E-Passport Survey

Serge Vaudenay and Martin Vuagnoux

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

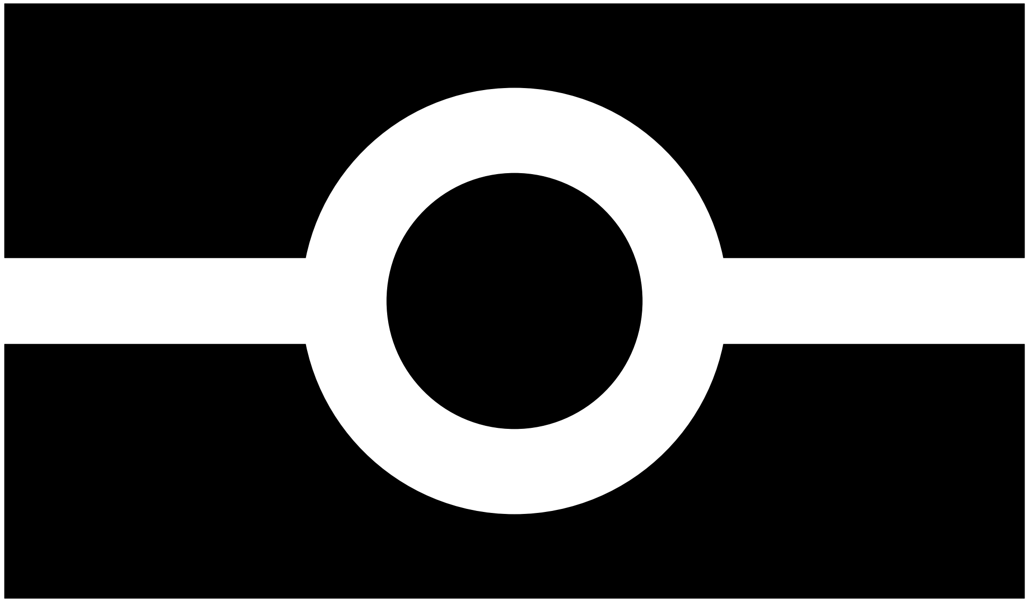
http://lasecwww.epfl.ch/

LASEC

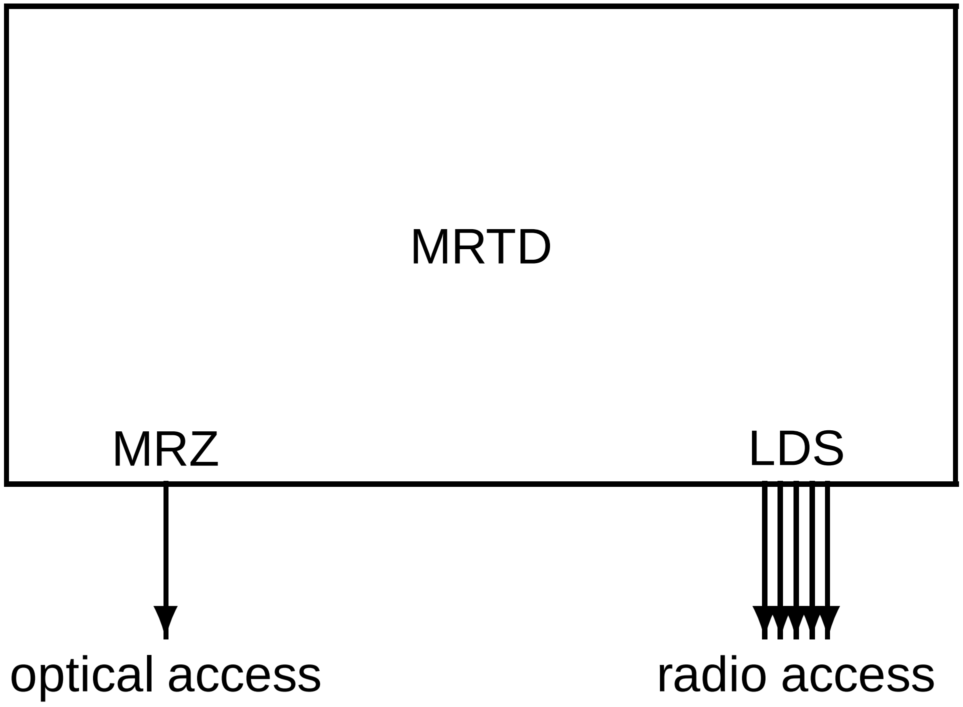
Machine-Readable Travel Document (MRTD) History

- 1968: ICAO starts working on MRTD
- 1980: first standard (OCR-B Machine Readable Zone (MRZ))
- 1997: ICAO-NTWG (New Tech. WG) starts working on biometrics
- 2001 9/11: US want to speed up the process
- 2004: version 1.1 of standard with biometrics and contacless ICC
- 2006: EU develops extended access control + more private data

How to Distinguish a Compliant MRTD



MRTD in a Nutshell



- data authentication by digital signature + PKI
  aka **passive authentication**
- access control + key agreement based on MRZ_info
  aka **basic access control (BAC)**
- chip authentication by public-key cryptgraphy
  aka **active authentication (AA)**

MRZ

- document type
- issuing country
- holder name
- doc. number + CRC
- nationality
- date of birth + CRC
- gender
- date of expiry + CRC
- options + CRC

LDS

- DG1 (mandatory): same as MRZ
- DG2 (mandatory): encoded face
- DG3: encoded finger(s)
- DG4: encoded eye(s)
- DG5: displayed portrait
- DG6: (reserved)
- DG7: displayed signature
- DG8: data feature(s)
- DG9: structure feature(s)
- DG10: substance feature(s)
- DG11: add. personal detail(s)
- DG12: add. document detail(s)
- DG13: optional detail(s)
- DG14: (reserved)
- DG15: KPu_{AA}
- *DG16: person(s) to notify*
- DG17: autom. border clearance
- DG18: electronic visa
- DG19: travel record(s)
- SO_D (mandatory): digital sign.

The Eurocrypt 07 Survey

# e-passports	3
# countries	3

Switzerland, **UK**, **France**

Shield (Faraday Cage)

prevent from unauthorized access by means of a metallic cover

Switzerland	no
UK	
France	

TBC: passports from the **USA** have shields

Privacy-Enhanced RFID Singulation

unlinkability by means of PRG

Switzerland **UK** **France**	08xxxxxx

TBC: passports from **Italy**, **New Zealand**, **USA** use constants
passports from **Australia** use xxxxxxxx (against ISO 14443B Part 3)

Basic Access Control

access control + secure messaging by means of symmetric-crypto

Switzerland **UK**	implemented
France	?

TBC: passports from the **USA** don’t have BAC

Data Beyond MRZ + Face

identification by means of (extra) biometrics

Switzerland **UK**	no
France	?

TBC: only passports from the **USA** have extra information (DG11–12)

Active Authentication

proof of genuity by means of public-key crypto

Switzerland **UK**	no
France	?

TBC: only passports from **Belgium** use AA

If you do hold an e-passport...

please contact us during the conference