



| ICAO

SECURITY & FACILITATION



# eMRTD PKI and eMRTD Validation

**R Rajeshkumar**

*International Organization for Standardization (ISO)*

July 2019/Windhoek



# Components of an e-Passport

In addition to the traditional printed passport security, an e-Passport incorporates a contactless smart card, which comprises:

1. A smart chip that stores digitally signed data.
2. Wireless antenna for communications with passport encoders/ readers.



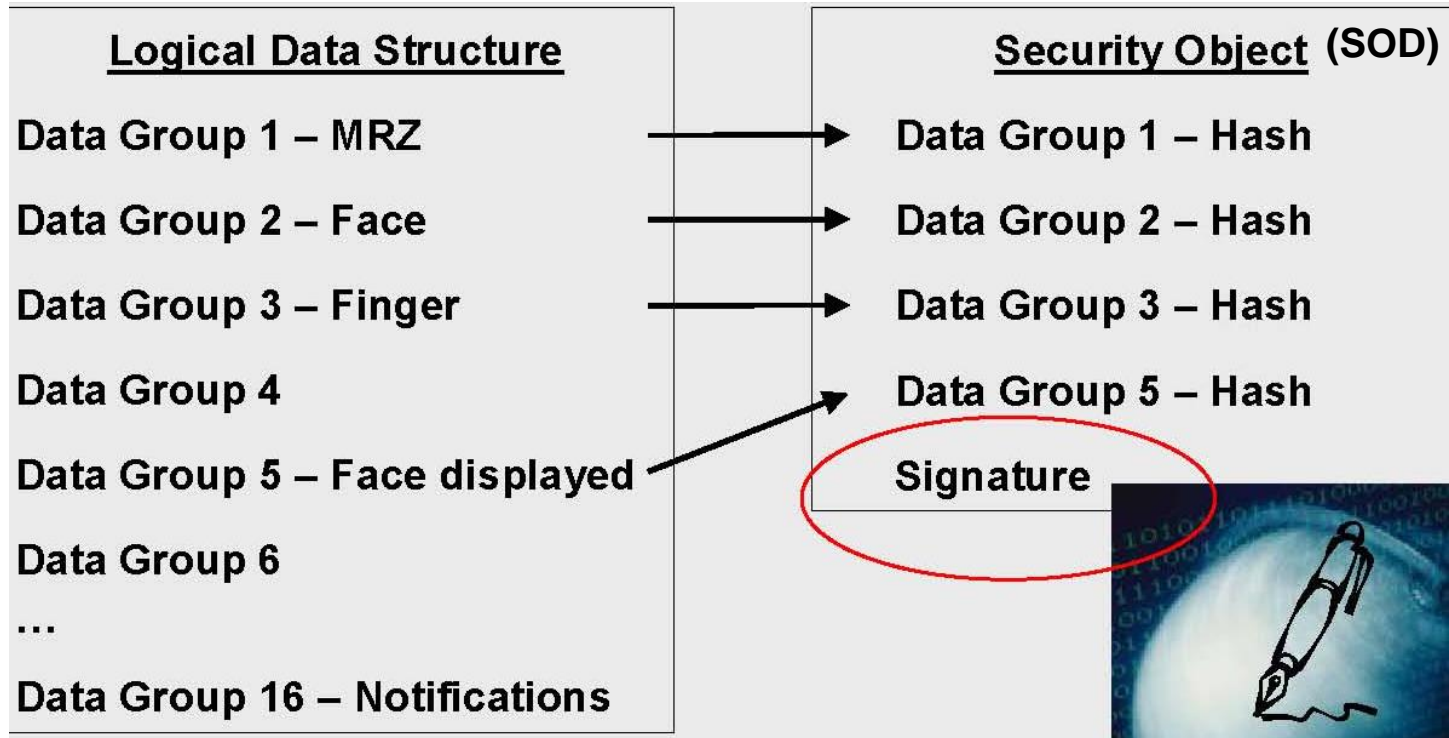


# What does the Chip contain?

- Chip contains **Logical Data Structure (LDS)** with 16 **Data Groups (DGs)**.
  - DG1 contains the contents of the MRZ - mandatory
  - DG2 contains facial biometric - mandatory
  - DG3 contains fingerprint biometric – optional
  - DG4 contains iris biometric – optional
  - DG5 contains portrait of face – optional
  - ... and so on
- Chip contains **Security Data Object (SO<sub>D</sub>)**
  - Contains hashes of the Data Groups present in LDS.
  - Contains a digital signature that encapsulates the stored hashes, together with the Signing Certificate and public key.



## Document Security Object (SOD)





# Issues with Contactless Chip

Adding a contactless chip to an e-Passport introduces two new attack possibilities:

- **Skimming** - the data stored in the chip can be electronically read without authorizing this reading of the document.
- **Eavesdropping** - the unencrypted communication between a contactless chip and a reader can be eavesdropped within a distance of several metres.

**A Chip Access Control mechanism is needed.**





ICAO

SECURITY & FACILITATION



# Supplemental Access Control (SAC)

- Password Authenticated Connection Establishment (PACE) has been adopted to eventually replace BAC.
- While BAC works only with the MRZ, PACE allows using randomly generated Card Access Numbers (CAN) - short keys printed on the document.
- PACE uses stronger cryptography (asymmetric cryptography) than BAC - raising the security of documents to the level of using contact chips.
- The e-Passport chip OS must be capable of supporting PACE.



| ICAO

SECURITY & FACILITATION



# BAC vs PACE Adoption

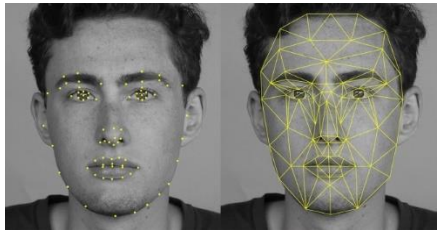
- For global interoperability, States **MUST NOT** implement PACE without implementing BAC until 31 December 2017.
- Starting 1<sup>st</sup> January 2018, States may implement PACE only, without BAC.
- Inspection systems **MUST** support all compliant ePassport configurations. Inspection Systems should implement and use PACE if provided by the ePassport chip.
- BAC may become deprecated in the future. In this case PACE will become the default access control mechanism.



# Biometrics

Doc 9303 considers only three types of biometric identification systems:

- Facial Recognition – MANDATORY.
- Fingerprint Recognition – OPTIONAL.
- Iris Recognition – OPTIONAL.





# Extended Access Control (EAC)

- Optional security feature to protect and restrict access to sensitive biometrics data – fingerprints and iris images.
- ICAO leaves the actual solution open to the implementing States.
- A chip protected by EAC will allow that this sensitive data is read (through an encrypted channel) only by an authorized passport inspection system.
- Only two known standards adopted – Singapore EAC and EU EAC.



ICAO

SECURITY & FACILITATION

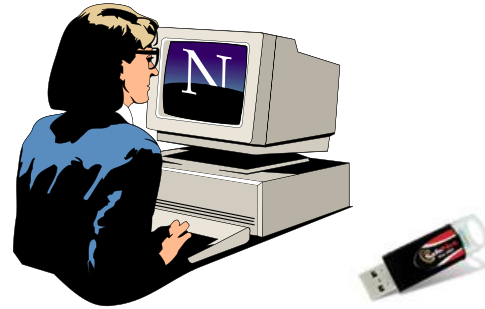


## Singapore EAC Standard

### Based on Asymmetric Key Encryption

The fingerprints are encrypted with a few special EAC encryption keys.

For decryption, the EAC private decryption keys are stored in separate USB crypto tokens, protected by a password.

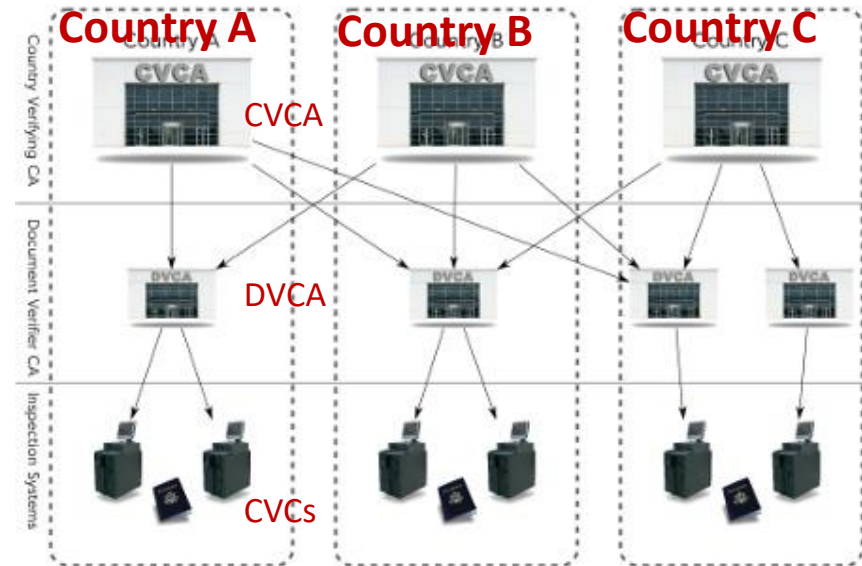


**USB crypto tokens**



# EU EAC Standard

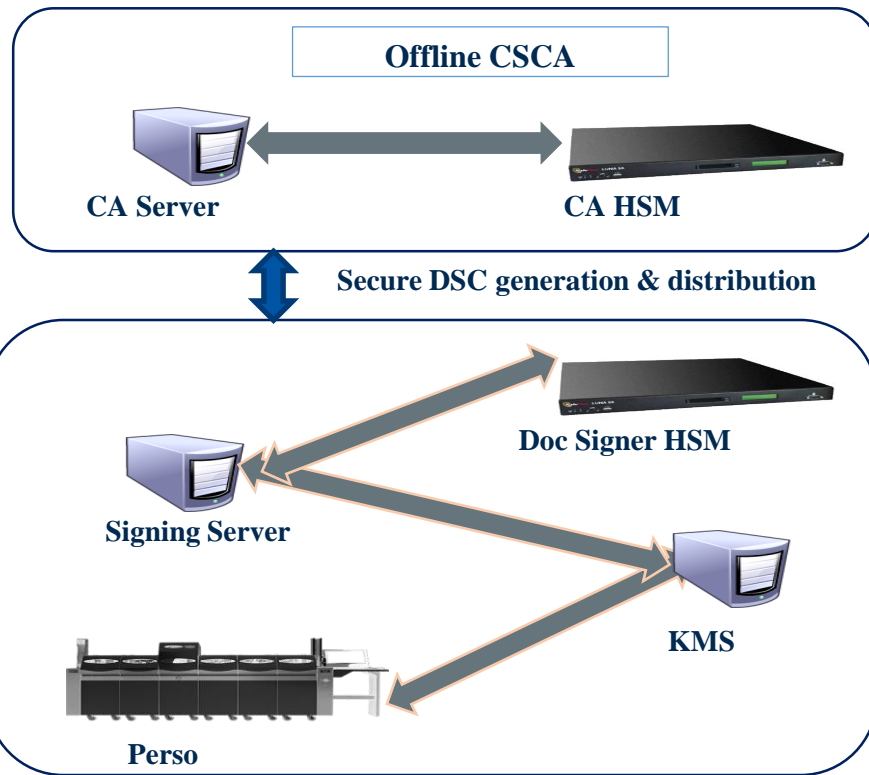
- Seen to be complex. Short term certificates.
  - *Country Verifying Certificate Authority (CVCA)*
  - *Document Verifier Certificate Authority (DVCA)*
  - *Card Verifiable Certificates (CVC)*
- Supports:
  - Chip Authentication
  - Terminal Authentication
- Counters Cloning





# Issuance System

- CSCA generation
- DSC generation and distribution to Personalisation system





# Security Considerations

- Five phases for security considerations
  - Security in Generation
  - Security in Transport to Personalisation systems
  - Proof of control over usage of Document Signer
  - Secure destruction of private key at end of lifetime
  - Monitoring of compromise and reporting
- Outsourcing of Passport personalisation should not lead to loss of control on the issuance process – Proper planning of PKI can help in retaining control over the issuance process



# Proof of control

- CSCA generation and usage
- DSC generation and usage
- Passport issuance
  - Outsourcing is okay. But control on data and who the document is issued to needs to be maintained
- Asserted by published Certificate Practise Statement (CPS) and Certificate Policy (CP) – backed by independent audit



# Certification Practice Statement (CPS)

- A CPS is a policy document which describes in detail the operational practices of a CA, as well as the responsibilities that the CA is willing to accept with respect to certificates it issues in accordance with these practices.
- If a CA operates according to the practices and responsibilities of a specific CPS, then the CA is said to be governed by this CPS.
- Defined in RFC 3647

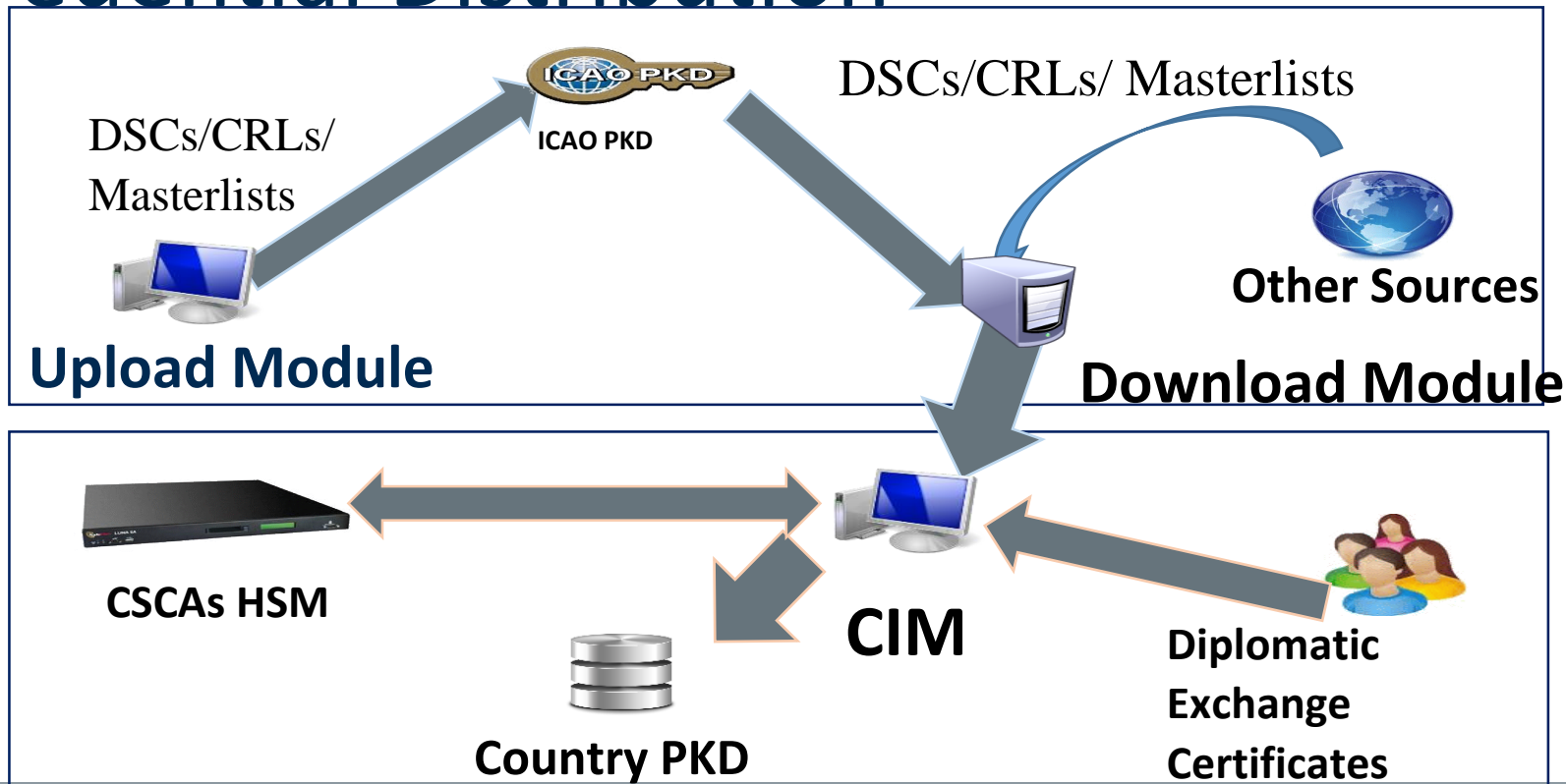


# Border Control

- eMRTD not automatically trusted
- Trust depends on
  - Confidence in process of issuance of the document
  - Confidence in control over signing credentials
- Asserted by published Certificate Practise Statement (CPS) and Certificate Policy (CP) – backed by independent audit
- Data analysis acts as a surveillance and ensures continued trust



# Credential Distribution



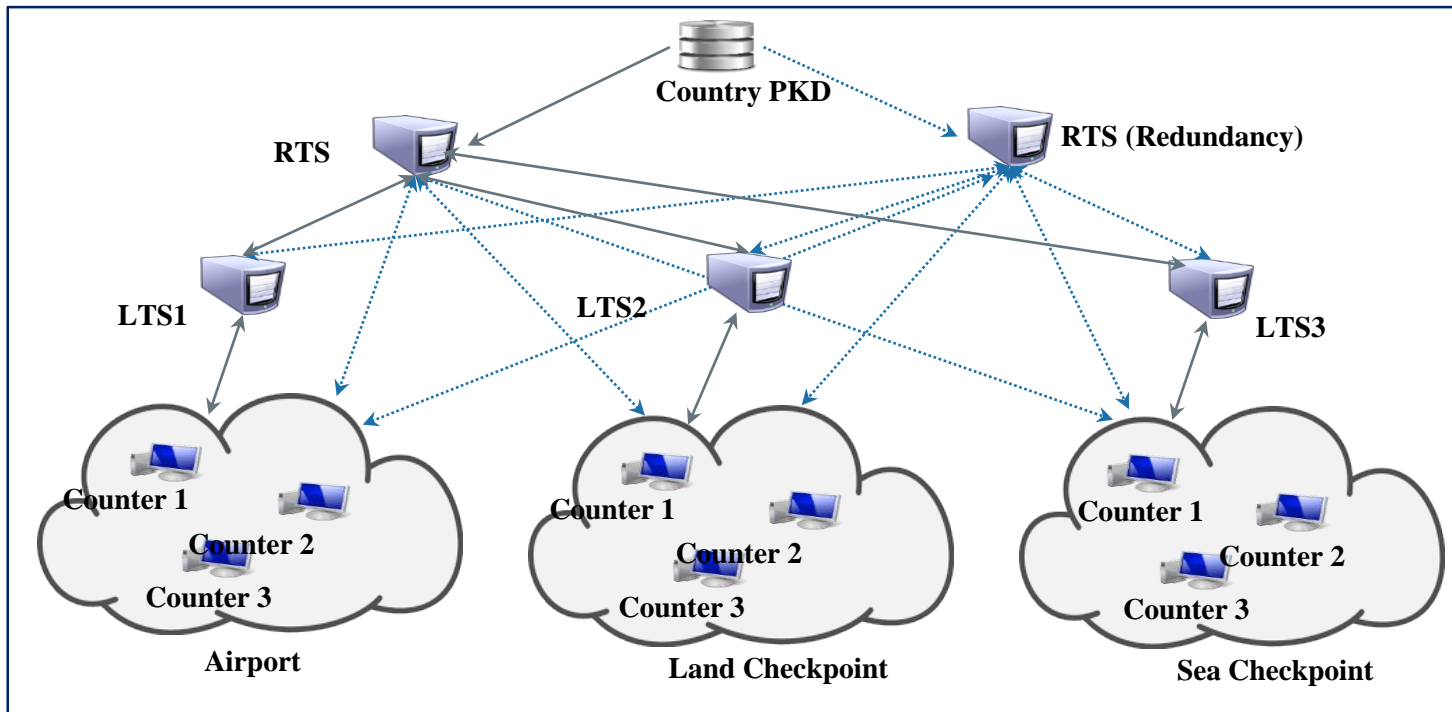


# Credential Distribution

- PKD Upload - Doc 9303 checks before upload
- Download Module
  - Scheduled downloads from ICAO PKD
  - Configurable to download from other sources
- Credential Import Module
  - Multi Party authorization for CSCA Import after due diligence
  - Doc 9303 conformance checks
  - Validation of DSC/CRL against CSCA in HSM
- CSCA distribution is always bilateral. Plan processes to establish trust in CSCAs received bilaterally.



# In Country distribution of credentials





# In Country

## Country PKD

Ensure protection against substitution attack – e.g. Store data as signed objects

Data can only be added after due diligence

## Distribution to Validation endpoint

Protect communication between terminal and Country PKD e.g 2-way SSL

Eliminate single point of failure/network chokepoints



ICAO

SECURITY & FACILITATION



# Summary – eMRTD PKI

- Issuing an E-Passport is useless unless other countries trust your process
- You need to distribute your CSCA and CRL at least for other countries to be able to validate your document. One mechanism is ICAO PKD
- You should have a process for verifying CSCAs, DSCs and CRLs that you receive before you use them at your border
- The credentials need to be securely distributed to the point of validation at the border
- PKI is a technology – proper processes makes it a solution



| ICAO

SECURITY & FACILITATION



## eMRTD Validation -Current State of Play

- More than 135 countries issuing E-Passports
- High Value Target Countries issuing only E-Passports
- Many Borders attempting validation of E-Passports
- Challenges remain



ICAO

SECURITY & FACILITATION



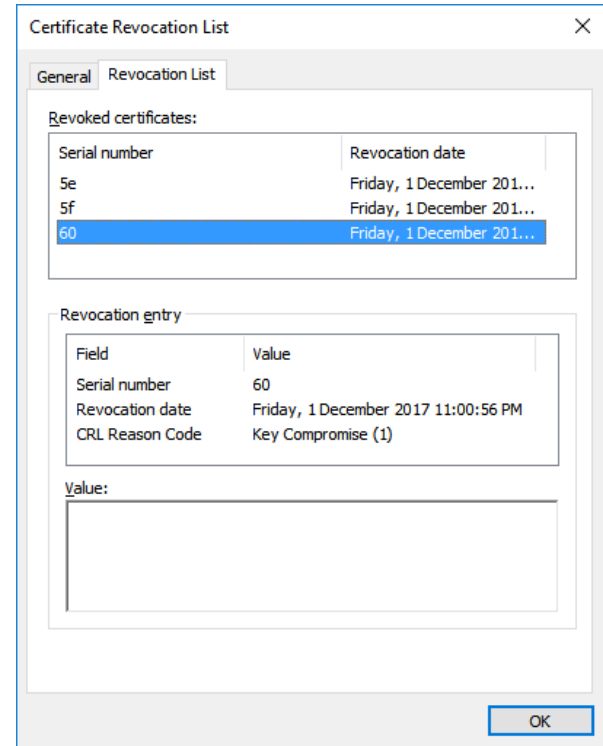
## Challenge 1 – Availability of CSCAs

- CSCA exchange expected to occur bilaterally.
- MasterLists are secondary source of CSCAs
  - CSCAs from 86 countries currently available from Masterlists – far short of the 135+ countries issuing ePassports
  - May still be missing some CSCAs from these countries



## Challenge 2 – Availability of CRLs

- ICAO PKD primary source of CRLs
- Secondary source: Publishing of CRL on website or publicly available LDAP
- PKD has CRLs from 37 countries
- From CRL DP, can obtain about 62 CRLs





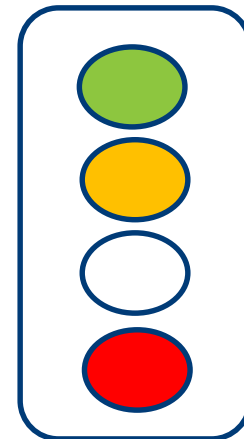
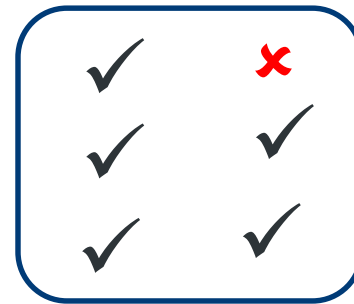
## Challenge 3 – Processing Time

- 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 – Easy to update. Network latency can be an issue
  - Crypto Toolkit – Brainpool curves take longer to verify – All countries implementing ECDSA are using brainpool curves



## Challenge 4 – Visualization of Results

- Too much information being given to officer who then needs to make a judgement call.
- Map the information to the expected outcome decisions
  - New scenarios can also be mapped, so officer training is simplified





| ICAO

SECURITY & FACILITATION



## Challenge 5 – Defective documents

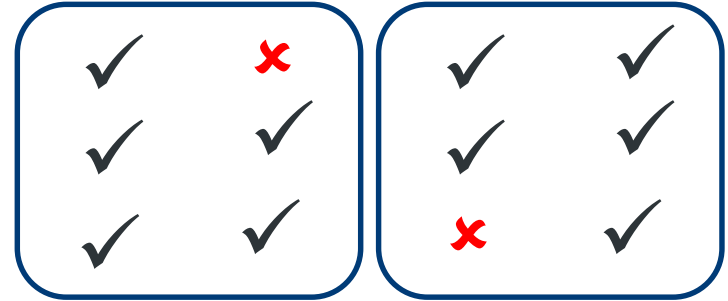
- Have identified 23 defects across 55 countries – will result in False Negative on these documents i.e. perfectly good documents being flagged as fraudulent.
- Based on our discussions with multiple border control agencies, numbers between 11% to 46% of all validations
  - Depends on the traveler profile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



# Challenge 5 – Defective documents

## Mitigation Strategy 1

- In case of failure, human fallback
- Most common mechanism in ABCs where a single officer is looking at screens from 4-6 ABCs and has to take a go/no go decision



**Desensitizes officer to possible frauds – Fatigue leads to error**



# Challenge 5 – Defective documents

## Mitigation Strategy 2

- Profile the document - Deviation List/Defect list approach

A typical workflow:

1. ePassport fails signature verification
2. Check if the country is in a list of known defective documents
3. Check if it passes Active Authentication/Chip Authentication
4. Check that the DG14/DG15 hash matches the hash in SOD. If so, declare ePassport to be good passport



# Challenge 5 – Defective documents

## Mitigation Strategy 2

- A known attack on this strategy

### What is known:

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



## Challenge 5 – Defective documents

### Mitigation Strategy 3

- Defect Handling - Modify Crypto Toolkit to verify in spite of Defect
- Requires detailed analysis of defect
- Modify Crypto Toolkit to verify in spite of the defect
- Ensure that Security is not compromised as a result of this modification



## Challenge 5 – Defective documents

### Mitigation Strategy 3

- Defect Handling – An example
- RSA signature is result of modular (division) operation
- Since it is division, value will be smaller than the divisor
- RFC requires that if length of remainder is smaller than the divisor, then zeroes to be padded in front to make it the same length

Let the divisor be  
“3B 9A CD F3”

If remainder is  
“80 4B 82”

Then result is encoded as  
“00 80 4B 82”



## Challenge 5 – Defective documents

### Mitigation Strategy 3

- Defect Handling – An example (cont'd)
  - Verification of RSA signature requires the following steps:
    - If length of signature longer than divisor, verification failure
    - If length equal to divisor, remove leading zeroes
    - Continue with computation
  - Remainder is “00 80 4B 82”
  - Divisor is “3B 9A CD F3”
  - Length is same
  - Remove leading zeroes to get value “80 4B 82”
  - Continue with the computation



## Challenge 5 – Defective documents

### Mitigation Strategy 3

- Defect Handling – An example (cont'd)

- The actual defect is ePassports issued by two countries is the addition of an extra leading zero
- Hence the length of the remainder is longer than the divisor and signature verification fails

Divisor is

“3B 9A CD F3”

Remainder is

“3A 04 4B 82”

Result is encoded as

“00 3A 04 4B 82”



## Challenge 5 – Defective documents

### Mitigation Strategy 3

- Defect Handling – An example (cont'd)

The solution to handle this defect:

- Remove the leading zeroes first
- Then compare value
- Continue with computation

Result is encoded as

“00 3A 04 4B 82”

Remove leading zeroes gives

“3A 04 4B 82”

Value smaller than divisor

“3B 9A CD F3”

Continue with computation



## Challenge 5 – Defective documents

### Mitigation Strategy 3

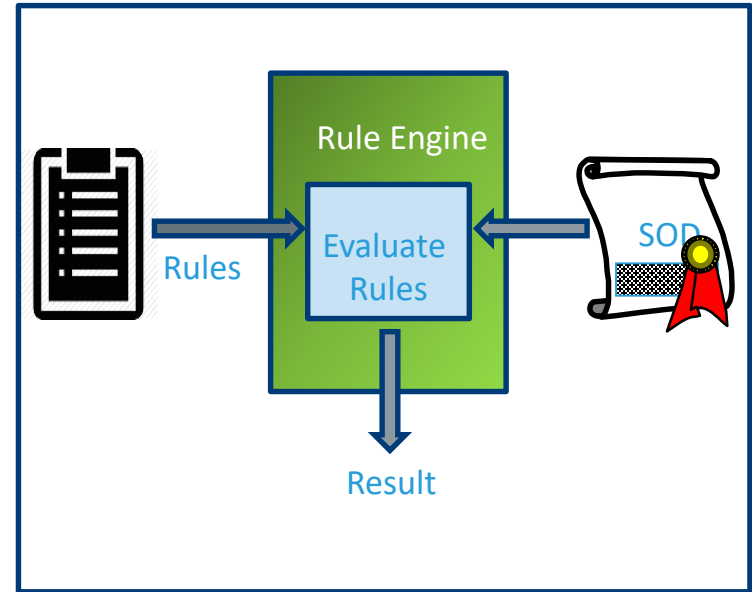
- Defect Handling – Does it work for all defects?
  - Based on our analysis, all known defects can be handled
  - We chose not to handle one defect of missing AKI
    - An AKI is the field in Document Signer that links the Document Signer to the CSCA.
    - Missing in the case of Venezuela and Somalia
  - An older defect of truncated SOD also cannot be handled



## Challenge 6 – Defining the anatomy of a fraud

- If hash comparison of DG2 fails, it is indication of substitution attack on the photo in the chip and should be considered a fraudulent document
- If hash comparison of DG11 fails, is that as serious as a DG2 hash mismatch?

**Every failure is not a fraud**





## ICBWG

- Has a non compliance sub group that analyzes defects and informs countries through ICAO state letters – rectify defect at source
- How to get in touch:

**Step 1** Send an email to the [icbwg@icao.int](mailto:icbwg@icao.int) along with a brief description of the concern and an image of the data page. For issues related to ePassports, include the SOD.

**Step 2** ICBWG will assess the reported issue and supporting information in context of the Doc 9303 standards.

**Step 3** Once confirmed, the ICBWG will contact the issuing State to lend assistance. The originator will also be advised of the outcome.



## Summary

- If you are not doing ePassport validation at border, all the investment in ePassports is a waste
- Do it right or trust in the document will be lost
- Engage with ICAO working groups to get it right



| ICAO

SECURITY & FACILITATION



## Contact Details

Name:

R Rajeshkumar

Email:

R.Rajeshkumar@Auctorizium.com