International Civil Aviation Organization

Eighth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards

ICAO Headquarters, Montréal, Canada
10 - 12 October 2012

IMPLEMENTING THE ePASSPORT IN SPAIN:

LESSONS LEARNT

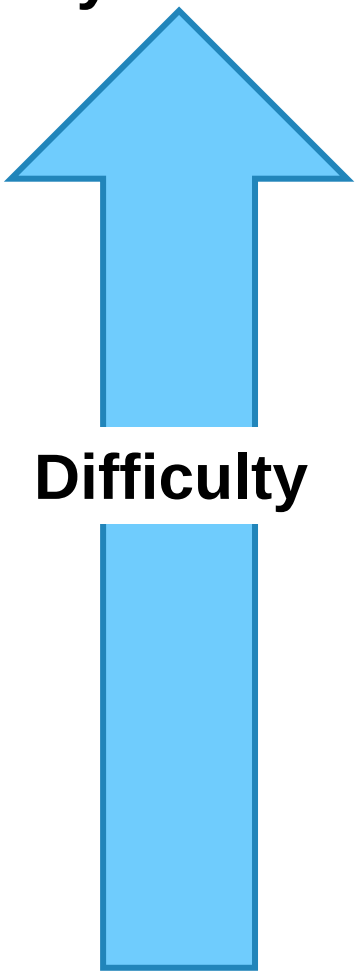
CARLOS GÓMEZ

HEAD OF R&D AND INNOVATION

FNMT-RCM, SPAIN

LESSON LEARNT No. 1

- Start guarantying the security and authenticity of breeder documents
- Define an ePassport according to the ICAO standards
- Establish a robust and secure issuance system
- Set up a PKI for ePassport issuance
- Distribute your keys. Subscribe to the PKD
- Develop an electronic border control programme



INDEX

BREEDER DOCUMENTS

Civil Registry

- Eclesiastic origin (baptisms, weddings, deceases) starting from the Trent Consilium (1545-1563)
- Created from the Civil Registry Law of 1870
- Depending on the Ministry of Justice
- Free and public.

BREEDER DOCUMENTS

- **Civil Registry (services)**
  - Enrollment
    - Birth, filiation
    - Name, surname and changes on them
    - Decease or absence declarations
    - Nationality and neighbourhood
    - Parental guardianship, custody
    - Weddings
    - Deceases

  - Certification
    - Literal birth certificate for the issuance of the National Identity Card

BREEDER DOCUMENTS

DNI – National Identity Document

- Issued from the information of the civil registry
- Mandatory by a national regulation from 1944
- Issuance started in 1951
- Electronic ID card introduced in February 2006

1937

1951

1996

2006

LESSON LEARNT No. 2

- **For ePassport issuance:**

Establish an electronic passport issuance system based on secure breeder documents, issued by trusted national authorities

ePASSPORT DEFINITION

- **Physical characteristics - construction**

Format

ePASSPORT DEFINITION

- **Physical characteristics - construction**

Dimensions

ePASSPORT DEFINITION

- **Physical characteristics - construction**

Data page

LESSON LEARNT No. 3

ICAO/OACI Doc 9303 on Machine Readable Passports

ePASSPORT DEFINITION

- **Security features**

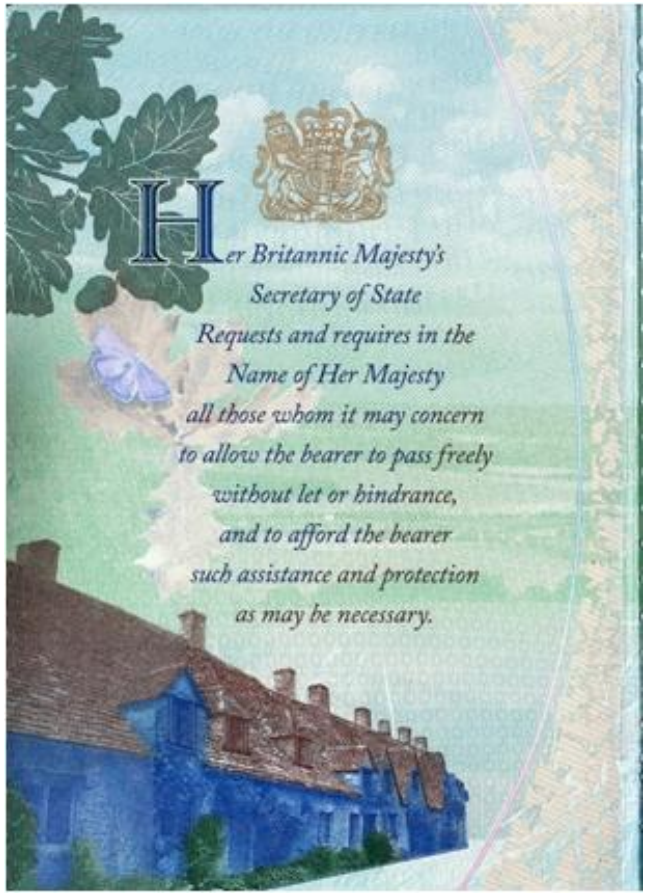
Cover

ePASSPORT DEFINITION

- **Security features**

Inside cover:

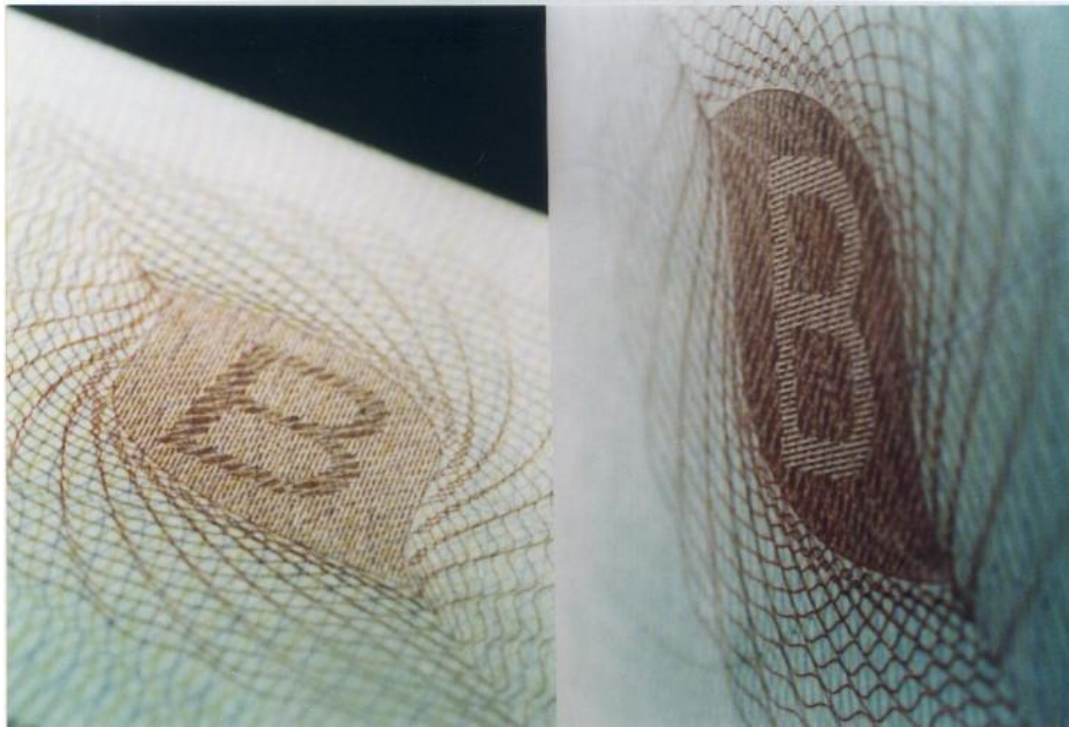
Intaglio printing in two colours



ePASSPORT DEFINITION

- **Security features**

Inside cover:

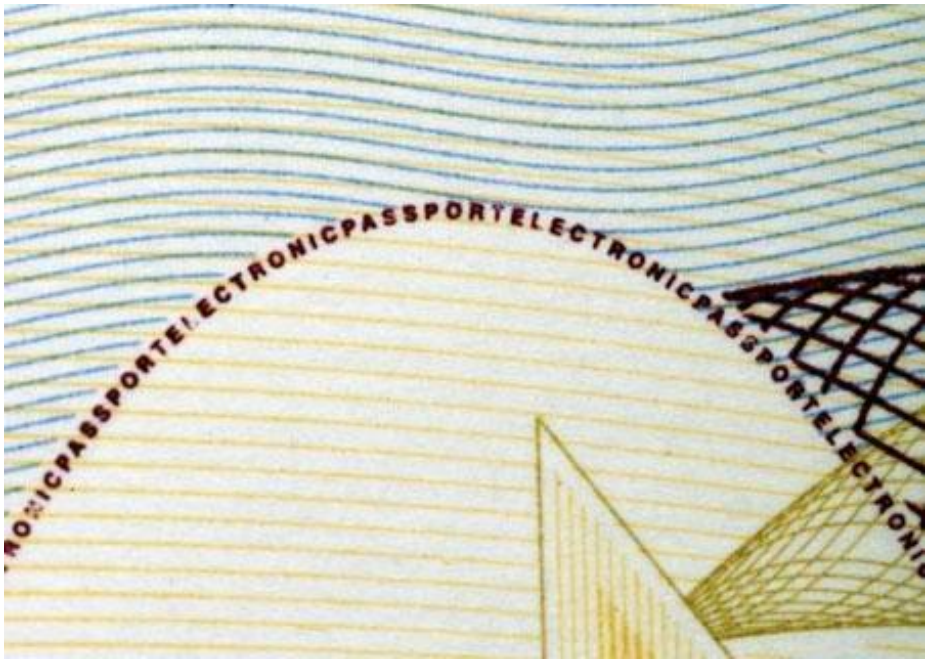


Latent image

ePASSPORT DEFINITION

- **Security features**

Inside cover:



Microtexts

ePASSPORT DEFINITION

- **Security features**

Inside cover:

Optically variable inks

ePASSPORT DEFINITION

- **Security features**

Paper:

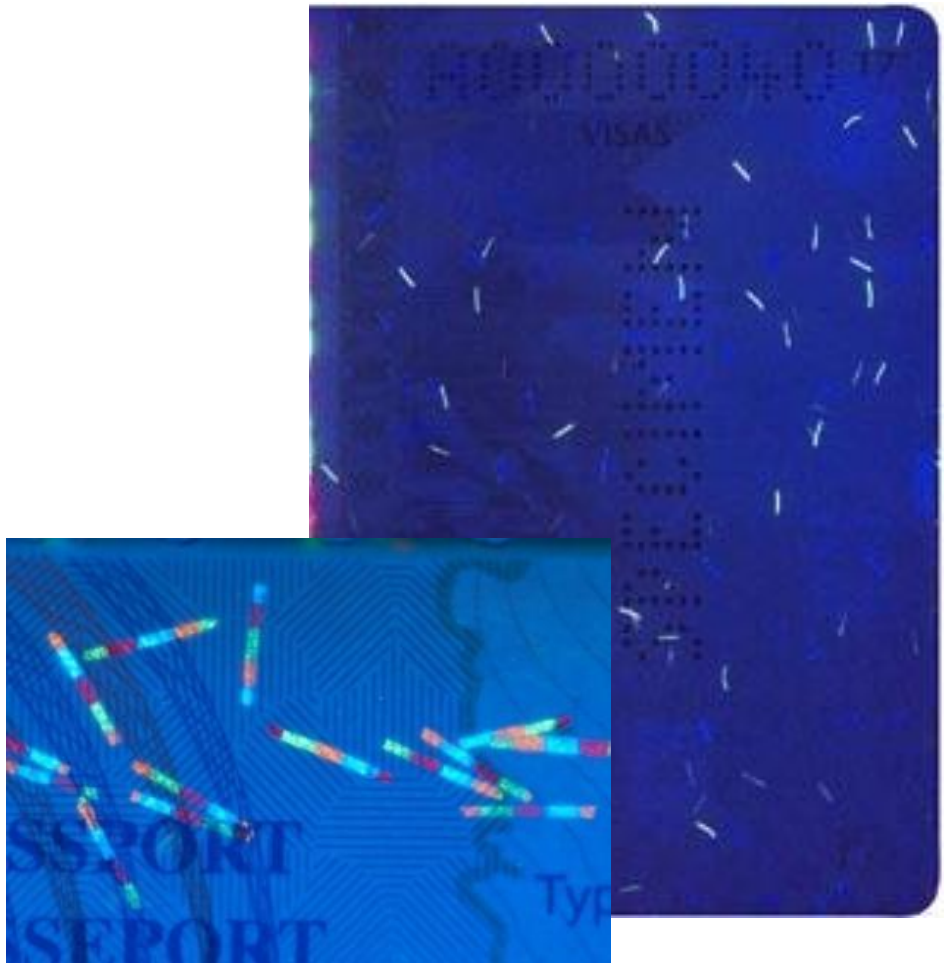
Multitone watermark

ePASSPORT DEFINITION

- **Security features**

Paper:

Invisible fibres

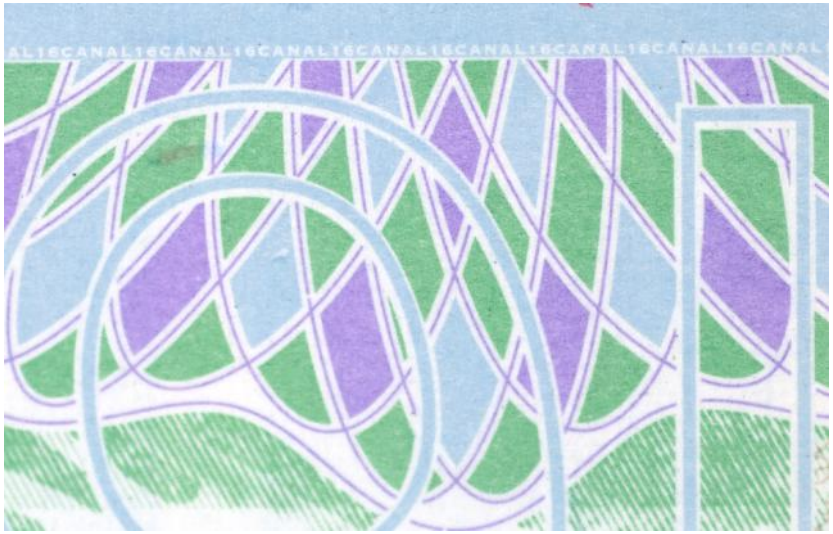


ePASSPORT DEFINITION

- **Security features**

Inner pages:

Guilloches in several colours



ePASSPORT DEFINITION

- **Security features**

Inner pages:

Offset security printing

ePASSPORT DEFINITION

- **Security features**

Inner pages:

Special security patterns

ePASSPORT DEFINITION

- **Security features**

Inner pages:

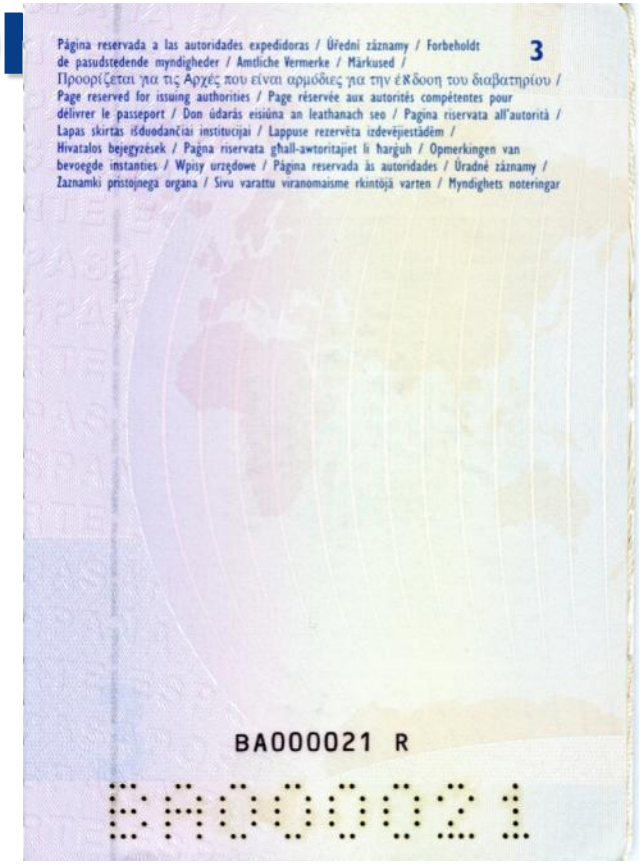
Invisible inks

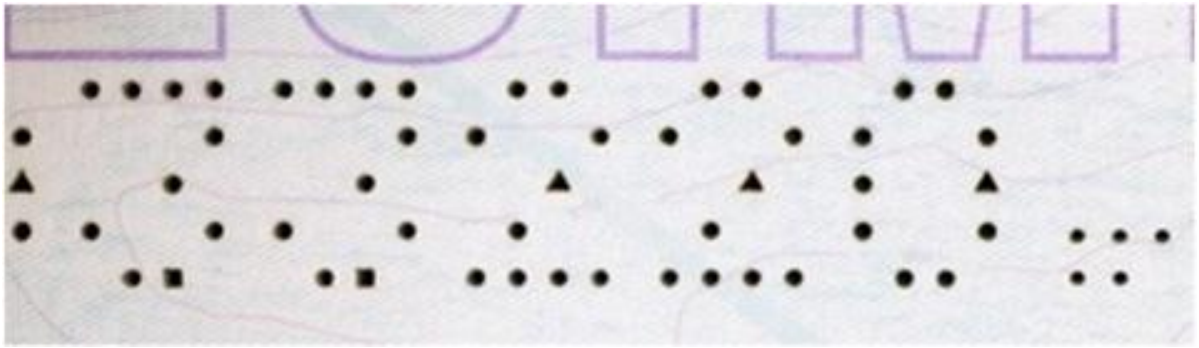
ePASSPORT DEFINITIO

- **Security features**

Inner pages:

Laser booklet numbering





ePASSPORT DEFINITION

- **Security features**

Data page:

Holographic film

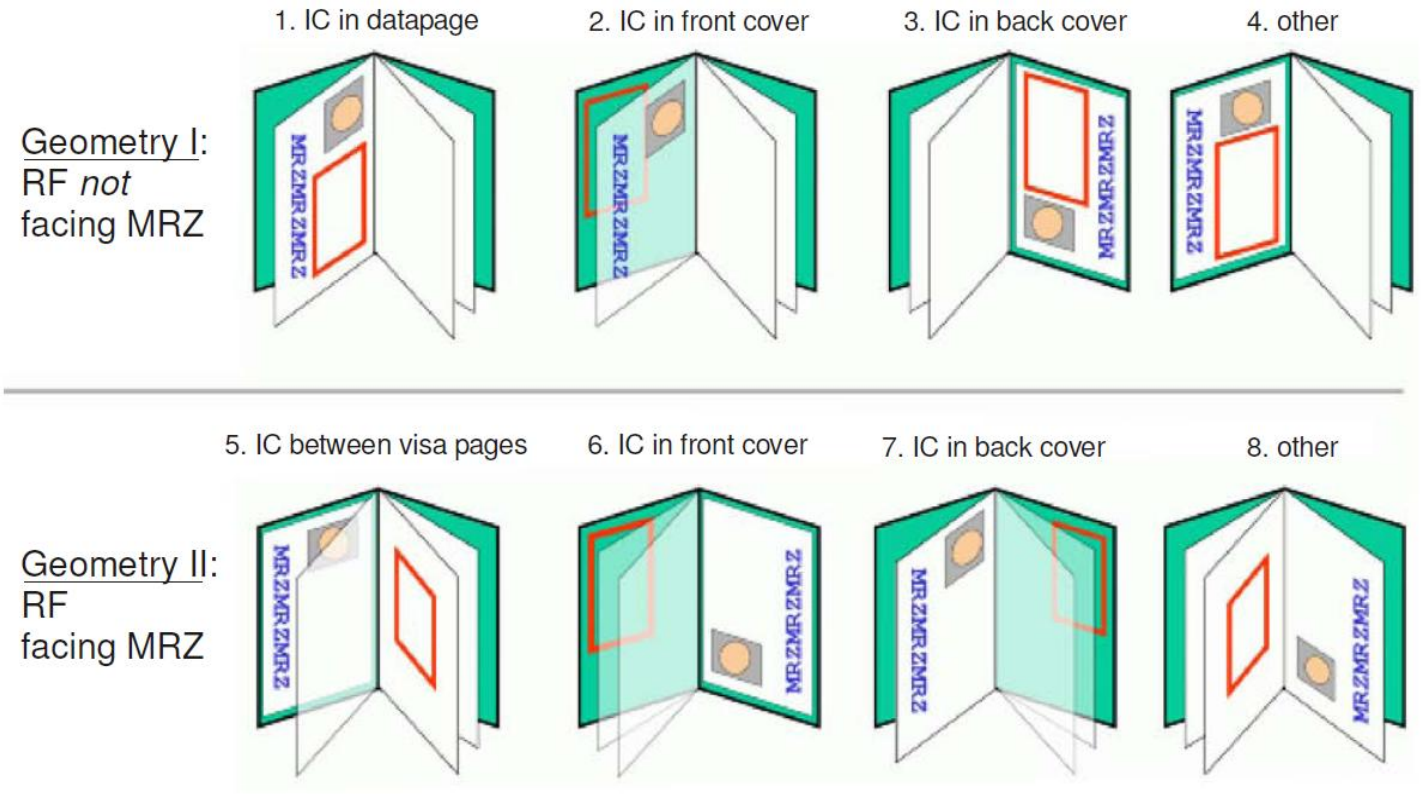
LESSON LEARNT No. 4

- Select the security features according to the ICAO 9303 recommendations
- Use proven technology already in use in similar documents
- Avoid the use of a single supplier’s proprietary technology
- Source out more than one supplier
- Carry out lab tests before approval of any material or security feature

ePASSPORT DEFINITION

- **Chip - antenna**

Integration options



ePASSPORT DEFINITION

- **Chip - antenna**

Data page in paper or polycarbonate

ePASSPORT DEFINITION

- **Chip - antenna**

Polycarbonate data page

✓ Impossible delamination	✗ Data page and chip in a single component
✓ Lamination protects background printings and personalization data	✗ Weakness in data page substitution
✓ Data personalization takes place in inner layers	✗ Background printings differs from inner pages' background printing
✓ Holograms integrated in inner layers	✗ Portrait personalization in black and white
✓ High durability	✗ Very expensive personalization systems
✓ Possibility of engraving data in relief	✗ Difficult integration of security features in the substrate
✓ Water resistant	✗ Need for extra security features
	✗ Re-engravable data page
	✗ Forgery threats by adhesion of personalized thin foils
	✗ Micro-cracks around chip location

ePASSPORT DEFINITION

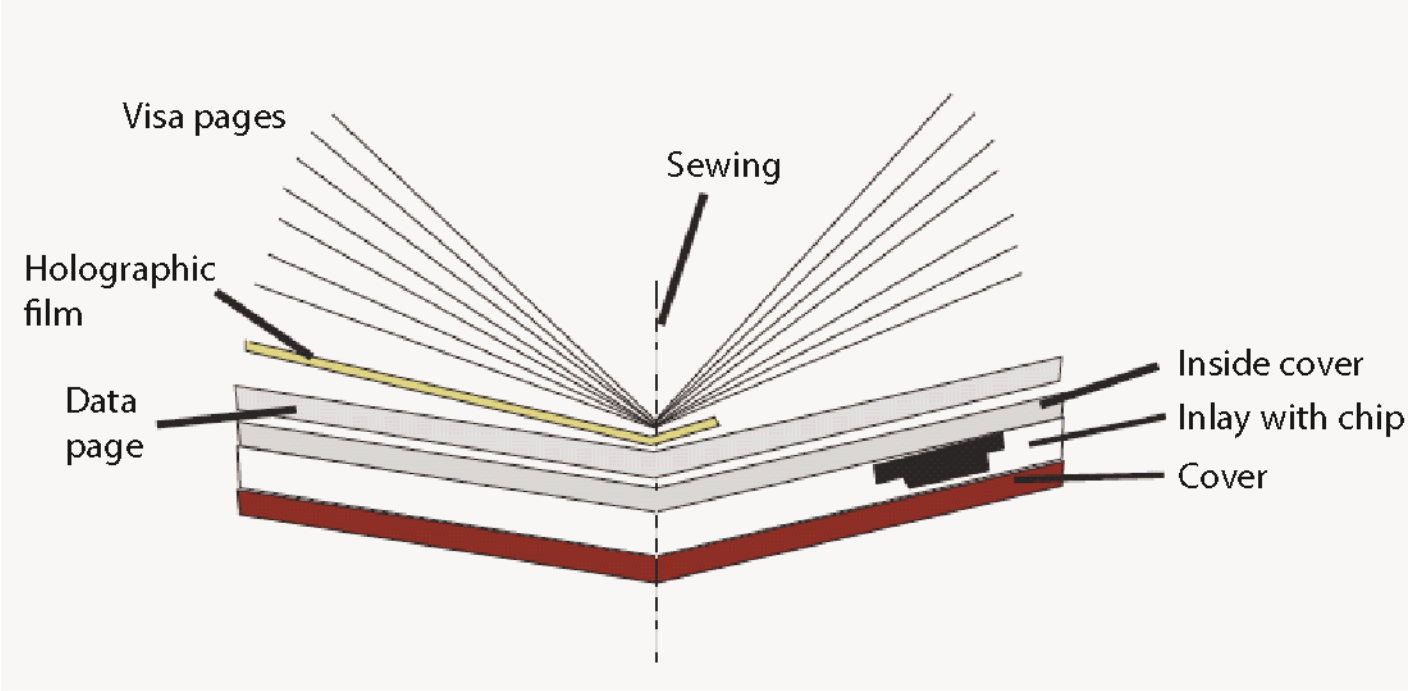
- **Chip - antenna**

Paper data page

✓ Data page and chip in different locations	✗ Data page protection required
✓ Harder data page substitution	✗ Expensive security films for data protection
✓ Background printing identical to inner pages	✗ Good integration of the inlay is a must
✓ Portrait printed in colour	✗ Insulating, stiff covers
✓ Inkjet personalization inks penetrate into the substrate	
✓ Low cost	
✓ Availability of several security features for integration in the substrate	
✓ Availability of personalization systems based on UV inks	

ePASSPORT DEFINITION

- **Chip - antenna**



Chip integration in the cover

LESSON LEARNT No. 5

- Carry out production and lab tests to determine the optimal location for chip and antenna
- Conduct research to determine whether polycarbonate or security paper data pages are adequate for the ePassport
- Use proven technology already in use in similar documents
- Source out more than one supplier for the chip, inlays and eCover

ePASSPORT DEFINITION

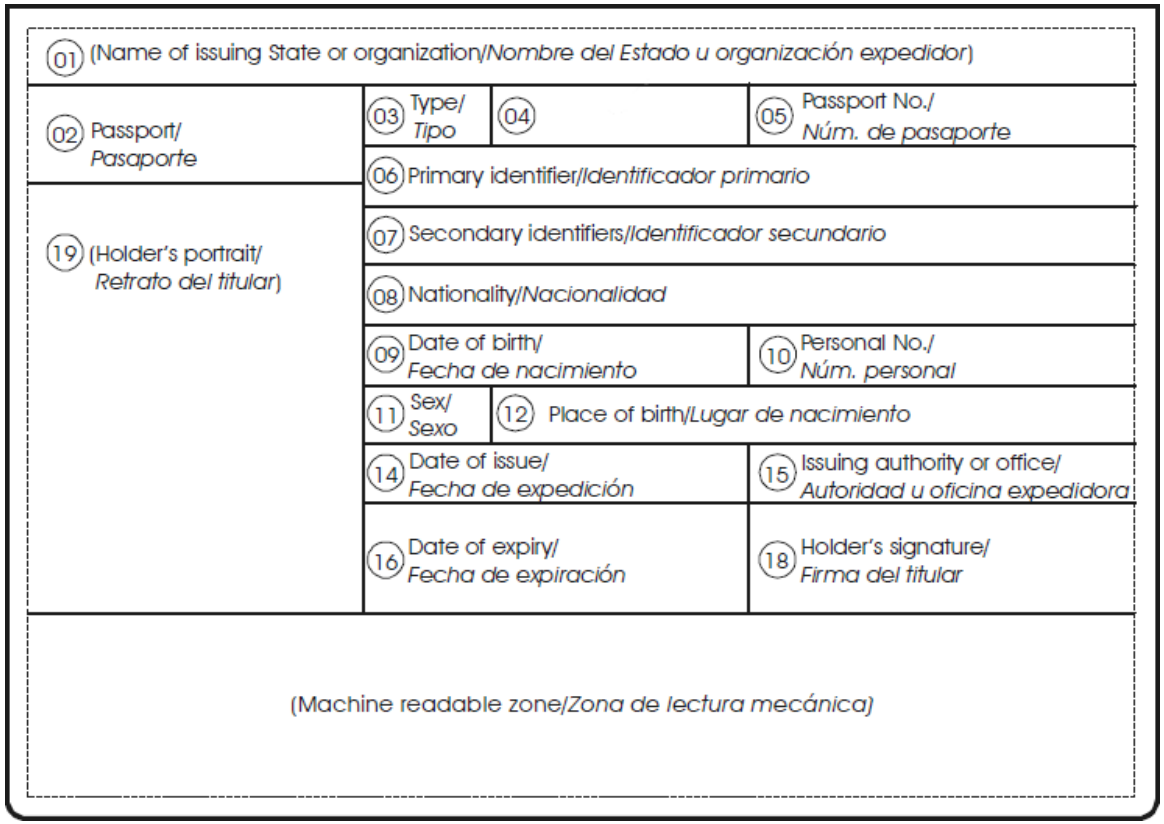
- **Operating system – LDS structure**
  - OS characteristics
    - Native vs JavaCard OS
    - Minimum characteristics:
      - Passive Authentication and BAC
      - Operating under two different HW platforms
      - LDS structure
      - Secure messaging
      - Personalization by secure channel
      - CC EAL 4+ Certification
      - Absolute control of chip's life cycle

LESSON LEARNT No. 6

- Use proven technology already in use in similar documents
- Search for an operating system that can operate on at least two different hardware platforms
- Carry out electrical and functional lab tests for the chip, antenna and operating system before product approval
- Demand a security certification of the products
- Control the life cycle of the operating system

ePASSPORT DEFINITION

- **Data page personalization**



ICAO layout

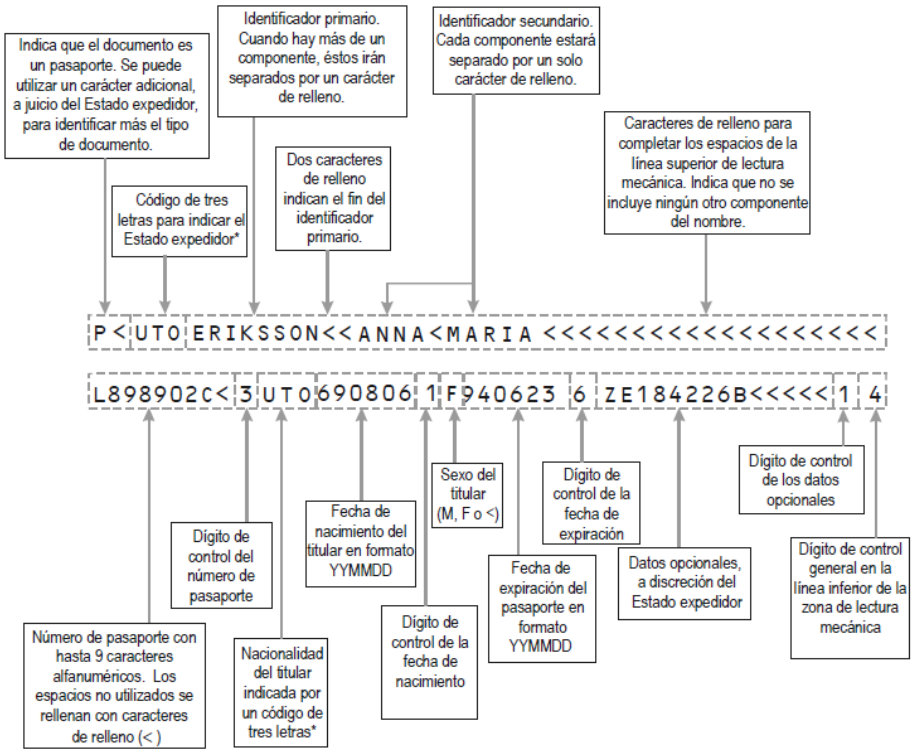
ePASSPORT DEFINITION

- **Data page personalization**

Keep it simple

ePASSPORT DEFINITION

- **Data page personalization**

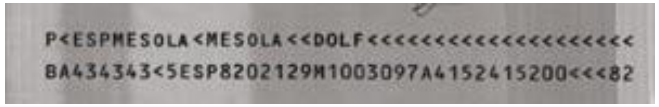


Machine readable zone

ePASSPORT DEFINITION

Interoperability

ePASSPORT DEFINITION



LESSON LEARNT No. 7

- Apply the layout for data personalization as defined in ICAO Doc 9303
- Keep the data page layout as simple as possible
- Use the page adjacent to the data page for optional data
- Make sure the format of OCR lines and the chip contents are codified correctly
- Verify the interoperability of the ePassport

ISSUANCE SYSTEM

- **ePassport issuance system in Spain**
  - Under responsibility of the Spanish Police
  - Centralized criminal and civil data bases
  - De-centralized ePassport issuance in 256 offices distributed in 52 provinces
  - National eID Card is the only breeder document valid for the ePassport issuance
  - Immediate ePassport issuance: the citizen obtains his ePassport or eID card in a single act in around 20 minutes

ISSUANCE SYSTEM

- **Centralized vs de-centralized systems**

  - Issues found during the development of the Spanish ePassport programme
    - Blank passports distribution
    - ePassport personalization devices and systems
    - Chip personalization
    - Security of the issuance process
    - Personnel
    - High cost

ISSUANCE SYSTEM

- **Security of the issuance process**

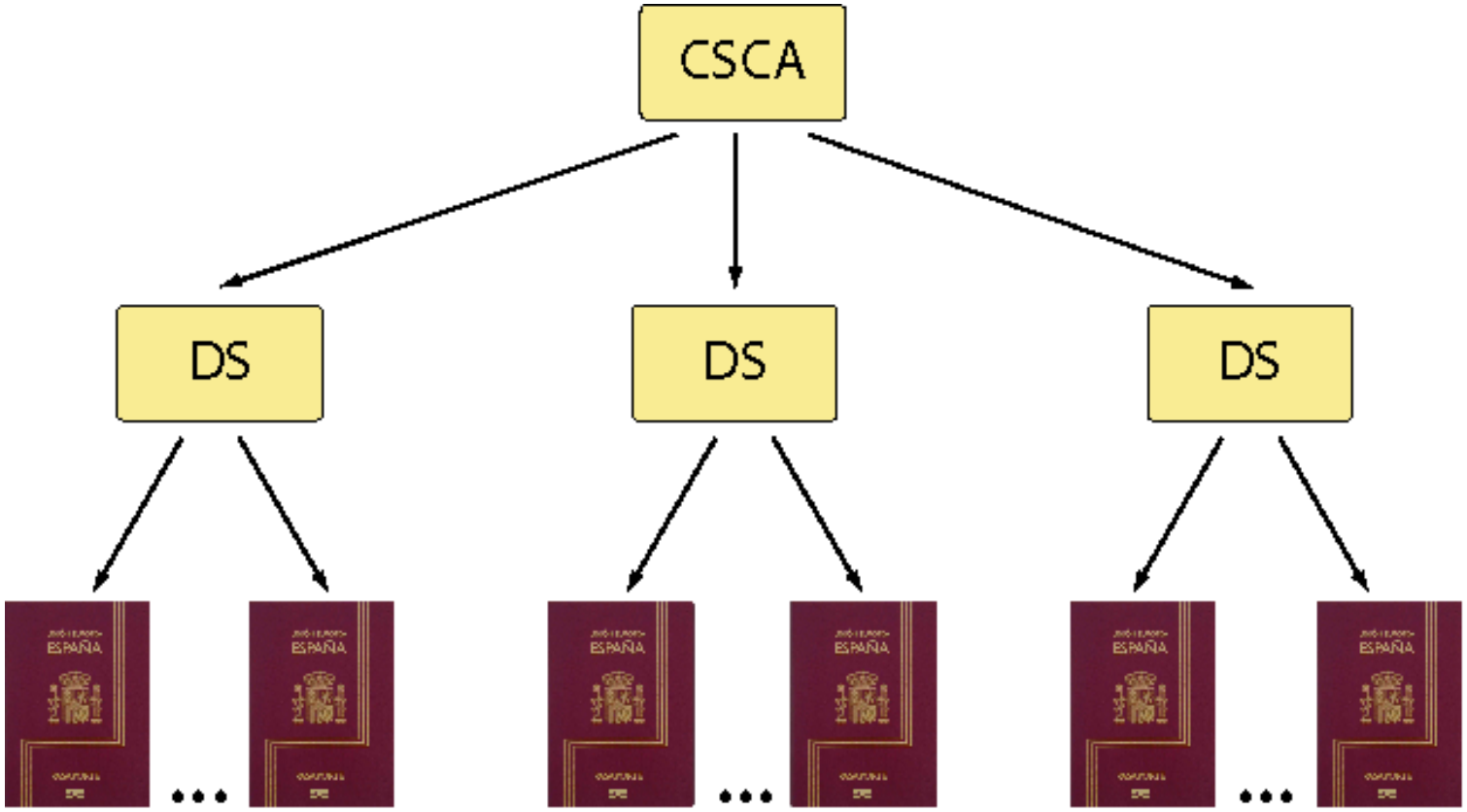
  - The citizen requests an scheduled appointment by telephone or internet
  - The citizen turns up at the Police office with his eID card
  - The Police officer authenticates in the system and captures the citizen's data and biometrics
  - Verification takes place against several data bases (ID cards, criminal records, blacklists, Europol, Interpol, etc)
  - ePassport data page and chip are personalized
  - The citizen gets his ePassport in 20 minutes

LESSON LEARNT No. 8

- Evaluate the feasibility of a centralized issuance system versus a decentralized system
- Establish a scheme for protection of blank passports
- Verify the security and trustworthiness of breeder documents at issuing time
- Control the security of the whole issuing process
- Set up security measures for personnel responsible for issuance
- Assess the costs of the process

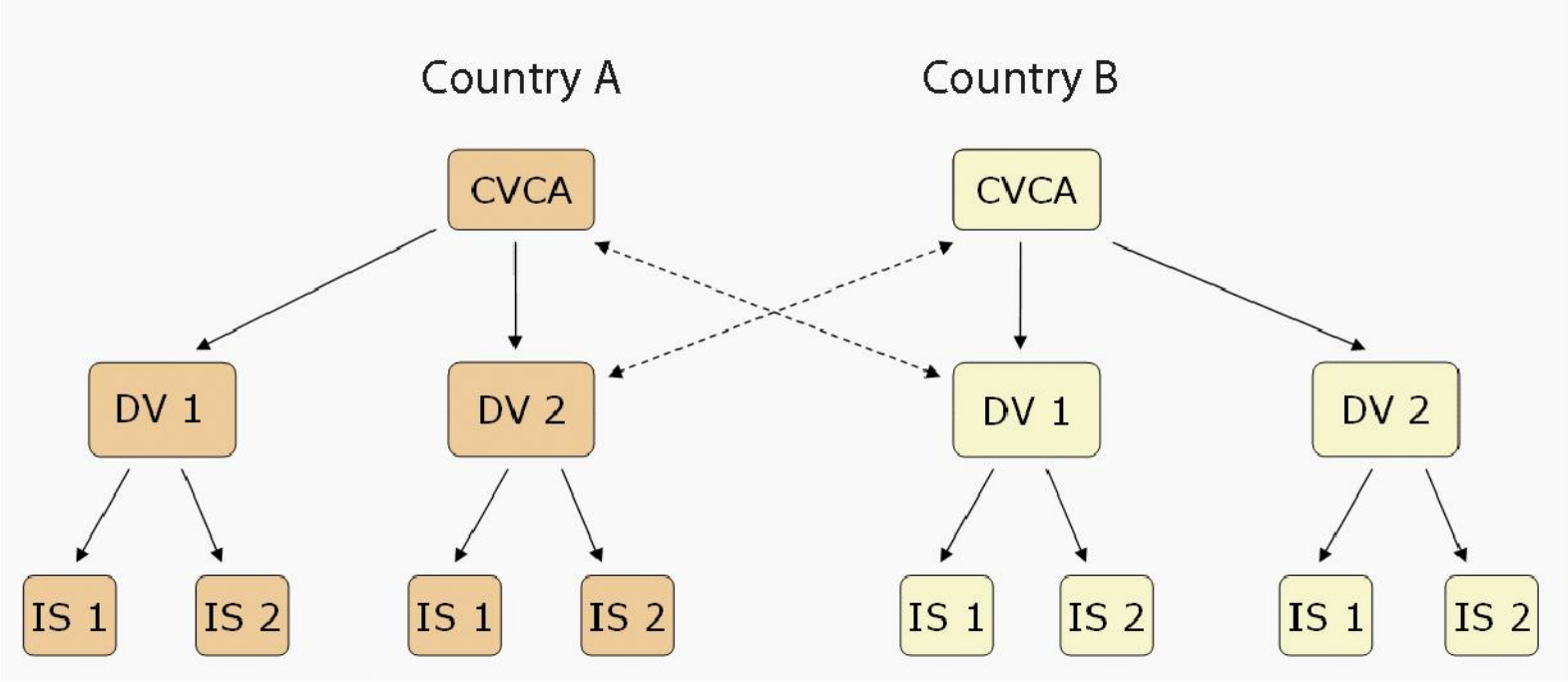
PKI and PKD

- 2006. PKI for BAC ePassport issuance in Spain



PKI and PKD

- 2009. PKI for EAC ePassport verification in the EU



PKI and PKD

- **Further steps**

  - Certificates and CRL distribution by bilateral exchange
  - July 2012: **Spain becomes the 32nd PKD participant**

  - End 2012: Start-up of the SPOC protocol for the exchange of verification certificates
  - 2014: Integration of Supplemental Access Control and PACE protocol

LESSON LEARNT No. 9

- Establish a PKI of ePassport issuance based on proven and trusted technologies
- Start with the issuance of BAC ePassports
- Evaluate the necessity of implementing EAC and its associated costs
- Distribute your keys
- Subscribe to the ICAO PKD

LESSON LEARNT No. 10

- Conduct a study on the present situation of your country's passport issuance system and draw up a thorough transition plan for migrating to ePassports
- Follow the recommendations of ICAO Doc 9303
- Use proven technologies already in use in similar documents from other countries
- Evaluate all the products and processes before approval
- Search for specialized support

THANK YOU

Contact Information:

CARLOS GÓMEZ

FNMT-RCM

E-mail: cgomez@fnmt.es

Tlf.: +34 915 666 651