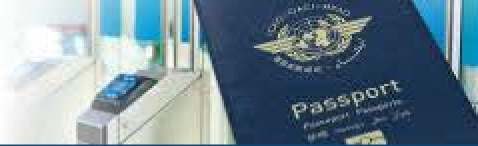
ICAO SECURITY & FACILITATION



24 hours Center

and

new Spanish eID Document 4.0

Enrique Taborda Álvarez

Principal Commissioner- Spanish National Police Force

Valentín Ramírez Prieto

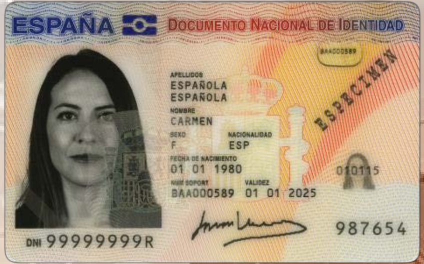
Project Manager - FNMT

Montréal / 23-25 october

Nowadays, DNIe 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.
- ❑ DNIe 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 DNIe:
  - ❑ 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.



ESPAÑA DOCUMENTO NACIONAL DE IDENTIDAD

BAA000589

APELLIDOS
ESPAÑOLA
ESPAÑOLA
NOMBRE
CARMEN
SEXO F
NACIONALIDAD ESP
FECHA DE NACIMIENTO 01 01 1980
NUM SOPORT BAA000589
VALIDEZ 01 01 2025

ESPECIMEN

010115

987654

DNI 99999999R

DNIe 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 DNIe or electronic Passport indistinctly). If the process is correct, the second door opens to allow the passage of the passenger.

POLICIA NACIONAL
Mº INTERIOR
e-passport
EU / EEA / CH citizens with electronic passport
Ciudadanos UE / EEE / CH con pasaporte electrónico o DNIe

New version:

DNIe 4.0

- ❑ LDS2 – Ready for the next generation of machine-readable passport.
- ❑ Common Criteria certification according the new European regulation EIDAS.
- ❑ New Chip with Architecture Cortex M.
- ❑ Updating the used algorithms.
- ❑ Updating the size of the keys.

LDS2

Ready for the next generation of machine-readable passport

❑ The new chip has 350kB of flash memory, for citizen data storage.

❑ Although the introduction of this data structure is not imminent, we must bear in mind that the validity of the documents is up to 10 years, so it is necessary to be very proactive.

❑ In addition, having a very large flash memory, allows to store higher resolution facial images, essential to obtain the best results in facial recognition, in fast border crossing by by means of ABC systems.

DNIe according the new European regulation EIDAS

- ❑ eIDAS: electronic IDentification, Authentication and trust Services.
- ❑ EIDAS is the European Regulation for the electronic identification and trust services for electronic transactions. It repeals Directive 1999/93/EC.
- ❑ Under eIDAS, citizens and businesses are able to use their native electronic identification schemes (eIDS) when accessing public services within other EU Member States that use eIDS.
- ❑ This regulation defines the conditions in which the Member States will recognize electronic identification from users.
- ❑ Nowadays DNIe 3.0 is an eIDAS compliant document. DNIe 4.0 will be compliant, as well.

DNIe according the new European regulation EIDAS

- In June of 2018, the CNP accredited before the European Commission that the DNIe 3.0 complies with the following items related to the eIDAS regulation, regarding electronic identification:
  - Meets its security requirements.
  - It meets its quality requirements.
  - It covers all its technical demands.
- It has been shown that DNIe 3.0 is "compatible with eIDAS", so the DNI has been accepted as the valid method of electronic identification, in its electronic infrastructure, by the other states that have notified its own schemes.
- The new DNIe 4.0 has been developed from the beginning, for this purpose.

Common Criteria certification according the new European regulation EIDAS

- ❑ The DNIe 4.0 is certified with two Protection Profiles:
  - ❑ Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application.
  - ❑ Common Criteria Protection Profile — Machine-Readable Electronic Documents.
- ❑ This [MR.ED-PP] includes:
  - ❑ Common Criteria Protection Profiles for Secure Signature Creation Device – Part 2: Device with key generation, prEN 14169-2:2012 ver. 2.01.
  - ❑ Common Criteria Protection Profile — Machine Readable Travel Document with “ICAO Application”, Extended Access Control with PACE (EAC PP).
  - ❑ Common Criteria Protection Profile — Electronic document implementing Extended Access Control Version 2 (EAC2).
- ❑ The certification level will be EAL4 +
- ❑ In this way, the DNIe compliance with the eIDAS Regulation will be automatically maintained.

New Chip with Architecture Cortex M

- We have gone from using a micro-controller of 16 bits, to one of 32 bits.
- Currently, in the industrial world, 90% of 32-bit chips have a Cortex M architecture. Mobile phones, for the most part, as well.
- Recently they have begun to be used in the world of smart cards. The expansion of the use of this architecture will have several advantages:
  - Easier to migrate developments from one chip to another chips manufacturer's.
  - Very low consumption, facilitating the use of battery readers, connected to other Bluetooth devices via low consumption BLE, very useful for mobile inspection posts.
  - An important jump in computing power.

Updated algorithms

- ❑ CNP and FNMT consider that the RSA algorithm is becoming obsolete in the world of Smart Cards:
  - ❑ The needed key sizes to maintain the security, are increasing.
  - ❑ The computing power of the chips does not grow at the same pace.
  - ❑ There are other more modern algorithms, which do not have this drawback.

Updated key sizes and used algorithms

- Chip authentication Certificate:
  Asymmetric cryptography: elliptic curves, 256-bit keys.
- Citizen Certificate:
  Asymmetric cryptography: elliptical curves (from 256 bits to 512 bits). A key size of 384 bits has been selected.
- Symmetric cryptography: AES-128
  Hash algorithm: SHA-256
- Support to Asymmetric cryptography with RSA algorithm, and keys of up to 3072 bits, in order to solve possible incidences in the future

What if I loose my documents abroad?

24 hours Center:

A speedy and efficient solution

Identity Documents Division

Part of the National Police integrates **two major are**as:

- ❑ Spaniards and Foreigners Documentation: Issuance, management and control of ID and Passport.
- ❑ Documentary Treatment and Archive Area: Manages searches and captures, reviews and various police files.

Average annual production: 9 million documents

- ❑ 6.940.000 eID
- ❑ 2.141.000 Passports.

ESPAÑA DOCUMENTO NACIONAL DE IDENTIDAD

BAA000589

ESPECIMEN

APELLIDOS
ESPAÑOLA
ESPAÑOLA

NOMBRE
CARMEN

SEXO F NACIONALIDAD ESP

FECHA DE NACIMIENTO
01 01 1980

NUM SOPORT BAA000589 VALIDEZ 01 01 2025

010115

987654

DNI 99999999R

24 Hour Center

- Part of the Identity Documents Division, the state agency responsible for issuing ID cards and passports.
- Access to identity databases for verification purposes.
- Instant verification capacity of identity and travel documents issued by Spain.
- Equipped with the necessary communications systems and trained personnel.

Receive requests from

- ❑ Police Departments, Courts, etc.
- ❑ Spanish Consulates and Embassies abroad.
- ❑ Other official bodies of the State Administration

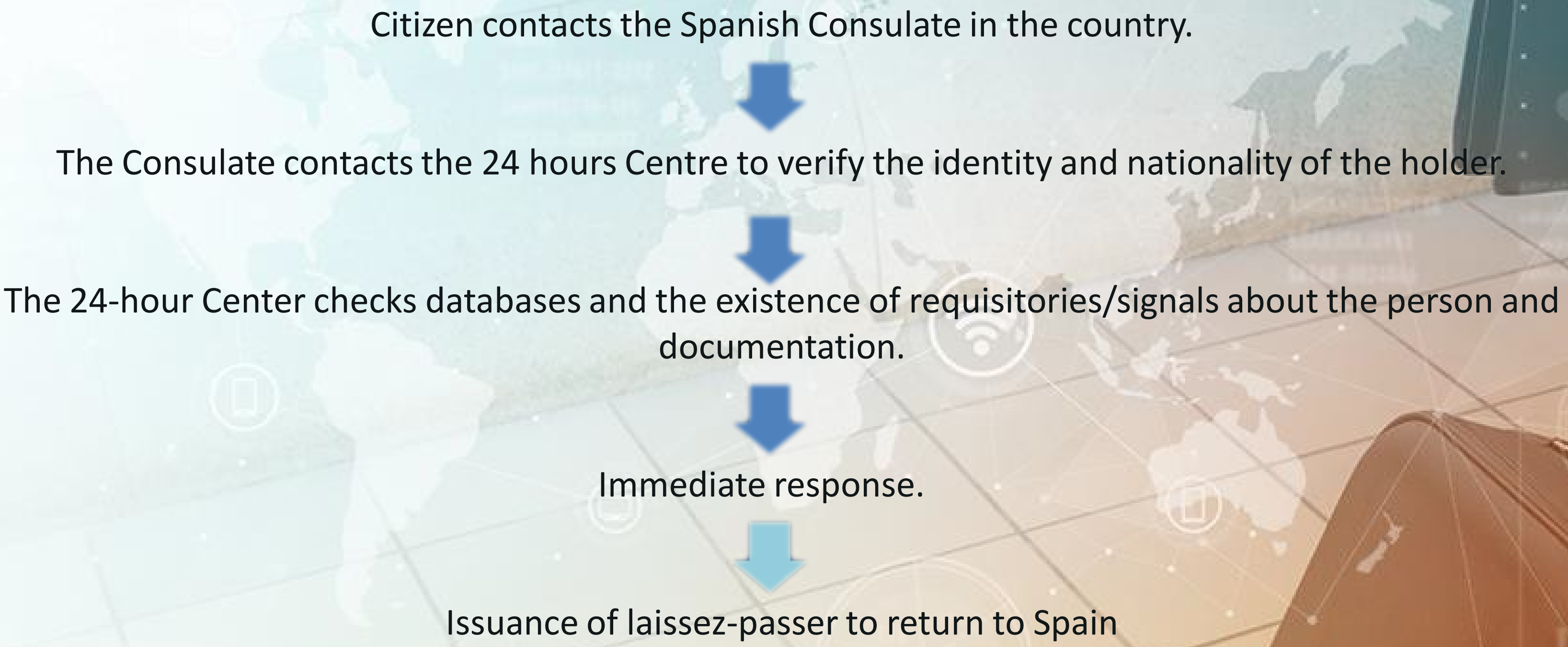
Urgent national and international consultations:

- ❑ Immediate urgent checks.
- ❑ Lost and stolen eID and passport reports.
- ❑ Consultations/Authorizations on legal situation prior to expedition. (in Spain and abroad).

Immediate response: Maximum 30 minutes

- ❑ Anomalies or discrepancies detected
- ❑ Detection of documents reported as lost or stolen.
- ❑ Other indications or criminal background on the document or the person.

Document loss abroad



Citizen contacts the Spanish Consulate in the country.

The Consulate contacts the 24 hours Centre to verify the identity and nationality of the holder.

The 24-hour Center checks databases and the existence of requisitories/signals about the person and documentation.

Immediate response.

Issuance of laissez-passer to return to Spain

Conclusions

□ 24 hour availability

□ Efficiency: Little need for material and personal resources

□ Immediate response

Mr. Enrique Taborda Álvarez
Principal Commissioner
Spanish National Police Force

Mr. Valentín Ramírez Prieto
Project Manager
FNMT-RCM