ICAO 9th Symposium and Exhibition on MRTDs, Biometrics and Border Security, 22-24 October 2013

Implementation of biometrics, issues to be solved

Eugenijus Liubenka, Chairman
of the Frontiers / False Documents Working Party
of the Council of the European Union,
SBGS of the Republic of Lithuania

Content

Physical security features of travel documents and purpose of Biometrics

Common physical security features of MRTDs

- Recommendation for travel documents physical security features are laid down in the ICAO doc. 9303 (Machine Readable Travel Documents)
- Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States

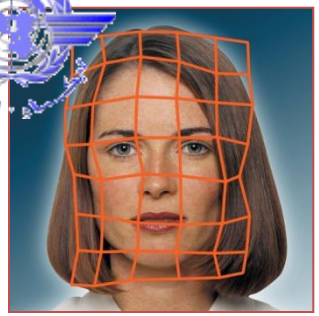
EUROPEAN UNION BIOMETRIC ACTIVITIES

- ICAO recommendations and specifications form the basis for Europe
- EU adopted Regulation 2252/2004 of 13 December 2004,

  which formed the basis for the upcoming European “intelligent passport”
- First biometric feature: **Digital frontal portrait**

  deadline for introduction - August 2006
- Second biometric feature: **Two flat digital fingerprints**

  deadline for introduction - June 2009
- Combination of the two will lead to enhanced biometric security
- Both features are stored on a contactless radio frequency (RF) chip. They are stored as images in JPEG format.



Introduction of e-documents

- Reasons to introduce electronics in passports (and other travel E-documents)
  - to increase document security (more difficult to forge)
    - cryptography
  - to establish the link between the document and holder
    - Biometrics (electronic –hardware & digital data)

Protection of biometrical data

What's in the chip?

- Basically the information is the same as printed in a travel document's data page
  - In the EU countries it is not allowed to store additional information not printed in the booklet (except fingerprints)
- Information stored in the form of files
  - Data groups containing data (DG1 - DG16)

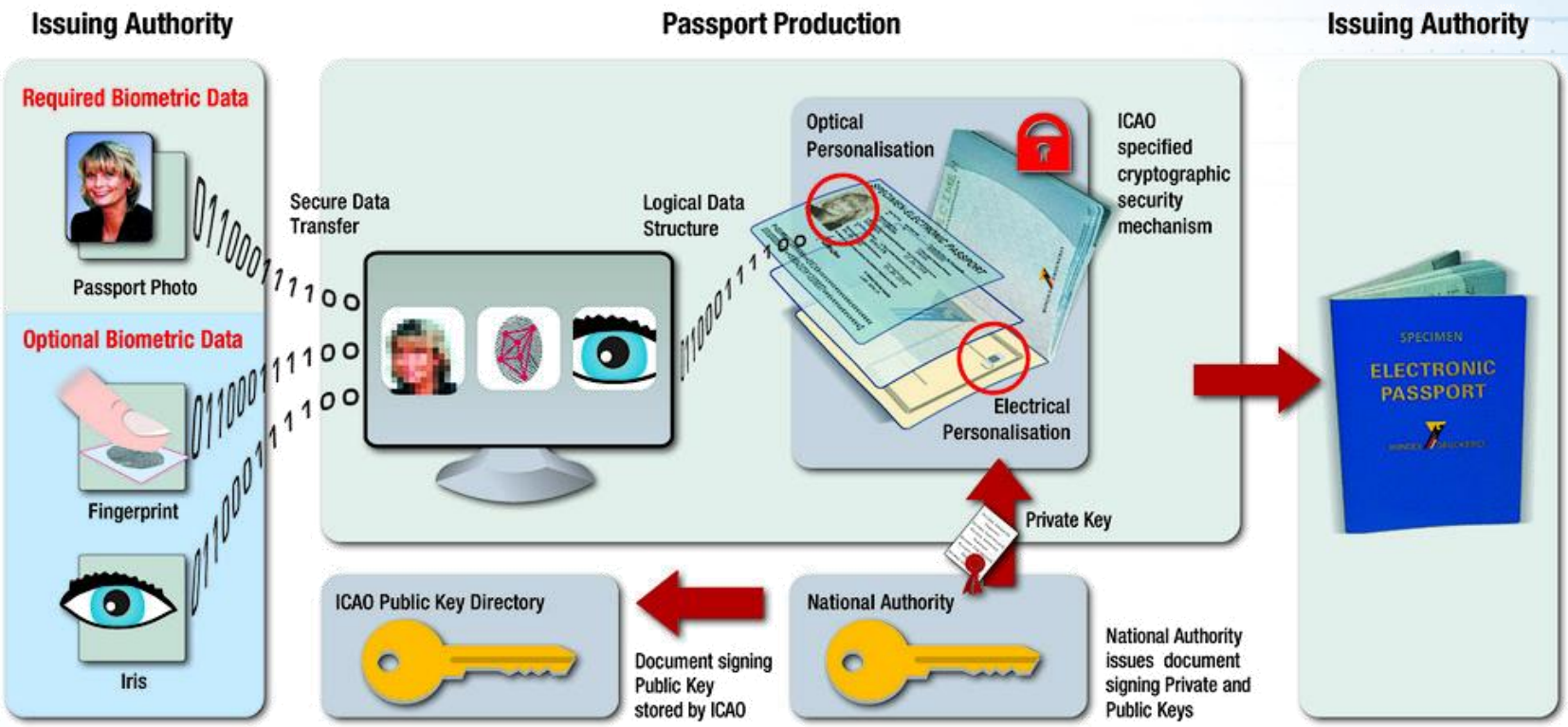
Data groups

Data group	Stored data
DG1	Machine readable zone (MRZ) – mandatory
DG2	Biometric data: face - mandatory
DG3	Biometric data: fingerprints
DG4	Biometric data: iris
DG5	Picture of the holder as printed in the passport
DG6	Reserved for future use
DG7	Signature of the holder as printed in the passport
DG8	Encoded security features – data features
DG9	Encoded security features – structure features
DG10	Encoded security features – substance features
DG11	Additional personal details (address, phone)
DG12	Additional document details (issue date, issued by)
DG13	Optional data (anything)
DG14	Data for securing secondary biometrics (EAC)
DG15	Active Authentication public key info
DG16	Next of kin

Data groups

- DG1 (MRZ) and DG2 (facial photo) are mandatory
- DG3 (Fingerprints) is mandatory in the EU countries
- Other data groups are optional

GENERAL WORKFLOW
for centralized passport production



- Digital data capture
- Secure data transfer
- Passport production

- Optical personalisation
- Electronic personalisation
- Digital signature

ELECTRONIC PERSONALIZATION: ICAO LDS SPECIFICATION

EU2013.LT

Authentication Method	Mandatory	Cryptographic Mechanism	Remarks
Passive authentication (PA)	YES	Digital Signature	Proof that LDS and Document certificate are authentic and not modified Does not prevent 1:1 copy or chip exchange
Basic Access Control (BAC)	No **EU: YES (required)**	Challenge/ Response Mechanism based on DES3 recommendation: Secure Messaging based on session key	Prevents skimming and eavesdropping, if there is a secure communication. Low security level. No prevention of 1:1 copy or chip exchange Higher complexity and requirements to the chip
Supplemental Access Control (SAC)	No **EU: YES (required) from December 2014**	Password Authenticated Connection Establishment (PACE v2) based on asymmetric key pair	Advanced prevention of skimming and eavesdropping due the stronger key cryptography No prevention of 1:1 copy or chip exchange
Extended Access Control (EAC)	No (Optional)	additional symmetric Key or asymmetric key pair	Prevents unauthorized access to sensitive data Prevents skimming Additional Key Management
Active authentication (AA)	No (Optional)	Challenge/ Response Mechanism based on Public Key Cryptography Digital Signature	Proof, that document certificate is no copy and refers to the right IC Chip has not been changed Higher complexity and requirements to the chip
Data encryption	No (Optional)	symmetric or asymmetric encryption method	Protection of sensitive data (e.g. fingerprint) No prevention of 1:1 copy or chip exchange

Privacy protection – Basic Access Control (BAC) and Supplemental Access Control (SAC)

- Role of BAC is to protect privacy of a passport holder
  - Data cannot be read from a remote distance without knowing the data of the MRZ;
- SAC – new, advanced privacy protection security mechanism based on Password Authenticated Connection Establishment (PACE)

Data integrity

- All data groups are digitally signed by the issuing country (they are encrypted)
- A digital signature is applied to reveal any tampering of the original data (hash functions – SHA)

- This is a significant security feature which increases document security
- This feature is called PASSIVE authentication (PA)

Passive authentication (PA)

- PA is able to recognize:
  - Data change (e.g. photo modification)
  - Digital signature not created by the proper authority
- PA requires a specific digital certificate of the issuing country – this is called the Country Signing Certification Authority (CSCA).
  - If the CSCA certificate of the issuing country is not available the digital signature cannot be verified and passport cannot be validated

Active Authentication (AA)

- Optional security feature to prevent RFID cloning.
- It is based on cryptographic challenge-response algorithm that can verify if the RFID contains in its secure memory a secret key stored during the personalization by the issuing country.
- The result of the AA is simple: PASS / FAIL. Fail suggests a forgery.

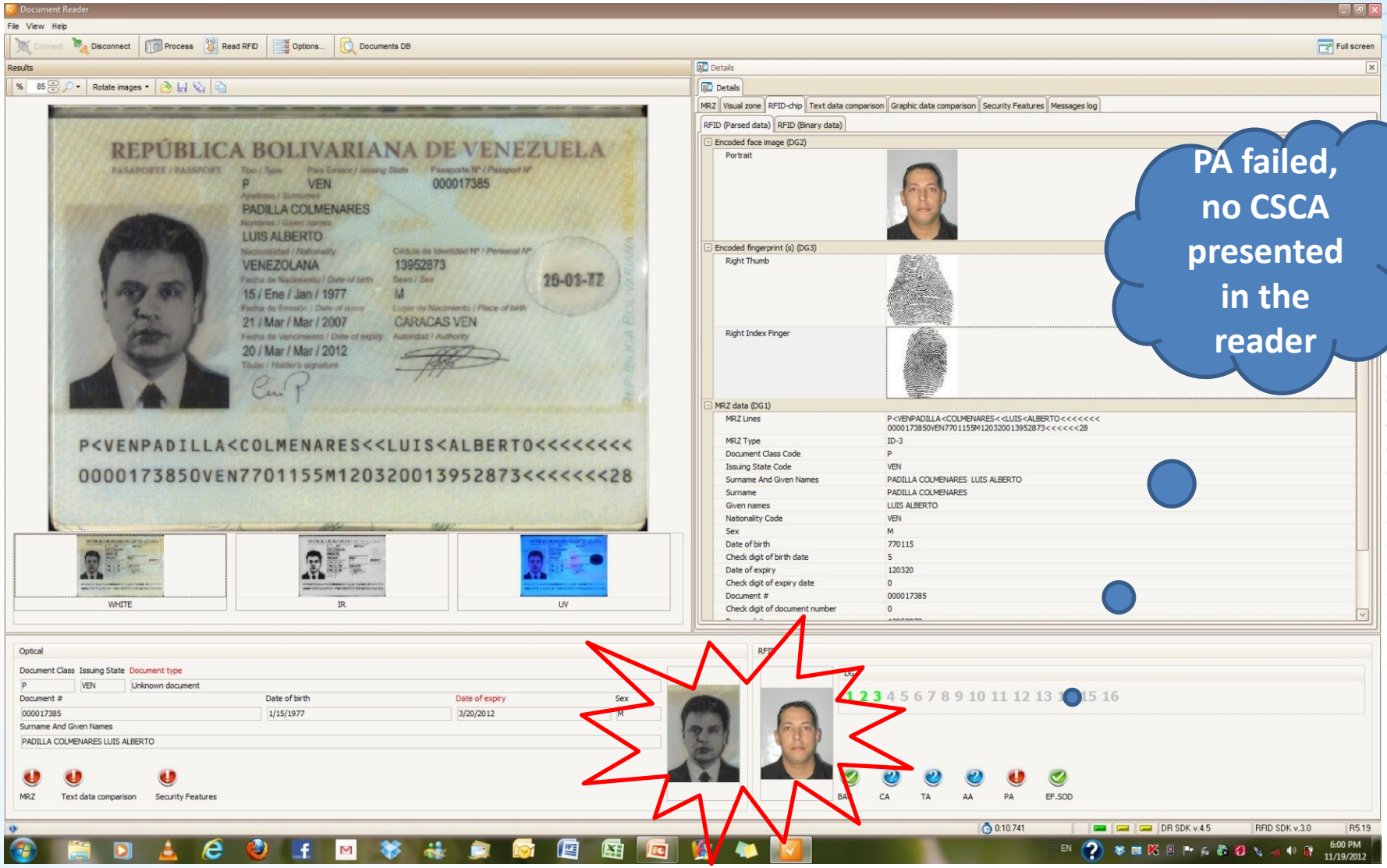
Privacy protection - EAC

- Fingerprints (stored in DG3) in the 2nd generation European passports are protected with additional mechanism called Extended Access Control (EAC).
- EAC requires additional secret key and certificate provided by the issuing country of the passport
- EAC protected data can be only read by authorized border authorities
- Only fingerprints (DG3) are EAC protected, all remaining data (DG1-2,5-16) is BAC-protected

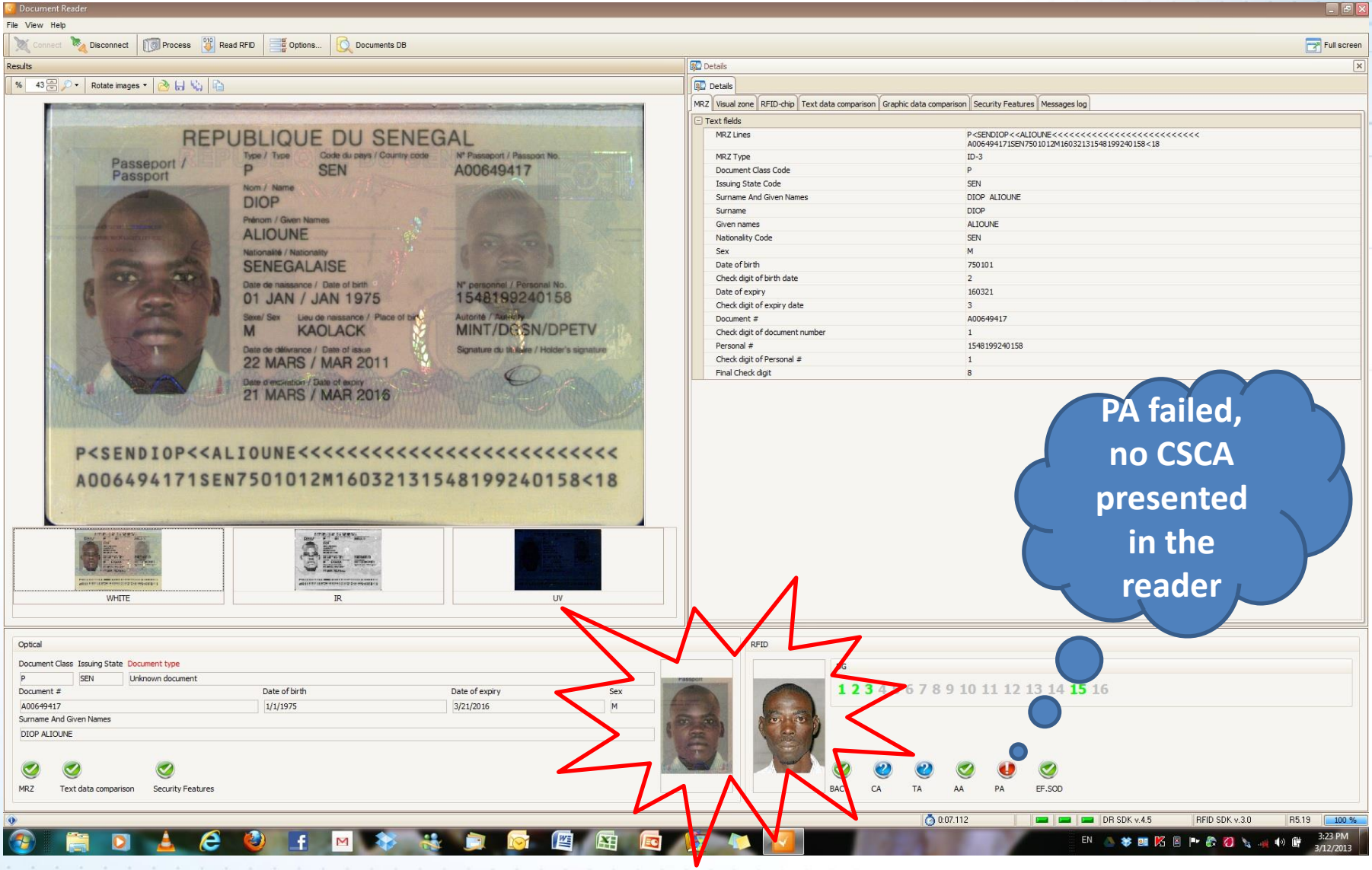
Control infrastructure examples

Helps or not??

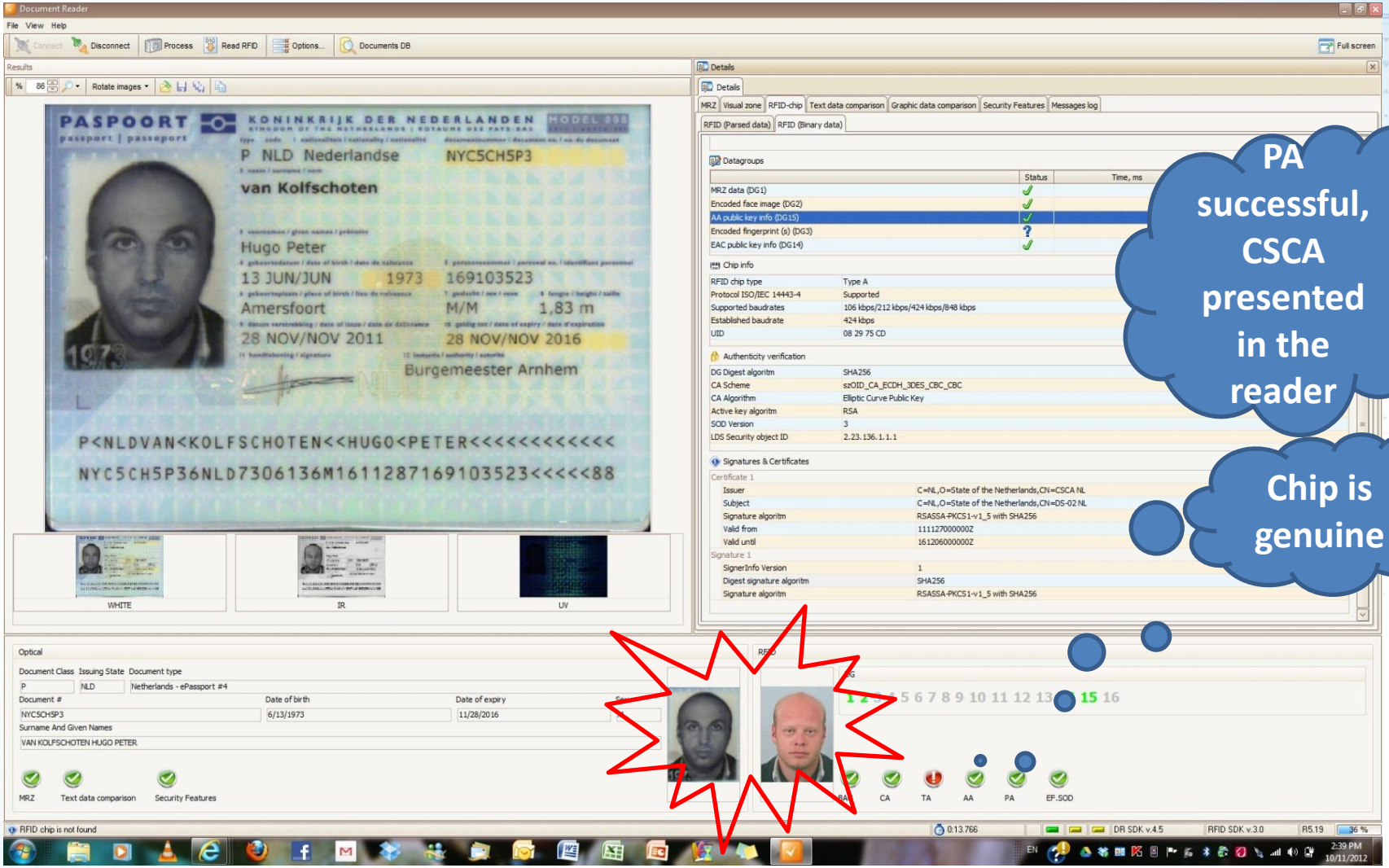
Checking of RFID helps if it is done in a right way



Checking of RFID helps if it is done in a right way



Checking of RFID helps if it is done in a right way



Does your ABS's or document readers check e-documents authenticity and compare digital signatures?

Opening RFID without checking digital signatures is needless and very expensive toy

Issued to be solved (conclusions)

Further improvements

- No strong need for improvement of physical security features of travel documents anymore (if minimum security level has been achieved);
- Biometrics increase security of a document ONLY if it is checked in a right way;
- Biometrics establish a strong link between a document and its holder ONLY if all electronical security features (signatures) are checked;

Further improvements (2)

- Exchange of CSCA (DSCA) certificates is ESSENTIAL :
  - ICAO Public Key Directory (PKD)
  - Bilateral agreements
- Verification of certificates **by the control authorities** is ESSENTIAL:
  - Passive authentication (PA)
  - Active authentication (AA)

Thank you for your attention

Eugenijus Liubenka, Chairman
of the Frontiers / False Documents Working Party
of the Council of the European Union,
State Border Guard Service
of the Republic of Lithuania
eugenijus.liubenka@vrm.lt