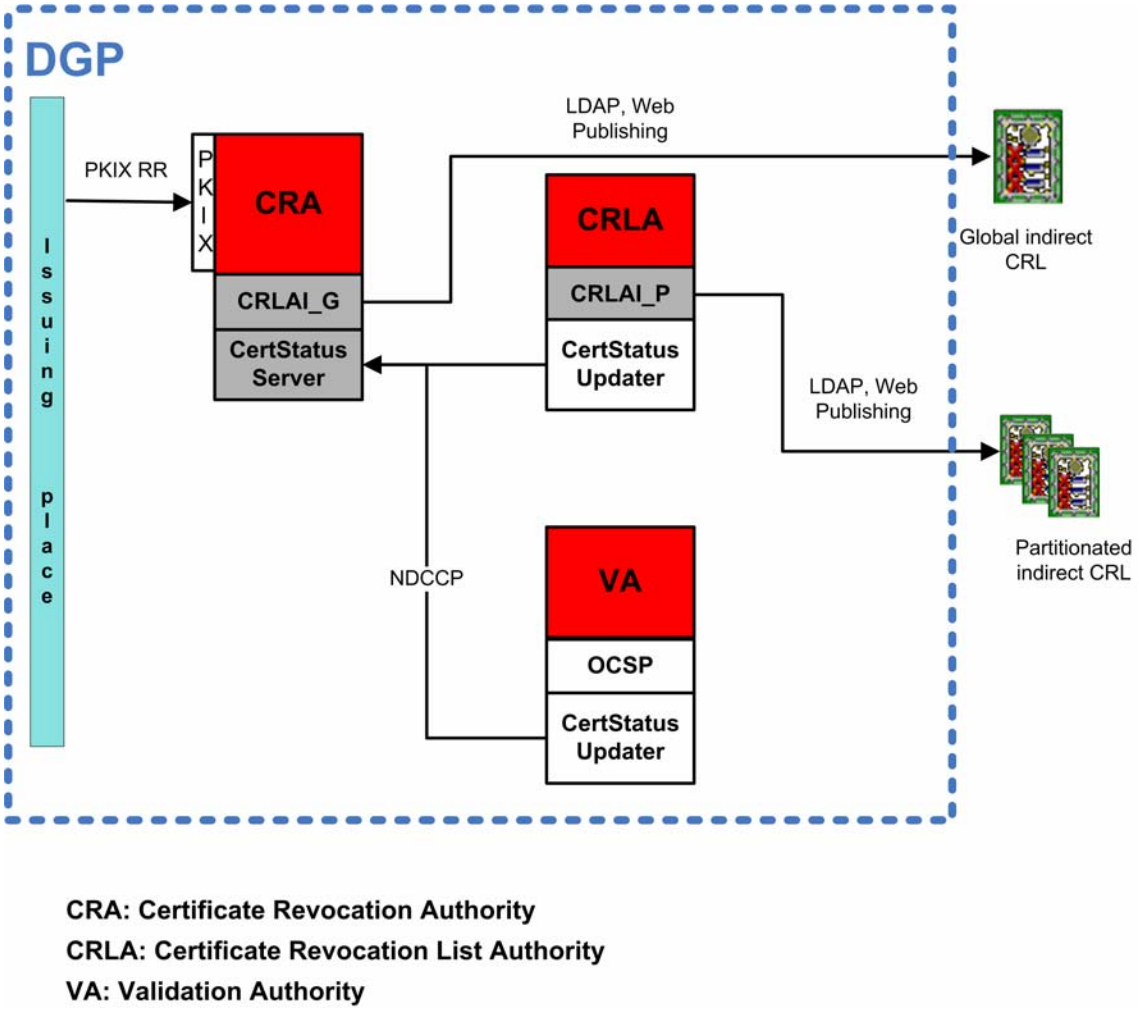

Figure 9. DNI-e revocation process

1. Availability. Generally, the CA issuing a certificate has to revoke it, if necessary. However, this procedure represents an obstacle to the above presented system, which can be solved by performing the revocation process on an isolated entity of the issuing CA.

2. Multi-technology. Since the PKI model presented above uses two different technologies, if the CA that issued the certificate was responsible for revoking it, there would be a problem to determine which of the two technologies issued it.

3. Validity. By using a Certificate Revocation List (CRL), an application will not refresh the current CRL until it expires. This has a direct effect of the speed of

the revocation process and the propagation of the certificate status to applications using it.

Online validation mechanisms have been chosen taking into consideration that the RFC 3280 (see [9]) states that the certificate revocation processes may not be linked to the issuing CA and that mechanisms not based on CRLs can be used. Furthermore, since it is still necessary to generate CRLs in the system but the DGP does not aim to gauge a system for a national validation authority with 80 million valid certificates in an DNI-e environment, different from the DGP's own processes, a mechanism is required to feed the status of certificates externally. There are two ways of procuring such mechanism:

- Batch processes. A global CRL is required. Since there are different CAs and only one revocation point, an indirect CRL has been chosen.

- External validation processes. The DNI-e incorporates the AIA OCSP[11] extension in its certificate with a national URL[12] that can be moved using different criteria (DNS, application, etc). The best mechanism to do so is to divide the CRL into smaller lists so that they can be updated by institutions or National Certification Service Providers more frequently than their own validity. These providers will be able to offer DNI-e validation services either based on the certificate presented by the citizen (OCSP, SCVP[13]) or validating the signatures carried out by them during the authentication/non-repudiation processes (DSS[14]).

The CRL is therefore a sub product used as a mechanism for transporting the status information of DNI-e certificates between the DGP and institutions.

References

1. CC EAL 4+, http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&display Page=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. R. Durían Díaz, L. Hernández Encinas and J. Muñoz Masqué, *El criptosistema* RSA, RA-MA, Madrid, 2005.
4. W. Feghhi, J. Feghhi and P. Williams, *Digital certificates*. Applied Internet Security, Addison-Wesley, Reading, MS, 1999.
5. A. Fúster Sabater, D. Guía Martínez, L. Hernández Encinas, F. Montoya Vitini and J. Muñoz Masqué, *Técnicas criptográficas de protección de datos*, RA-MA, Madrid, 3a ed., 2004.

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

6. National Institute of Standards and Technology, Secure hash standard, *FIPS PUB*, 180-1 (1995).
7. A.J. Menezes, P.C. van Oorschot and S. Vanstone, *Handbook of applied cryptography*, CRC Press, Boca Raton, FL, 1997.
8. PKIX-CMP, http://www.entrust.com/resources/docs/protocols pki.htm
9. RFC 3280, http://www.faqs.org/rfcs/rfc3280.html
10. R.L. Rivest, The MD4 message digest algorithm, *Proc. Crypto'90, LNCS* 741 (1991), 303-321.
11. R.L. Rivest, RFC 1321: The MD5 message-digest algorithm, *Internet Activity Board*, 1992.
12. R. Rivest, A. Shamir and L. Adelman, A method for obtaining digital signatures and public key cryptosystems, *Comm. ACM* 21 (1978), 120-126.
13. W. Stallings, *Cryptography and network security*, 2nd. ed., Prentice Hall, 1999.
14. Legislation regarding electronic signature: *Directive 1999/93/CE* and *Law 59/2003*.
15. Legislation regarding Personal Data Protection: *Directives 1995/46/CE, 97/66/EC, 2002/58/CE, Regulation (EC) 45/2001, L.O. 15/1999, Royal Decree 994/1999, Laws 34/2002 and 32/2003*.
16. Legislation regarding the DNI and DNI-e: *Decree 196/1976 regulating the DNI, Partially modified by R.D. 1189/1978, 2002/1979, 2091/1982, 1245/1985, L.O. 1/1992, regarding Citizen Security Protection, Interior Ministry Order of 12/7/1990 26/4/1996, R.D. 896/2003 regarding Passport Regulation.*