Biometrics (CSE 40537/60537)

Lecture 10: Biometric passports

Adam Czajka

Biometrics and Machine Learning Group
Warsaw University of Technology, Poland

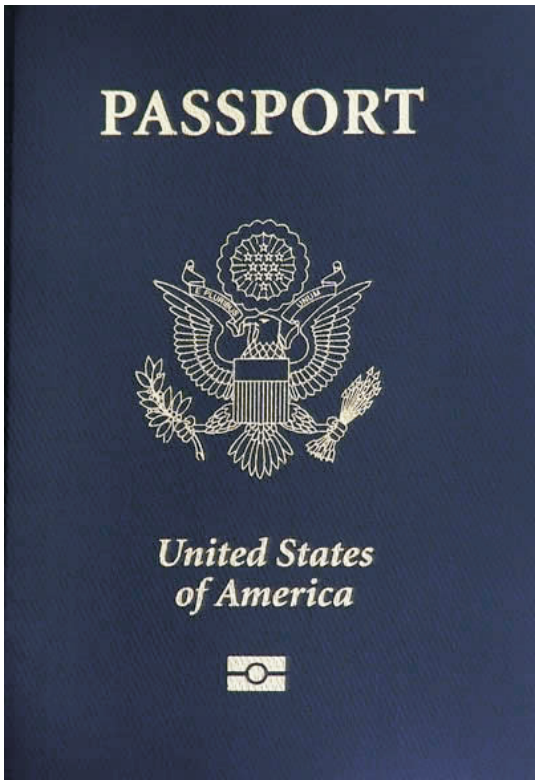
Fall 2014
University of Notre Dame, IN, USA

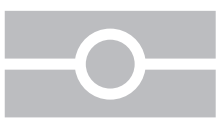
Lecture 10: Biometric passports

- What is the biometric passport?
- Biometrics in e-passports
- Cryptography basics
- Biometric passport structure
- Security of e-passports (selected issues)

Biometric passport (or e-passport)

1. Identity document (ID) possible to be read by machines (*Machine Readable Travel Document – MRTD*)
2. Document equipped with microprocessor for secure data storage and making selected cryptographic operations using these data
3. Specifically, e-passports store biometric data used for automatic identity authentication (off-card)





Deployment of biometric e-passports

Motivation

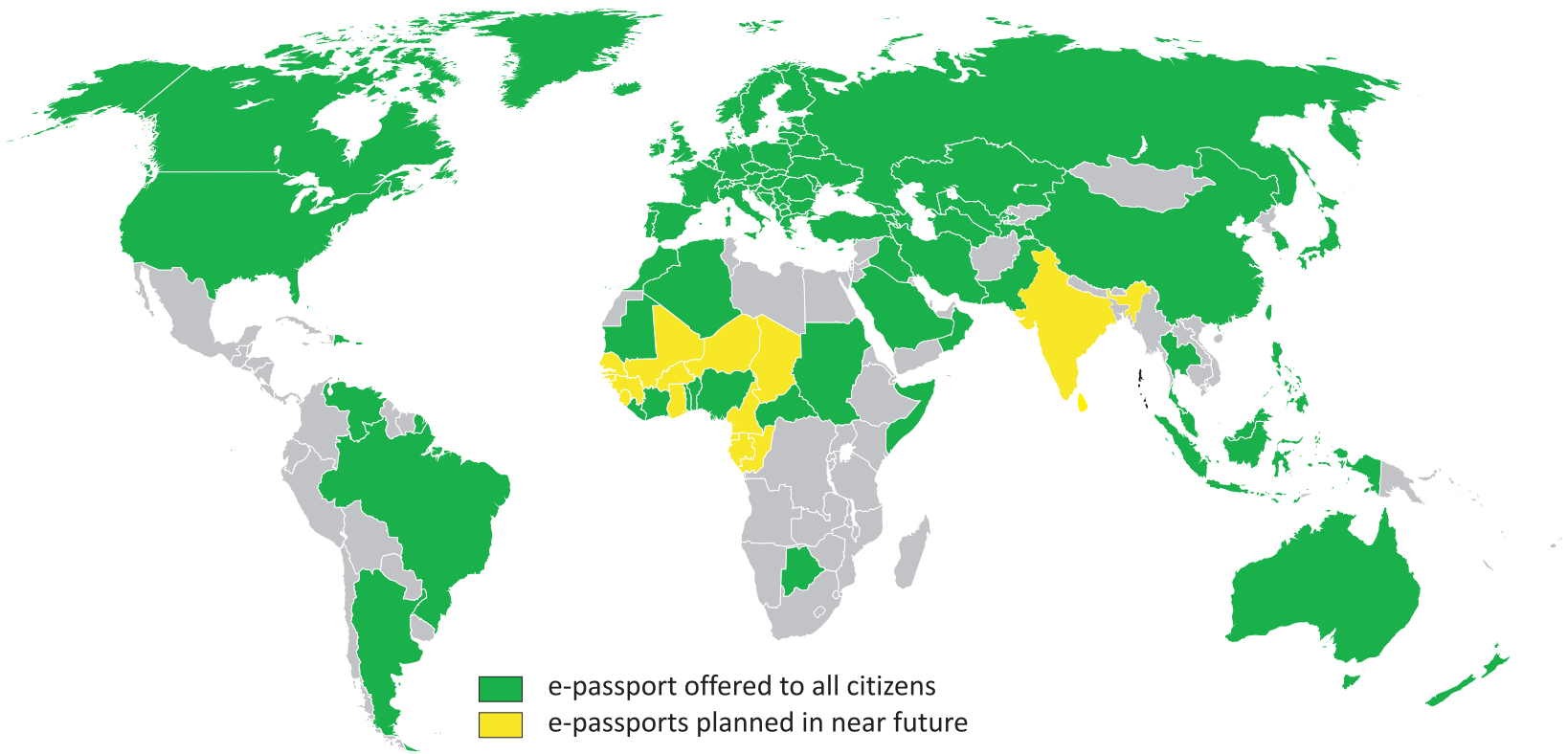
1. Security: need for a stronger link between the person and his/her ID; preventing from spoofing and document duplication
3. Convenience: automatic border control, higher throughput with the same (or better) level of security

Deployment of biometric e-passports

Milestones

1. October 2004: one of the US requirements related to participants of the *Visa Waiver Program* (`http://travel.state.gov`)
2. Recommendations of International Civil Aviation Organization: ICAO Doc 9303 recommending technical standards for implementation of biometric passports
3. December 2004 and June 2006: decisions of European Commission regulating data and security aspects of EU e-passports

Biometric e-passport in the world



Biometric e-passport in the world

First biometric e-passports

1. March 1998: Malaysia
   - not compliant with the requirements for Visa Waiver Program
   - starting from February 2010 Malaysia issues ICAO-compliant passports
2. May 2004: Dominican Republic
   - the only e-passport that does not have the e-passport logo
3. October 2004: Pakistan, USA, Belgium, Germany, Sweden, Norway

Components of the biometric e-passport system

Components of the biometric e-passport system

1. E-passport (a booklet with the microprocessor)

Components of the biometric e-passport system

1. E-passport (a booklet with the microprocessor)
2. Readers communicating with the booklet

Components of the biometric e-passport system

1. E-passport (a booklet with the microprocessor)
2. Readers communicating with the booklet
3. Graphical and electronic personalization system

Components of the biometric e-passport system

1. E-passport (a booklet with the microprocessor)
2. Readers communicating with the booklet
3. Graphical and electronic personalization system
4. Public Key Infrastructure

Components of the biometric e-passport system

1. E-passport (a booklet with the microprocessor)
2. Readers communicating with the booklet
3. Graphical and electronic personalization system
4. Public Key Infrastructure
5. Document control systems (controlling authenticity of the microprocessor and the booklet)

Components of the biometric e-passport system

1. E-passport (a booklet with the microprocessor)
2. Readers communicating with the booklet
3. Graphical and electronic personalization system
4. Public Key Infrastructure
5. Document control systems (controlling authenticity of the microprocessor and the booklet)
6. Biometric system
   - sensors with presentation attack detection and ready to be used by non habituated users
   - efficient recognition engines (must be accurate and fast)

Lecture 10: Biometric passports

- What is the biometric passport?
- Biometrics in e-passports
- Cryptography basics
- Biometric passport structure
- Security of e-passports (selected issues)

Biometrics in e-passports

1. Biometric data
   - 2D image of the face
   - images of fingerprints
   - images of irides (planned)
   - NOTE: we store biometric samples not biometric reference (interoperability)
2. Data formats
   - image intensity: color for face, gray scale for fingerprint and iris
   - compression: JPEG or JPEG2000 for face and irides, WSQ for fingerprints
3. Biometric matching realized off the card

Face images

based on publications of Polish Ministry of Interior

1. Recent photo (last month)
2. Neutral colors and correct reproduction of the skin color
3. Uniform face illumination and gray or white background
4. Eyes open, square in the camera, no "red-eye" effect
5. Neutral face expression, no face tilt, face should cover 70-80% of the image area
6. No head coverage (with exceptions), no sun glasses or other objects covering eyes
7. Size of the image file <24kB

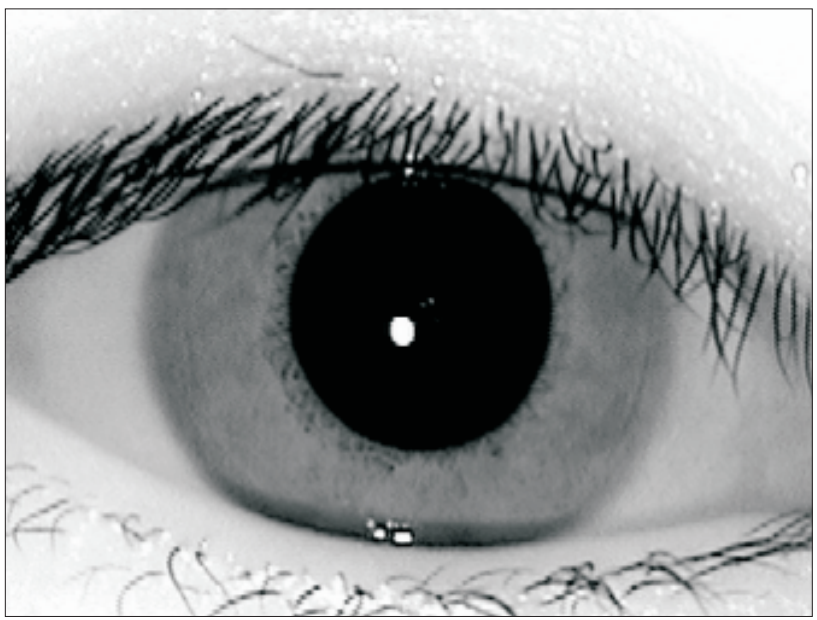
Fingerprint images

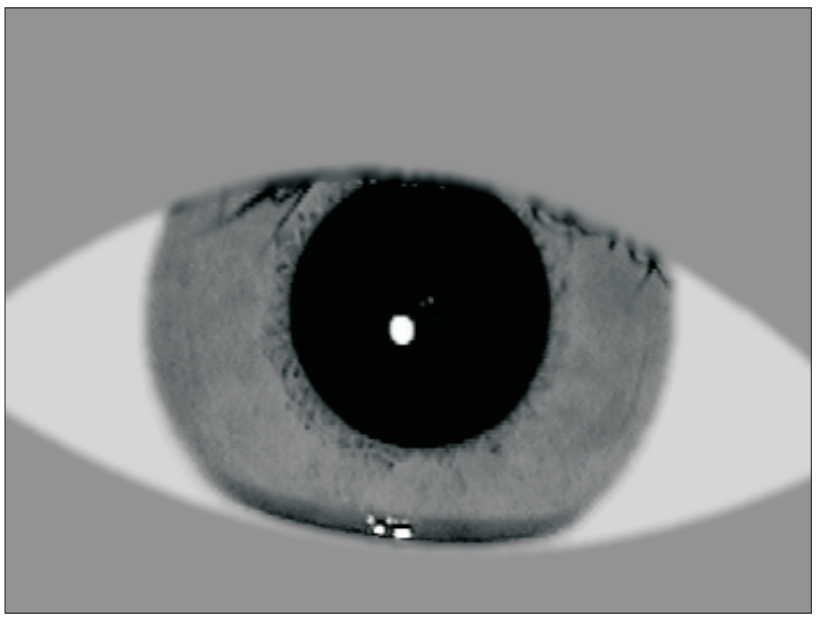
1. Impressions of the left and right index fingers
2. If FTA: impressions of thumbs and middle/ring fingers
3. Scanning resolution 500 dpi, size of the image file 12-15 kB

based on publications of Polish Security Printing Works (PWPW S.A.)

Iris images (planned)

1. Images of both eyes in Cartesian coordinate system
2. Minimum 120 pixels across the iris
3. Size of a single image file < 24 kB





Left: ISO_CROPPED. Right: ISO_CROPPED_AND_MASKED. Source: ISO/IEC 19794-6

Lecture 10: Biometric passports

Symmetric cryptography

Symmetric cryptography

1. One key (private) used for information ecryption and decryption
2. Confidentiality ensured if the key is not compromised
3. Example algorithms: AES (Rijndael), RC4/5/6, DES, 3DES, Blowfish, Twofish, Serpent

Cryptographic hash function

Cryptographic hash function

1. Transformation of any message into a fixed-length hash (typically: 128b, 160b, 192b, 224b or 256b)
2. Hashing is not injective function but it is very difficult to:
   - generate two different messages that have identical hash
   - generate a message given the hash
   - modify the message without modification of the hash
3. Hashing prevents from intentional or accidental change in original message
4. Example algorithms: MD2/4/5, SHA-1/2/3, RIPE-MD, HAVAL (MD4 variant)

Asymmetric cryptography

Foundation of Public Key Infrastructure (PKI)

Asymmetric cryptography

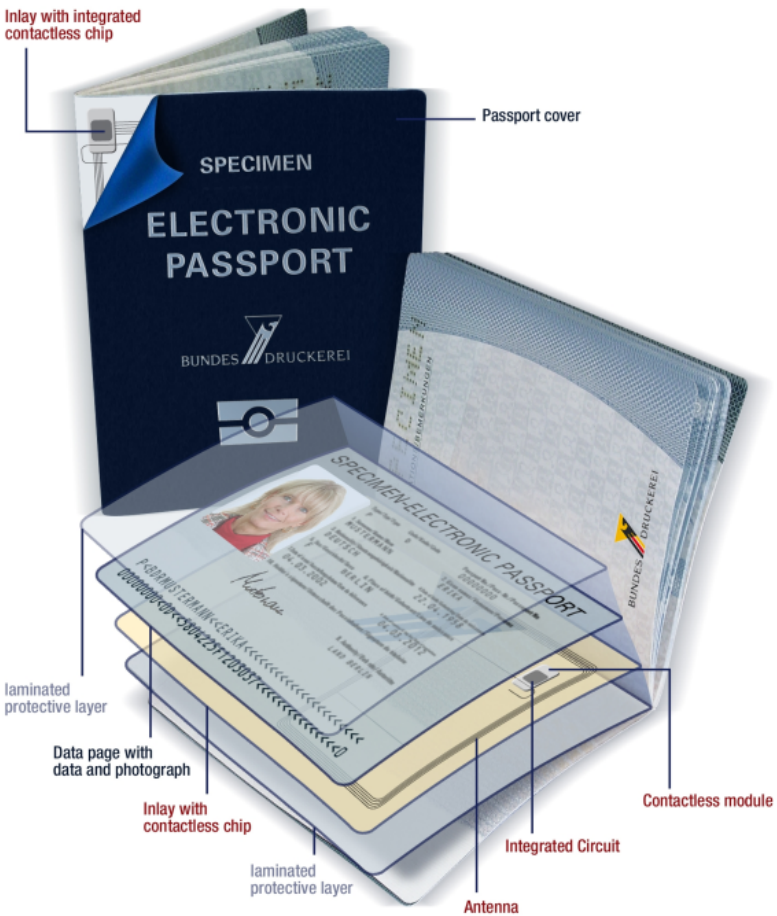
Foundation of Public Key Infrastructure (PKI)

1. Two complementary keys: private (Pr) and public (Pu)
2. If we encrypt a message using one of the keys, we can decrypt it only with the other (complementary) key
   - encryption with Pu – decryption with Pr:
     transferring some confidential information (only the person having Pr can decrypt the message)
   - encryption with Pr – decryption with Pu:
     proof that we know Pr (everyone can decrypt the message since Pu is public), digital signature
3. We need ensure the authenticity of Pu $\longrightarrow$ we need digital certificates issued by trusted third party
4. Example algorithms: RSA, DSA, EC (Elliptic Curve), ElGamal

Lecture 10: Biometric passports

- What is the biometric passport?
- Biometrics in e-passports
- Cryptography basics
- Biometric passport structure
- Security of e-passports (selected issues)

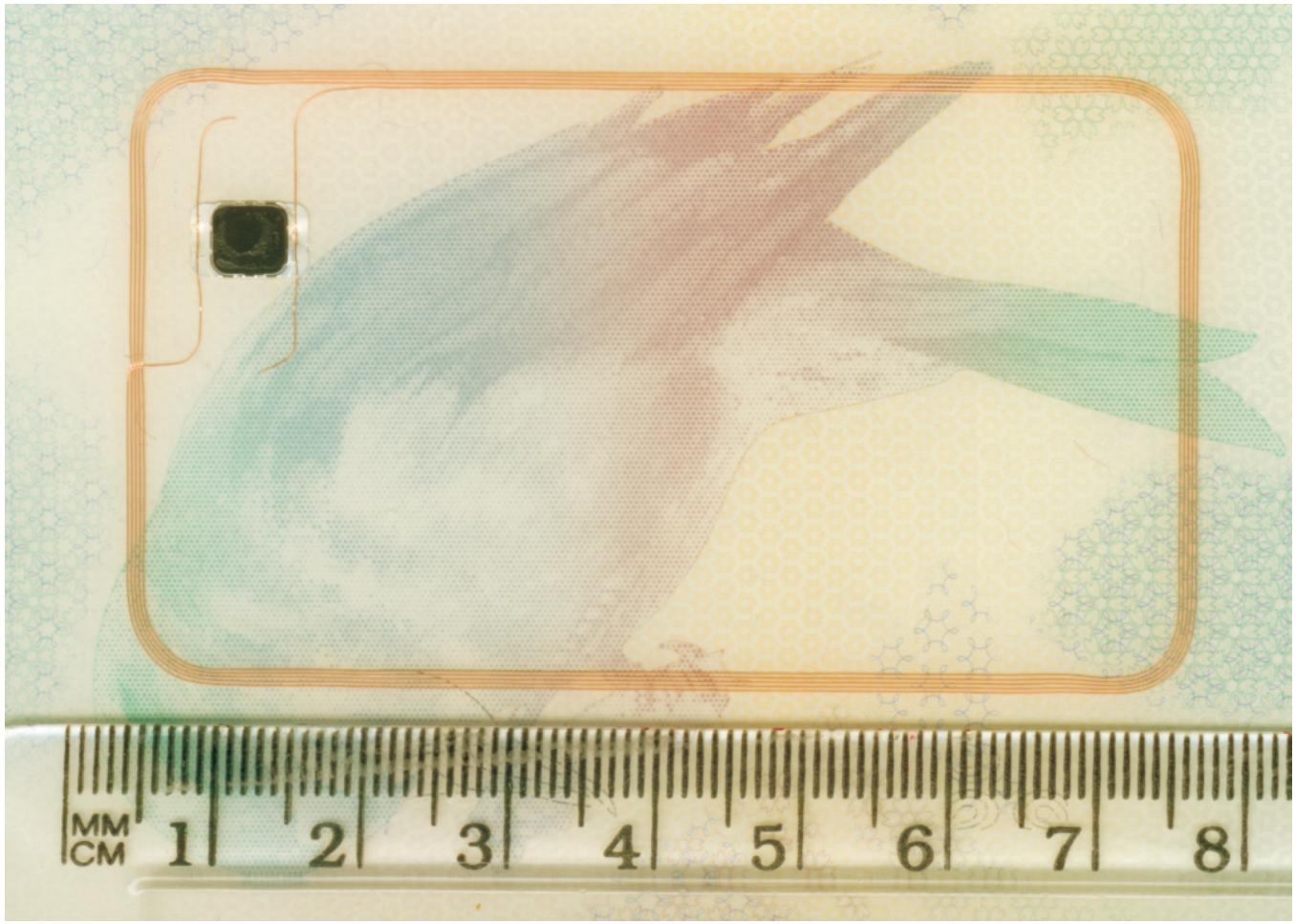
How the e-passport booklet is built?



Source: Bundesdruckerei GmbH

▶ The contactless chip can be integrated into either the cover page or the data page.

How the e-passport booklet is built?



Example based on UK e-Passport; source: en.wikipedia.org

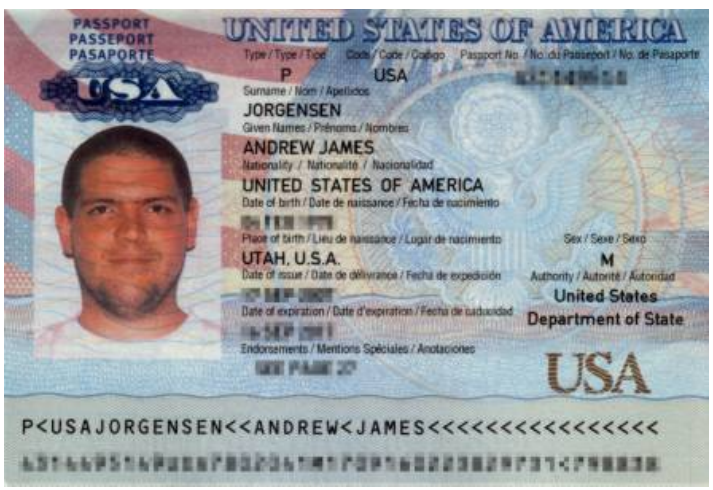
How the e-passport booklet is built?

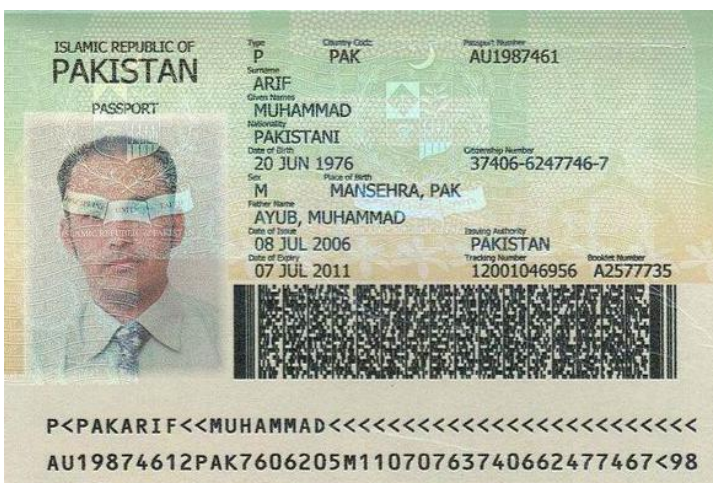
Smart card in the inlay

1. A microcomputer (8 bit architecture) with memory (EEPROM, RAM, ROM) and cryptographic co-processor
2. Minimum 32kB of EEPROM (passport's "hard drive")
3. Card Operating System (COS) controls the card hardware and ensures the security
4. Interface
   - physical: contactless, compliant with ISO/IEC 14443, power supply based on electromagnetic induction
   - logical: compliant with ISO/IEC 7816-4, based on APDU (Application Protocol Data Units) – a set of specialized COS system commands
5. Additional frameworks (above COS) facilitate programming and introduce new functionality (JavaCard OS, Multos)

How the e-passport booklet is built?

Machine Readable Zone – MRZ





How the e-passport booklet is built?

Machine Readable Zone – MRZ

```
P<PHLPEREZ<<ELEA<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<
DP12345674PHL7810222F1206038<<<<<<<<<<<<<<<<<<<<8
```

- type of the document (e.g., 'P' – passport)
- country of issue
- first and last name
- passport number and expiry date
- citizenship, DOB, gender
- control digits (for integrity check)

Logical structure

1. Data Group (DG)
   - logical container for data of certain type
   - currently 19 DGs: DG1 – MRZ data, DG2 – face image, DG3 – fingerprint images, DG4 – iris images, etc.
2. Logical Data Structure (LDS)
   - logical organization of DGs
   - smart card file system as defined in ISO/IEC 7816-4 is used
3. Document Security Object (SOD)
   - digital signature of all Data Groups (technically: the signature of concatenated hashes of all DGs)
   - digital certificate of the signer ("signer" is the institution issuing the biometric passports of behalf of the country)

Lecture 10: Biometric passports

Potential problems

Interoperability vs. security

Potential problems

Interoperability vs. security

1. Invisible scanning, skimming and tracking

Potential problems

Interoperability vs. security

1. Invisible scanning, skimming and tracking
2. Cloning if digital signature is not linked with a booklet

Potential problems

Interoperability vs. security

1. Invisible scanning, skimming and tracking
2. Cloning if digital signature is not linked with a booklet
3. Eavesdropping if transmission channels are not secured

Potential problems

Interoperability vs. security

1. Invisible scanning, skimming and tracking
2. Cloning if digital signature is not linked with a booklet
3. Eavesdropping if transmission channels are not secured
4. Data leakage in particular biometric data after reading from the passport (to make an off-card matching)

Potential problems

Interoperability vs. security

1. Invisible scanning, skimming and tracking
2. Cloning if digital signature is not linked with a booklet
3. Eavesdropping if transmission channels are not secured
4. Data leakage in particular biometric data after reading from the passport (to make an off-card matching)
5. Data aging: biometric passport is valid 10 years (!)

Countermeasures

Radio frequency blocking covers

Countermeasures

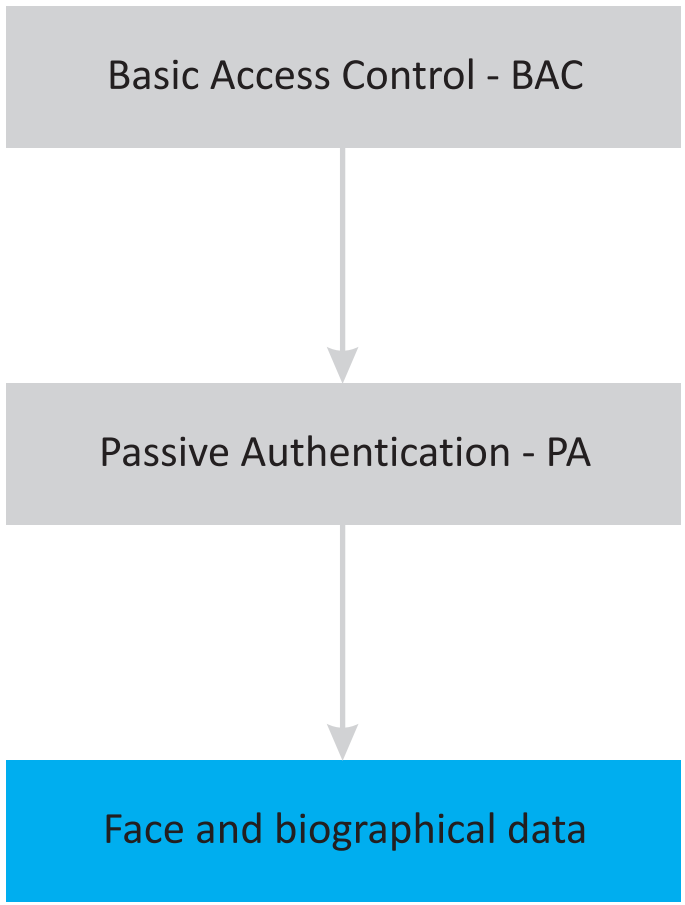
Radio frequency blocking covers

Countermeasures

Protocols

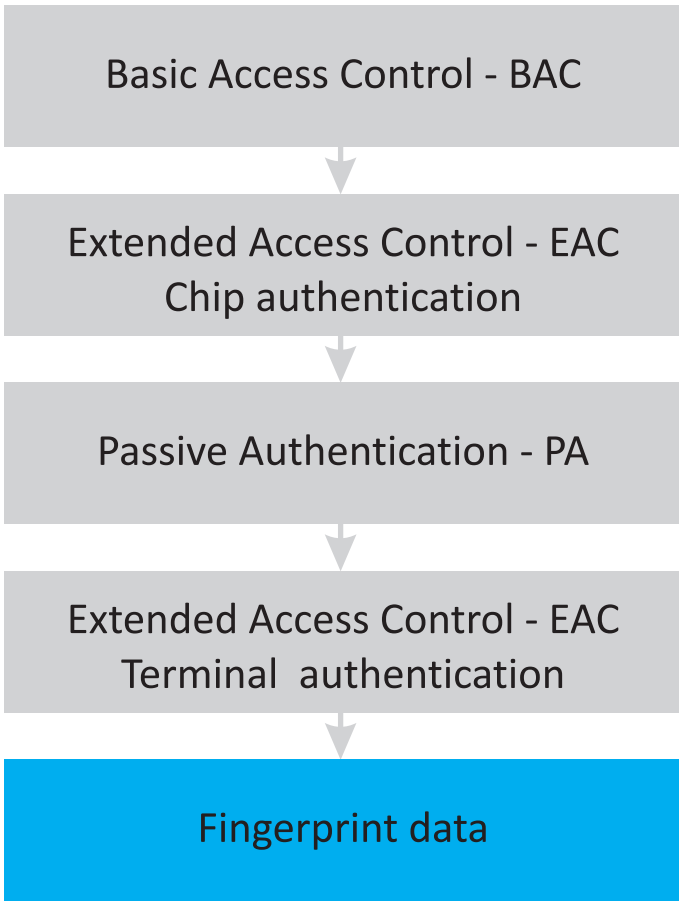
1. Access to face and biographical data
   - Basic Access Control (BAC)
   - Passive Authentication
2. Access to fingerprint data
   - Extended Access Control (EAC)
   - Active Authentication (optional)

Access to face and biographical data



based on publications
of Polish Security Printing Works (PWPW S.A.)

Access to fingerprint data



based on publications
of Polish Security Printing Works (PWPW S.A.)

Access to face and biographical data

Basic Access Control – BAC

1. Prevents from data access if there is no mutual authentication of the terminal and the passport
2. Microprocessor has a symmetric key but the terminal has not
3. How the terminal can get the proper key?

Access to face and biographical data

Basic Access Control – BAC

1. Prevents from data access if there is no mutual authentication of the terminal and the passport
2. Microprocessor has a symmetric key but the terminal has not
3. How the terminal can get the proper key?
   Answer: read the MRZ
   - passport number, DOB, expiry date, control digits
   - NOTE: small entropy of keys (approximately 56 bits) due to some predictability of passport serial numbers and expiry dates

Access to face and biographical data

Basic Access Control – BAC

4. Application of challenge-response protocol: generation of session keys based on *cryptographic seed* and secure transmission channel
5. BAC proofs that the document was opened for the inspection
6. BAC does not protects against cloning and replacement of the microprocessor

Access to face and biographical data

Passive Authentication – PA

1. Verification of a digital signature in SOD
2. Requires verification of the certificate of issuing country
3. PA proofs that LDS and SOD are authentic and non altered, i.e. the microprocessor was not replaced with a fake one
4. PA does not protect against:
   - microprocessor cloning
   - non authorized data access
   - eavesdropping and skimming