TRIP2017

Traveller Identification Programme

Regional Seminar Montego Bay

E-Passport Validation: A practical experience

R Rajeshkumar

International Organization for Standardization (ISO)

ICAO TRIP: Making the Air Travel more Secure and Efficient

TOWARDS A BETTER TRAVELLER IDENTIFICATION MANAGEMENT

FOR ENHANCED BORDER CONTROL INTEGRITY

Note

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

Three key areas

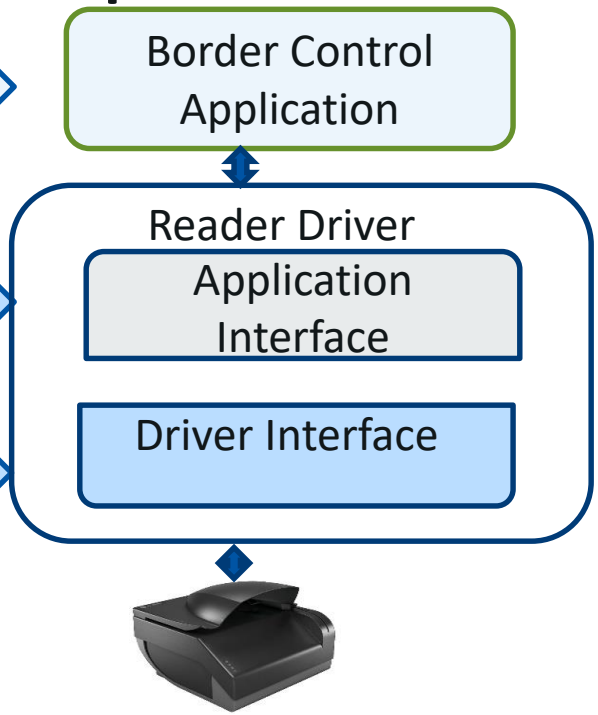
- Architecture
- Defect Handling
- Human Interface

Architecture Components

Visa Lookup
Hotlist lookup
Biometric Matching

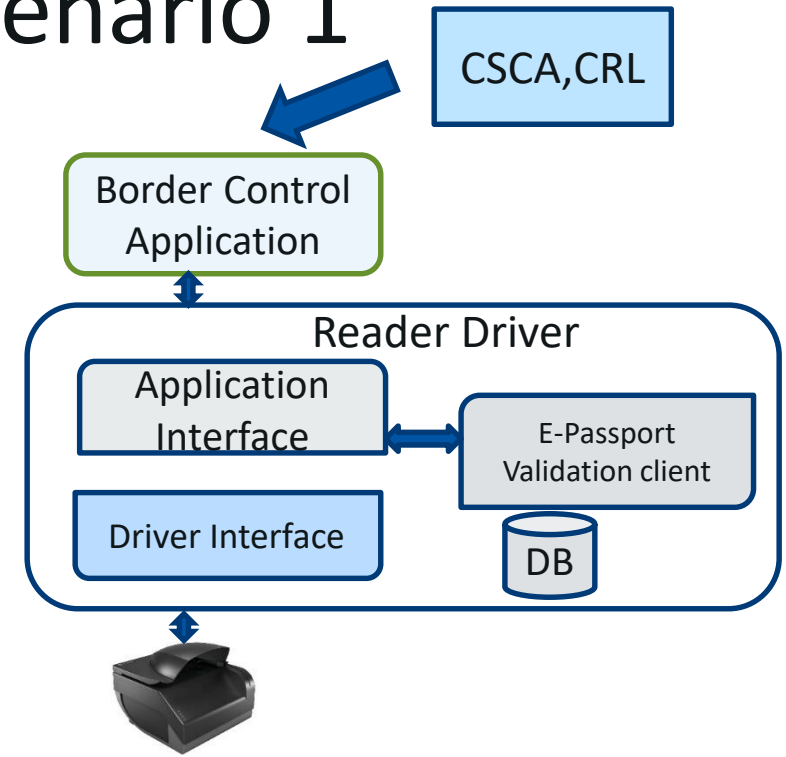
Interface used by applications to communicate with reader

Interface used by Reader Driver to communicate with reader



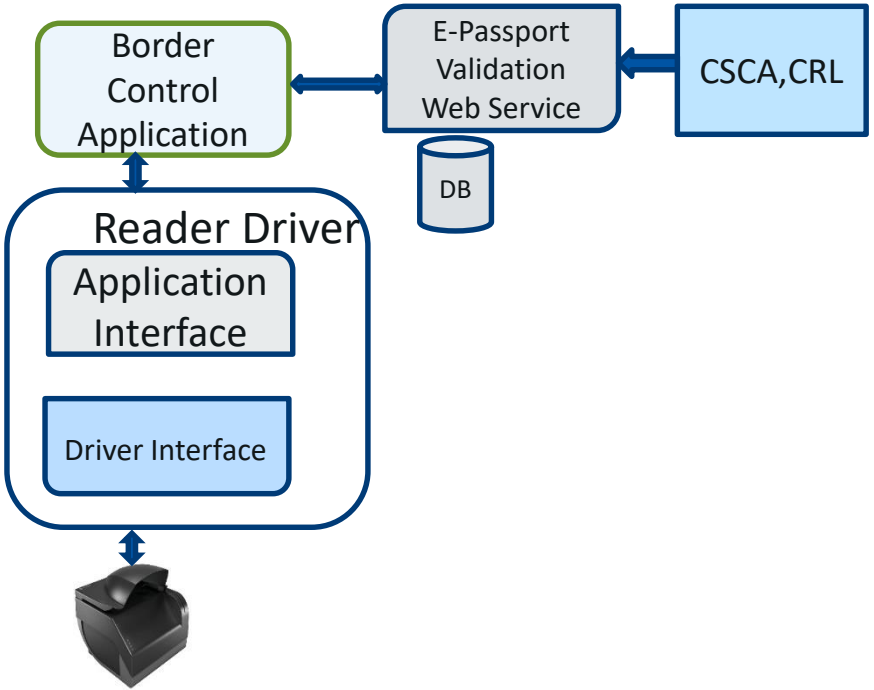
For E-Passport Validation, there are typically three deployment scenarios

Scenario 1



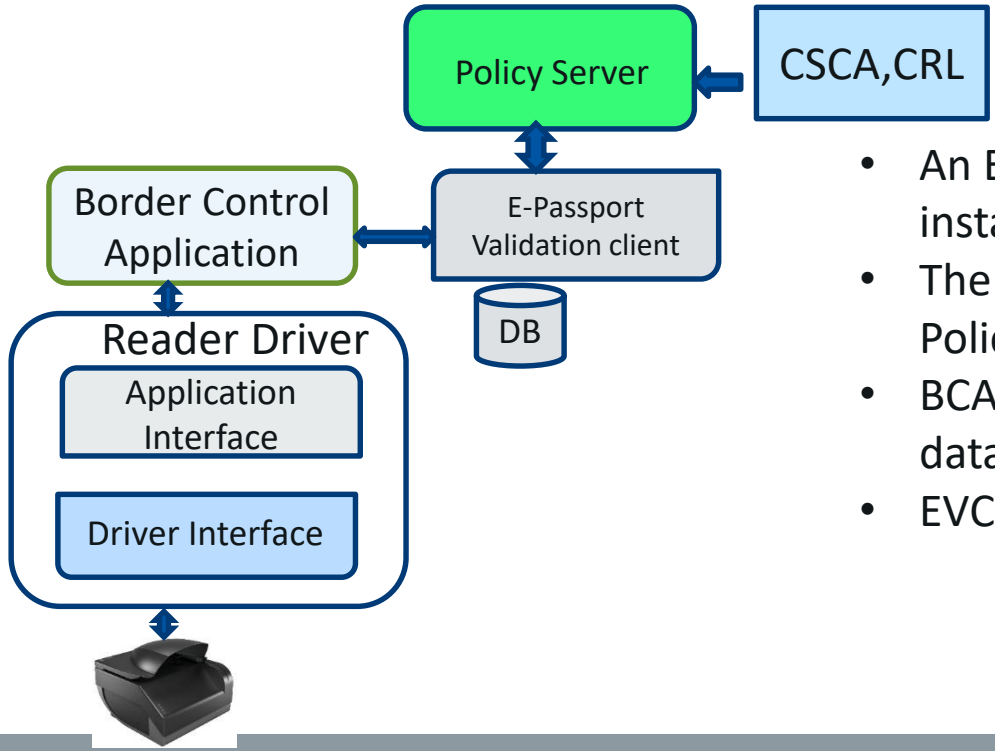
- E-Passport Validation Client (EVC) is built in to the reader driver
- The Border Control Application(BCA) fetches the CSCAs and CRLs and updates the reader driver, which stores these in a local DB
- BCA uses function call to get status of verification of E-Passport

Scenario 2



- E-Passport Validation is done by a web service, which has the necessary CSCA/CRLs for the validation
- BCA uses the reader driver to read the LDS and SOD and sends it to the Web Service
- Result is returned to the BCA by the Web Service

Scenario 3



- An E-Passport Validation Client (EVC) is installed along with the BCA.
- The EVC gets the CSCAs and CRLS from a Policy Server
- BCA reads LDS and SOD and calls EVC with data
- EVC returns the result to the BCA

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

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

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?

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”
- 14 countries have this issue

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 a small number of passports with this problem.
- 1 country – 65% of all documents issued

Issue 6

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

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
- Currently 5 countries

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

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
- 10 countries have this issue

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
- Currently two countries

Issue 11

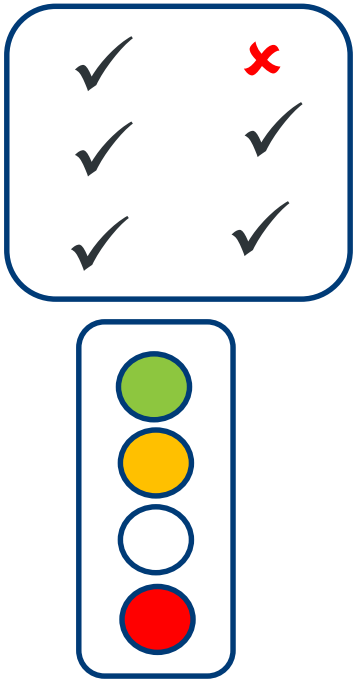
- Document Signer has CA bit set
  - CA bit identifies Country Signer
  - Document Signer is not country Signer and should not have this bit set
  - Setting CA bit in Document Signer breaks path validation of the SOD
- 5 countries

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

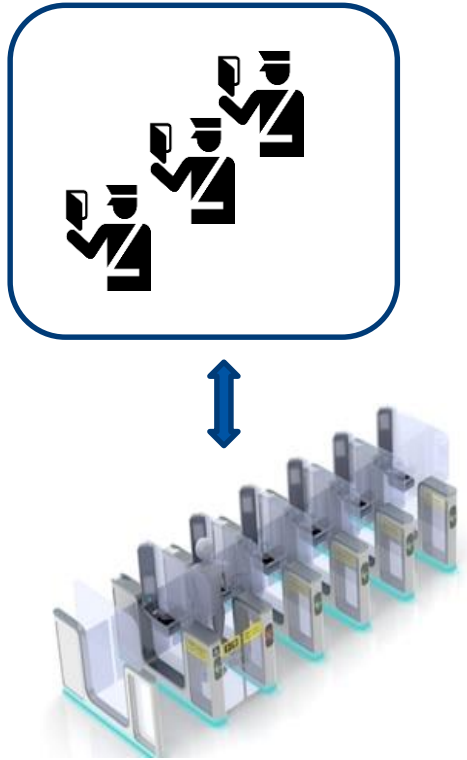
Interface

- Too much data on screen confuses officers
- Better to map outcomes to confidence levels



Interface

- Relevance for ABCs
  - In case of success, it is an automatic response.
  - In case of failure, the fallback is a human being



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.

Summary

- Different deployment scenarios for E-Passport validation
- Architecture, defect handling and human interface are important considerations
  - Plan your own implementation. Don’t copy
  - Continuous improvement necessary
- Plan for failure – plan the fallback
- Engage with ICAO working groups to help you

Contact Details

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