ICAO SECURITY & FACILITATION

How to ensure integrity of travel documents by implement a robust public key infrastructure

Yolanda Pérez Tocino

Spanish National Police Force

Valentín Ramírez Prieto

FNMT-RCM

Montréal / 25-28 June

Spanish eID and passport

- Issuance of DNI and passport in Spain: **Spanish National Police Force**
- 68 years of experience
- Dispatch via decentralized system

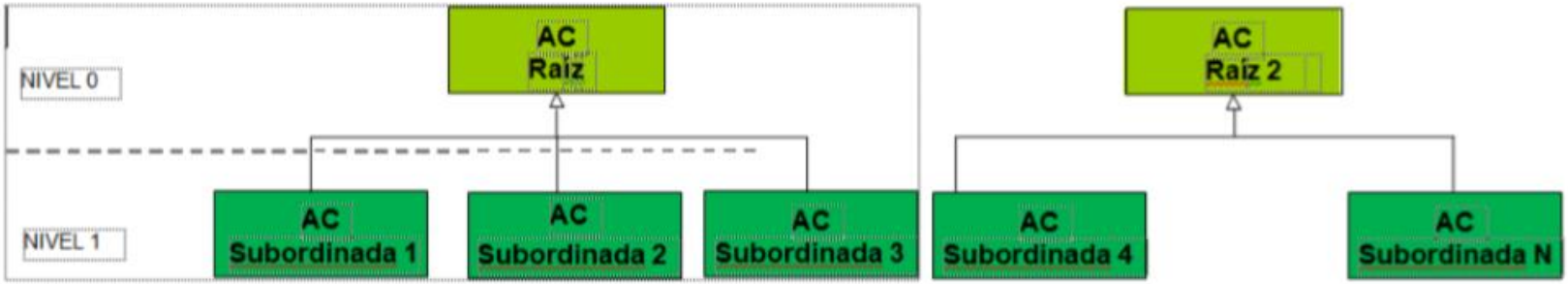
Spanish eID

Passport

New PKI features (I)

- A new Root Certificate Authority was deployed (ACRaizDNIE2).
- It has three subordinate Certificate Authorities (AC004, AC005 and AC006).
- A new certification authority revocation list was published (ARL).
- Deployment of a new Certificate Revocation Authority (CRA)
- Deployment of a new database of revoked certificates (DB-CRL)

New PKI features (II)



New PKI features (II)

- A new Root Certificate Authority was deployed (ACRaizDNIE2).
- It has three subordinate Certificate Authorities (AC004, AC005 and AC006).
- A new certification authority revocation list was published (ARL).
- Deployment of a new Certificate Revocation Authority (CRA)
- Deployment of a new database of revoked certificates (DB-CRL)

New PKI features (III)

- Different types of Validation Authorities:
  - An internal Validation Authority: used by the ID card issuing stations and the digital certificate updating kiosks (PAD).
  - External Validation Authorities: used to verify the validity of the digital certificated on behalf of DGP (General Directorate of Police), FNMT-RCM (Spanish Mint) and @Firma application of the Department of Treasury.

- Updating of the ID Card web page (www.dnielectronico.es)
  - New PKI public keys.
  - New Certification Practice Statement (CPS).

ICAO

Speaker: Yolanda Pérez Tocino
yolanda.perez@policia.es

THANK YOU

2019, a new beginning

- FNMT has developed a new operating system, in native code, for these electronic documents.
- During pre-personalization process in FNMT the new operating system can be configured to work as a passport, as a DNIe or as a residence permit.
- The entire Public Key Infrastructure is updated.
- The issuing infrastructure is updated.

Travel Documents. Common features

- Product with a vocation to last.
- This O.S. will be a totally new development, with the most advanced technical requirements, and certified with the most advanced protection profiles.

- Maximize security
- All global trends in security will be incorporated, and will be integrated naturally into the overall design.
- Two asymmetric key algorithms will be supported, so that any cyber attack could be solved by switching to the use of the second algorithm.

Travel Documents. Common features

- The time necessary to carry out the process of issuing a document should be smaller.
- It is an essential requirement to reduce the time invested in the generation of asymmetric keys (ID card).

Travel Documents. Common features

- Manufacturing flexibility.
- Product can be configured in FNMT-RCM as DNIe, as a PACE Passport, or as a Residence Permit. All of them certified, and according to international regulations.

Travel Documents. Common features

- Use of a 32-bit hardware platform.
- The selected architecture for the DNIe 4.0, is called ARM Cortex M0, and has 32-bit buses.
- ST Microelectronics already had a first version, and Infineon is migrating its platform "Integrity Guard" to this architecture.
- In response to the deadlines, we chose the platform of ST.

Specific features for DNIe 4.0

- New O.S. will be certified with three P.P: eID, ePassport, eSign. This guarantees that will be in accordance with the eIDAS Regulation.
- b) DNIe 3.0 through contactless antenna is managed by Microsoft with some limitations. It is necessary developments to resolve it.

Results:

- The new development is significantly faster: Shorter times of issuance of these documents.
- More powerful: The asymmetric keys generation is now ultra-fast.
- Significant improvements in citizen satisfaction are achieved.

Results:

- All the safety recommendations have been included natively.
- Now offers full support for RSA and elliptic curves algorithms.
- International interoperability: certified with the three P.P. eID, eSIGN, ePassport.
- It can be configured as a DNIe, as a PACE Passport, or as a Residence Permit.

Speaker: Valentín Ramírez Prieto
vramirez@fnmt.es
FNMT-RCM
Jorge Juan 106
Madrid 28009

THANK YOU