# E-Passport validation: A practical experience

R Rajeshkumar

*Implementation & Capacity Building Working Group*

Antigua & Barbuda ICAO TRIP Regional Seminar

# Note

This is an edited version of the presentation and is cleared for public dissemination

# 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
  - Check that DG hash values match the hash values stored in SOD
  - Compare DG1 with MRZ
  - Compare DG2 with printed photo and the holder

# Initial Findings

- E-Passports from 112 countries
- 55 countries have issues with LDS and/or SOD
- Roughly 45% of all E-Passports issued by these countries
- Works out to about 34% of all E-Passports presented at border

# Implications

- 1 in 3 documents cannot be verified for authenticity
- Officer cannot decide if it is a defect or a fraud
- Lowers the bar for fraudsters

# Types of defects

- EF.COM has different number of DGs from LDS/SOD
  - LDS has DG but hash missing in SOD
  - SOD has hash but no DG in LDS
  - Hash mismatch
- Structural issues with SOD
  - Some can cause certain crypto toolkits to crash
  - Cryptographic issues with SOD

# Response

- Decided to collect as much data as possible
- Rolled out to all borders – Air, Sea and Land
- Do detailed analysis on collected data

# Result

- Collected data from 117 countries
- Analyzed defects, fixed defect handling and redeployed – iterative process

# Details

- Wrong DN of Issuer in SOD
- Instead of “cn=Country DSC,  c=CC”, the DN is encoded as “c=CC, cn=Country DSC”

# Details

- DSC expires before passport
  - DSC should be valid as long as the passport is valid.
  - If not, document verification will fail

# Details

- Length Encoding issues
  - Length encoding defined by ASN.1 standards
  - Parsers will not handle wrong length encodings

# Details

- Single DSC to sign all E-Passports
  - DSCs should be changed often to prevent compromise
  - Reduces trust in the E-Passport of that country

# Details

- Missing Authority Key Identifier
  - AKI is used to identify the CSCA that issued the DSC
  - If it is missing, there is no way to complete the verification

# Details

- Country Code is wrong or missing in CSCA
  - Country code identifies the issuer
  - The code is defined in ISO 3166 and in Doc 9303

# Current status

- Handled all the possible defects and deployed
  - Except for missing AKI and missing or wrong country code for Issuer. These defects can be used to create fraudulent documents and hence will not be handled. These documents will be treated as fraudulent.
- Reading is between 4 and 7.5 seconds. Full validation takes a maximum of 200 milliseconds. Hence entire process including reading now is under 8 seconds in the worst case scenario

# ICBWG

- Since 2009, ICBWG has:
  - Monitored readability issues related to MRTDs
  - Contacted states through ICAO to highlight issues
  - Provided guidance when requested

# ICBWG

- E-Passport issues first discussed in Ottawa meeting – October 2015
- Decided to focus on:
  - Structural issues with SOD than can cause toolkits to crash
  - Cryptographic issues

# ICBWG

- Decided to get opinion from WG3/TF5 on suspected issues
  - Discussed during the Wellington meeting of WG3 – April 2016
- Outcome of WG3 meeting discussed in Den Haag – May 2016

# ICBWG

- Decided that non-compliance subgroup will expand scope to include E-Passport non-compliance/defects
- Identified three major defects to notify respective states

# Issue 1

- Caused by confusion on language in RFC 5754
- " DigestAlgorithmIdentifiers MUST omit "Null" parameters, while the SignatureAlgorithmIdentifier (as defined in RFC 3447 ) MUST include NULL as the parameter if no parameters are present, even when using SHA2 Algorithms in accordance with RFC 5754. Implementations MUST accept DigestAlgorithmIdentifiers with both conditions, absent parameters or with NULL parameters."
- SOD is encoded with parameters missing in both DigestAlgorithmIdentifier and SignatureAlgorithmIdentifier
- Passports from 5 countries have this defect

# Issue 2

- RFC 3852 defines Digest Algorithm and Signature algorithm.
- The digest algorithm is used to hash the contents of the eContent (DG Hashes), which is then used as the value in MessageDigest field in Signed Attributes.
- The signed attributes are then hashed using the same digest algorithm and then signed using the signature algorithm.
- One country uses SHA512 to hash the eContent and then uses SHA256 to hash the signed attributes.
- All crypto toolkits fail to verify this SOD – 78% of all E-Passports seen from this country

# Issue 3

- Issuer DN of Document signer as follows:
- CN = XXX CSCA,OU = Civil Registry Agency,O = Ministry of Justice of COUNTRY ,L = LOCATION ,C = AA

- Subject DN of Document signer as follows:
- CN = DOCUMENT SIGNER KEY,OU = SOMEOU,O = SOMEO,C = BB

- So, country AA has issued a Document Signer to country BB
  - When checking issuing country of passport, which country code would you choose?

# ICBWG Intent

- Not to be a compliance checking or certification lab
- Effort to improve quality of E-Passports to realize their promise
- Interested in receiving information about suspected non-compliance/interoperability issues
- ISO acts as technical consultant to ICBWG
- Contact: Abdennebi, Narjess
  NAbdennebi@icao.int

# Next steps

- The new findings (mentioned in the initial slides) will be discussed in ISO WG3/TF5
- Based on the outcome of the discussions, ICBWG will deliberate on the defects that need to be addressed
- Additional state letters will be sent out regarding these new defects

# Message

- Passport defects have to be identified and fixed to realize the real value of E-Passports
- If proper validation of the E-Passport is not done, TRIP has a whole new meaning…..

# Contact Details

Name: R Rajeshkumar
Email:
R.Rajeshkumar@auctorizium.com