

The Spanish eID document

Both a national identification and a compliant travel one



History



- **Since 1824** the Spanish Police, under the Ministry of Interior, has the competency for **ID Documents issuance** (National ID Document, Passport and foreigners residence Permit).
- The identity documents have evolved with the technologies of each era until 2006, when the first eID was issued.
- It was a pioneer document with chip and authentication, signature and Match-on-Card functionalities.



Decentralized issuing system



- The expedition system has also been varying, from a centralized system to the decentralized system existing today.
- Both Identity Card and Passport can be issued in **350 offices all over Spain.**
- All communications are centralized in a **single Spanish Police Server.**



Novelties of new 3.0 eID Document

- Technological breakthrough.
- New security features.
- Dual interface chip.
- Roll out in the whole country in a very short time (year 2015).



- There are **two PC cores**, in order to allow the insertion of an inlet with antenna.
- The collating is completed with two transparent layer in obverse and one in reverse. Total
- thickness is $760 \mu\text{m} \pm 80 \mu\text{m}$, according to ISO.

LAYER STRUCTURE

1	POLYCARBONATE OVERLAY
2	POLYCARBONATE OVERLAY WITH KINEGRAM
3	OBVERSE POLYCARBONATE CORE
4	INLET: ANTENNA LAYER
5	REVERSE POLYCARBONATE CORE
6	POLYCARBONATE OVERLAY

Novelties of new 3.0 eID Document



Novelties of new 3.0 eID Document



Security Background

- Rainbow printing
- Guilloches
- UV Rainbow



Novelties of new 3.0 eID Document

OVI and OASIS Ink



OVI ink blue / purple

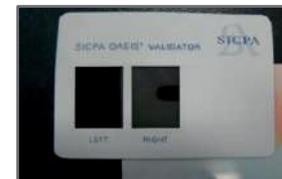


Light background



Dark background

Change from transparent to orange WITHOUT polarized filter



Change from green to orange WITH polarized filter

Novelties of new 3.0 eID Document



Kinegram



Surface relief

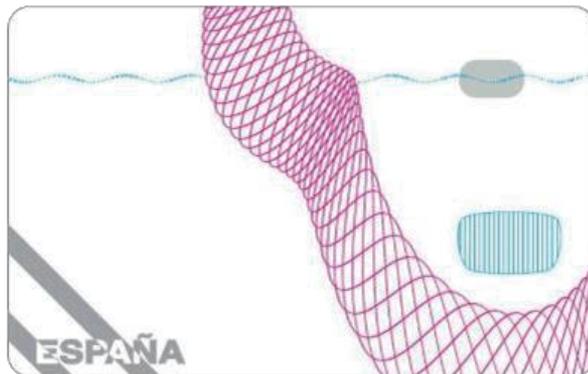


Cinematic effects

Novelties of new 3.0 eID Document



Surface embossing



BLUE = LOW RELIEF

RED = HIGH RELIEF

GREY = MATT EFFECT



Novelties of new 3.0 eID Document

Low relief CLI



Evolution of Spanish Electronic ID Card

as identity and travel document

- First version of **Spanish Electronic ID Card “DNle”** was developed in 2005-2006 years, and started to be issued in March 2016.
- Viewed from the current perspective, the project had two major restrictions:
 1. In these early versions, Spanish Electronic ID Card DNle did not have NFC (RFID) **only contacts interface**.
 2. Data of the citizens was not of free access under ICAO rules. They were only intended to police uses.



Why?



1. Only **contacts interface**:

- The reason was that in 2006 RFID readers were not intended for the use of citizens. They were expensive devices, and in Spain, it was almost impossible to find them in computer stores or malls.
- However, by 2014, everything had changed, and NFC technology was already present in many mobile phones and some models of tablets.
- When DNI3.0 was developed in 2014-2015, Spanish Police wanted to give services to mobile phone users.



Why?



2. Data of the citizens was not of free access, under ICAO rules. They were only for polices uses.

- This was a decision in order to secure citizens data.
- In 2009 ICAO defined Supplemental Access Control (SAC) as a set of security features for protecting data contained in electronic travel documents.

It is based in PACE protocol (Password Authenticated Connection Establishment), a mutual authentication mechanism between terminal and chip.



Why?



The following risks were addressed:

- **Skimming** - retrieving data from the chip without being in possession of the passport and without the holder's approval. Skimming is an online attack (the attacker must communicate with the chip for the duration of the attack).
- **Eavesdropping** - data is intercepted while the passport chip communicates with the reader. As the data is analysed after the attack has taken place, eavesdropping is an offline attack.

Once implemented as an ICAO standard, PACE provide long-term protection against these kind of threats.

In December 2014, these mechanisms were included in European rule EN 419212 (Application Interface for smart cards used as Secure Signature Creation Devices).

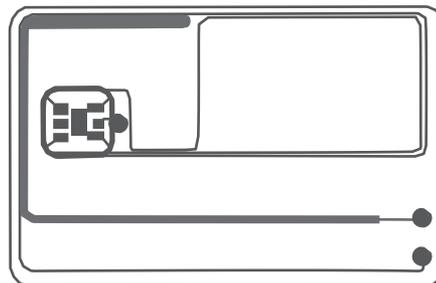
When we developed DNle 3.0 Electronic Identity Card, we used a working draft of this rule thanks to the WG16 Working Group of CEN, so PACE mechanism was incorporated to Spanish ID Card from the very beginning of the project.

Nowadays, DNle 3.0

Spanish Electronic Identity Card, 3.0 version



- DNI is a dual interface card, so it is possible to read it by using contacts or antenna interface.
- DNle card makes compatible its specific functionalities as national identity document, with its travel document functionalities, and it is a compliant travel identification, aligned with Document 9303 Machine Readable Travel Documents.
- Spanish DNle:
 - **Spanish ID Card**
 - **Travel Document**
- Moreover:
 - As Spanish Electronic ID Card, it is aligned with European eIDAS Regulation (EU) 910/2014 and it is certificated according to EN 419211-European Standard (Protection profiles for secure signature creation device), as well.



DNle 3.0 In a mobile world



- Spanish Police, working together with FNMT-RCM (Spanish Mint), has made a big effort in order to offer a free suite of Android Studio projects, to help to develop this kind of applications.
- On the website of the DNle you can download three complete projects, included source code, for Android mobile applications in Android Studio environment. Source code of other examples can be requested to Spanish Police.

<https://www.dnielectronico.es/PortalDNle/>

From these examples, it is very easy to develop a new app adapted to your particular needs.

- Android covers more than 86% of the mobile phone market in Spain. Apple has just released part of its development API for NFC.

All compiled examples of Apps are available in the Play Store.

Developer: CNP-FNMT



DNle 3.0 mobile applications



The image displays a collection of mobile application screens for various services. On the left, a large smartphone shows the 'dni.e' app interface with a hand icon pointing at the bottom. To its right, eight smaller smartphones are arranged in two rows, each displaying a different app's interface. The background features a large, faint 'dni.e' logo and a city skyline silhouette at the bottom.

APPLICACIONES

HOTELS APP

CITY COUNCIL APP

DRIVER LICENSE APP

SOCIAL SECURITY APP

TAX AGENCY APP

EDUCATION APP

DRUGSTORES APP

POST OFFICE APP

DNle 3.0 mobile applications

Flights purchase app



DNle 3.0 mobile applications

Hotel registration app



DNle 3.0 as travel document



- ABC, Automated Border Control Gates
- The ABC of Barajas Airport consists of a two barriers system within which an Identification Module is located.
- The passenger passes a first door, where he performs the whole process of identification and verification (by using his DNle or electronic Passport indistinctly). If the process is correct, the second door opens to allow the passage of the passenger.



Next version: DNle 4.0

LDS2 – Ready for the next generation of machine-readable passport.

Common Criteria certification according the **new European regulation EIDAS**.

Updating the algorithm used.

Updating the size of the keys.

New Chip with **Architecture Cortex M**.



DNle 3.0 video



Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre



NATIONAL ID CARD
AND TRAVEL DOCUMENT



Mr. Enrique Taborda Álvarez
Principal Commissioner
Spanish National Police Force



Mr. Valentín Ramírez Prieto
Project
Manager
FNMT-RCM

