Non-compliant E-Passports: Implications to Border Inspection

R Rajeshkumar

ICAO Implementation and Capacity Building Working Group (ICBWG)

Strengthening Aviation Security through Improved Traveller Identification

E-Passports: The Promise

- Assurance in the authenticity of the travel document
- Faster processing of passengers due to machine assisted verification of document
- Improved fraud detection

E-Passports: The Reality

- 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

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

Contact Details

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