9 Myths of ePassport Validation

R Rajeshkumar

ISO SC17-WG3/TF5 Leader

Myth 1
CSCAs are a secret

THE PROPOSITION

- *Sharing CSCA will compromise the security of the ePassport*

- *CSCAs should not be shared and kept a secret*

REALITY CHECK

- The ePassport trust model uses Public Key Cryptography
- It is called PUBLIC for a reason
- If you do not share your CSCA, your ePassport cannot be verified. Without the CSCA, the ePassport will be treated like a passport without a chip – A waste of your investment in ePassports
- More than 160 countries issue ePassports. Currently, only 104 of them share CSCAs.
- Please share your CSCA with others – all your CSCAs.
- Ensure that you distribute your new CSCA before your citizen turns up at a foreign border with a passport issued with the new CSCA

Myth 2
Control of private key can be outsourced

THE PROPOSITION

- *The entire CSCA can be outsourced*

- *A remote authorization is sufficient for control on the signing process*

REALITY CHECK

- The private key of CSCA is the root of trust of the country
- Anyone with access to the private key can issue an ePassport in your name
- Outsourcing brings huge benefits, but control on private key should not be lost
- There have been documented cases of passports being issued without the country's knowledge.
- Ensure control over the possession and usage of the CSCA private key

Myth 3
ePassport chip cannot be modified after issuance

THE PROPOSITION

- *The chip in the ePassport cannot be modified*

- *Data from the chip can always be trusted and no verification is necessary*

REALITY CHECK

- If the chip has been locked after personalization, the data in the chip cannot be modified
- There have been a few cases where the chip was still unlocked after issuance
- One observed fraud pattern is that the entire chip is expertly replaced by the forgers
- Another pattern observed is copying over the contents of the chip to a completely new booklet
- Passive Authentication and Clone Detection are necessary after reading the chip to ensure the authenticity and integrity of the data

Myth 4
An ePassport validation gives a binary decision

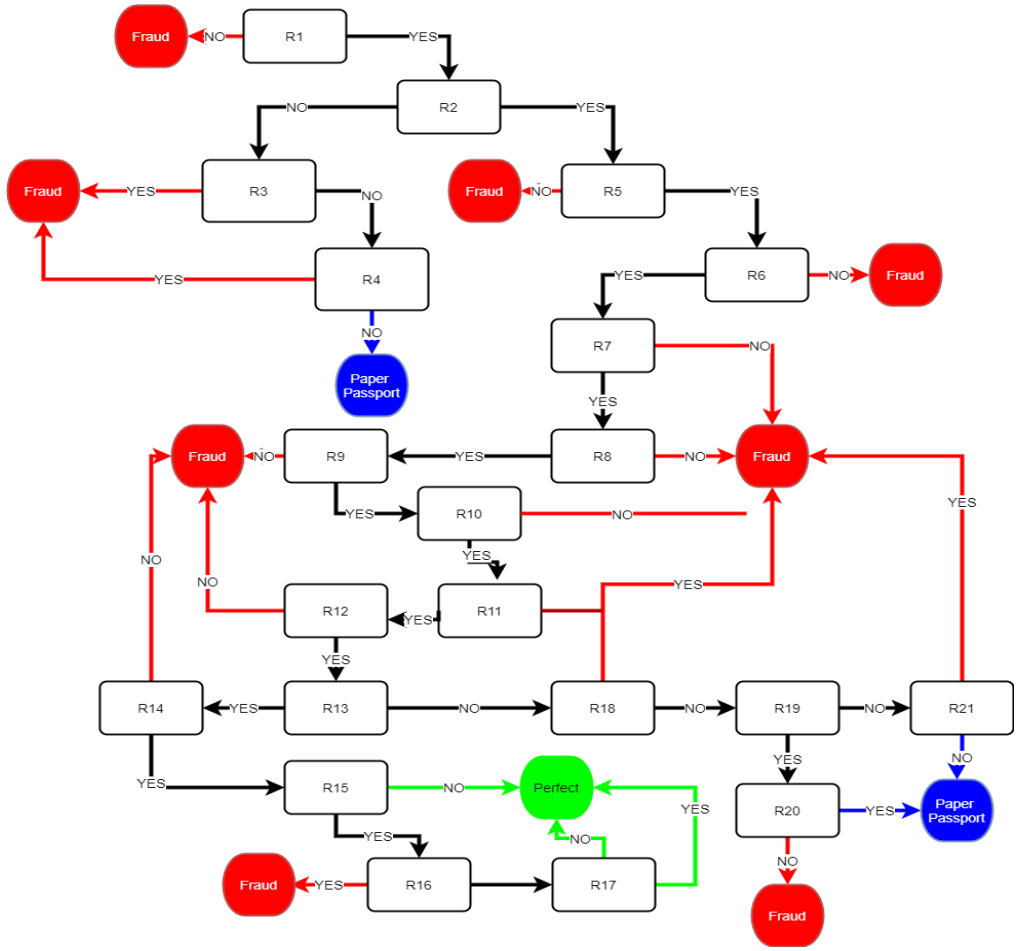
THE PROPOSITION

- *Passive authentication of the SOD is sufficient to check the authenticity of the ePassport*

- *It can only have two results – Success or Failure*

REALITY CHECK

- Proper ePassport validation is more than just Passive Authentication
- It can have about 21 different outcomes
- 16 of those are indication of a Fraud
- 3 of those outcomes indicate that the chip cannot be validated with certainty
- Only 2 of these outcomes can be accepted as being indicators of a genuine document



Myth 5
All Failures are Frauds

THE PROPOSITION

- *Any failure in validation is indication of fraud*

- *All failures must reject in the acceptance of the ePassport*

REALITY CHECK

- Many passports have defects – I have covered this in great detail in previous presentations
- These defects cause False Negatives – The passport is genuine but fails validation
- It is necessary to examine the entire document along with physical security features to determine its authenticity

Myth 6
Defect lists help with handling false negatives

THE PROPOSITION

- *If the defects in certain passport are known, these can be put into a defect list*

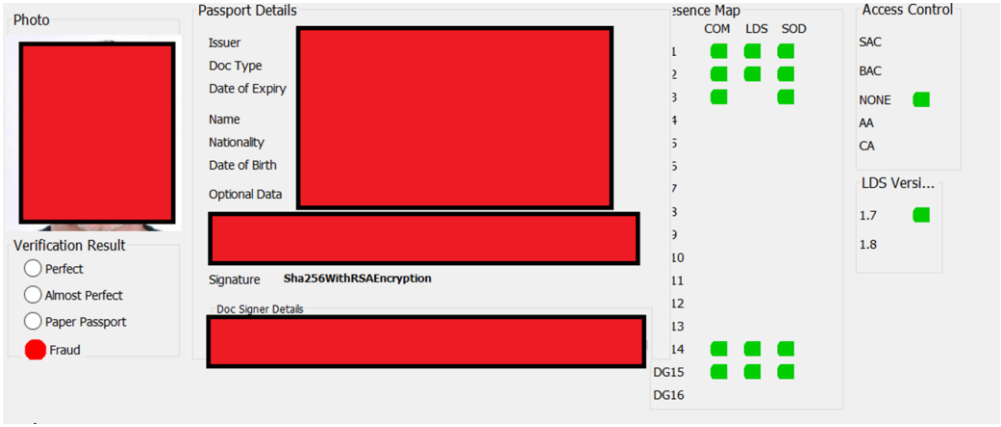
- *Any failing passports can be checked against the list for the failure reason and then accepted*

REALITY CHECK

- Fraudulent documents are being created to mimic the same result as a defective document
- There is no way for the border control officer to differentiate between a defective document and the fraudulent document

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



Myth 7
It is not possible to validate defective documents

THE PROPOSITION

- *It is not possible to do a Cryptographic Verification of defective documents*

- *False negatives cannot be eliminated*

REALITY CHECK

- All known defects can be handled with proper analysis and coding.
- It is possible to completely validate all known defects

An example:
The SOD claims that the hashing algorithm used for creating the hash of the Data groups is SHA1
But in reality the hashing algorithm used is SHA256 – Hence Passive Authentication fails

The solution:
Each hashing algorithm has a fixed length
Look at the length of the hashed output –Use the hashing algorithm associated with that length

Myth 8
Defects lead to frauds

THE PROPOSITION

- *Defects in documents allows fraudsters to modify the document*
- *This allows them to hide alterations to the document*
- *Defective documents must always be considered to be frauds*

REALITY CHECK

- It is just as impossible to modify a defective document as it is to modify a good document
- The main mechanism of fraud is officer fatigue
- If the officer sees a lot of false negatives, he is not in a position to identify the real negative
- Defect management should be implemented to eliminate false negatives – Any failure after that is an indication of attempted fraud

Myth 9
Only fully compliant documents can be verified

THE PROPOSITION

- *If a document has some deviation from the specifications, it cannot be verified*

- *Only a 100% compliant document can be verified*

REALITY CHECK

- The different profiles defined in the specifications have definitive functionality associated with them
- The verifier needs to determine which ones are crucial for verification

An example:
Subject - *countryName. MUST be present. The value contains a country code that MUST follow the format of two-letter country codes, specified in Doc 9303-3.*

Issuer Alternate Name - *if this country code does not uniquely define the issuing State or organization, the attribute stateOrProvinceName SHALL be used to indicate the ICAO assigned three-letter code for the issuing State or organization*

Only current use case is China, Hong Kong and Macau, which all use the same country code for China. The Issuer Alternate Name does not matter for other countries

A Takeaway Message

If your border control system has never detected a fraudulent document based on chip data, there is something wrong in the implementation

No News is not always Good News

Thank you!

R.Rajeshkumar@auctorizium.com