THE NEW SPANISH ELECTRONIC IDENTITY CARD: DNI-e¹;

J. Espinosa García, L. Hernández Encinas, and A. Queiruga Dios

Dpt. Information Processing and Coding, Applied Physics Institute, CSIC
{javier.espinosa, luis, araceli}@iec.csic.es
Spain

Abstract: The new Spanish Electronic Identity Card (DNI-e) provides a modern and secure identifying way for Spanish citizens as well as digital signature capabilities and confidence in Information Society. In this work the main physical (card and chip) and logical (certificates, digital signature, and keys) properties of the DNI-e, are shown. Moreover, we put special emphasis on the public key infrastructure (PKI) that supports its development and future use.

Key words: e-Government, Electronic citizen’s identification, DNI-e, Digital certificates, Public key cryptography.

1. INTRODUCTION

Nowadays, Information Technologies are growing inside common society, and it means that new user’s requests frequently appear. Some of those aims are to give the necessary resources and ensure that these guarantee people privacy, freedom and rights within a democratic framework.

Personal electronic identification is a challenge that the Spanish Government faced up to by means of a new identification mechanism based on the traditional Spanish Identity Card (Documento Nacional de Identidad: DNI).

The DNI is a document issued by the Spanish Government (Spanish Police, DGP, to be precise) that authenticates its holder as genuine and justifies the holder’s identity. Since it was developed (more than 50 years ago), the DNI has been an

¹ This work is supported by Ministerio de Educación y Ciencia (Spain), under grants SEG2004-02418 and MTM2005-00173, and Consejería de Educación y Cultura, Junta de Castilla y León under grant SA110A06.
essential document to officially justify, per se and inside Spain (and in the European Community), holder’s identity. Furthermore, the DNI guarantee the personal details showed on the card and that its holder has the Spanish citizenship.

The new DNI-e (see DNI-e) has putted some goals into action. The main ones are the following:

1. To provide a physical and electronic holder’s identification mechanism.
2. To make electronic signature possible by identification, authentication and digital signature protocols.
3. To promote citizens’ confidence in the Information Society and new digital context by providing a suitable mechanism that ensures citizens’ identity, privacy and basic rights.
4. To cooperate with different European projects related to digital identity.
5. To keep its characteristics and functions as a travel document.

In order to achieve these goals, the DGP has introduced a public key infrastructure that provides the new DNI-e with the necessary mechanisms.

2. PHYSICAL SUPPORT: Card and Chip

The DNI-e card is a polycarbonate support whose durability has been estimated for at least 10 years. The size of this card is similar to any credit card or smart card we can find today (see Figure 1).

![Fig. 1. The new Spanish Electronic Identity Card: DNI-e](image)

In order to provide DNI-e with high physical security, the card is personalized by a destructive recording laser treatment. This operation has three security levels:

1. Level 1 is made up of elements that can be observed with the naked eye:
   a. Hologram or kinegram protected by a 100 nm. artistic overlay.
   b. Optically variable inks (see Figure 2).
d. Touch detectable letters.

e. Embossed surface structures

Fig. 2. Level 1 of security: Optically variable inks

2. Level 2 is characterized by marks that are just noticeable with electronic and mechanical:
   a. Security background: guilloches graphics that can have logotypes.
   b. Ultraviolet or infrared visible inks and fluorescent inks (see Figure 3).
   c. Subject's picture is laser recorded at card background and counterfeit protected.

3. Level 3 consists of elements that only can be detected at laboratory:
   a. Cryptographic measures.
   b. Biometric Measures.

Fig. 3. Level 2 of security: Ultraviolet and infrared visible inks

Chip’s Security requirements are the following:
1. Common Criteria certification, level CC EAL 4+ or upper (see CCEAL4+).
2. CWA 14890-3 (see CWA14890).
3. Applications that run at card must be, at least, EAL4+ certified.
4. Chips will be supplied, at least, by two purveyors.

The whole information saved on the chip is digital signed by the DNI-e certification authority (CA), in order to preserve integrity and authenticity. This information is the following:
1. Personal citizen details.
2. Digitalized citizen’s photo.
3. Digitalized citizen’s homemade signature.
4. Fingerprint template.
5. Cryptographic data.
6. Biometric data.
7. A “match on card” application.
8. A cryptographic processor that ensures private key will not be exported from the card.
10. A signature (non repudiation) certificate, X509v3.
11. The issuer CA certificate.

Such content is organized in three areas:
1. The first one contains citizen's certificates, and, if its holder wants, it can be accessed via PKCS#11.
2. The second area contains citizens fingerprint, and it can be accessed only by authorized Spanish Security Forces and Corps personnel. This area will be used with “match on card” applications on necessary process such as certificates deletion, renovation, etc. This fingerprint is used to check a citizen’s identity immediately, and to unblock the card (there is no PUK number).
3. The last area has all personal details, and it can be accessed only by authorized Spanish Security Forces and Corps personnel too.

3. LOGICAL SUPPORT

The new DNI-e has some focal points: Confidentiality, integrity, authentication, and no repudiation. These points are covered by the next digital certificates.
1. Citizen Authentication X.509 certificate, which electronically provides and guarantees citizen’s identity when faced with third parties.
2. Citizen Digital Signature (no repudiation) X.509 certificate, which ensures no changes on electronically signed documents, signer identity and document’s origin.
3. Certification Authority Root X509 certificate.

There are different stages in order to issue the DNI-e to the Spanish citizens in a safe way in order to guarantee a complete security in the whole process. The two phases are: Card pre-personalization and personalization.

For the first phase (see Figure 4), the Spanish National Factory of Currency and Stamp (Fábrica Nacional de Moneda y Timbre, FNMT) supplies batch of cards that will become DNI-e as well as cards (Place Identify Card, TIP) to identify issuing places (Police Stations).

In order to achieve this phase, an Issuing Root CA, located in DGP offices, issues two certificates:
- An X.509 certificate for FNMT Subordinated CA dedicated to DNI-e. This CA will issue two X.509 certificates:
• A TIP card identification certificate, that is stored in the TIP card with Issuing Root Certificate.
These cards are personalized before they are used, in order to ensure the security, by adding two card verificable certificates:
• A DNI-e card identification certificate (ICC), that is stored in the DNI-e card with Issuing Root Certificate.
• A Card Verifiable certificate for DGP Subordinated CA dedicates to intermediate terminals.

![Diagram of pre-personalization process]

Once DNI-e cards are electronically (chip) and physically (plastic) pre-personalized, they are distributed to issuing places. As soon as an issuing place has its personalized card (TIP) and the pre-personalized cards of the DNI-e, it authenticates each pre-personalized DNI-e card and conversely, in order to avoid forgeries. This authentication is as follows: The DNI-e card will validate the X509 TIP certificate of the issuing place, whereas the issuing place will validate the X509 certificate of the DNI-e card. Both processes of authentication are possible due to the fact that a confidence chain is established. In this way, an issuing place only will personalize the cards issued by the FNMT, and the DNI-e cards only will be personalized by the authorized issuing places. Then, the personalization of the DNI-e card process begins (see Figure 5). This phase consists in saving inside the chip and in engraving in the plastic card the citizens’ personal information, who asked for an DNI-e.
REFERENCES

CCEAL4+, www.cesg.gov.uk/site/iacs/index.cfm