E-Passport validation: A practical experience

R Rajeshkumar

Implementation & Capacity Building Working Group

Hong Kong ICAO TRIP Regional Seminar

Note

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

Core Concepts

- Hashing
  - A Mathematical process applied to the process
  - Output is called a Message Digest
  - Input cannot be recreated from the output – hence one way function
  - Same input always gives the same output
  - Any change in input changes the output
  - Ensures that message is not tampered

Core Concepts

- Digital Signature
  - A process of encryption
  - Message cannot be decrypted using the key used for encryption
  - The two keys have a mathematical relationship with each other and form a unique pair
  - You keep one part of the key with you – private key
  - You distribute the other key to others – public key
  - You encrypt message with private key and send the message to others
  - If they can decrypt with your public key, then the message originated from you and has not been modified – Digital Signature

Core Concepts

- Message signing
  - First hash the message using a well known hashing algorithm to create a message digest
  - Encrypt the message digest using your private key
  - Send the message and the encrypted hash to recipient
- Signature Verification
  - Decrypt the encrypted hash using the public key of the sender. This gives you the message digest.
  - Hash the received message to create a new message digest.
  - If the two match, then the message is from the sender and has not been modified
  - If the decryption of the encrypted hash fails or the message digests do not match, then the message has been modified in transit

Core Concepts

- Public key
  - Public key used to sign messages (Document Signer) must be renewed regularly to avoid compromise
  - To avoid having to distribute these keys every time you renew them, you use a Master Public Key(Country Signer) to sign the Document Signer
  - Distribute Country Signer to recipients
  - Include the Document Signer with your message

Core Concepts

- E-Passport
  - Data groups defined to hold messages
    - DG1 is a copy of the MRZ
    - DG2 holds the image of the passport holder
    - 16 such data groups for different pieces of information
  - Store the Data Groups on chip – “Logical Data Structure (LDS)”
  - Hash each datagroup
  - Encrypt all the hashes with your private key (Document Signer Certificate (DSC)) and store in the “Document Security Object (SOD)” – Store the SOD on the chip along with DSC

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 – create a document that has the same defect as a well known document instead of trying to create a perfect document

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

- Collected data from 127 countries and 3 organizations
- Analyzed defects, fixed defect handling and redeployed – iterative process
- Major defects outlined in the next few slides

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 9 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?
- One country has E-Passports with this defect

Issue 4

- Wrong DN of Issuer in SOD
- Instead of “cn=Country DSC, c=CC”, the DN is encoded as “c=CC, cn=Country DSC”
- 11 countries have issued documents with this defect

Issue 5

- DSC expires before passport
  - DSC should be valid as long as the passport is valid.
  - If not, document verification will fail
- 7 countries have issued ePassports with this defect
- 2 countries have this defect with a majority of documents they have issued – has been corrected now but there are still a significant number of documents in circulation with this defect.

Issue 6

- Length Encoding issues
  - Length encoding defined by ASN.1 standards
  - Parsers will not handle wrong length encodings
- One country has issued a batch of e-Passports with this defect

Issue 7

- Single DSC to sign all E-Passports
  - DSCs should be changed often to prevent compromise
  - Reduces trust in the E-Passport of that country
  - E-Passports from these countries will be treated as paper passports
- 5 countries have this defect

Issue 8

- 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
  - These E-Passports will be treated as paper passports
- 4 countries have this defect with all the E-Passports that they have issued

Issue 9

- Country Code is wrong or missing in CSCA
  - Country code identifies the issuer
  - The code is defined in ISO 3166 and in Doc 9303
  - Proper validation will flag these documents as fraudulent documents
- 10 countries have issued E-Passports with this defect

Issue 10

- Wrong encoding of RSA signature value
  - RSA signature is encoded as OctetString with length of string equal to Modulus value
  - Assumed to be positive integer. Hence do not need to add 0x00 in front to make the value positive in two's complement encoding
  - 0x00 added in front of Signature value making the signature value longer than modulus
  - All tookits that we have tested flag these E-Passports as fraudulent documents
- 2 countries have this defect – in the case of one of them, 60% of all e-Passports issued by that country has this defect

Issue 11

- Document Signer has CA bit set
  - CA bit identifies Country Signer
  - Document Signer is not country Signer and should not have this bit set
  - Setting CA bit in Document Signer breaks path validation of the SOD
  - E-Passports with this defect as treated as paper passports
- 5 countries have this defect

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
- Decided to notify respective states through ICAO state letters

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

Intended Target – Border Control Agencies

- Countries not validating E-Passports at border
  - Waste of all the investment in E-Passports.
  - No excuses – Validation can be done and it does not slow down border control process
- Countries attempting to validate E-Passport and having issues
  - You are not alone. ICBWG can help. Please get in touch with us.
- Countries doing E-Passport validation and have never seen any defects
  - Not possible. Check your E-Passport validation solution!

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