ICAO

TRIP 2022

SEAMLESS AND CONTACTLESS

Sharing data to accelerate the recovery

13 - 15 SEPTEMBER 2022

e-Passport Validation and Fraud Detection

R Rajeshkumar

Chair – ISO SC17/WG3/TF5

Editor – Doc 9303-12, DTC, VDS-NC

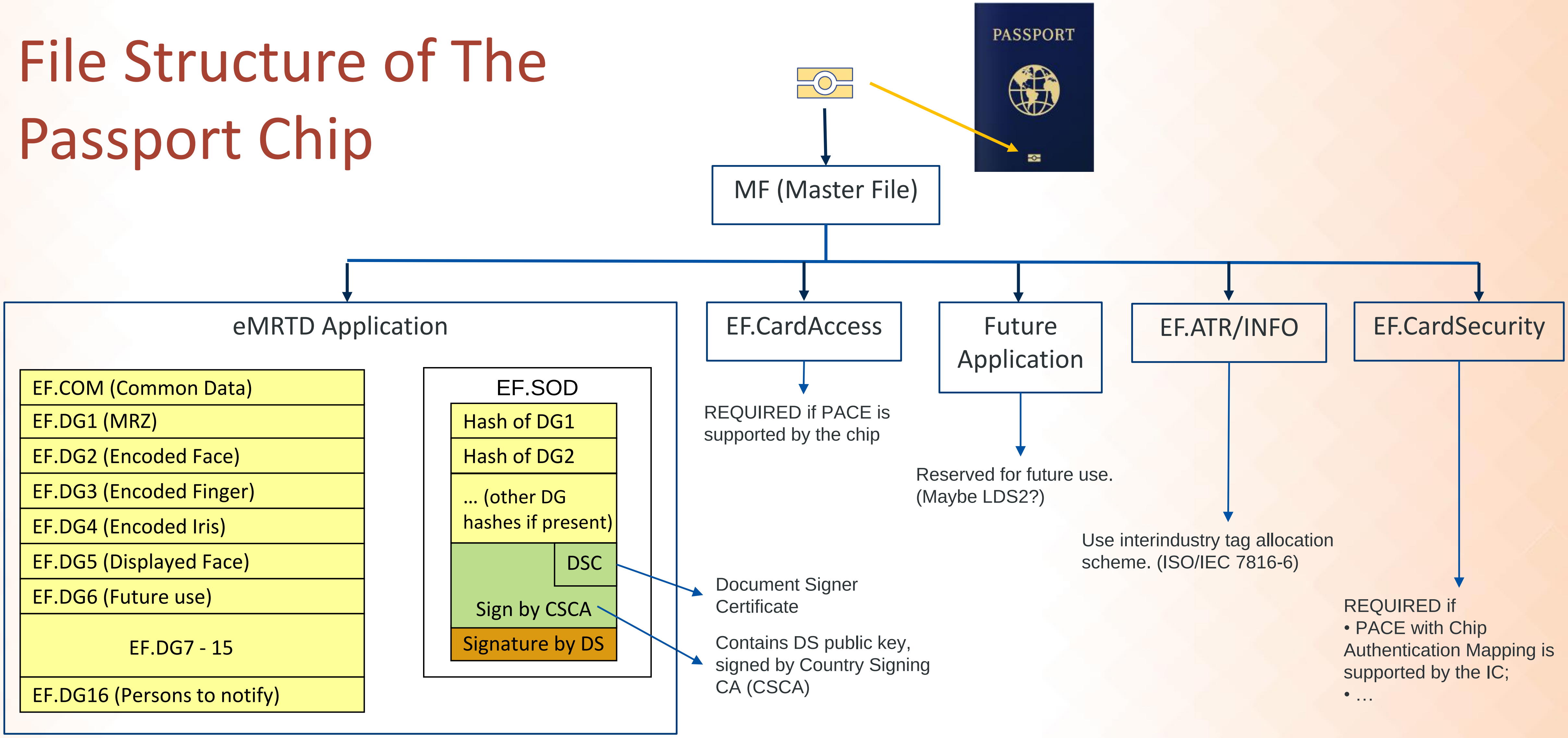
Chief Executive – Auctorizium Pte Ltd, Singapore

R.Rajeshkumar@auctorizium.com

SC17 WG3/TF5

1. ePassport Validation

File Structure of The Passport Chip



MF (Master File)

eMRTD Application

- EF.COM (Common Data)
- EF.DG1 (MRZ)
- EF.DG2 (Encoded Face)
- EF.DG3 (Encoded Finger)
- EF.DG4 (Encoded Iris)
- EF.DG5 (Displayed Face)
- EF.DG6 (Future use)
- EF.DG7 - 15
- EF.DG16 (Persons to notify)

EF.SOD

- Hash of DG1
- Hash of DG2
- … (other DG hashes if present)
- DSC
- Sign by CSCA
- Signature by DS

Document Signer Certificate

Contains DS public key, signed by Country Signing CA (CSCA)

EF.CardAccess

REQUIRED if PACE is supported by the chip

Future Application

Reserved for future use. (Maybe LDS2?)

EF.ATR/INFO

Use interindustry tag allocation scheme. (ISO/IEC 7816-6)

EF.CardSecurity

REQUIRED if
- PACE with Chip Authentication Mapping is supported by the IC;
- …

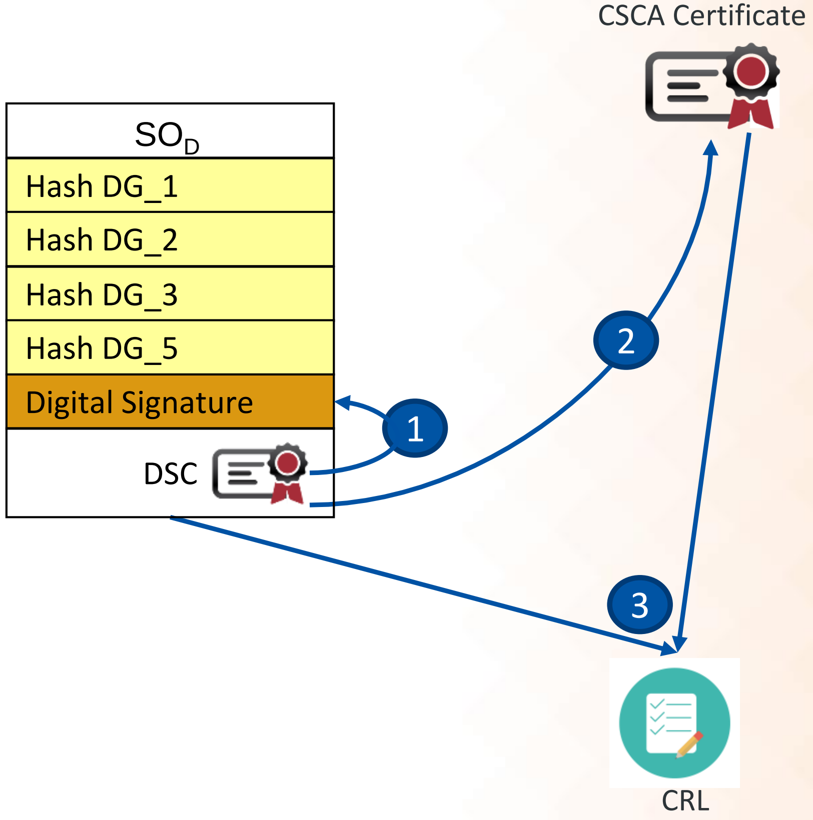
SC17 WG3/TF5

Understanding E-Passport validation

- Trust is established by proper verification of the e-Passport
  - SOD is valid
  - LDS is valid
  - eMRTD is valid
  - Traveller is valid

SOD is Valid

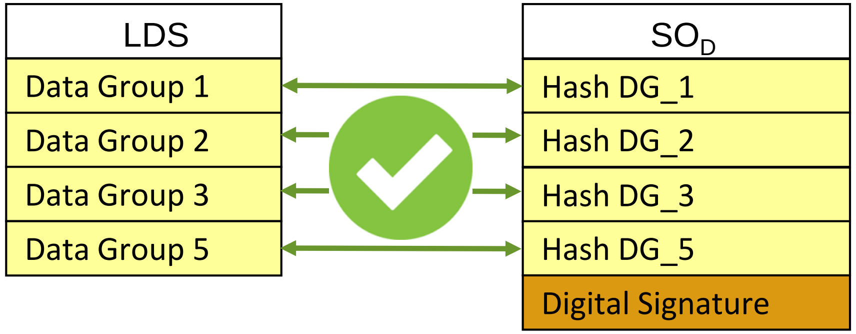
1. Verify SOD against DSC
2. Verify DSC against CSCA
3. Verify DSC & CSCA not in CRL



SO_D
Hash DG_1
Hash DG_2
Hash DG_3
Hash DG_5
Digital Signature
DSC

LDS is Valid

- Check that DG hash values matches the hash values stored in SOD



LDS

Data Group 1

Data Group 2

Data Group 3

Data Group 5

SO_D

Hash DG_1

Hash DG_2

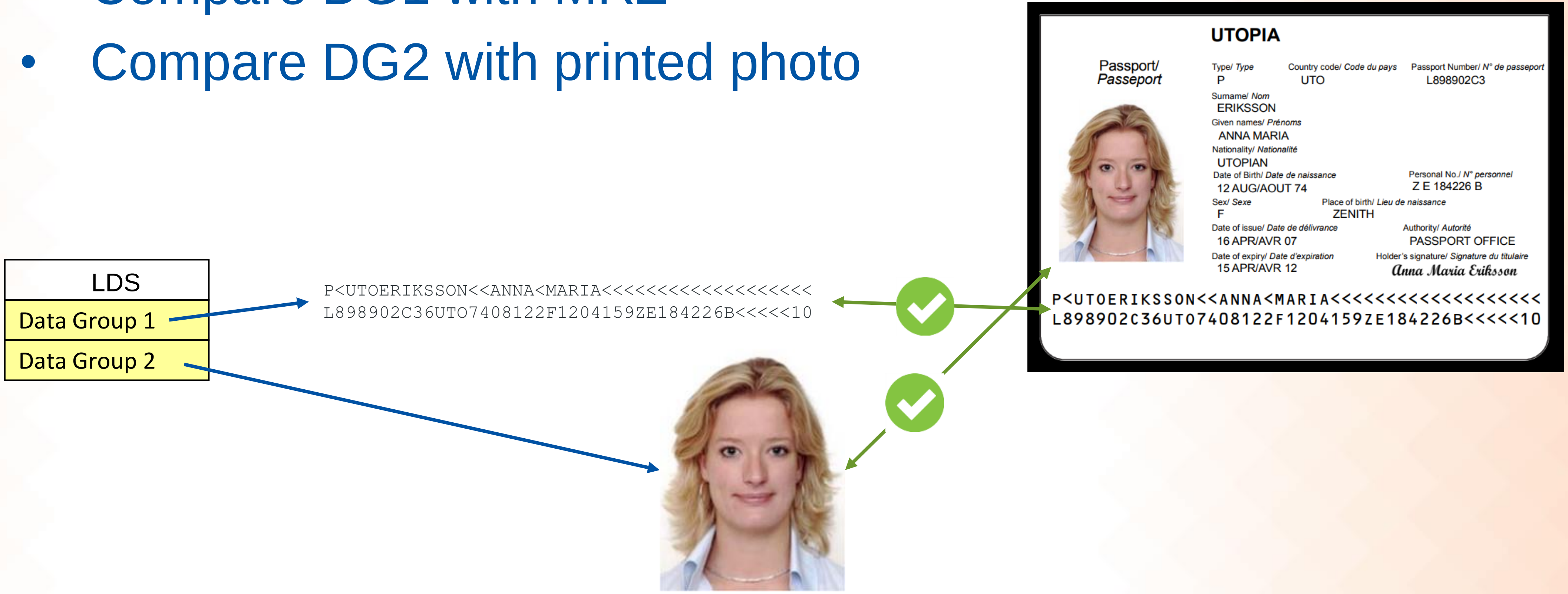
Hash DG_3

Hash DG_5

Digital Signature

eMRTD is Valid

- Compare DG1 with MRZ
- Compare DG2 with printed photo



LDS

Data Group 1

Data Group 2

P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C36UTO7408122F1204159ZE184226B<<<<<10

UTOPIA

Passport/ *Passport*

Type/ *Type* P

Country code/ *Code du pays* UTO

Passport Number/ *N° de passeport* L898902C3

Surname/ *Nom* ERIKSSON

Given names/ *Prénoms* ANNA MARIA

Nationality/ *Nationalité* UTOPIAN

Date of Birth/ *Date de naissance* 12 AUG/AOUT 74

Personal No./ *N° personnel* Z E 184226 B

Sex/ *Sexe* F

Place of birth/ *Lieu de naissance* ZENITH

Date of issue/ *Date de délivrance* 16 APR/AVR 07

Authority/ *Autorité* PASSPORT OFFICE

Date of expiry/ *Date d'expiration* 15 APR/AVR 12

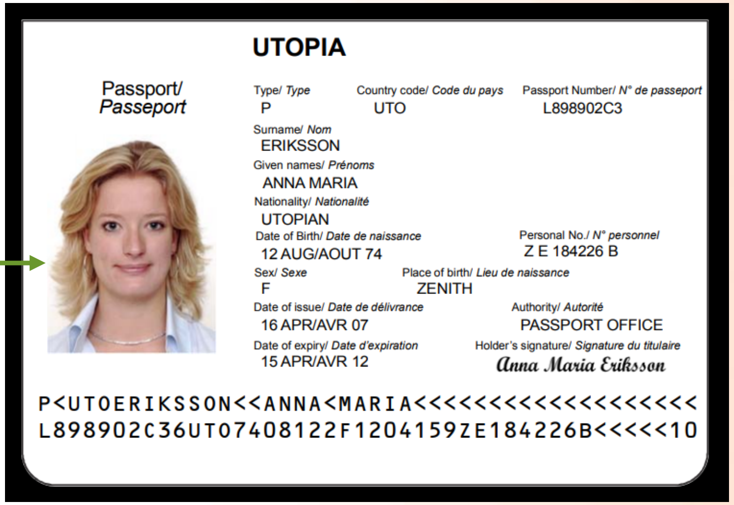
Holder's signature/ *Signature du titulaire* Anna Maria Eriksson

P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C36UTO7408122F1204159ZE184226B<<<<<10

Traveller is Valid

- Compare photo to holder of passport

Passport holder at the border



UTOPIA

Passport/ *Passport*

Type/ *Type*
P

Country code/ *Code du pays*
UTO

Passport Number/ *N° de passeport*
L898902C3

Surname/ *Nom*
ERIKSSON

Given names/ *Prénoms*
ANNA MARIA

Nationality/ *Nationalité*
UTOPIAN

Date of Birth/ *Date de naissance*
12 AUG/AOUT 74

Personal No./ *N° personnel*
Z E 184226 B

Sex/ *Sexe*
F

Place of birth/ *Lieu de naissance*
ZENITH

Date of issue/ *Date de délivrance*
16 APR/AVR 07

Authority/ *Autorité*
PASSPORT OFFICE

Date of expiry/ *Date d'expiration*
15 APR/AVR 12

Holder's signature/ *Signature du titulaire*
Anna Maria Eriksson

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C36UTO7408122F1204159ZE184226B<<<<<10
```

Understanding E-Passport validation

- Trust is established by proper verification of the e-Passport

  - Verify SOD against DSC
  - Verify DSC against CSCA
  - Verify DSC not in CRL

SOD is valid

  - Check that DG hash values matches the hash values stored in SOD

LDS is valid

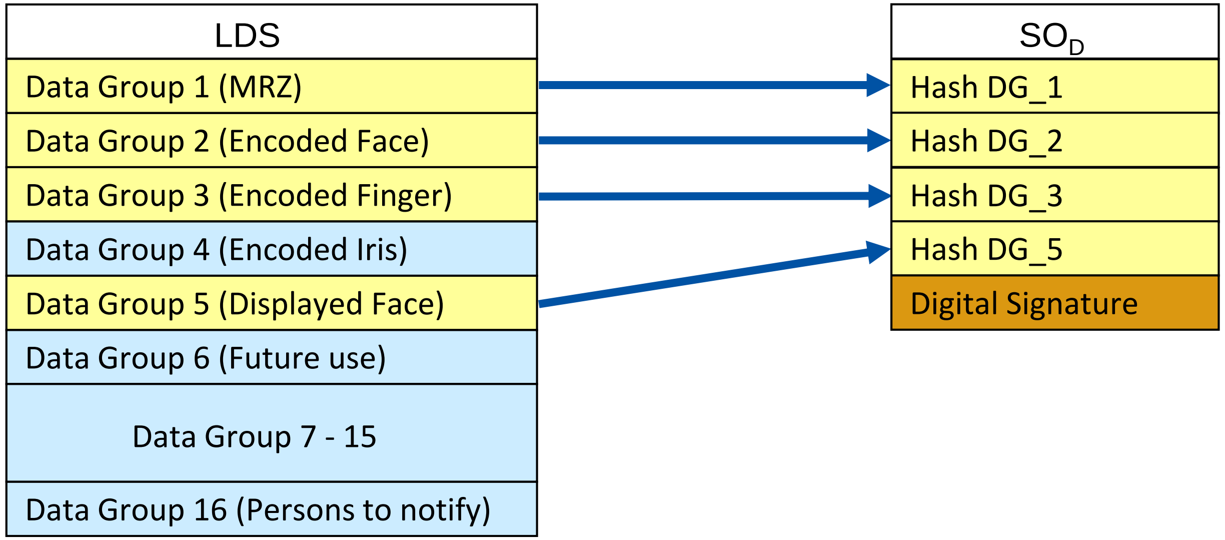
  - Compare DG1 with MRZ
  - Compare DG2 with printed photo

eMRTD is valid

  - Compare photo to holder of passport

Traveller is valid

Passive Authentication

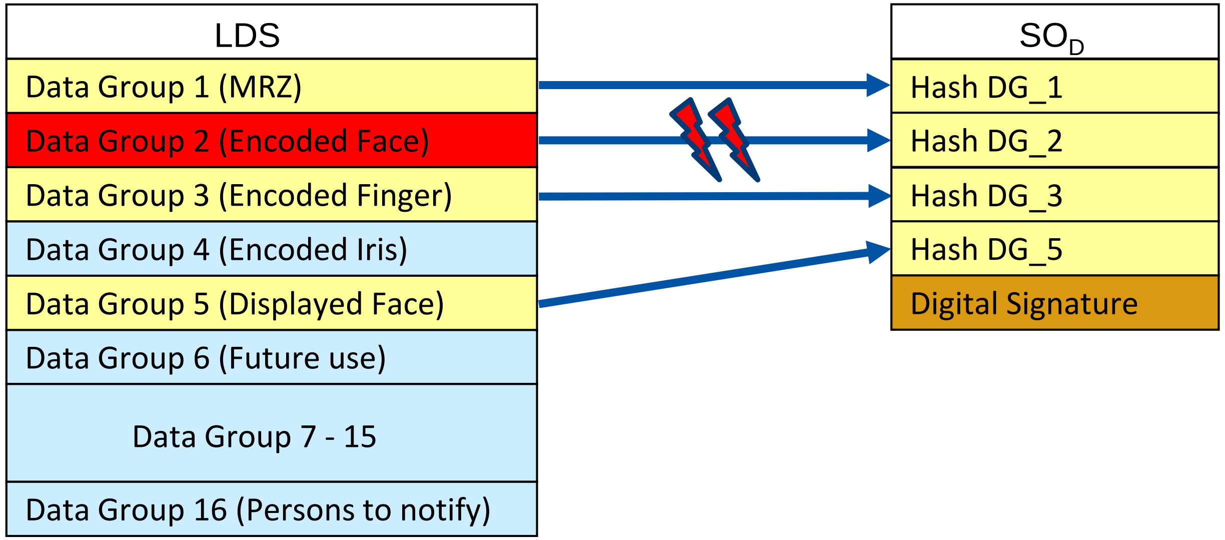


LDS
Data Group 1 (MRZ)
Data Group 2 (Encoded Face)
Data Group 3 (Encoded Finger)
Data Group 4 (Encoded Iris)
Data Group 5 (Displayed Face)
Data Group 6 (Future use)
Data Group 7 - 15
Data Group 16 (Persons to notify)

SO_D
Hash DG_1
Hash DG_2
Hash DG_3
Hash DG_5
Digital Signature

- Hash of each data group is stored in SOD
- Hash of the hashes is then signed and also stored in the SOD

Passive Authentication

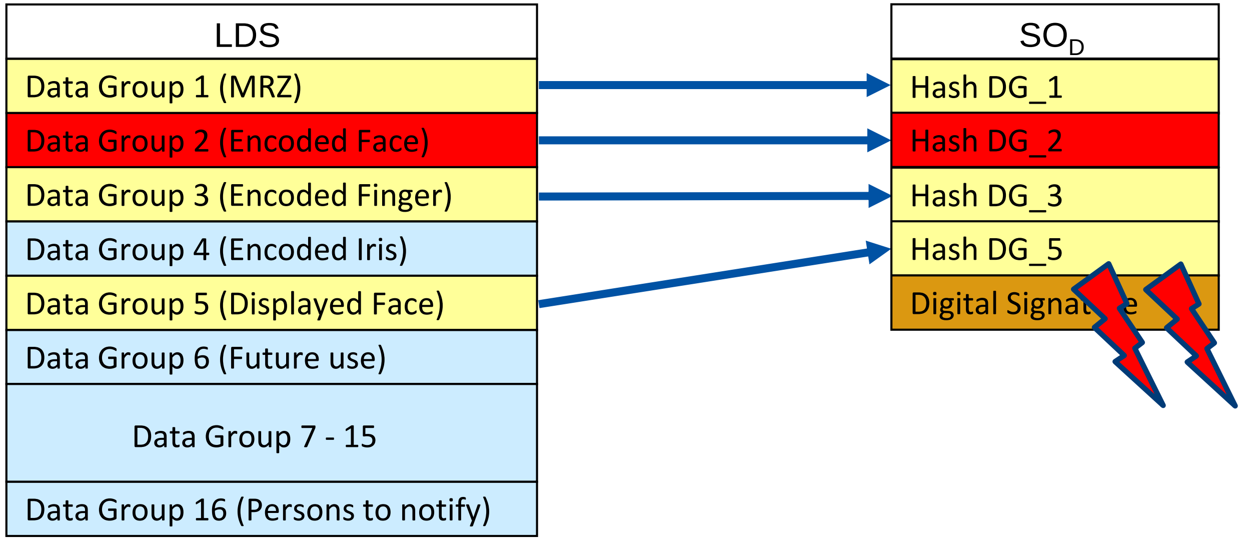


LDS
Data Group 1 (MRZ)
Data Group 2 (Encoded Face)
Data Group 3 (Encoded Finger)
Data Group 4 (Encoded Iris)
Data Group 5 (Displayed Face)
Data Group 6 (Future use)
Data Group 7 - 15
Data Group 16 (Persons to notify)

SO$_D$
Hash DG_1
Hash DG_2
Hash DG_3
Hash DG_5
Digital Signature

- DG2 content changed
- Hash in SOD not changed
- Hash Comparison will fail

Passive Authentication



LDS

Data Group 1 (MRZ)

Data Group 2 (Encoded Face)

Data Group 3 (Encoded Finger)

Data Group 4 (Encoded Iris)

Data Group 5 (Displayed Face)

Data Group 6 (Future use)

Data Group 7 - 15

Data Group 16 (Persons to notify)

SO_D

Hash DG_1

Hash DG_2

Hash DG_3

Hash DG_5

Digital Signature

- DG2 content changed
- Hash in SOD also changed
- Hash Comparison will succeed but signature verification will fail

Current State of Play

- More than 150 countries issuing E-Passports
- High Value Target Countries issuing only E-Passports

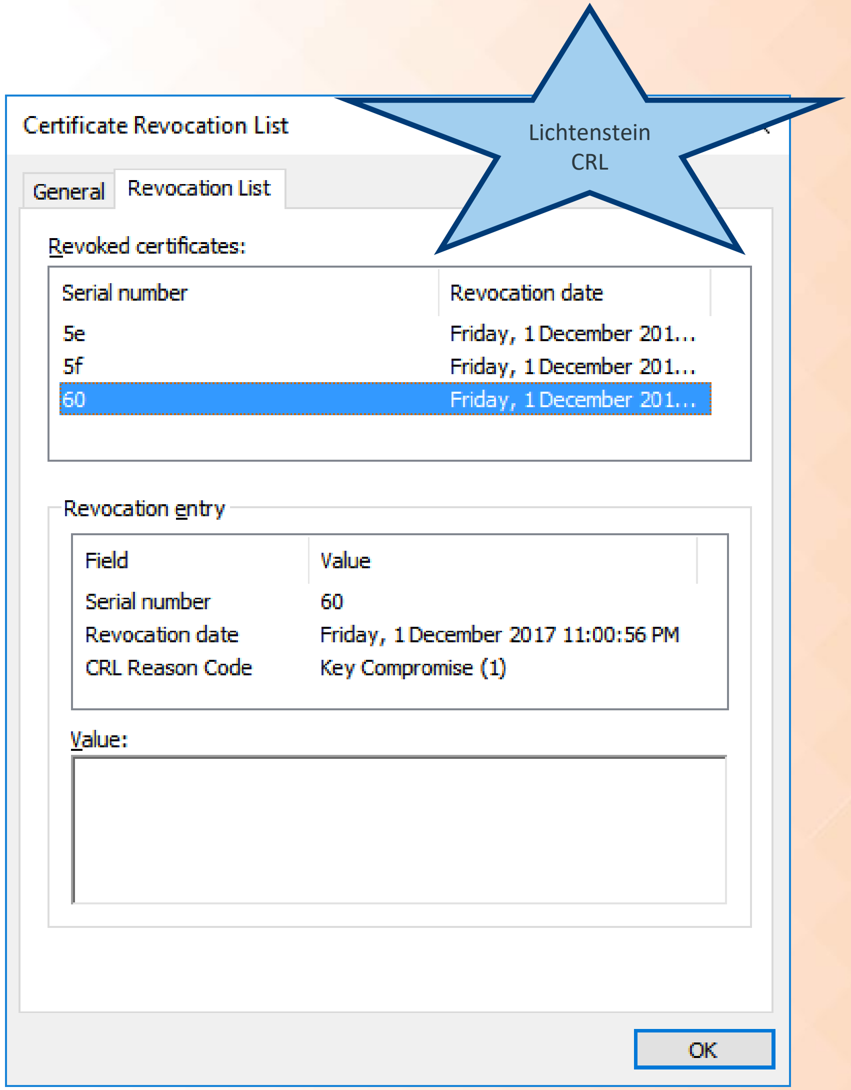
- Many Borders attempting validation of E-Passports
- Challenges remain

Availability of CSCAs

- To validate an ePassport, you need the Root of Trust of that country
- CSCA exchanges are expected to occur bilaterally
- Master Lists are secondary source of CSCAs
  - ICAO Masterlist contains CSCAs from 66 issuers
  - All Masterlists combined contain CSCAs from 107 issuer
    - Still short of 150 countries
  - Some CSCAs still missing from these countries
  - Bilateral Exchange is a necessity

CRLs

- Document Signers (DSCs) do get revoked
- Passport signed by revoked DSC is not trusted as an ePassport
- CRL verification is necessary
- ICAO PKD primary source of CRLs
- Secondary source: Publishing of CRL on website or publicly available LDAP
- PKD has CRLs from 47 countries
- From CRL DP, can obtain another 16 CRLs



Certificate Revocation List

Revoked certificates:

Serial number	Revocation date
5e	Friday, 1 December 201...
5f	Friday, 1 December 201...
60	Friday, 1 December 201...

Revocation entry

Field	Value
Serial number	60
Revocation date	Friday, 1 December 2017 11:00:56 PM
CRL Reason Code	Key Compromise (1)

Value:

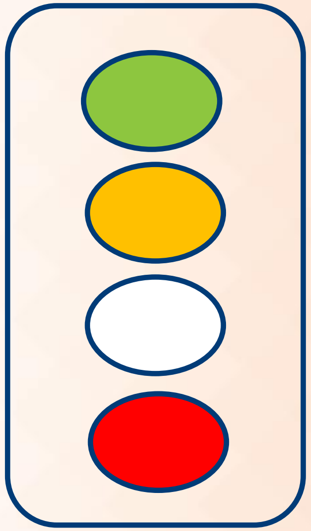
SC17 WG3/TF5

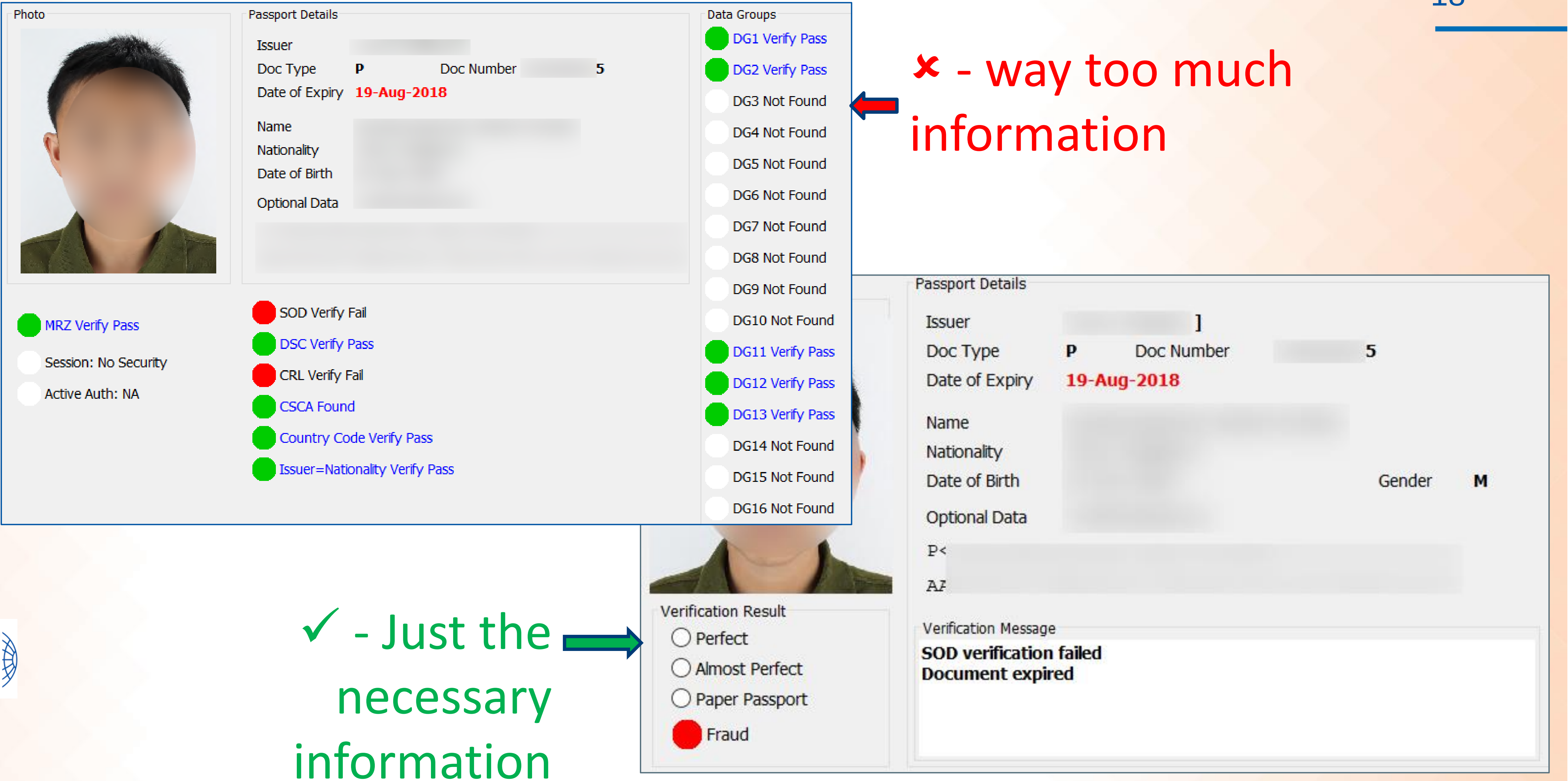
Visualization of result

- ePassport validation result is seldom a binary result
- Usual method is to provide all information to officer who needs to make a judgement call - WTMI

Recommendation:

- Map result to expected outcome decisions
- New Scenarios can also be mapped – so simplified training for front line officers





Photo

Passport Details

Issuer	[redacted]		
Doc Type	P	Doc Number	[redacted]5
Date of Expiry	19-Aug-2018		
Name	[redacted]		
Nationality			
Date of Birth			
Optional Data			

[redacted]

Data Groups

- ● DG1 Verify Pass
- ● DG2 Verify Pass
- ○ DG3 Not Found
- ○ DG4 Not Found
- ○ DG5 Not Found
- ○ DG6 Not Found
- ○ DG7 Not Found
- ○ DG8 Not Found
- ○ DG9 Not Found
- ○ DG10 Not Found
- ● DG11 Verify Pass
- ● DG12 Verify Pass
- ● DG13 Verify Pass
- ○ DG14 Not Found
- ○ DG15 Not Found
- ○ DG16 Not Found

- ● MRZ Verify Pass
- ○ Session: No Security
- ○ Active Auth: NA

- ● SOD Verify Fail
- ● DSC Verify Pass
- ● CRL Verify Fail
- ● CSCA Found
- ● Country Code Verify Pass
- ● Issuer=Nationality Verify Pass

✘ - way too much information

Passport Details

Issuer	[redacted]]		
Doc Type	P	Doc Number	[redacted]5
Date of Expiry	19-Aug-2018		
Name	[redacted]		
Nationality			
Date of Birth		Gender	M
Optional Data			

P<[redacted]

AA[redacted]

Verification Result

- ○ Perfect
- ○ Almost Perfect
- ○ Paper Passport
- ● Fraud

Verification Message

SOD verification failed
Document expired

✓ - Just the necessary information

Traffic Light Problem

- What to do if the outcome is RED or Amber?
- Many reasons for such outcomes
  - The passport could not be read
  - The biometric match is below the threshold value
  - The verification of the passport failed or did not succeed
    - Passport may be valid but has a defect
  - A cloned passport chip was detected
  - There was a hit on a watchlist
- Process flow to manage exceptions is very important

Processing Time

- Passenger processing time should be as short as possible – usual target is under 10 seconds
- Depends on:
- Architecture – validation done in:
  - Reader – Fastest response. Updates are a nightmare
  - Inspection Terminal – Almost as fast as Reader. Easier updates
  - Centralized Service – Easiest to update. Network latency can be an issue
- Crypto Toolkit – Brainpool curves take longer to verify – All countries implementing ECDSA are using brainpool curves

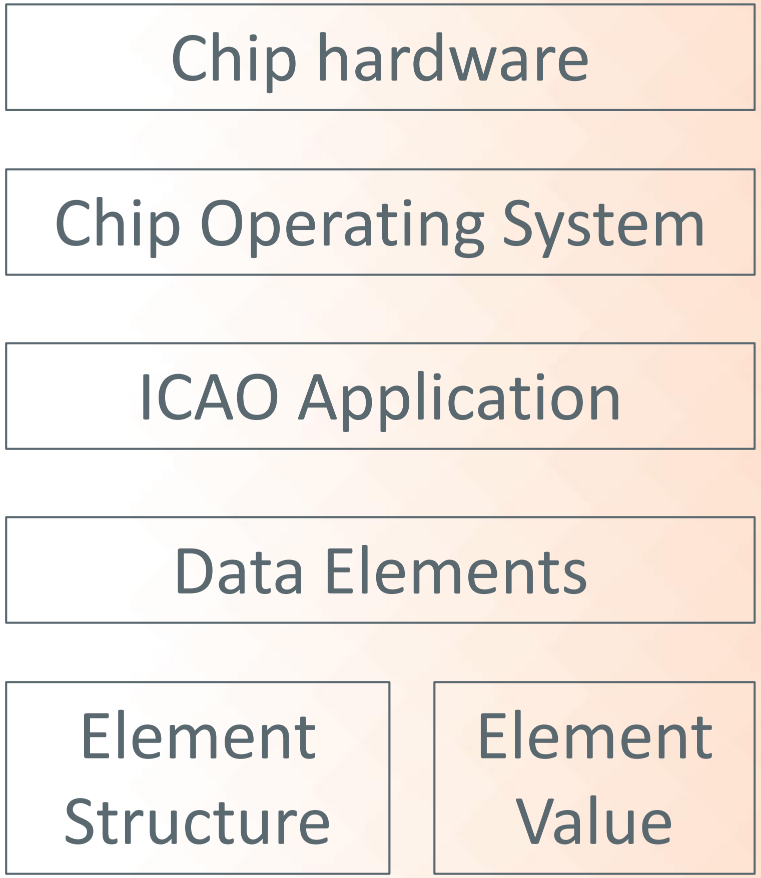
Quality of CSCAs and DSCs

- PKI is complicated – people make mistakes
- 395 CSCAs from 107 countries in PKD MasterLists
  - 10 countries have errors – 17 CSCAs
  - 9 countries have warnings – 15 CSCAs
- 16053 DSCs from 45 countries
  - 14 countries have errors – 1844 DSCs
  - 3 countries have warnings – 2019 DSCs
- 45 CRLs from 45 countries
  - 6 CRLs have errors
  - 2 CRLs have warnings
- These errors and warnings will impact ePassport Validation.
- Mechanism to handle these exceptions are necessary

Data from December 2021

What is defect?

- Chip Hardware is very stable
- Chip OS is standard – some strange behaviors , but readers know how to handle it
- ICAO application – No issues till now
- Data element (Elementary Files) all good
- Structure and Value have issues



Chip hardware

Chip Operating System

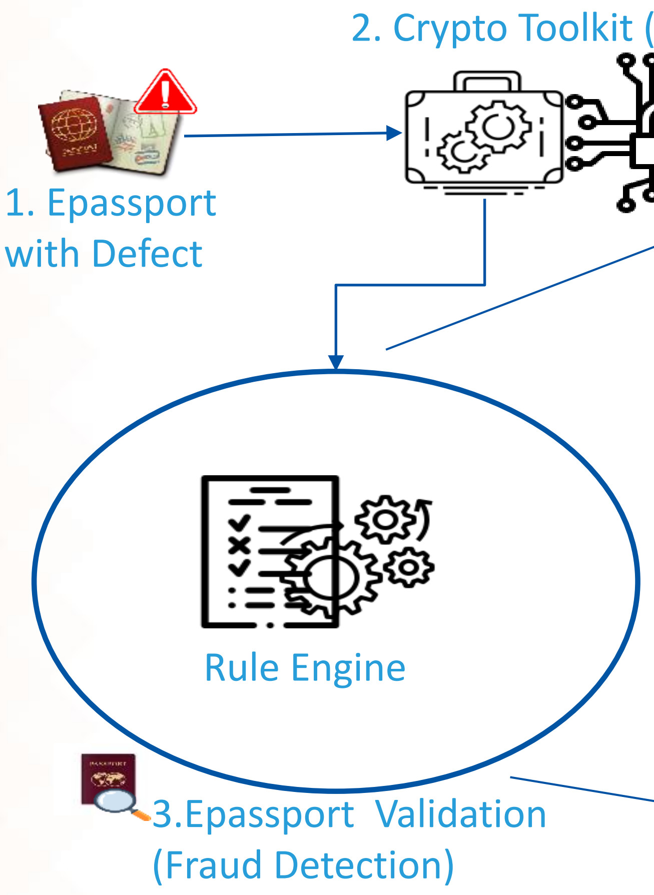
ICAO Application

Data Elements

Element Structure

Element Value

Overview (Defect Handling and Validation)



2. Crypto Toolkit (defect Handling)

1. Epassport with Defect

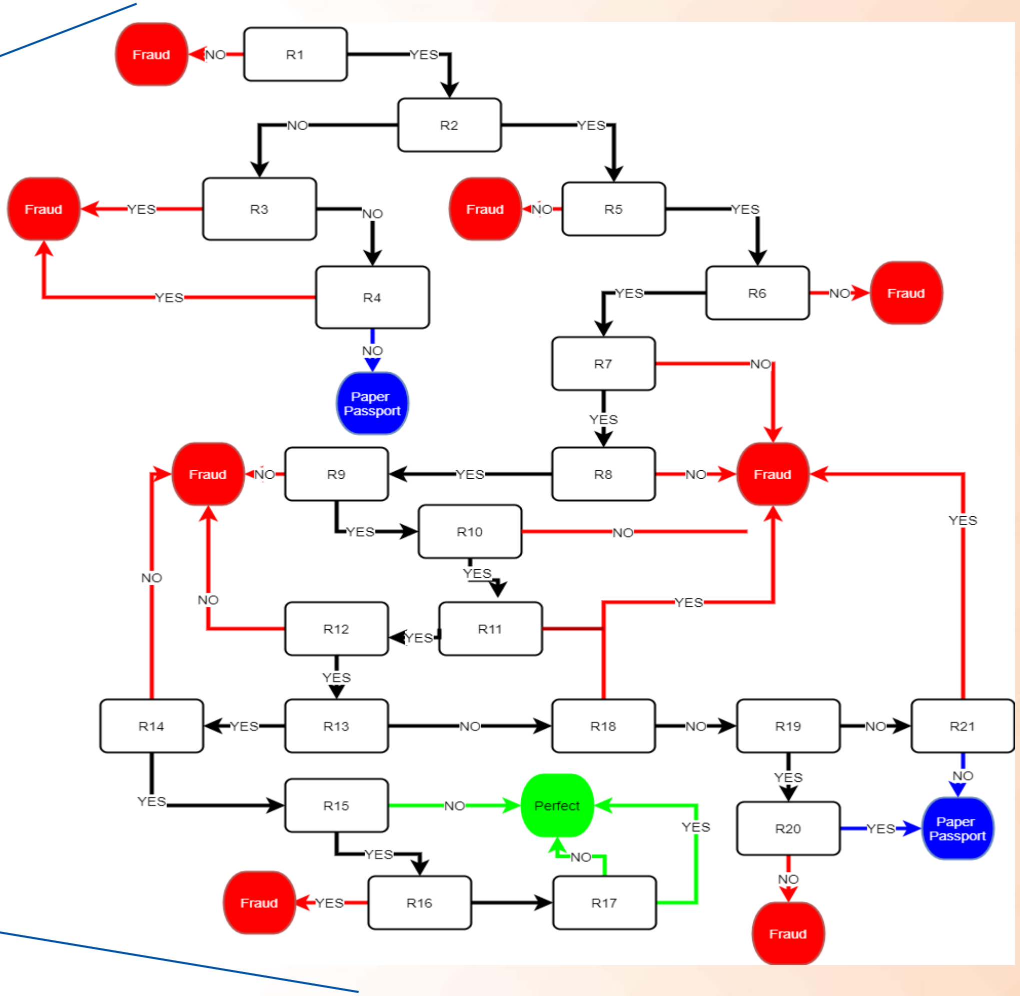
Rule Engine

3.Epassport Validation (Fraud Detection)

Fraud – 16 exits

Don’t know – 3 exits

Perfect – 2 exits

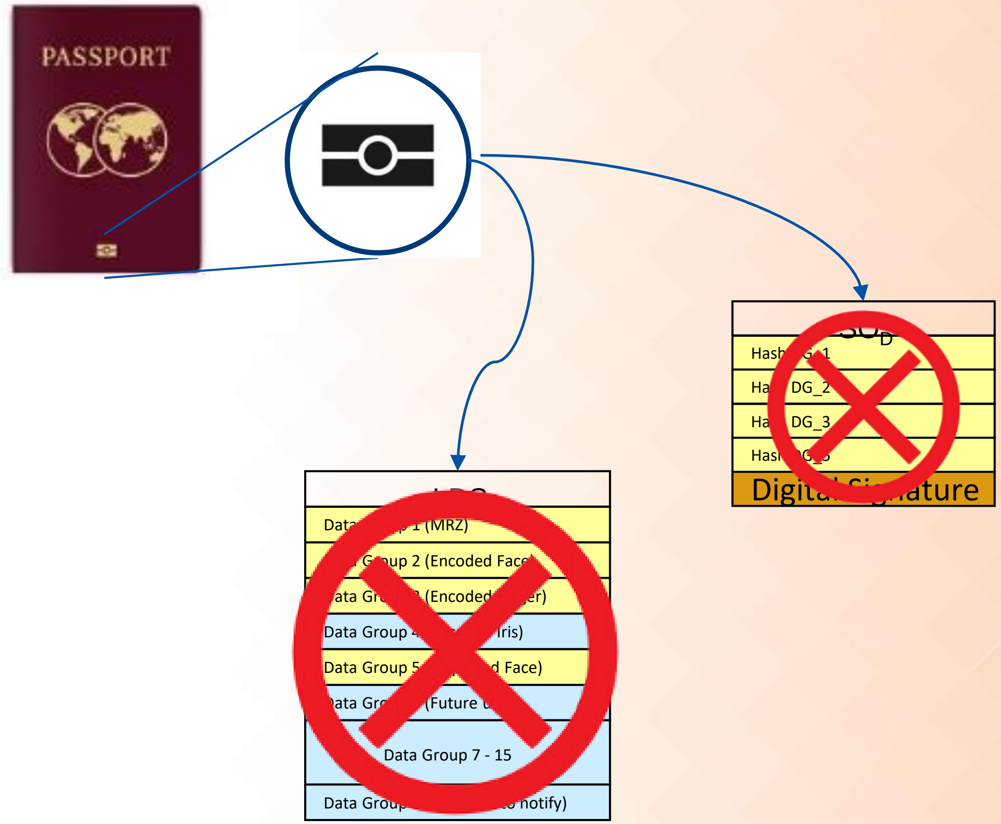


SC17 WG3/TF5

2. Fraud Detection

Fraud Patterns - Broken chips

- Stolen document
- Datapage expertly modified
- Chip cooked/Antenna broken – hence cannot read or verify chip
- Will be assumed to be a damaged chip, but is actually a fraud

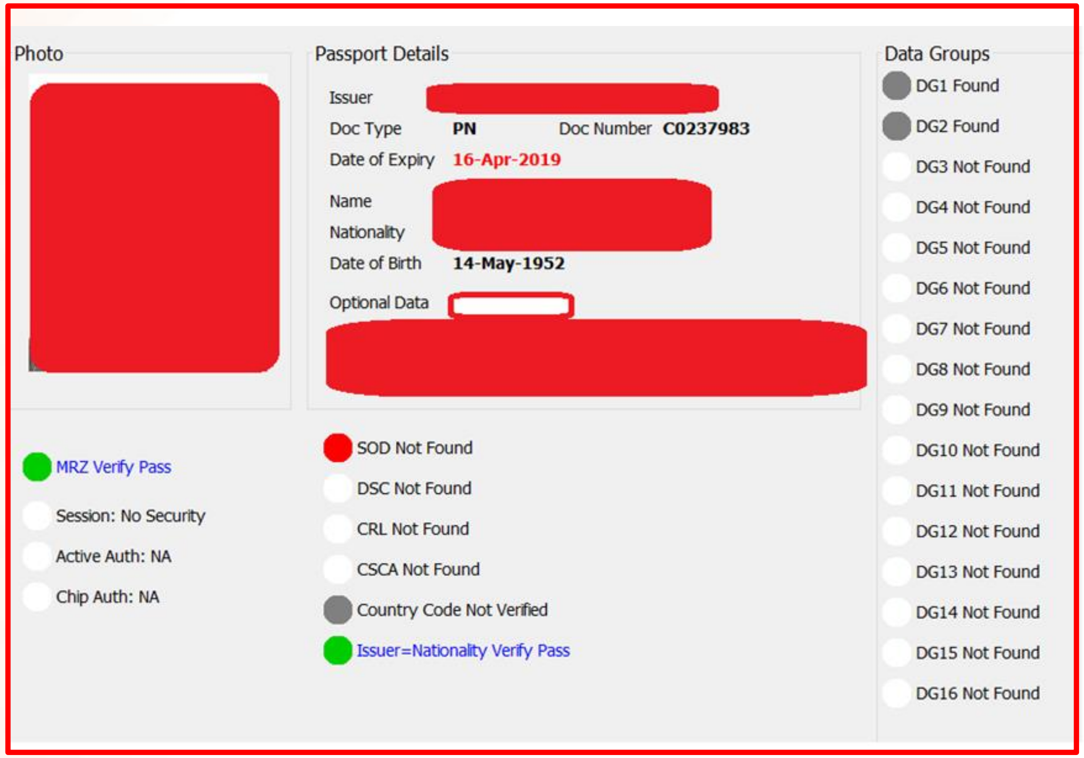


Fraud Pattern - Replaced chips

- Lost blank booklet
- Personalized with passport number different from document control number
- Chip replaced with a fantasy chip
- Three variations seen:
  - Chip data signed with fantasy CSCA
  - DG1 present, DG2 present and SOD missing – so cannot verify. Will be treated as incomplete read
  - SOD also present, but no document signer in chip, so cannot verify for non-PKD member

Variation 1

- DG1 present, DG2 present and SOD missing – so cannot verify. Will be treated as incomplete read



Photo

[redacted]

● MRZ Verify Pass

○ Session: No Security

○ Active Auth: NA

○ Chip Auth: NA

Passport Details

Issuer [redacted]

Doc Type **PN** Doc Number **C0237983**

Date of Expiry **16-Apr-2019**

Name [redacted]

Nationality

Date of Birth **14-May-1952**

Optional Data [redacted]

[redacted]

● SOD Not Found

○ DSC Not Found

○ CRL Not Found

○ CSCA Not Found

● Country Code Not Verified

● Issuer=Nationality Verify Pass

Data Groups

● DG1 Found

● DG2 Found

○ DG3 Not Found

○ DG4 Not Found

○ DG5 Not Found

○ DG6 Not Found

○ DG7 Not Found

○ DG8 Not Found

○ DG9 Not Found

○ DG10 Not Found

○ DG11 Not Found

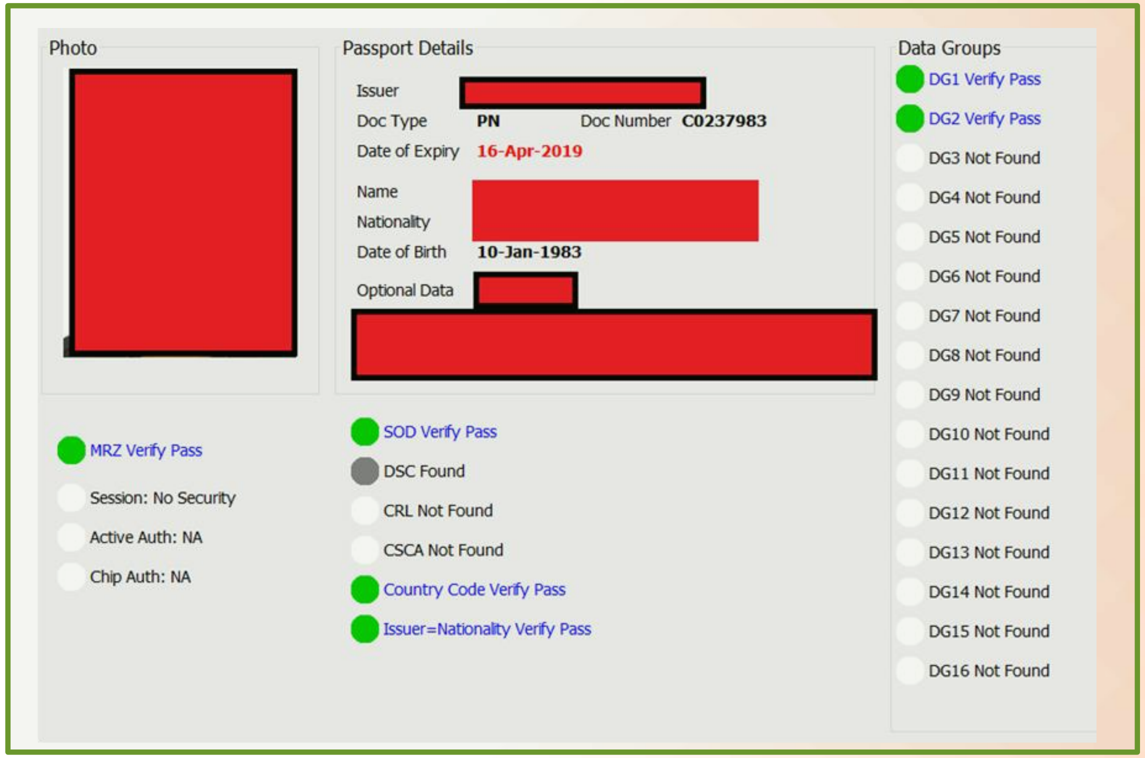
○ DG12 Not Found

○ DG13 Not Found

○ DG14 Not Found

○ DG15 Not Found

○ DG16 Not Found



Photo

[redacted]

● MRZ Verify Pass

○ Session: No Security

○ Active Auth: NA

○ Chip Auth: NA

Passport Details

Issuer [redacted]

Doc Type **PN** Doc Number **C0237983**

Date of Expiry **16-Apr-2019**

Name [redacted]

Nationality

Date of Birth **10-Jan-1983**

Optional Data [redacted]

[redacted]

● SOD Verify Pass

● DSC Found

○ CRL Not Found

○ CSCA Not Found

● Country Code Verify Pass

● Issuer=Nationality Verify Pass

Data Groups

● DG1 Verify Pass

● DG2 Verify Pass

○ DG3 Not Found

○ DG4 Not Found

○ DG5 Not Found

○ DG6 Not Found

○ DG7 Not Found

○ DG8 Not Found

○ DG9 Not Found

○ DG10 Not Found

○ DG11 Not Found

○ DG12 Not Found

○ DG13 Not Found

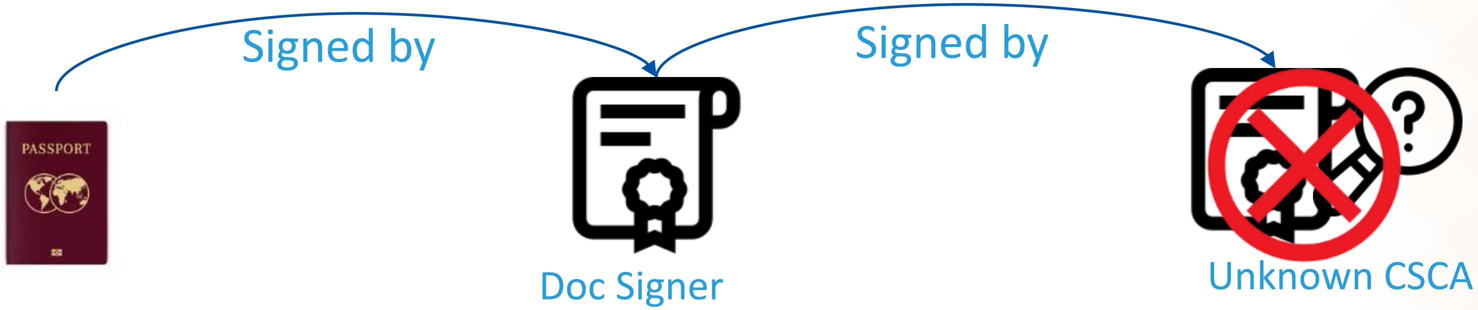
○ DG14 Not Found

○ DG15 Not Found

○ DG16 Not Found

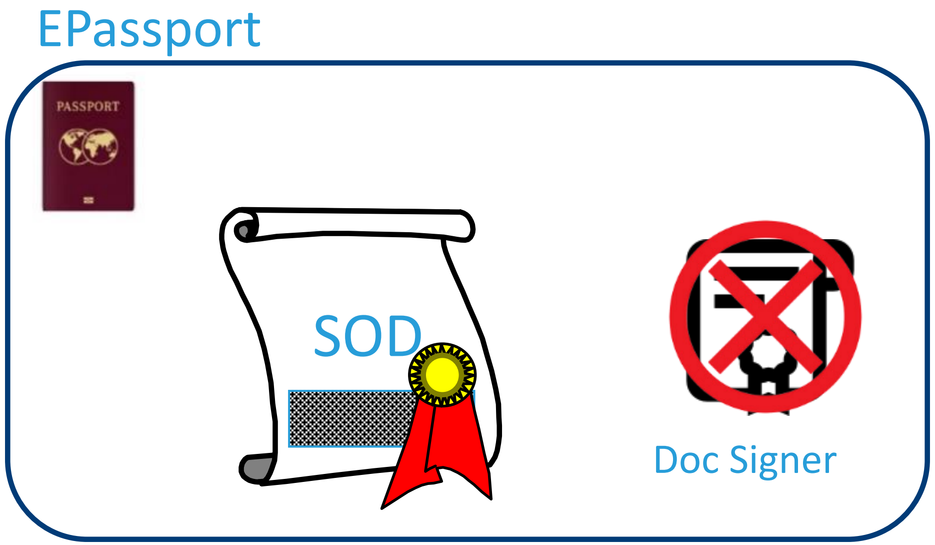
Variation 2

- Chip data signed with fantasy CSCA
  - SOD signed by Doc Signer
  - Doc Signer signed by CSCA.
  - CSCA not found in masterlist or bilateral exchange



Variation 3

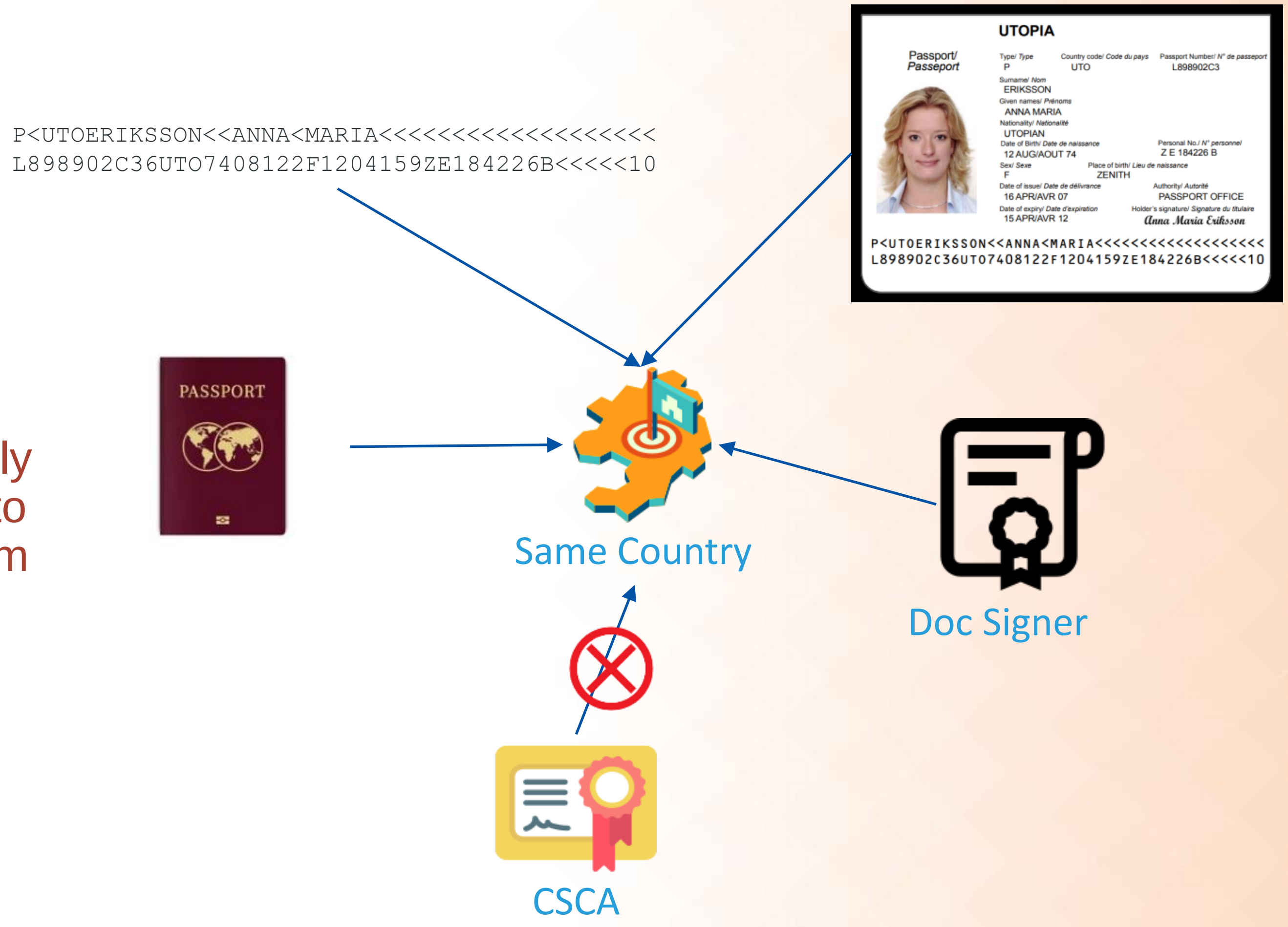
- SOD also present, but no document signer in chip, so cannot verify for non-PKD member



- According to Doc9303-12, all EPassport must have document signer certificate in the chip.

Fraud Pattern – Country Code issue

- Passport cover says Country A
- MRZ says country A
- DG1 says country A
- Document Signer says country A
- CSCA says country B
  - Claimed to be a test passport mistakenly personalized. Suspect it to be a probe to check reaction of Border Control System



```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C36UTO7408122F1204159ZE184226B<<<<<10
```

UTOPIA

Passport/ *Passeport*

Type/ *Type* P

Country code/ *Code du pays* UTO

Passport Number/ *N° de passeport* L898902C3

Surname/ *Nom* ERIKSSON

Given names/ *Prénoms* ANNA MARIA

Nationality/ *Nationalité* UTOPIAN

Date of Birth/ *Date de naissance* 12 AUG/AOUT 74

Personal No./ *N° personnel* Z E 184226 B

Sex/ *Sexe* F

Place of birth/ *Lieu de naissance* ZENITH

Date of issue/ *Date de délivrance* 16 APR/AVR 07

Authority/ *Autorité* PASSPORT OFFICE

Date of expiry/ *Date d'expiration* 15 APR/AVR 12

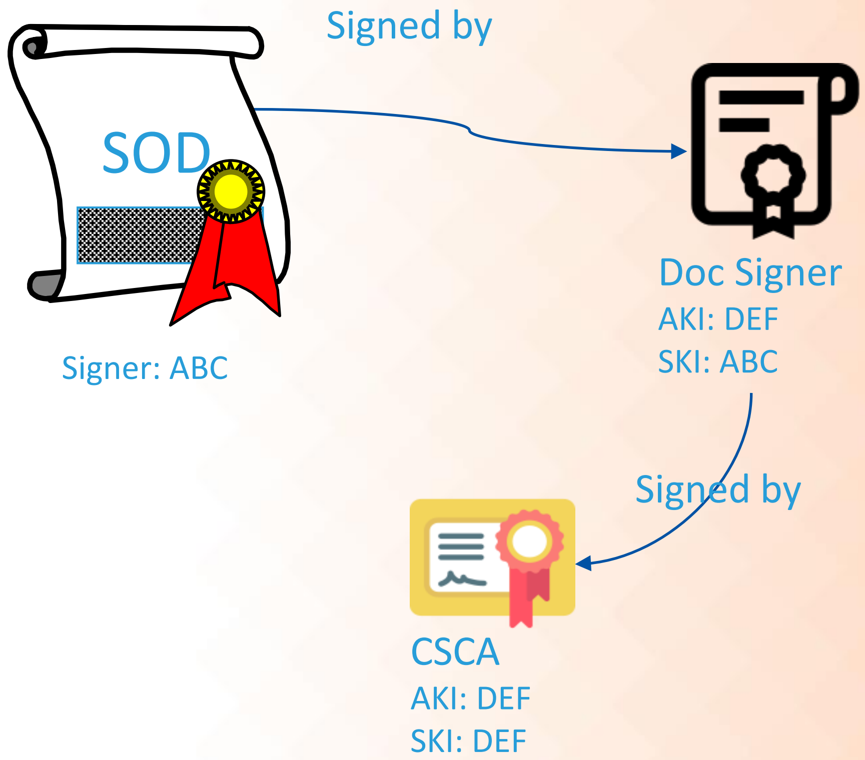
Holder's signature/ *Signature du titulaire* Anna Maria Eriksson

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<
L898902C36UTO7408122F1204159ZE184226B<<<<<10
```

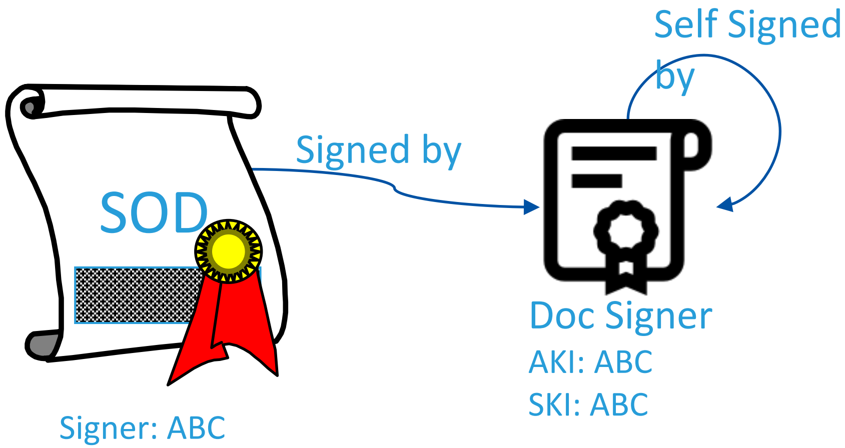
Fraud Pattern – Self Signed Document Signer

1. Usually
   - SOD signed by Doc Signer
   - Doc Signer signed by CSCA
2. Doc Signer is self signed, hence passport verification succeeds

1.



2.



Fantasy Passport

- Passport claims to be from a country that does not issue ePassports
- Managed to cross border as officer seemed to trust a passport with a chip

Defective Documents

- Have identified 23 defects across 55 countries – will result in False Negative on these documents i.e. perfectly good documents being flagged as fraudulent.
- Based on our discussions with multiple border control agencies, numbers between 11% to 46% of all validations
- Depends on the traveler profile and toolkit (not all toolkits give the same result)

Need a defect management method.

Conversely, if you do not see any errors at your border, you have a problem

Handling False Negatives

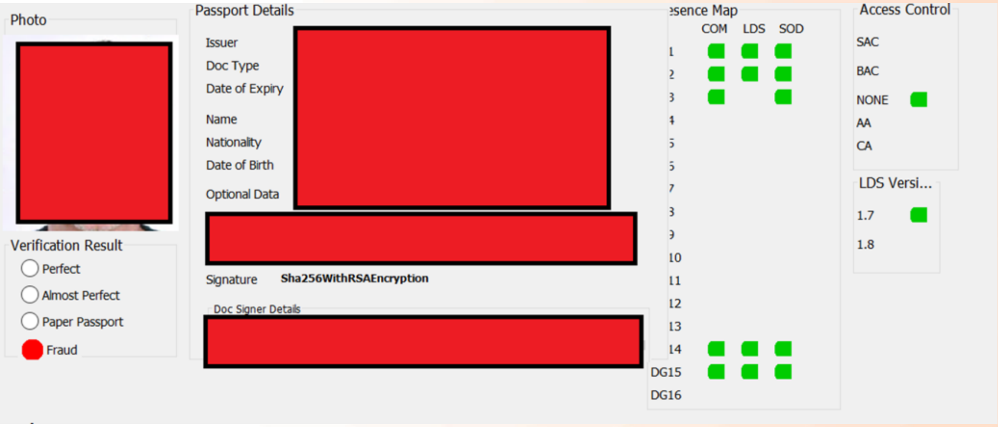
- Three strategies
  - Show result to officer and let them decide
  - Use a DefectList
    - If passport from X country and Verification fails due to Y reason, then it is a good passport
    - Difficult to differentiate between a False Negative and a Fraud
  - Implement Defect Handling
    - Implement logic to do verification in spite of defect – reduce False negatives to near zero

DefectList Exploitation

- Countries deploy defect list in their inspection systems
- Fraudsters exploit the workflow

A known attack:

1. ePassport from this target country fails verification due to a small defect in the Document Signer.
2. Country does support Active Authentication
3. Fraudulent document with chip contains proper LDS including DG15 and implements Active Authentication using this public key
4. The SOD contains the correct hash of DG15, but the Signerinfos is copied from a proper SOD.
5. Signature verification fails – No means to differentiate between actual signature verification failure (real failure) and failure due to Doc Signer defect. Hence previous method of profiling returns the document as a valid document



Photo

[redacted]

Verification Result

○ Perfect
○ Almost Perfect
○ Paper Passport
● Fraud

Passport Details

Issuer
Doc Type
Date of Expiry
Name
Nationality
Date of Birth
Optional Data

[redacted]

[redacted]

Signature Sha256WithRSAEncryption

Doc Signer Details

[redacted]

ɜsence Map

	COM	LDS	SOD
1	🟩	🟩	🟩
2	🟩	🟩	🟩
3	🟩		🟩
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14	🟩	🟩	🟩
DG15	🟩	🟩	🟩
DG16			

Access Control

SAC	
BAC	
NONE	🟩
AA	
CA	

LDS Versi...

1.7	🟩
1.8	

Is Defect Handling possible?

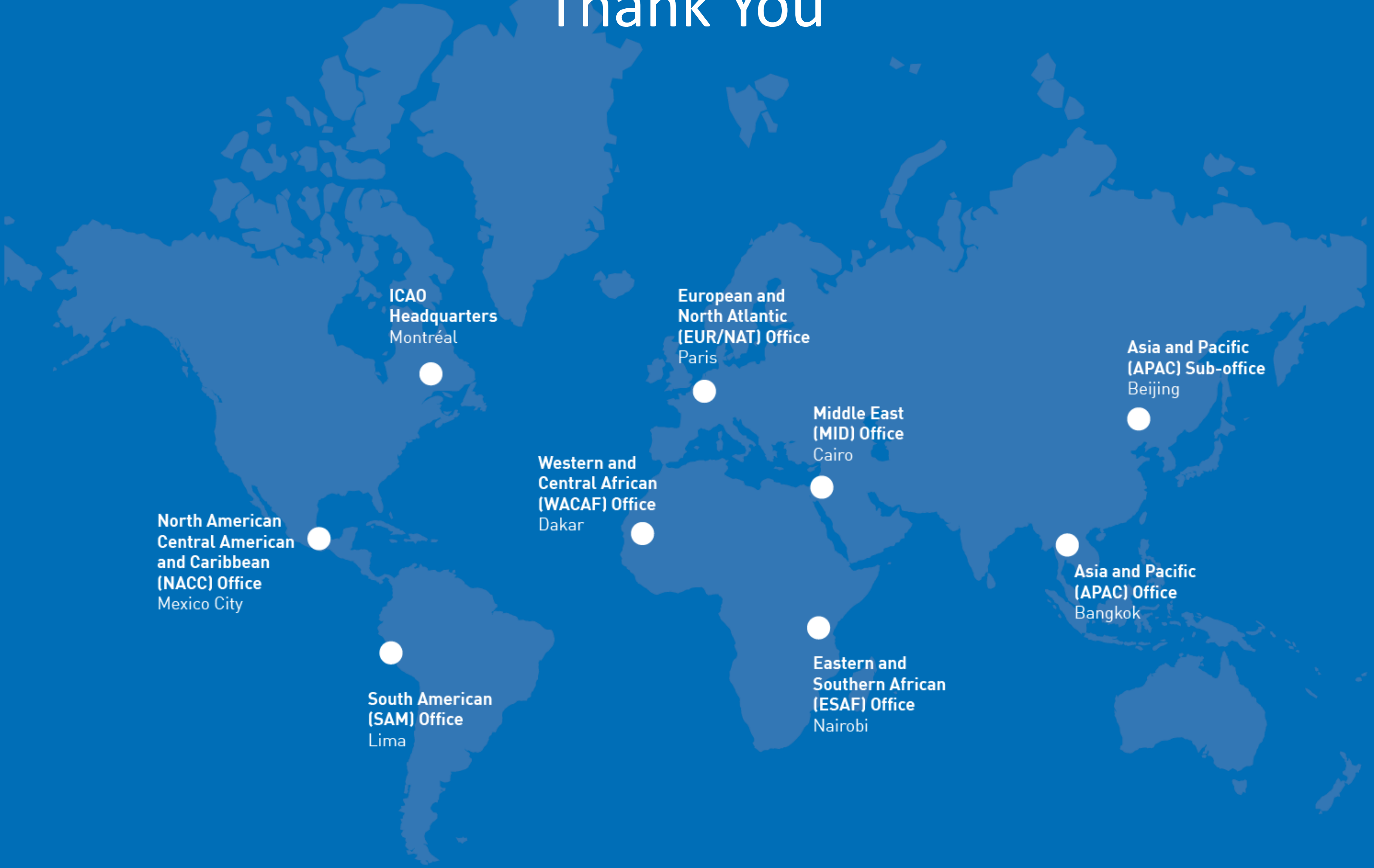
- Defect Handling – Reduce false negatives to near zero
- Based on our analysis, most defects can be handled
- We chose not to handle one defect of missing AKI
  - An AKI is the field in Document Signer that links the Document Signer to the CSCA.
  - Missing in the case of Venezuela and Somalia
- An older defect of truncated SOD (US passports 2005) also cannot be handled
- We recently discovered a new defect in a European passport that we are analysing

Summary

- CSCA distribution is key. Source using multiple methods
- CRL checking is necessary. Source using multiple methods
- Visualization and presentation to officer must be simple
- Exception handling is important – especially for eGates
- Defect management must be thought through

ePassport validation = Fraud detection

Thank You


ICAO Headquarters
Montréal
European and North Atlantic (EUR/NAT) Office
Paris
Asia and Pacific (APAC) Sub-office
Beijing
Middle East (MID) Office
Cairo
Western and Central African (WACAF) Office
Dakar
North American Central American and Caribbean (NACC) Office
Mexico City
Asia and Pacific (APAC) Office
Bangkok
Eastern and Southern African (ESAF) Office
Nairobi
South American (SAM) Office
Lima

ICAO