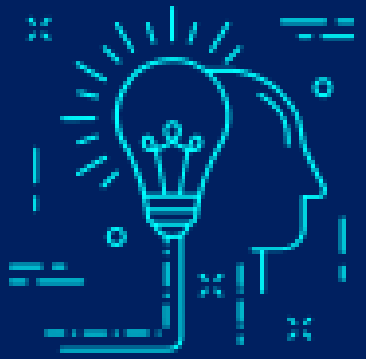
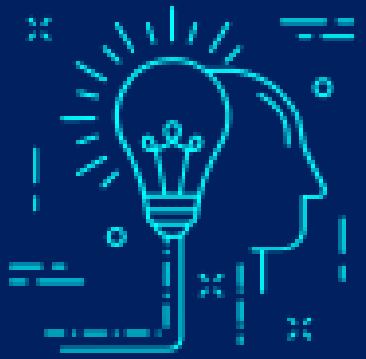
The Evolution of the Spanish Electronic ID Card

DNI foreword



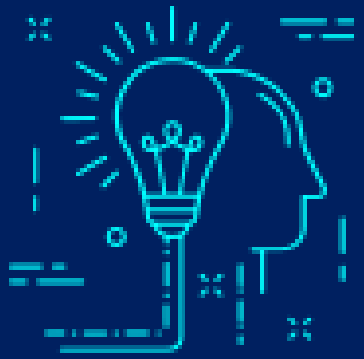
- Ministry of Interior is the public administration in charge of Spanish Identity Card called DNI (Identity National Document).
- Inside Ministry of Interior, Spanish National Police (DGP) is responsible for the management of all systems related with the DNI including the enrollment and issuance of the document which are done in the Police Stations spread along the whole country.
- The design, development and manufacture of DNI is done by Spanish Royal Mint (FNMT-RCM) which is also a public administration.

The importance of the DNI



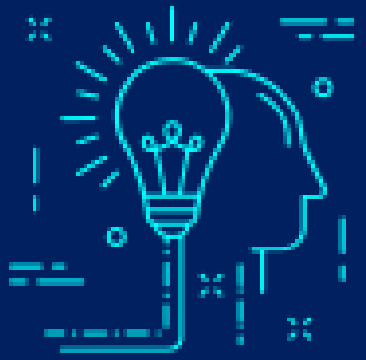
- DNI is absolutely integrated in Spanish society.
- Universal and mandatory Spanish identification card since 1937.
- Compulsory for all main documents acquisition.
- Involved in most of the relationships between citizens and public and private institutions.
- 97% of the Spanish electronic records with personal data include the DNI personal number.
- Schengen territory travel document.

Non electronic DNI



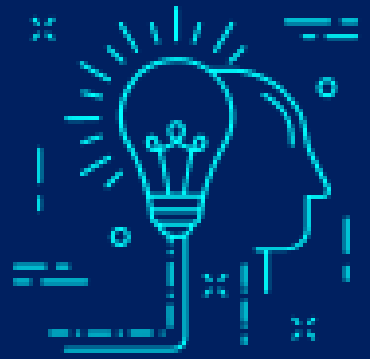
- Until 2005 citizens had to go twice to Police Stations in order to get their ID Cards. In the first visit they were enrolled.
- After that, their personal data were processed and their DNI was issued in the FNMT-RCM facilities. It was a centralized scheme, so the personalized identity document had to be delivered to the corresponding Police Station and citizen had to pick it up in a second visit.
- The whole process took between 10 and 15 days.

DNIe 0.0

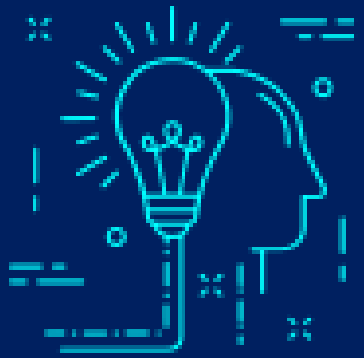


- Spanish Electronic ID Card (DNIe) was born in 2005.
- The electronic part was designed, developed and tested by FNMT-RCM.
- First proof of concept consisted of a small PKI which generated keys and its certificates, and stored them in a smart card without operation delays.
- This pilot confirmed that the target defined by Spanish National Police of issuing electronic DNI using a distributed infraestructure was technically feasible.
- Citizens had their identity document in a single visit.

DNIe issuing process workflow

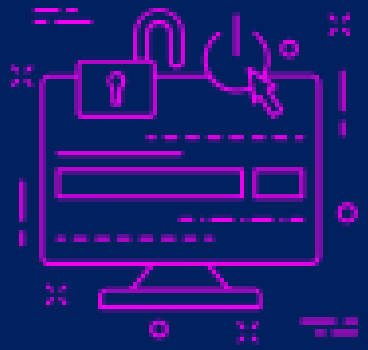


Information stored in the chip



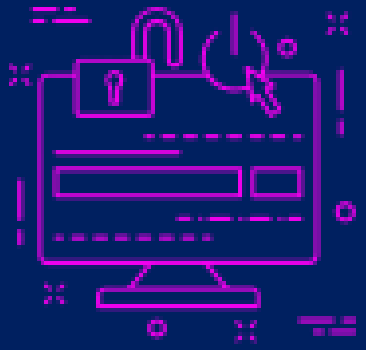
- Public zone
  - Public keys of subscriber
  - Intermediate CA Certificate
  - Component Certificate
- Private zone
  - Private keys of subscriber
  - Authentication Certificate
  - Signature Certificate
- Security zone
  - Biometric data
  - Identification data of citizen

DNIe 1.0 (2006)



- First DNIe was issued in 2006.
- It was a card with a contact chip, but it didn’t have a RFID antenna.
- Data stored in the card were citizen’s biographic and biometric data and two electronic certicates with its private keys.
- Citizen data were only accesible by Police.
- The product was certified as a Secure Signature Creation Device under Common Criteria Scheme.
- As it was a new infraestructure, a very restrictive data protection policy was adopted in order to analyze how was the evolution of the project.

DNIe 1.0 CC Certificate



In accordance with the authority granted under Act 11/2002, regulating the National Intelligence Centre, and applying articles 1 and 2, second paragraph, letter c, of Royal Decree 421/2004, 12th March, regulating the National Cryptologic Centre, I hereby:

Certify that the security of the smartcard DNIe version 1.13, configuration DNIe 1.13 A11 H4C34 EXP 1-1 and DNIe 1.13 B11 H4C34 EXP 1-1 , developed by FNMT-RCM, located at Jorge Juan 106, Madrid, fulfills its Security Target identified as «Declaración de Seguridad Tarjeta DNIe» version 1.0 and revision 6, to the extent defined by the evaluation assurance level EAL4+ (ALCFLR.1, AVA-MSU.3, AVA-VLA.4) with Strength of Functions claimed as HIGH, using the norms «Common Criteria for Information Technology Security Evaluation» and the «Common Methodology for Information Technology Security Evaluation», version 2.2.

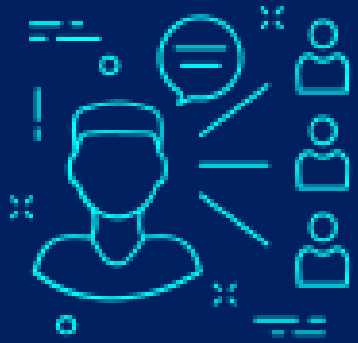
Claimed Protection Profiles: CWA 14169 Secure Signature-Creation Devices "EAL4+" v1.05 Level 3 March 2002
Evaluated Plataform: ST19WL34
Evaluation Facility: INTA-CESTI
Certification Report: INF-148

This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información".

The above-mentioned Security Target and Certification Report are available at the National Cryptologic Centre.

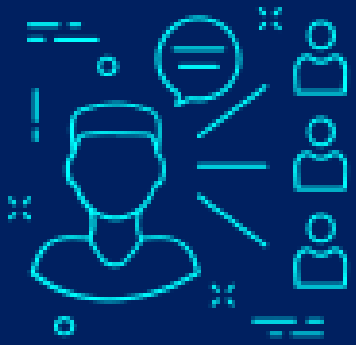
Madrid, May 16th 2007
Secretary of State Director
Alberto Sáiz Cortés

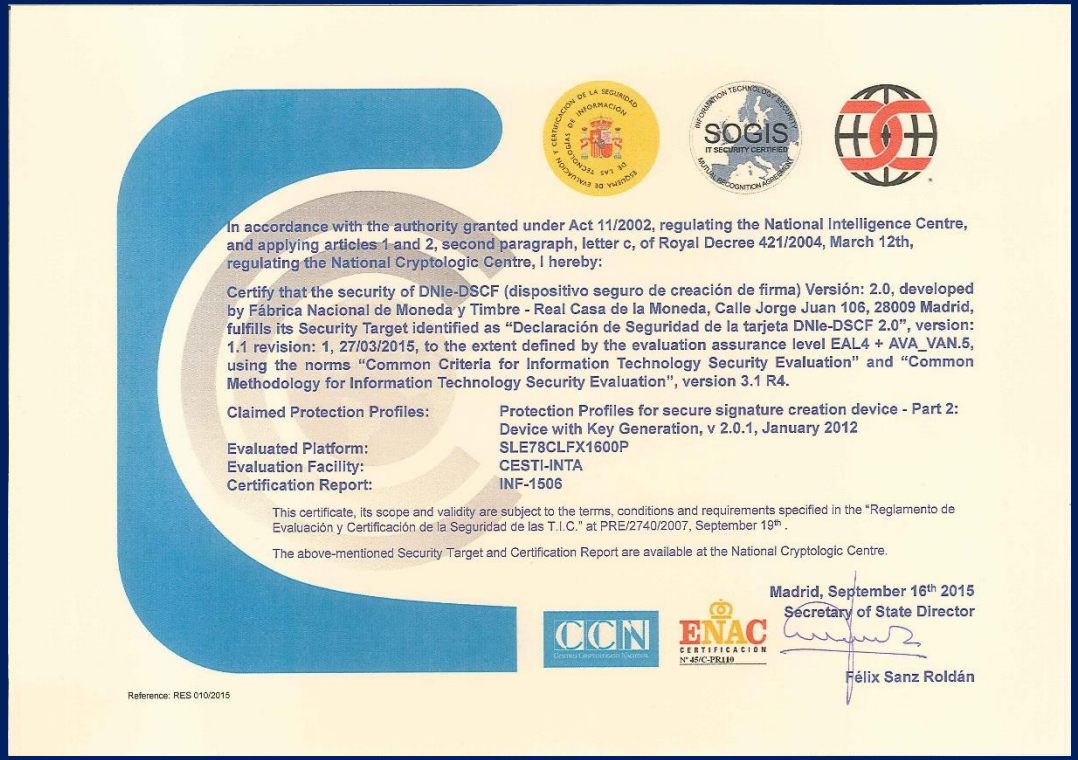
DNIe 2.0 (2014)



- It was a new version of the DNIe 1.0 built on a chip from another manufacturer in order to have two different hardware suppliers and to update the product.
- Besides, some improvements were done and little new functionalities were added.
- It was also certified as a Secure Signature Creation Device under Common Criteria Scheme.

DNIe 2.0 CC Certificate





In accordance with the authority granted under Act 11/2002, regulating the National Intelligence Centre, and applying articles 1 and 2, second paragraph, letter c, of Royal Decree 421/2004, March 12th, regulating the National Cryptologic Centre, I hereby:

Certify that the security of DNIe-DSCF (dispositivo seguro de creación de firma) Versión: 2.0, developed by Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, Calle Jorge Juan 106, 28009 Madrid, fulfills its Security Target identified as "Declaración de Seguridad de la tarjeta DNIe-DSCF 2.0", version: 1.1 revision: 1, 27/03/2015, to the extent defined by the evaluation assurance level EAL4 + AVA_VAN.5, using the norms "Common Criteria for Information Technology Security Evaluation" and "Common Methodology for Information Technology Security Evaluation", version 3.1 R4.

Claimed Protection Profiles:	Protection Profiles for secure signature creation device - Part 2: Device with Key Generation, v 2.0.1, January 2012
Evaluated Platform:	SLE78CLFX1600P
Evaluation Facility:	CESTI-INTA
Certification Report:	INF-1506

This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las T.I.C." at PRE/2740/2007, September 19th .

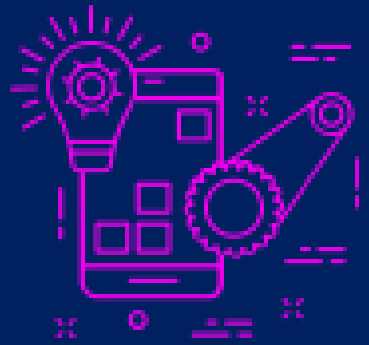
The above-mentioned Security Target and Certification Report are available at the National Cryptologic Centre.

Madrid, September 16th 2015
Secretary of State Director

Félix Sanz Roldán

Reference: RES 010/2015

DNIe 3.0 (2015)

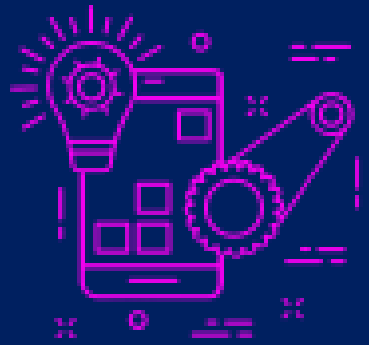


- Usage of mobile devices by citizens was becoming more and more popular. DNIe should support these devices.
- A contactless interface was included and controlled access to citizen’s biographical data was allowed.
- A new RFID antenna was added using NFC (Near Field Communication) technology parameters.
- A data structure equivalent to passport LDS was created in order to allow controlled access to citizens’ biographical data.
- Data could be read just typing the CAN (Card Access Number) printed on the front of the document.
- It was also certified as a Secure Signature Creation Device and a Qualified Signature Creation Device.

DNIe 3.0 (Apps)

- FNMT has also developed several Android Apps in order to show some of the many options in which the DNIe 3.0 can be used.

DNIe 3.0 CC Certificate



CCN
CENTRO CRIPTOLÓGICO NACIONAL

CERTIFICATE

CCN-CC-022/2016

DNIe-DSCF (dispositivo seguro de creación de firma) Versión: 3.0

Type of product	Smartcard. Secure Signature Creation Device
Conformance of functionality	PP Conformance functionality
Protection Profile Conformance	Protection Profiles for secure signature creation device - Part 2: Device with Key Generation, v 2.0.1. Protection profiles for Secure signature creation device - Part 5: Extension for device with key generation and trusted communication with signature creation application", versión 1.0.1.
Evaluation Facility	CESTI-INTA
Certification Report	CCN-CC/2014-39/INF-1766

Pursuant to the authority vested in me under Act 11/2002 regulating the National Intelligence Centre, and under Article 1 and Article 2.2.c of Royal Decree 421/2004 of March 12th regulating the National Cryptologic Centre, I hereby:

Certify that the security of DNIe-DSCF (dispositivo seguro de creación de firma) versión: 3.0, developed by Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, Calle Jorge Juan 106, 28009 Madrid, has been evaluated using the "Common Methodology for Information Technology Security Evaluation", version 3.1 R4 and the "Common Criteria for Information Technology Security Evaluation", and it has met the requirements of its Security Target identified as "Declaración de Seguridad de la tarjeta DNIe-DSCF 3.0, versión 1.1, revisión 1, de 13 de septiembre de 2016", for evaluation assurance level EAL4 augmented by AVA_VAN.5.

Madrid, December 23rd, 2016
Secretary of State Director

Félix Sanz Roldán

This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las T.I.C." at PRE/2740/2007, September 19th.

The above-mentioned Security Target and Certification Report are available at the National Cryptologic Centre.

CCN
CENTRO CRIPTOLÓGICO NACIONAL

CERTIFICATE

CCN-CC-017/2018

DNIe-DCCF (dispositivo cualificado de creación de firma) versión 3.0

Type of product	Qualified Signature Creation Device (QSCD)
Conformance of functionality	PP Conformance functionality
Protection Profile	EN 419211-2:2013 and
Conformance	EN 419211-5:2013
Evaluation Facility	Applus Laboratories
Certification Report	CCN-CC/2017-26/INF-2389

Pursuant to the authority vested in me under Act 11/2002 regulating the National Intelligence Centre, and under Article 1 and Article 2.2.c of Royal Decree 421/2004 of March 12th regulating the National Cryptologic Centre, I hereby:

Certify that the security of the product DNIe-DCCF (dispositivo cualificado de creación de firma) versión 3.0, developed by Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda, C/ Jorge Juan 106, 28009, Madrid, has been evaluated using the "Common Methodology for Information Technology Security Evaluation", and the "Common Criteria for Information Technology Security Evaluation" version 3.1 R4, and it has met the requirements of its Security Target identified as "Declaración de Seguridad de la tarjeta DNIe-DCCF 3.0, Versión: 1.1 Revisión: 5, de 28 de noviembre de 2017", for evaluation assurance level EAL4+ (AVA_VAN.5).

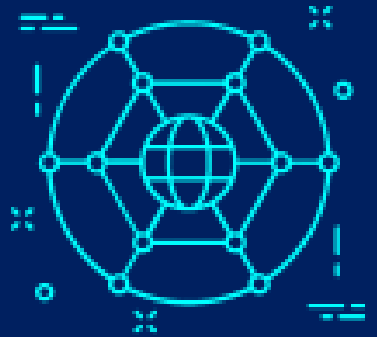
Madrid, 15 June 2018
Secretary of State Director

Félix Sanz Roldán

This certificate, its scope and validity are subject to the terms, conditions and requirements specified in the "Reglamento de Evaluación y Certificación de la Seguridad de las T.I.C." at PRE/2740/2007, September 19th.

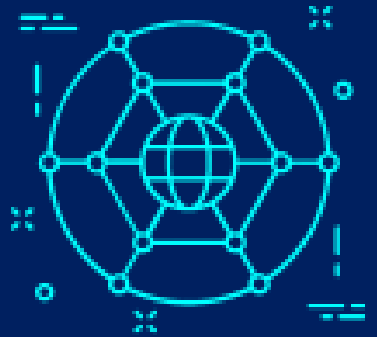
The above-mentioned Security Target and Certification Report are available at the National Cryptologic Centre.

DNIe 4.0, a new beggining



- DNIe 3.0 was a cutting edge ID card which complied with all national and international requirements.
- Nevertheless, as it was a product which was created more than ten years ago a new redesign was needed.
- With lessons learned during these past years, it was the appropiate moment to start a new design.
- Requirements were well defined.

DNIe 4.0 requirements



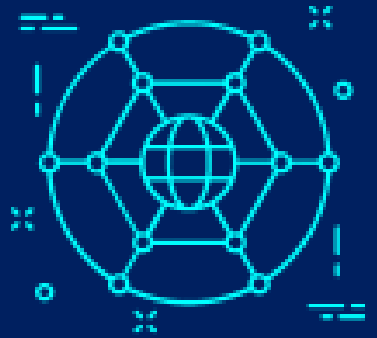
- DNIe 4.0 is called to last.

It should be totally redesigned and developed taking into account the latest technical requirements not only in chip selection but also in available functionalities and certification standards.

- Security maximization.

New security trends should be included in the new software arquitecture design. Besides, two different asymmetric keys algorithms should be supported. In this way, if a cyberattack breaks the security of an algorithm, it could be easily solved switching to the second algorithm.

DNIe 4.0 requirements



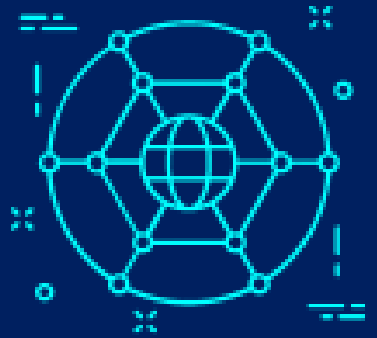
- Maximum interoperability.

New DNIe should be compliant with eIDAS Regulation and three different Protection Profiles: eID, ePassport and QSCD in order to guarantee a broad interoperability.

- Solve Microsoft limitations

DNIe 3.0 contactless communications channel is managed by Microsoft with some limitations. Restrictions should dissapear. DNIe 4.0 should be used with contact and contactless readers indistinctly.

DNIe 4.0 requirements



- Manufacturing flexibility

The new product should be designed in such a way that the document could be configured at FNMT premises as a DNIe, Passport or Residence Permit.

- Improve citizens experience during the issuance of the document.

One of the goals was to reduce as much as possible the time spent by the card in the asymmetric keys generation which is the most time consuming step.

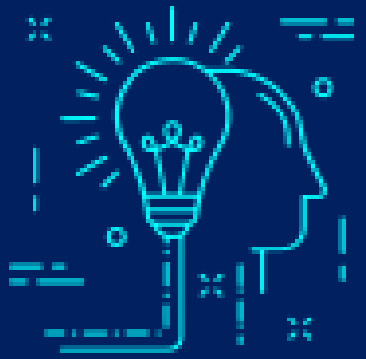
Obtained results

- DNIe 4.0 is much faster than 3.0, so the issuing times at Police Stations is less time consuming.
- 32 bits ARM Cortex chip used is much more powerful than the previous one.
- Key generation is ultra fast and it is also possible to use contactless readers for issuing which communications protocol performance is better.
- These aspects will allow to increase citizens satisfaction with the issuing process of the document.

Obtained results

- On security matter, recommendations done by evaluation labs, JHAS group, Spanish Certification Body and hardware providers had been included natively.
- Operating System supports a wide range of RSA and Elliptic Curves key sizes.
- It is a extremely flexible product which can be configured at FNMT premises as DNIe, ePassport or Residence Permit.
- Common Criteria Certification in progress based on eID, QSCD and ePassport Protection Profiles.

eDNI main figures



- Since 2.006, more than 72M eDNI have been issued
- More than 7M documents per year
- 400 enrollment and issuing stations (fixed and mobile)
- It costs 12€
- Physical security features:

https://www.consilium.europa.eu/prado/en/ESP-BO-05001/index.html

Thank you!

Rubén Romero Muñoz
rromeromunoz@fnmt.es
FNMT-RCM
Jorge Juan, 106
Madrid 28009

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre