Regional Seminar on MRTDs and Traveller Identification Management
Madrid, Spain, 25 to 27 June 2014

DNI 3.0

Seguridad Informática y Comunicaciones;
Cuerpo Nacional de Policía.

DNI 3.0 Proyect

INDEX

- The Update of the issue of infrastructure
- Regulations modification.
- New structure of the layers.
- New security measures// Lay-out customization.
- Data included in the chip.
- New funcionalities for the “kiosko”
- Electronic travel document.
- More powerful chips with variety of communication interfaces.
- Cryptographic Algorithms.
- New functionalities.
- Request for renewal of documents throught the net.

DNI 3.0 Proyect

	NOWADAYS	EVOLUTION
Root Certification Authority	Hash algorithm SHA-256 y SHA-1, and a lenght of key RSA 4096.	Hash algorithm SHA-256, and a lenght of key RSA 4096.
Subordinated Certification Authorities	Hash algorithm SHA-256 y SHA-1, and a lenght of key RSA 2048.	Hash algorithm SHA-256, and a lenght of key RSA 4096.
Citizen Certificates	Hash algorithm SHA-1 y and a lenght of key RSA 2048.	Hash algorithm SHA-256 and a lenght of key RSA 2048.

DNI 3.0 Proyect

- LFE modifitacion to allow the DNI validity certificates for 5 years.
- New DPC publication: change of CA roor, key sizes, use of SHA-2 and change of the certificate profiles to include email.
- RD 1553/2005 of the DNIe modification to allow for children under 18 the expedition of authentication certificates separated of signature certificates RD 869/2013 8th November)

DNI 3.0 Proyect

New flayers structure

- It is composed of two polycarbonate cores, to allow the introduction between them of a sheet with the antenna and the chip without contacts.
- The piece is completed with two transparent front sheets and one back sheet.
- The total thickness is 760 µm ± 80 µm, as ISO rules.

Flayers structure

1	OVERLAY POLYCARBONATE
2	OVERLAY POLYCARBONATE WITH KINEGRAM
3	POLYCARBONATE FRONT CORE
4	INLET: ANTENNA BASE SHEET
5	POLYCARBONATE BACK CORE
6	OVERLAY POLYCARBONATE

DNI 3.0 Proyect

Documento Nacional de Identidad - DNIe 3.0

DNI 3.0 Proyect

New Data Structure

- The information kept in the functionality of travel document, will be set in the proper Data Group (DG):
- DG1. Data inside the OCR lines, mechanic reading area, used now in the passport..
- DG2. Picture. Used now in the passport..
- DG3. Fingerprints picture. Used now in the passport..
- DG7. Handwritten signature picture. Will be used in the future DNI, with funcionality of electronic travel document, and so in the passport. pasaporte.
- DG11 ó DG13.. Full Name and Surname, date and place of birth, name of the parents, Adress

DNI 3.0 Proyect

Figura III-1. Datos obligatorios y opcionales definidos para la LDS

DNI 3.0 Proyect

New functionalities of PAD:

- Renewal of certificates in the PAD everymoment.
- Full verification of certificates status.
- Email update in the authentication certificate (and also in the signature certificate for future uses)
- Cloud Registry for DNI.

DNI 3.0 Proyect

Future trends - More powerful chips with different communication interfaces

- ***CPU:***
- The chip core will be based in CPU 16/32 bits
- Operative System in NVM (flash technology), instead of ROM
- RAM: 64 kB
- Chip dual interface, CC EAL 6+ certificated
- Integral Security mechanisms.
- VHBR

- ***Scale Integration:***
- The chips that will be used should be build with 90nm technology.

- ***Dedicated hardware modules that can be integrated:***
- SHA-2 accelerator.
- ECC Module (Elliptic Curve Cryptography)
- NFC Module (Near Field Communication)
- AES accelerator.

DNI 3.0 Proyect

Future trends – Cryptographic Algorithms

- The tendency is to use new signature algorithms base on ECC (elliptic curves cryptography) and also RSA.
- A signature operation using elliptic curves with a key length of 256 bits has a security level close to the RSA 4096 bits signature.
- Advantages of ECC versus RSA: shoter keys, quicker computation, less energetic waste, less memory need….

DNI 3.0 Proyect

Future trends – New data structure

- CEN/TC234/WG15-European Citizen Card Data structure
- German DNIe is used since november 2010 and follows European EN15480 rule
- DNIe profile has been included in the informative side of this European rule instead of normative side, making easier compabilities and interoperability with other European schemes of electronic identification

DNI 3.0 Proyect

Renewal through the net

- The request for the renewal of documents through the net is done within a comprehensive management web page where citizen ask for an appointment, pay the expedition fee and provides the appropiate documentation.

DNI 3.0 Proyect

- Identity and electronic Signatures are essential tools for the development of legal relations, economics…. Through the net, the Information Society.

Contact Details:
Comisario Jose Luis Diez Aguado
Email: joseluis.diez@policia.es