International Civil Aviation Organization

Eighth Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards

ICAO Headquarters, Montréal, Canada
10 - 12 October 2012

VALIDATING E-PASSPORTS AT THE BORDER: THE ROLE OF THE PKD

R RAJESHKUMAR

CHIEF EXECUTIVE

AUCTORIZIUM PTE LTD

THE TRUST IMPERATIVE

E-Passports are issued by entities that assert trust

Trust depends on the requirements of the relying party – Border Control of foreign countries

E-Passports are Passports with a chip. The chip augments the security of the Passport, it does not replace it.

Improper validation of E-Passport leads to a “false” sense of security.

WHAT DOES CHIP CONTAIN?

Chip contains Logical Data Structure (LDS) with 16 Data Groups (DGs).

- DG1 contains the contents of the MRZ - mandatory
- DG2 contains photograph of the holder - mandatory
- DG3 contains fingerprint biometric – Optional
- … and so on

Chip contains Security Data Object (SO_D)

- Contains hash of the Data Group present in LDS
- Contains a signature that encapsulates the stored hashes.

VALIDATING CONTENTS OF CHIP

Extract each DG from LDS and hash it. Compare with hash stored in SO$_D$

If all hashes match, then verify signature of SO$_D$ using the Document Signing Certificate (DSC) used to sign the SO$_D$

- DSC may be available on chip
- If not, DSC must be received from Issuing Authority

VALIDATING CONTENTS OF CHIP

If signature passes, verify DSC using Country Signing Certificate Authority (CSCA)

- CSCA must be received from Issuing Authority

If DSC is verified, check Certificate Revocation List (CRL) to check if DSC and CSCA are still valid

- CRL must be received from Issuing Authority
- CRL checking is blacklist checking

VALIDATING CONTENTS OF CHIP

IF ALL STEPS SUCCEED, THEN CHIP IS NOT TAMPERED – HOWEVER THIS IS NOT THE END OF THE VALIDATION.

DG1 must match MRZ of the passport

DG2 must match the face of the holder

AT THIS POINT, FULL ASSURANCE OF INTEGRITY OF DOCUMENT

VALIDATION ISSUES

DSC may not be on chip and not available through diplomatic means

CRL may not be available or may not be latest

CSCA exchange may not have been done with that country

So, can you trust the E-Passport?

TRUST LEVELS

Ideally, entire process must be completed. In real life, “ideally” does not exist.

Treat E-Passport validation as a series of increasing confidence in the validity of the document.

TRUST LEVELS

- 🟩 DSC is in whitelist – Pre-approved DSCs
- 🟩 CSCA and DSC verified against CRL
- 🟩 DSC verified against CSCA
- 🟨 Signature Verification successful
- 🟨 DG hash compare successful
- 🟥 Any check fails

PRE-APROVED DSC

Reliability of DSC

- Any certificate issued under the CSCA can sign a document
- Document Signer - has intent and authorization to sign travel documents

Receive list of DSCs used to sign passport from the Issuing Authority – White List of Document Signers.

OPERATIONAL ISSUES

Getting a white list of Document Signers from all E-Passport Issuing agencies

- DSCs are issued at least every three months by 70 Passport issuers. Bilateral Exchange is complicated and time consuming

CRL distribution

- CRLs are issued at least once every 90 days. Some Issuers are issuing CRL every 48 hours.
- If there is a compromise, an emergency CRL will be issued between the regular updates.

CSCA distribution

- Diplomatic channels may not be in place to exchange CSCAs in time

OPERATIONAL ISSUES

Issuing Authority Contacts

- If a batch of passports fail validation, the Issuing Agency must be contacted to check on this. There is no “Address Book” which lists all the addresses of the Passport Issuers and their contact details.

Compliance to Doc 9303

- Certificate Profile has 18 fields
- With the different values allowed per field, total permutations possible is not manageable
- Managing the consequences of the various permutations is not practical
- Best if all issuers followed a single profile – Need a reference implementation and control

THE PUBLIC KEY DIRECTORY

Single repository of “validated” DSCs and CRLs

Repository of Master Lists published by Participants

CSCA Registry – Yellow Pages for the Passport Issuance Agency of the Participant

Compliance reference for DSC/CRL/ML against Doc 9303

MASTER LIST

- For CSCA Exchange:
  - If all countries published the list of CSCAs that they have received, comparison and validation can be done
  - CSCA Master List

Country C

- Country A

- Country B

Country A ML

- Country A

- Country B

- Country C

Country B ML

- Country A

- Country B

- Country C

- Country D

OTHERS HAVE THE SAME CSCA

If we trust Country B, then we can use Country D CSCA at border

STRUCTURE OF THE PKD

Country upload point – a mailbox for Passport Issuers to upload their DSC, CRL and Master List

An internal process of validation and due diligence

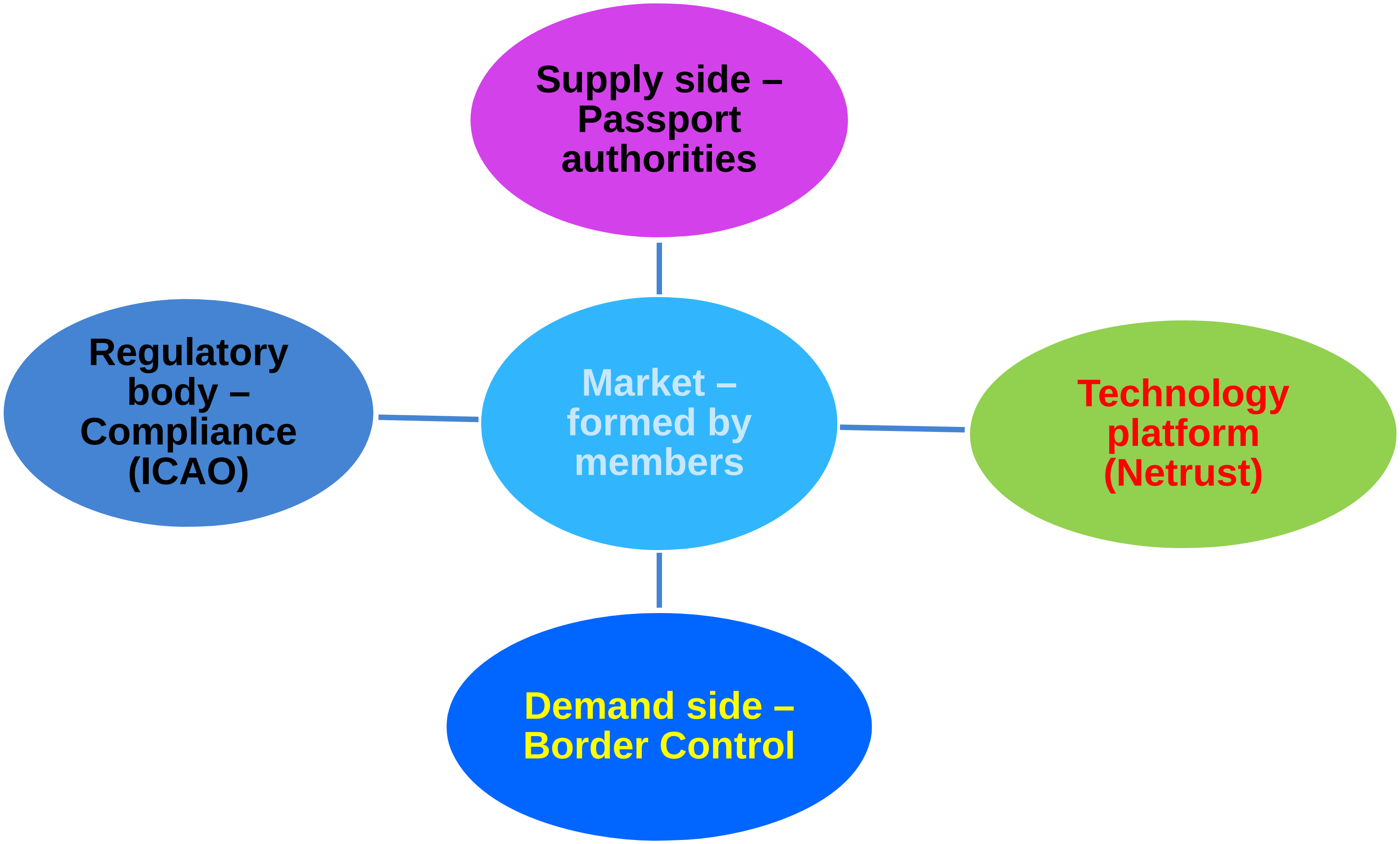
A Download directory where validated entries are available for download

ICAO PKD

AUCTORIZIUM

NETRUST

STRUCTURE OF THE PKD


Supply side – Passport authorities

Regulatory body – Compliance (ICAO)

Market – formed by members

Technology platform (Netrust)

Demand side – Border Control

COMPONENTS OF THE PKD

Two locations – connected through redundant MPLS connection – Synchronised in real time

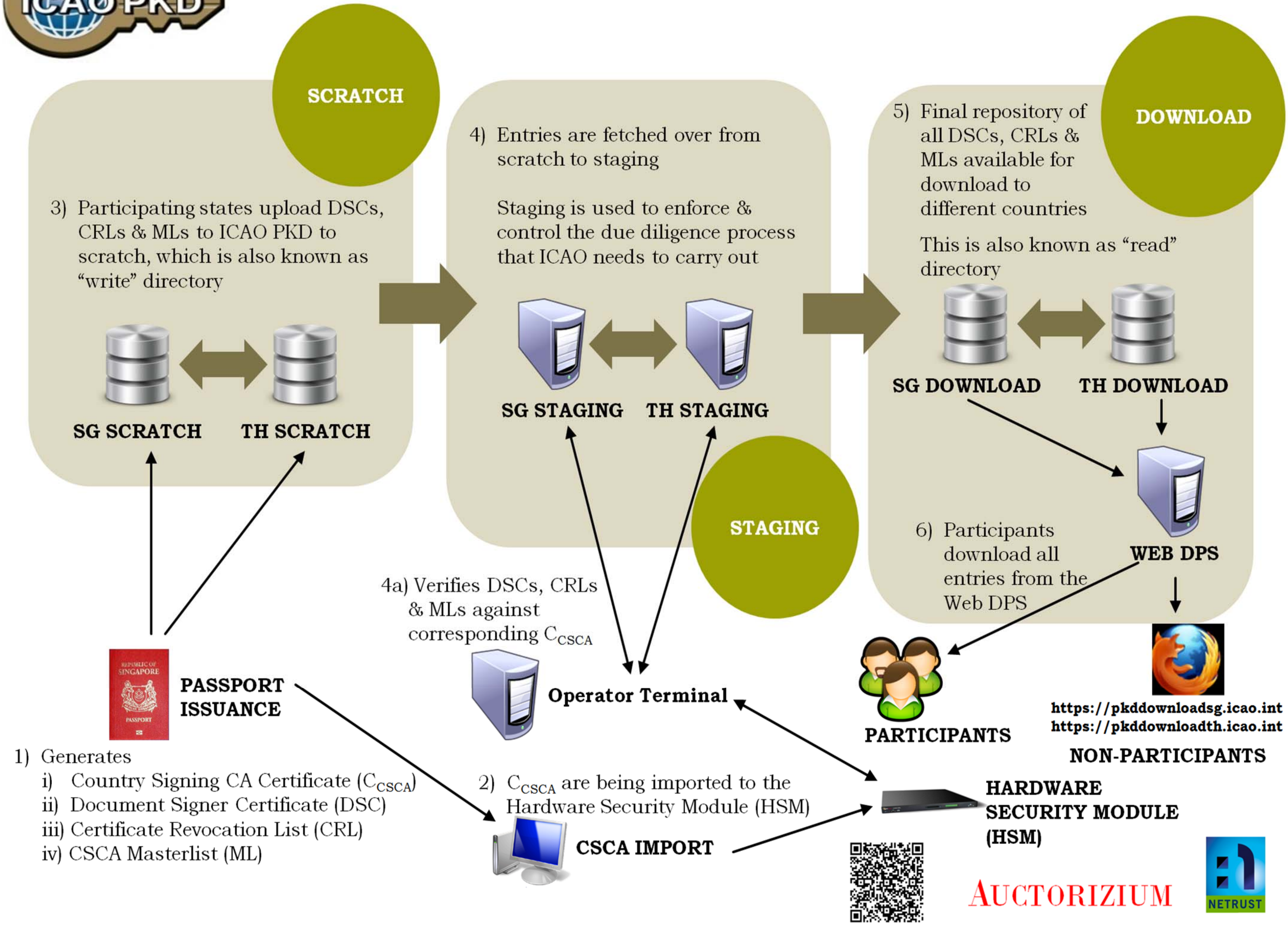
4 directories each location + 2 backup directories

Upload is the only directory that can be accessed by the internet. Copy of data from Upload to Staging directory handled by software

Montreal Operations office

- Can only connect to Netrust datacenter through VPN
- CSCAs of Participants are maintained in HSM

ICAO PKD



3) Participating states upload DSCs, CRLs & MLs to ICAO PKD to scratch, which is also known as "write" directory

4) Entries are fetched over from scratch to staging

Staging is used to enforce & control the due diligence process that ICAO needs to carry out

5) Final repository of all DSCs, CRLs & MLs available for download to different countries

This is also known as "read" directory

6) Participants download all entries from the Web DPS

4a) Verifies DSCs, CRLs & MLs against corresponding C_{CSCA}

1) Generates
   i) Country Signing CA Certificate (C_{CSCA})
   ii) Document Signer Certificate (DSC)
   iii) Certificate Revocation List (CRL)
   iv) CSCA Masterlist (ML)

2) C_{CSCA} are being imported to the Hardware Security Module (HSM)

NON CONFORMANT ENTRIES

A Participant’s CSCA, DSC or CRL may not be compliant to Doc 9303

There are valid passports in circulation issued using these non-conformant credentials and cannot be ignored

PKD allows for the publishing of non-conformant entries

PUBLISHING OF ENTRIES

The PKD board has approved a list of Machine Readable Error Codes (MREC) to list the deviations in the CSCA, DSC or CRL.

All entries with deviations are published along with MREC to allow downloading entities to differentiate the entries and decide whether to accept them at border or not in an automated fashion.

PUBLISHING OF ENTRIES

The intent is to allow all entries into the PKD, while ensuring that all Participants will eventually be fully compliant to Doc 9303.

DOWNLOADING OF ENTRIES

Web based access – anybody can download

- only complete ldif can be downloaded.

Participants use LDAP access to download

- Either full LDIF or can do ldap query.
- Authentication is username+password over SSL
- Main concern is quality of service, not access control

DOWNLOADING OF ENTRIES

Accessible at

- https://pkddownloadsg.icao.int
- https://pkddownloadth.icao.int

Script prevention measures in place

Version number is listed and file is available for download

Checksum available at

- https://pkddownloadsg.icao.int/ICAO/pkdChksum.jsp
- https://pkddownloadth.icao.int/ICAO/pkdChksum.jsp

Soon, law enforcement of non-Participants will be able to automate download as well

VENDOR TEST BENCH

Available to any vendor interested in implementing the PKD interface.

A one time charge of US$9,600

Allows for access and support for 6 months for implementing the PKD interface and allows access to Doc 9303 compliance tool.

If Interface Specifications change, registered vendors will get another 6 months of access for free.

Currently five registered vendors:

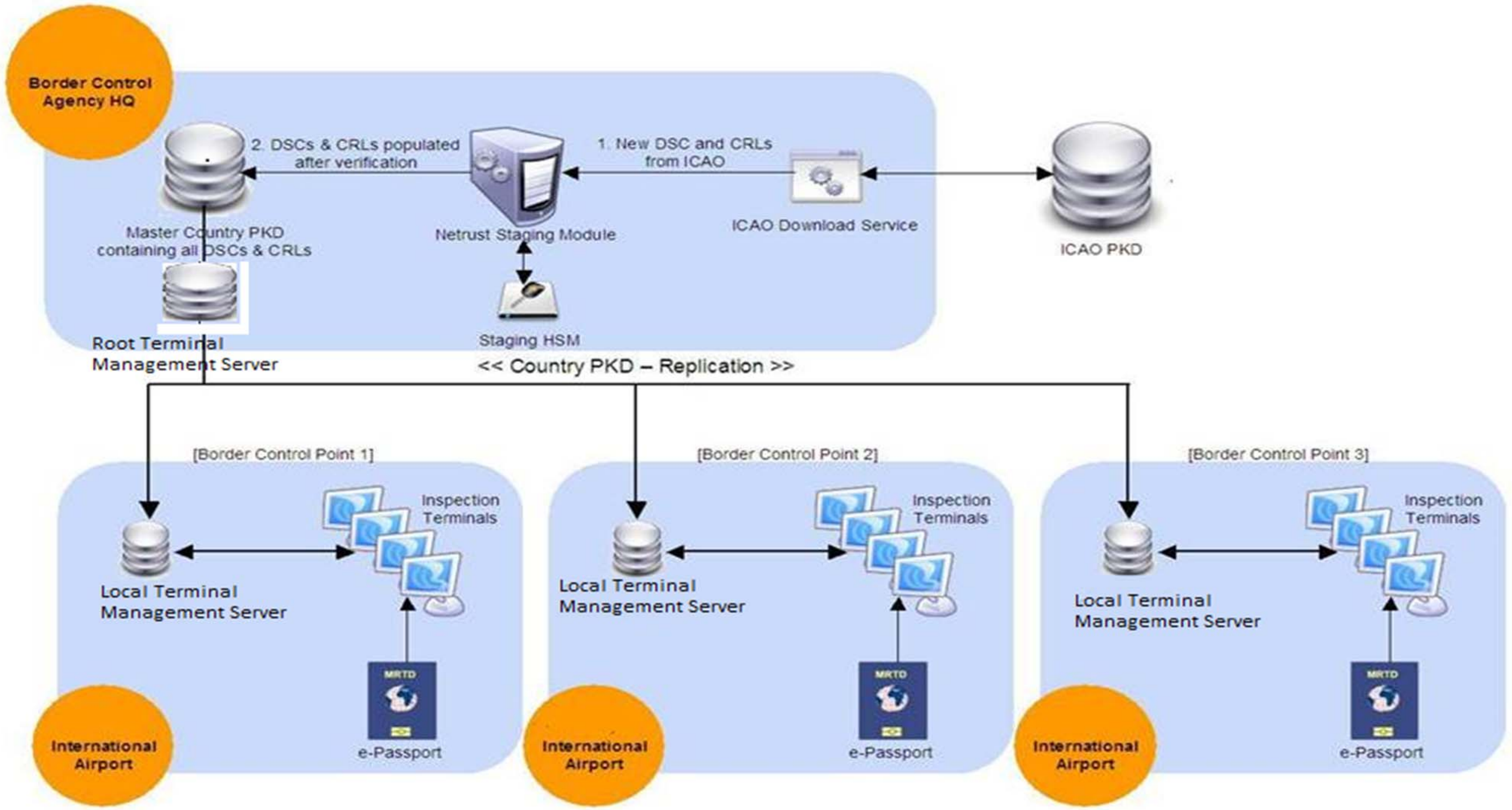
- Entrust, Bundesdrukerei, Primekey, IRIS/Digicert, Oberthur

PKD ADVANTAGES

- Authoritative source of validated DSCs and CRLs
- Authoritative source of country CSCAs through CSCA master list
- Yellow pages for contacting the Passport Issuing agency of each Participant
- A reference for compliance to Doc 9303 for Certificates and CRLs
- Defect lists are being discussed and might soon be a part of the PKD

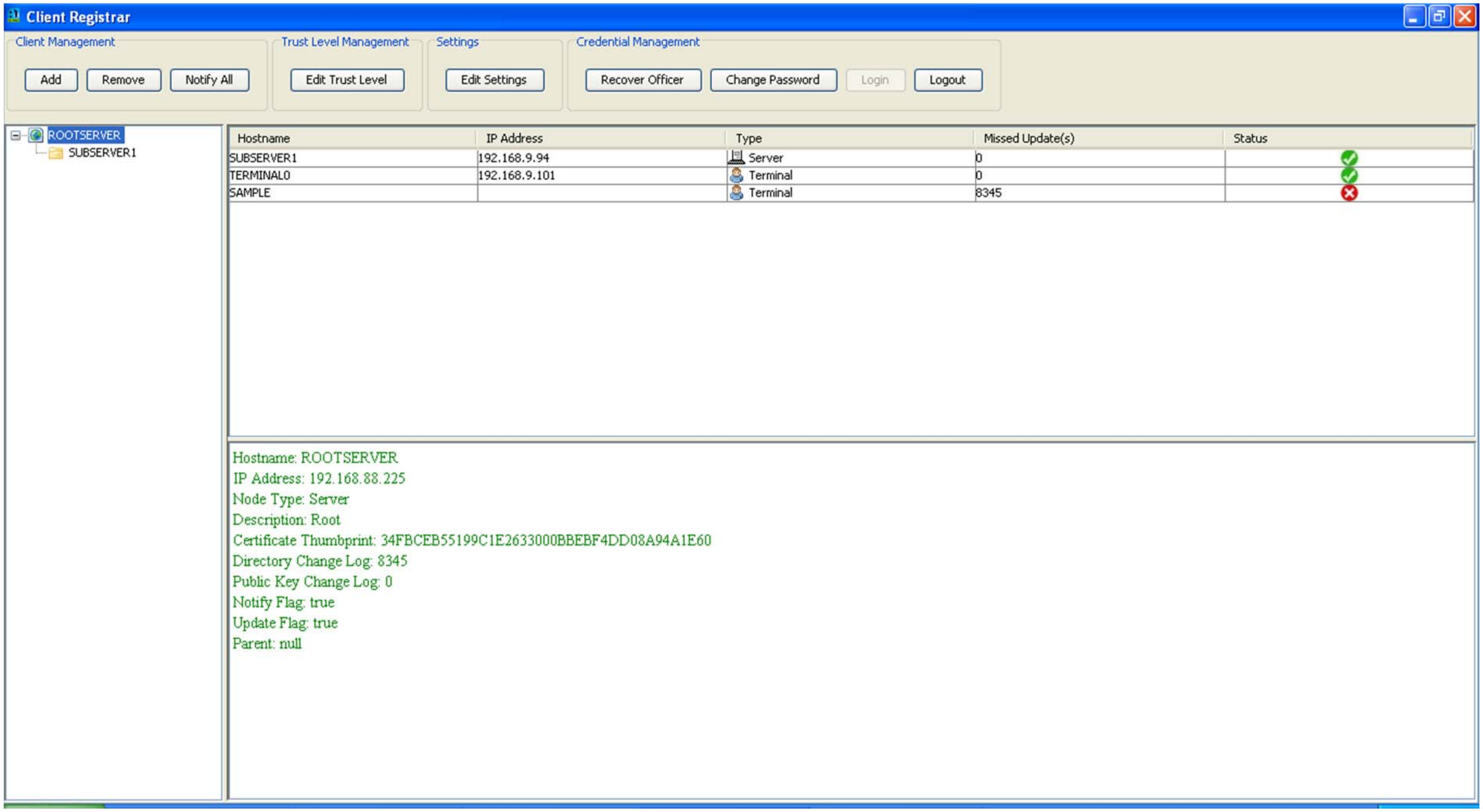
OTHER CONSIDERATIONS AT BORDER

DSC, CRL and CSCA must be available at each terminal



OTHER CONSIDERATIONS AT BORDER

All Terminals must be up to date with CRL at least



Hostname	IP Address	Type	Missed Update(s)	Status
SUBSERVER1	192.168.9.94	Server	0	✓
TERMINAL0	192.168.9.101	Terminal	0	✓
SAMPLE		Terminal	8345	✗

Hostname: ROOTSERVER
IP Address: 192.168.88.225
Node Type: Server
Description: Root
Certificate Thumbprint: 34FBCEB55199C1E2633000BBEBF4DD08A94A1E60
Directory Change Log: 8345
Public Key Change Log: 0
Notify Flag: true
Update Flag: true
Parent: null

TRUST LEVEL

Too Many Error Codes can confuse officer

Concept of mapping error codes to trust level

5 trust levels

- -1 – Forged document
- 0 – Not an E-Passport
- 1 – Document okay but full validation not possible
- 2 – Document okay and fairly confident about document integrity
- 3 – Document integrity guaranteed

THANK YOU

R Rajeshkumar

E-mail: R.Rajeshkumar@auctorizium.com

rraj88@gmail.com