INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO Regional Seminar on MRTDs, Biometrics and Border Security

30 November - 2 December 2011
Singapore

ICAO Public Key Directory

R Rajeshkumar
Deputy Chief Executive
Netrust 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

Trust Decisions

- Verification of signature on passport validates that data in chip has not been tampered
- Does not automatically guarantee who put in the data
- Path Validation of the signing certificate crucial to ensuring the identity of the issuer

Trust Decisions

- For path validation:
  - Trusted 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

OTHERS HAVE THE SAME CSCA

Trust Decisions

- For path validation:
  - Check CRL as part of signature validation
  - Receive latest CRL from country on a regular basis
  - If country publishes CRL on a web site, check that site frequently

Trust Decisions

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

Trust Decisions

- Sources of DSC
  - Receive through bilateral exchange – exchange mechanism needs to secure
  - Harvest from passports presented at Border

Trust Decisions

- Compliance to Doc 9303
  - Certificate Profile has 18 fields
  - With the different values allowed per field, total permutations possible is almost as large as the US Debt!!
  - Managing the consequences of the various permutations is not practical
  - Best if all issuers followed a single profile

Trust Decisions

- Compliance to Doc 9303
  - TF5 has prepared a guidance document detailing the mandated requirements of the attributes of CSCA, DSC, CRL and Master List.
  - Current observation – at least 40% of all issuers are non compliant, some seriously so…….

Trust Decisions

- Other considerations
  - Since E-Passports are “difficult” to forge, find the easy target – an insider.
  - A Country may try to issue valid travel documents in the name of another country.. We saw this in Paper Passports, not impossible in E-Passports.
  - If we need to contact the Issuing Agency for a specific Passport, do we know how to contact them?

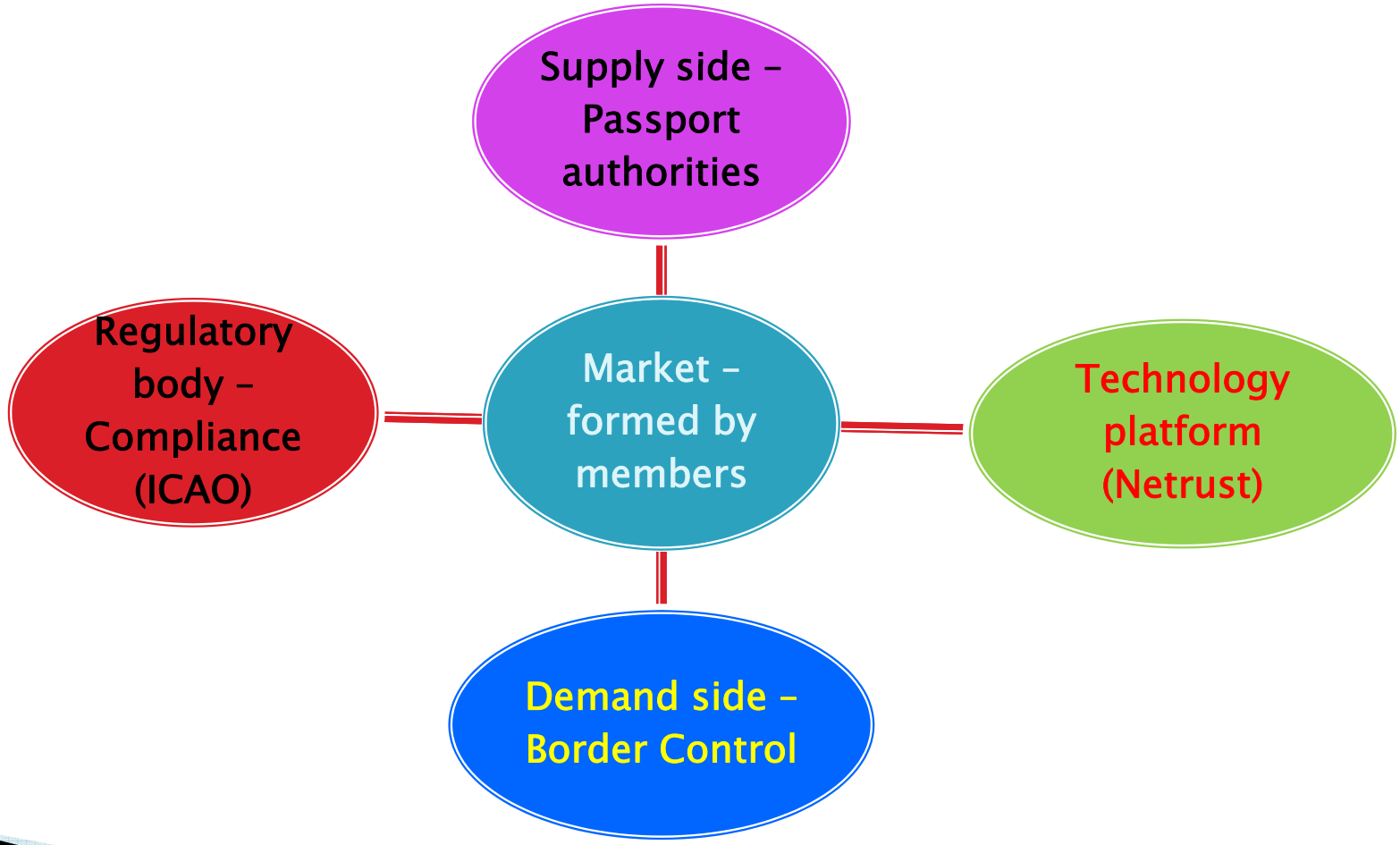
Role of the PKD

- 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

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

Structure of the PKD

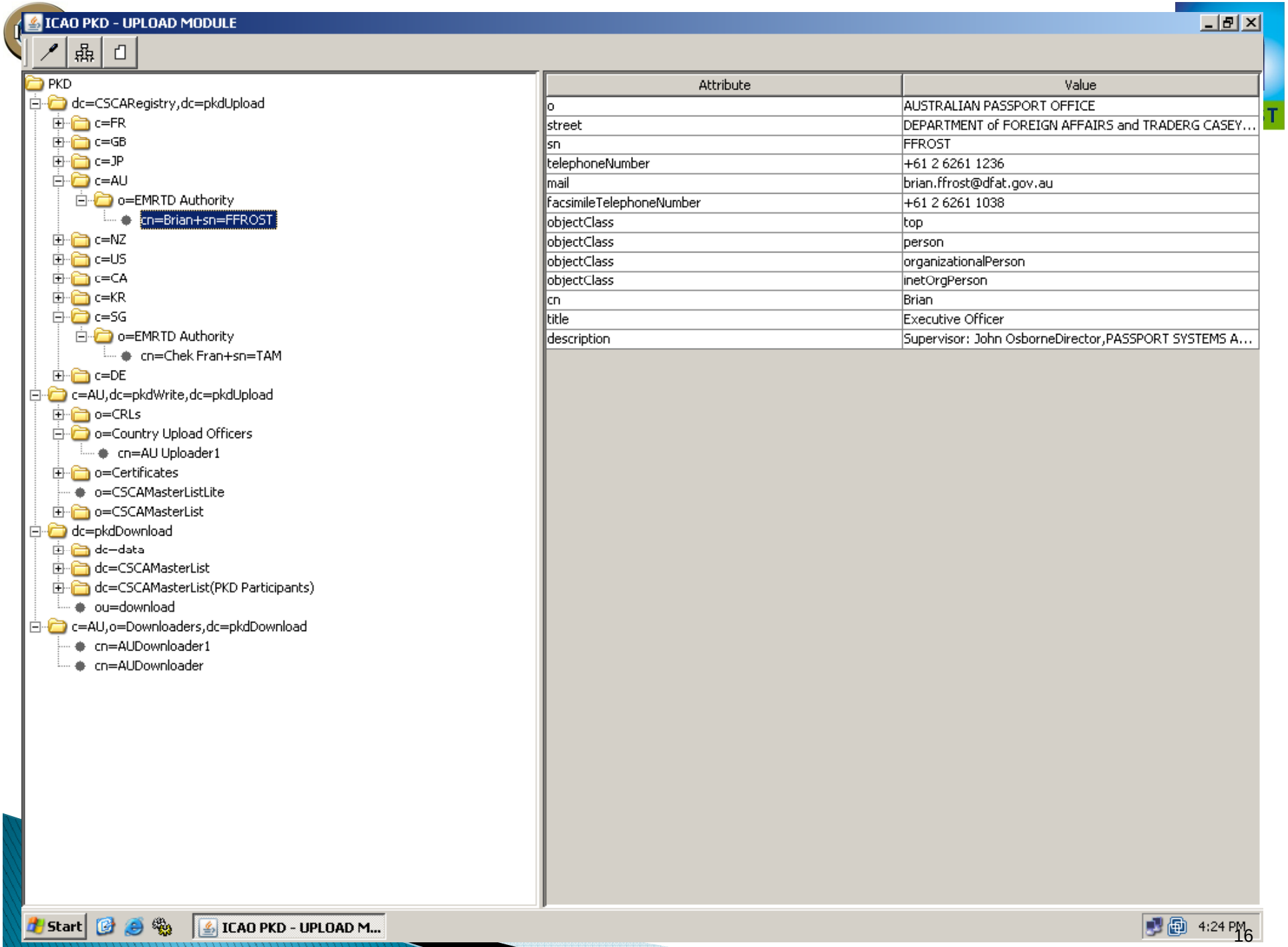


Components of the PKD

- 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

Workflow of the PKD

- Import of CSCA into HSM at Montreal – a ceremonial process
- Upload of DSC/CRL/Masterlist by participant
- Verification and Approval
- Publish to live
- Download – Participant and non-participant


ICAO PKD - UPLOAD MODULE
PKD
dc=CSCARegistry,dc=pkdUpload
c=FR
c=GB
c=JP
c=AU
o=EMRTD Authority
cn=Brian+sn=FFROST
c=NZ
c=US
c=CA
c=KR
c=SG
o=EMRTD Authority
cn=Chek Fran+sn=TAM
c=DE
c=AU,dc=pkdWrite,dc=pkdUpload
o=CRLs
o=Country Upload Officers
cn=AU Uploader1
o=Certificates
o=CSCAMasterListLite
o=CSCAMasterList
dc=pkdDownload
dc=data
dc=CSCAMasterList
dc=CSCAMasterList(PKD Participants)
ou=download
c=AU,o=Downloaders,dc=pkdDownload
cn=AUDownloader1
cn=AUDownloader
Attribute
Value
o
AUSTRALIAN PASSPORT OFFICE
street
DEPARTMENT of FOREIGN AFFAIRS and TRADERG CASEY...
sn
FFROST
telephoneNumber
+61 2 6261 1236
mail
brian.ffrost@dfat.gov.au
facsimileTelephoneNumber
+61 2 6261 1038
objectClass
top
objectClass
person
objectClass
organizationalPerson
objectClass
inetOrgPerson
cn
Brian
title
Executive Officer
description
Supervisor: John OsborneDirector,PASSPORT SYSTEMS A...
Start
ICAO PKD - UPLOAD M...
4:24 PM

Internal validation process

- Compliance check against Doc 9303
- Validation against CSCA stored in Montreal HSM
- Email notification of receipt of new entry to the Participant
- Cool down period of 4 days for DSC and Master List – Allows for Participant to check if they really intended to upload the entry and if it is a valid entry – Protection against **internal fraud**
- No cool down period for CRLs – "An assertion of trust is always verified, an assertion of mistrust is always accepted"

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

Non Conformant entries

- PKD board has published a document that details the variations to Doc 9303 that are acceptable, and variations that are not acceptable.
- Entries with acceptable variations will be allowed into the PKD with a warning

Non Conformant entries

- If CSCA is non conformant in an non-acceptable way
  - Netrust will prepare a discussion paper for the PKD Board detailing the non-conformance found along with possible impact to validation process.
  - The PKD board will vote on whether to allow import of the CSCA. Participant has to promise to rollover CSCA and become compliant within 6 months.
  - If PKD Board votes to allow import, Netrust prepares a signed token which is sent to the software in Montreal to allow for a one time exception for that specific CSCA.

Non Conformant entries

- If DSC is non conformant in an non-acceptable way
  - Entries that are uploaded to the PKD get automatically quarantined if they are not acceptable.
  - Netrust will prepare a discussion paper for the PKD Board detailing the non-conformance found along with possible impact to validation process.
  - The PKD board will vote on whether to allow import of the CSCA. Participant has to promise correct the non-compliance in the next cycle of DSC generation.
  - Netrust runs a manual process to allow processing of quarantined entries. Any future non compliance will be rejected

Publishing of entries

- All conformant entries and entries with acceptable non conformance are published in a “good entries” branch of the PKD.
- All non-conformant entries with unacceptable deviations, but approved by the board are published in a “bad entries” branch of the PKD.

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 three registered vendors:
  - Entrust, Bundesdrukerei, Primekey

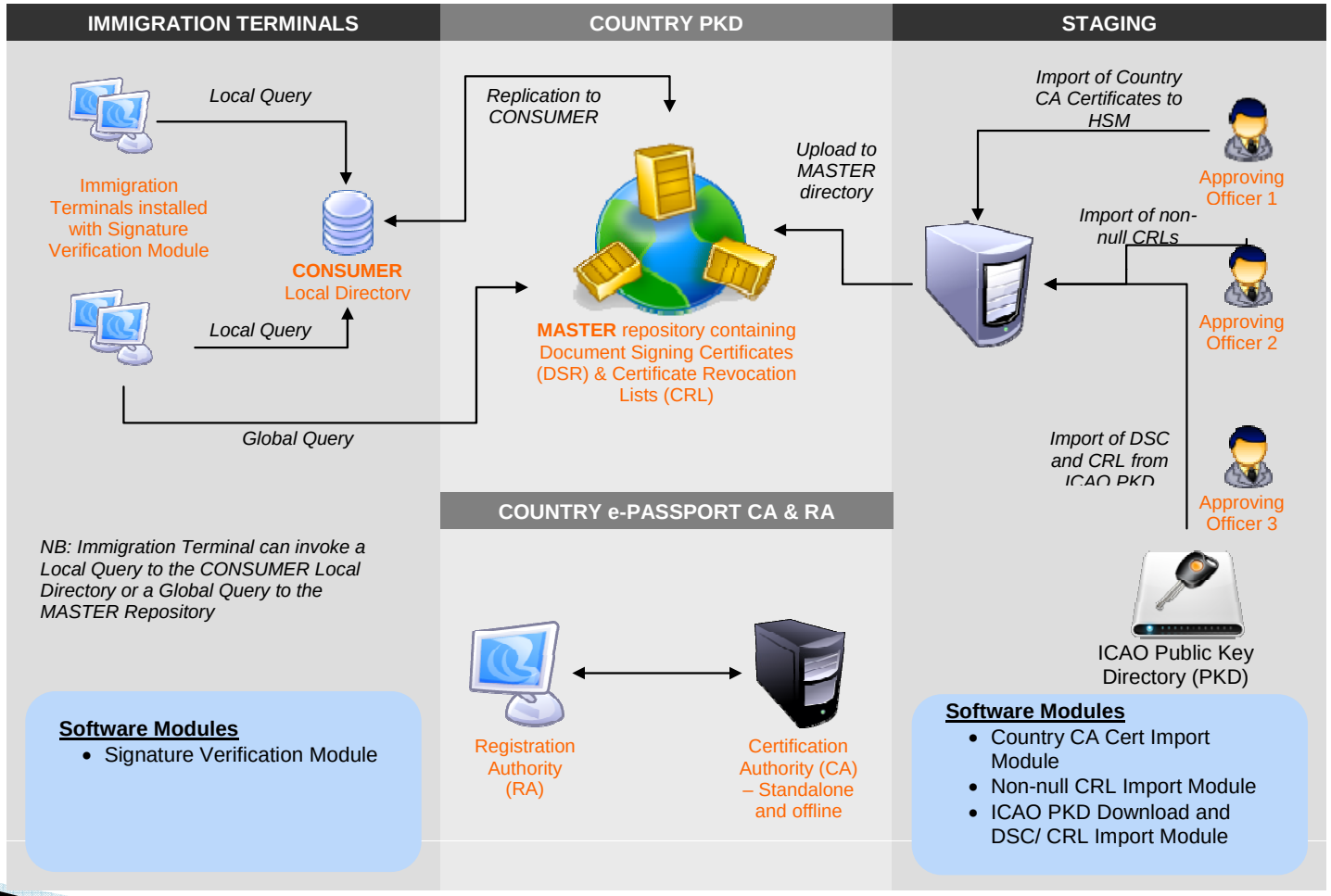
PKD Advantages

- 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

In country Management of Trust

- In country authoritative source for own DSCs
- Automated download from PKD and validation of own country data
- Automated import of PKD contents to local repositories
- Secure import of CSCAs – ceremonial
- Verification of CSCAs received through bilateral means using the CSCA Master Lists
- Secure import of DSCs/CRLs received through diplomatic means
- Harvesting of new DSCs from Passports for future decisions.

In country Management of Trust



Summary

- PKD is an essential component of verification at Border
- PKD is a tool for ensuring compliance to Doc 9303
- PKD participation ensures wider acceptance of your travel documents – Your citizens benefit from ease of travel

Thank You

R Rajeshkumar
R.Rajeshkumar@netrust.net
Rajesh@netrust.net
RRaj88@gmail.com
Deputy Chief Executive
Netrust Pte Ltd
http://www.netrust.net