ePassport: Securing International Contacts with Contactless Chips

Gildas Avoine, Kassem Kalach, Jean-Jacques Quisquater

UCL, Louvain-la-Neuve, Belgium

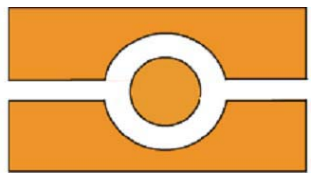
Summary

- EPassport Specifications
- Cryptographic Tools
- Attack on BAC Keys
- Improvements & Weaknesses

A Few Facts About Passport History

- International Civil Aviation Organization (ICAO)
- ICAO works on electronic passport (ePassport) since late 90s
- ICAO Standard (Doc 9303) released in 2004
- First ICAO-compliant electronic passport issued end 2004
- More than 50 countries today

- Securing passports with chip: Davida & Desmedt Eurocrypt'88
- First electronic passports: Malaysia (1998)



Technical Specifications

Contactless chip = microcircuit + antenna = RFID tag

Chip ⇒ Security, Contactless ⇒ Convenience

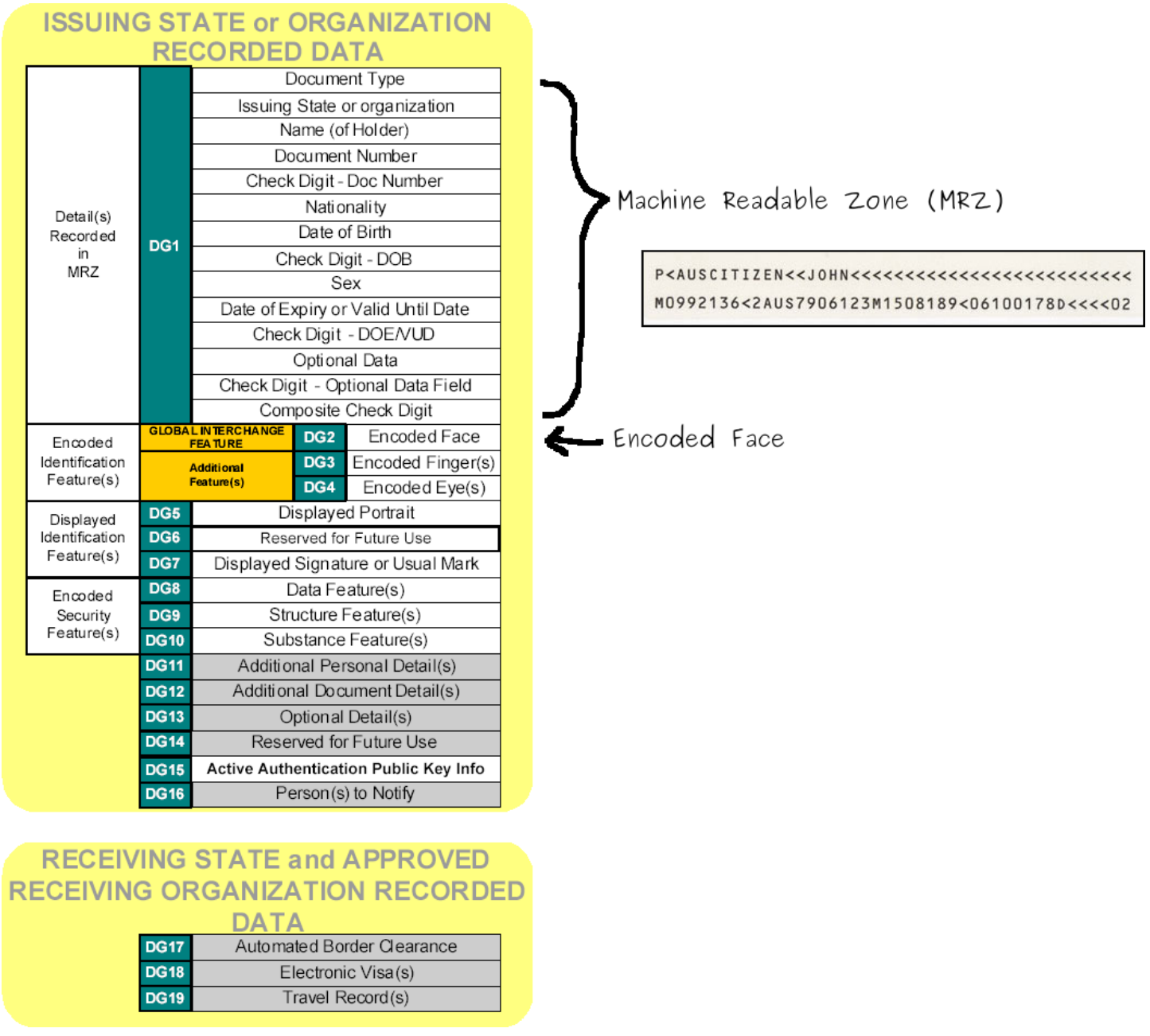
Tag is passive ie no internal battery

Tag has a microprocessor (public-key crypto)

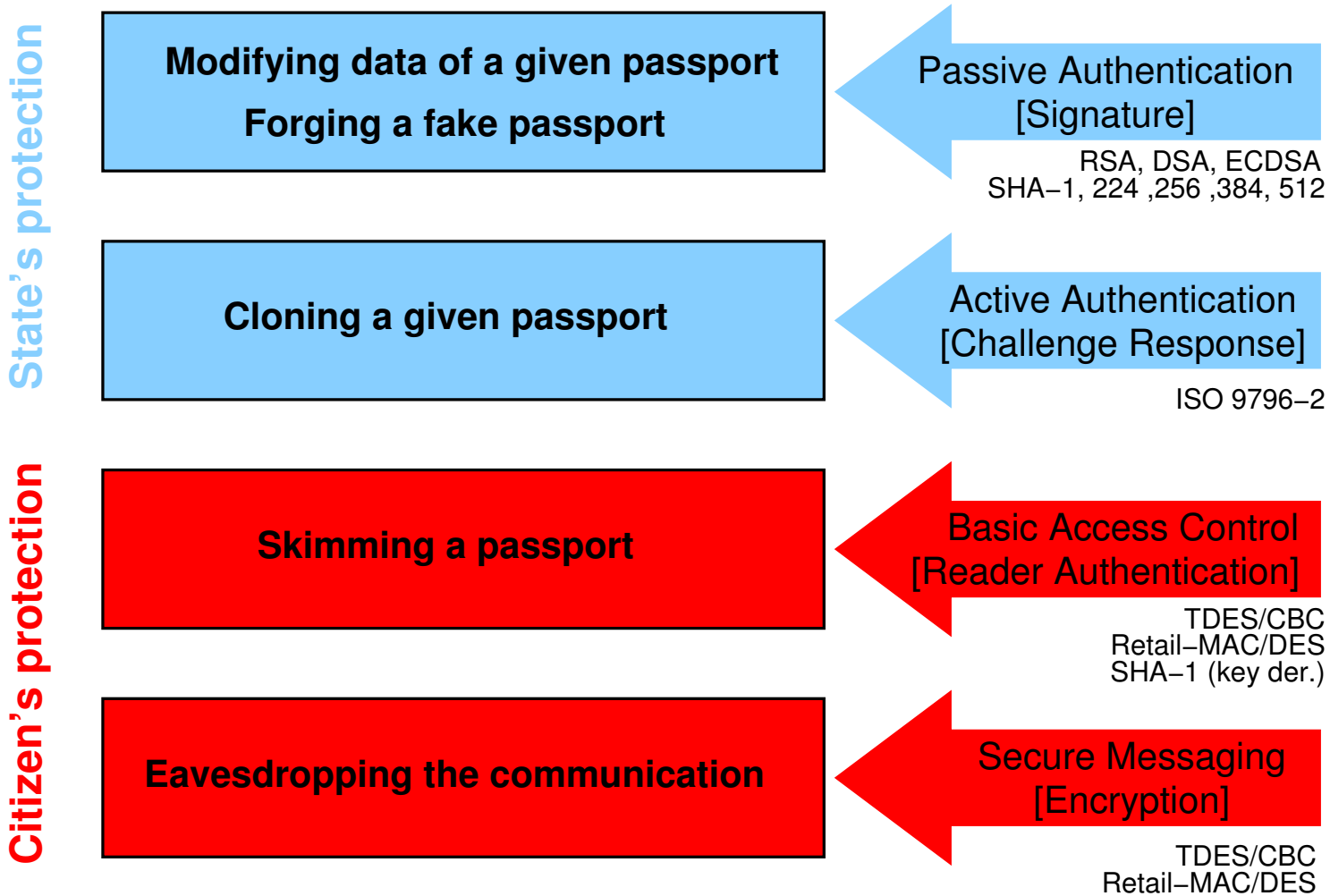
Compliant ICAO Doc 9303 and ISO 14443

Distance 10 cm, 70–100 cm (exp)

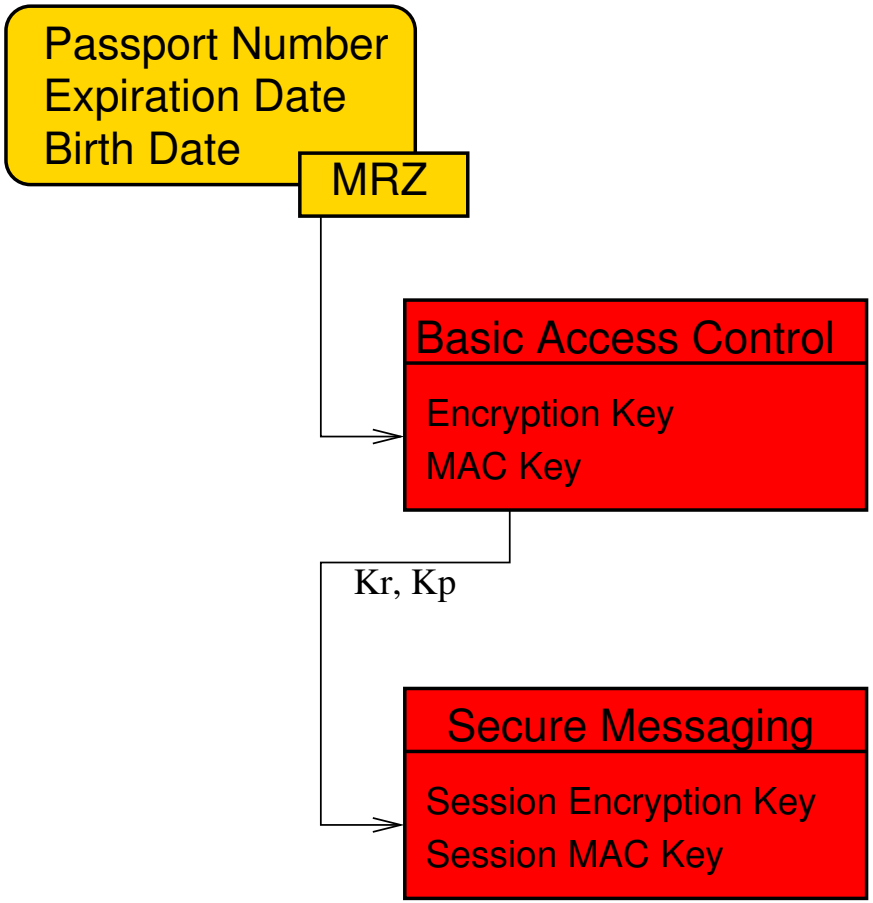
Logical Data Structure

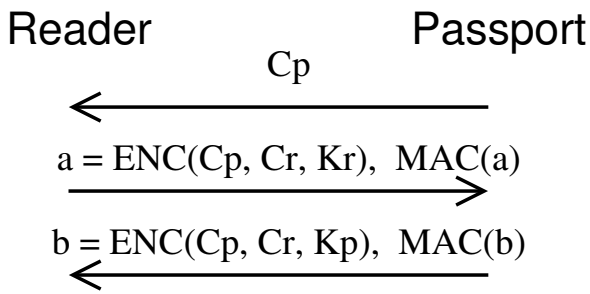


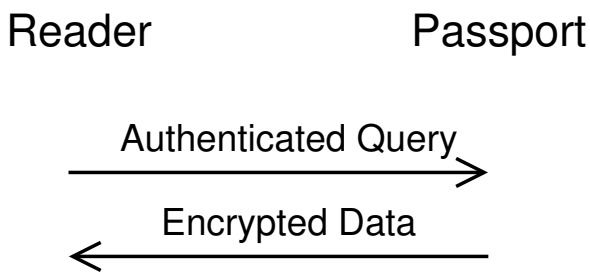
State and Citizen's Protection



Basic Access Control and Secure Messaging







BAC Keys' Entropy

- According to ICAO, birth year must be encoded on 2 digits (15.15 bits), expiry delay should be max 10 years (11.83 bits), and passport number must contain no more than 9 alphanum characters (46.53 bits)

Theory	73

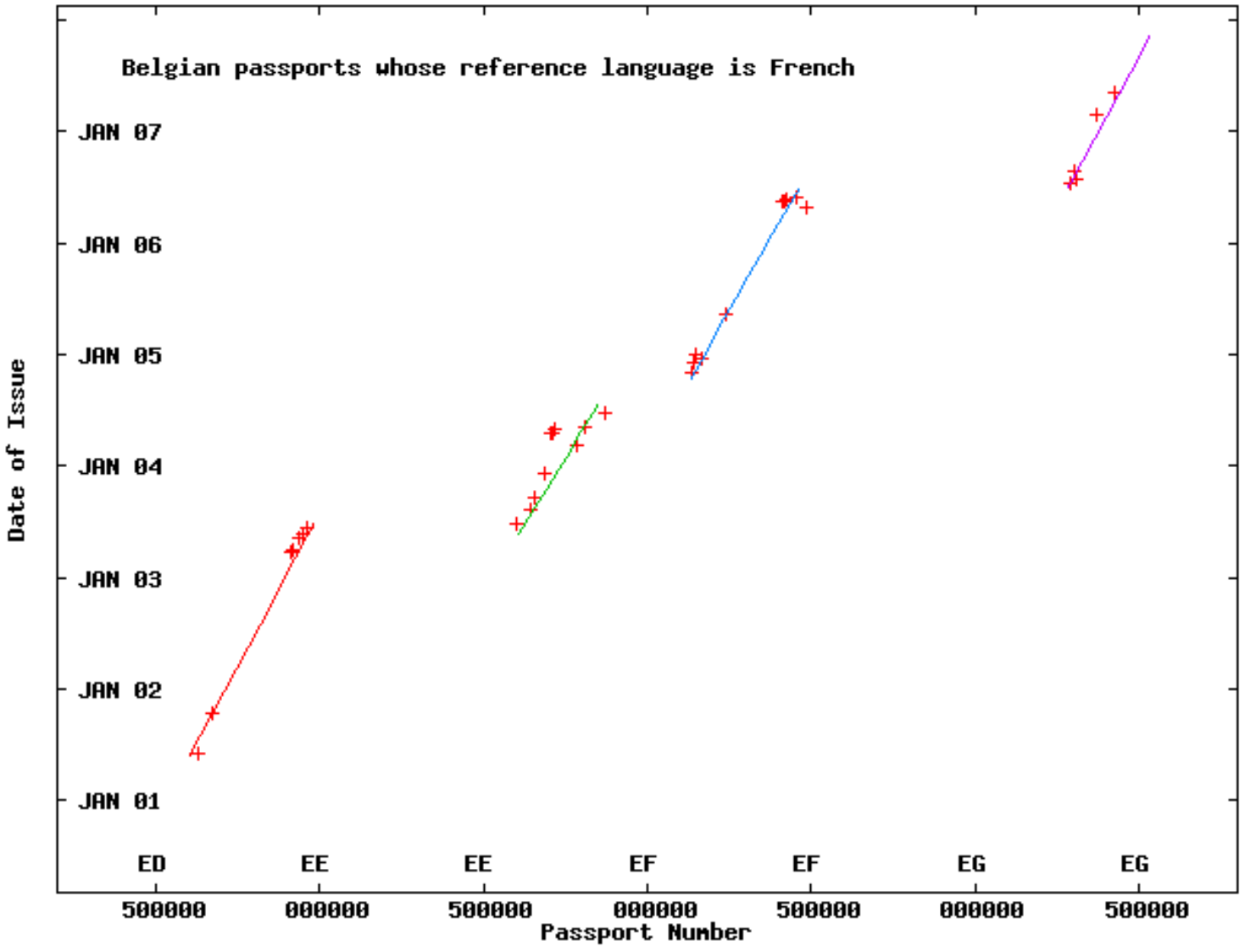
- In practice, generation of passport numbers let to discretion of countries. Numbers are structured (eg 00AA00000) with some non-random parts (eg letters represent the issuing office).

Germany	55	[CarluccioLPS]
USA	54	[JuelsMW]
Netherlands	50	[Robroch]

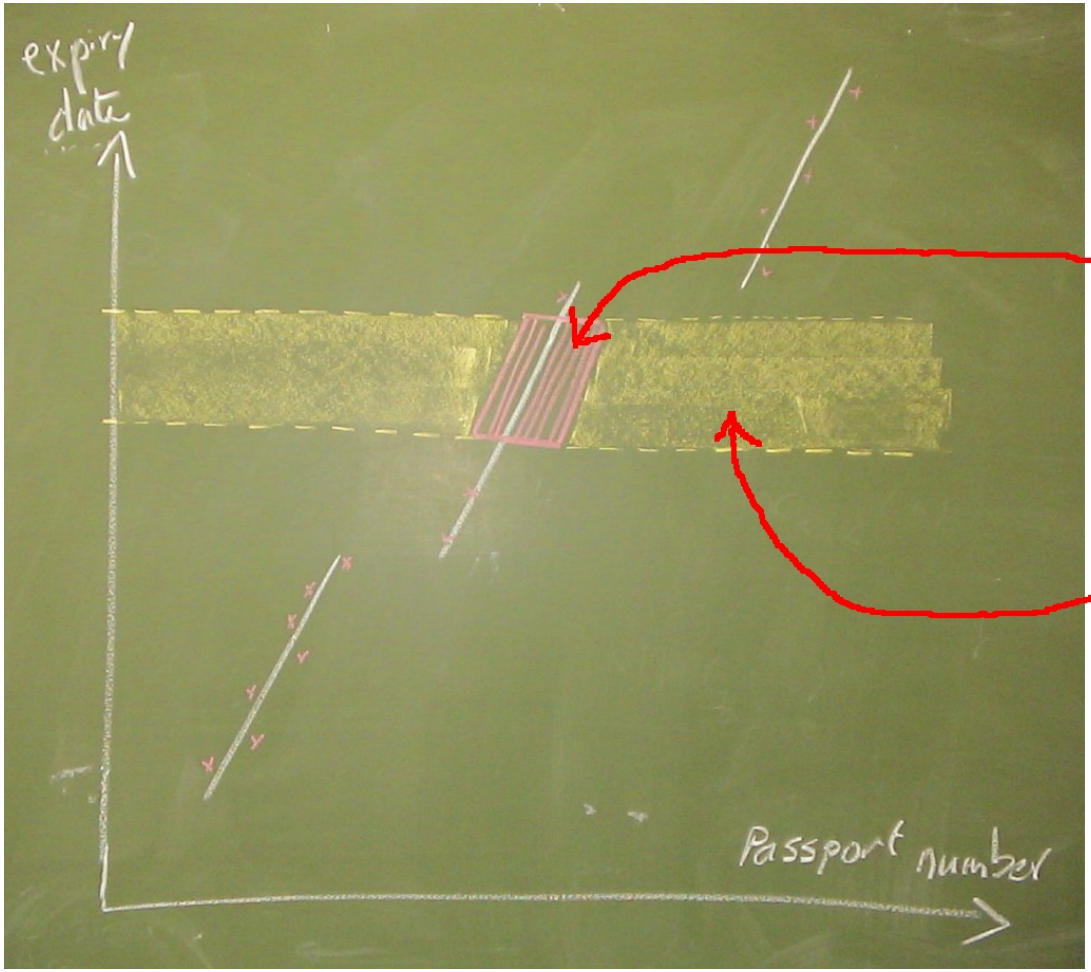
Heuristics on Belgian Passport

- Expiration delay is 5 years only
- No passports issued during week-ends and vacation days
- Passport numbers have only 8 characters (6 digits, 2 letters)
- Passport numbers do not look like random numbers

Analysis of Belgian Passport Numbers



Reducing Searching Area



Birth date given

Searching area with heuristics
24000 tests / expiry date

Searching when pass nub random
101559956668416 tests /expiry date

Belgian Passport Entropy

Country	Effective	Birth date known
Belgium	38	23

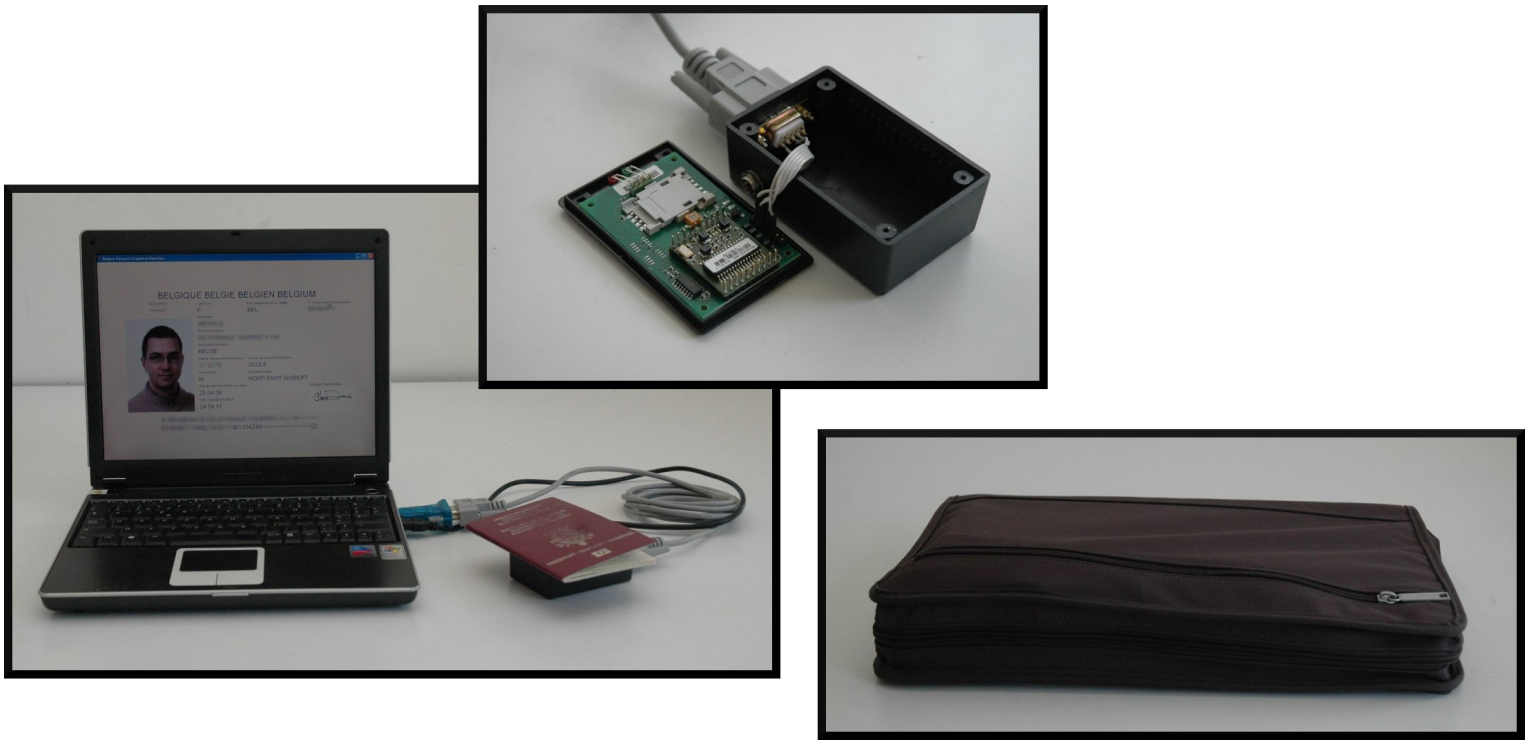
Attack do-able in practice?

Various Attacks on Belgian Passports

- On-line attack (Skimming): about 400 queries/min
  - The passport acts as an oracle
  - In lab: Easy to Hard, In real life: Hard to Infeasible
- Off-Line attack (Eavesdropping): about 2^{23} tests/s (Doe's PC)
  - Require material to be decrypted $\Rightarrow$ eavesdropping, not skimming
  - Signal sent by the reader can be listened at several meters
  - In real life: Very easy
- Pragmatic attack
  - In real life: Cannot be easier

Type	Number
Machine-readable	430 000
ePassport Gen 1	720 000
ePassport Gen 2	350 000
Total	1 500 000

Skimming a Gen 1 Belgian Passport



Improvements & Weaknesses

Possible Improvements:

- Radio blocking shield
- Delay chip answers
- Random passport numbers
- Add entropy with the optional field of the MRZ
- Separate BAC keys and MRZ

Potential other weaknesses:

- The administration interface is not standardized
- Combination of algorithms not standardized
- Everyone can require the chip to sign (random) data
- Relay attacks
- Analysis of the encrypted communication
- And probably more...