PKD Services and Architecture

R Rajeshkumar
Dy. CEO, Netrust
November 25, 2010
R.Rajeshkumar@netrust.net

Trust Decisions

- Verification of signature on passport validates that data in passport 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
- Master Lists published in PKD are excellent means to ensure trust in CSCA

Country C	Country A ML	Country B ML
- Country A	- Country A	- Country A
- Country B	- Country B	- Country B
	- Country C	- Country C

OTHERS HAVE THE SAME CSCA

Trust Decisions

➔ For path validation:

- Check CRL as part of signature validation
- Check PKD frequently for latest CRL
- 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

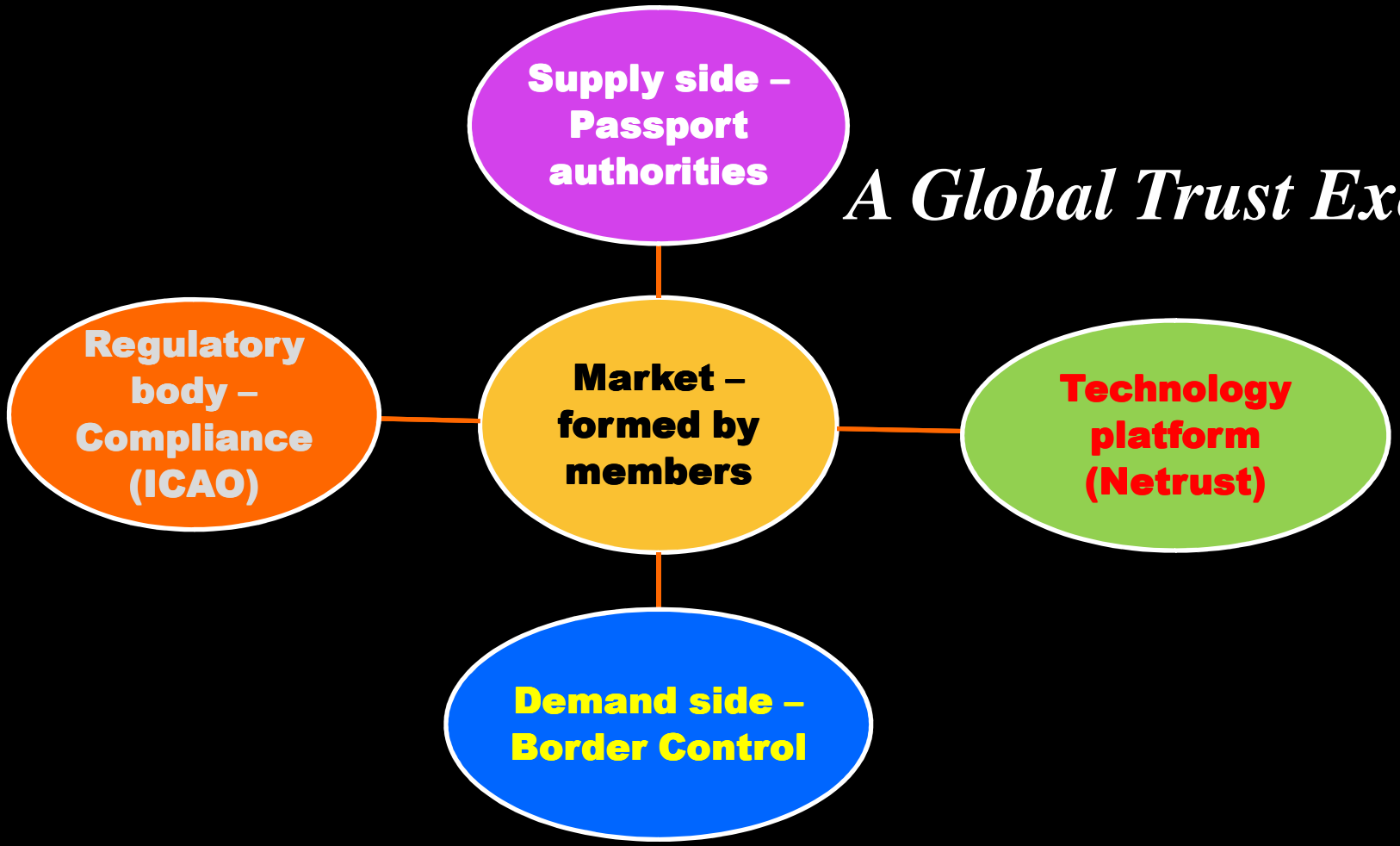
Trust Decisions

Sources of DSC

- PKD
- Received through bilateral exchange – exchange mechanism needs to secure
- Harvest from passports presented at Border

PKD Concept

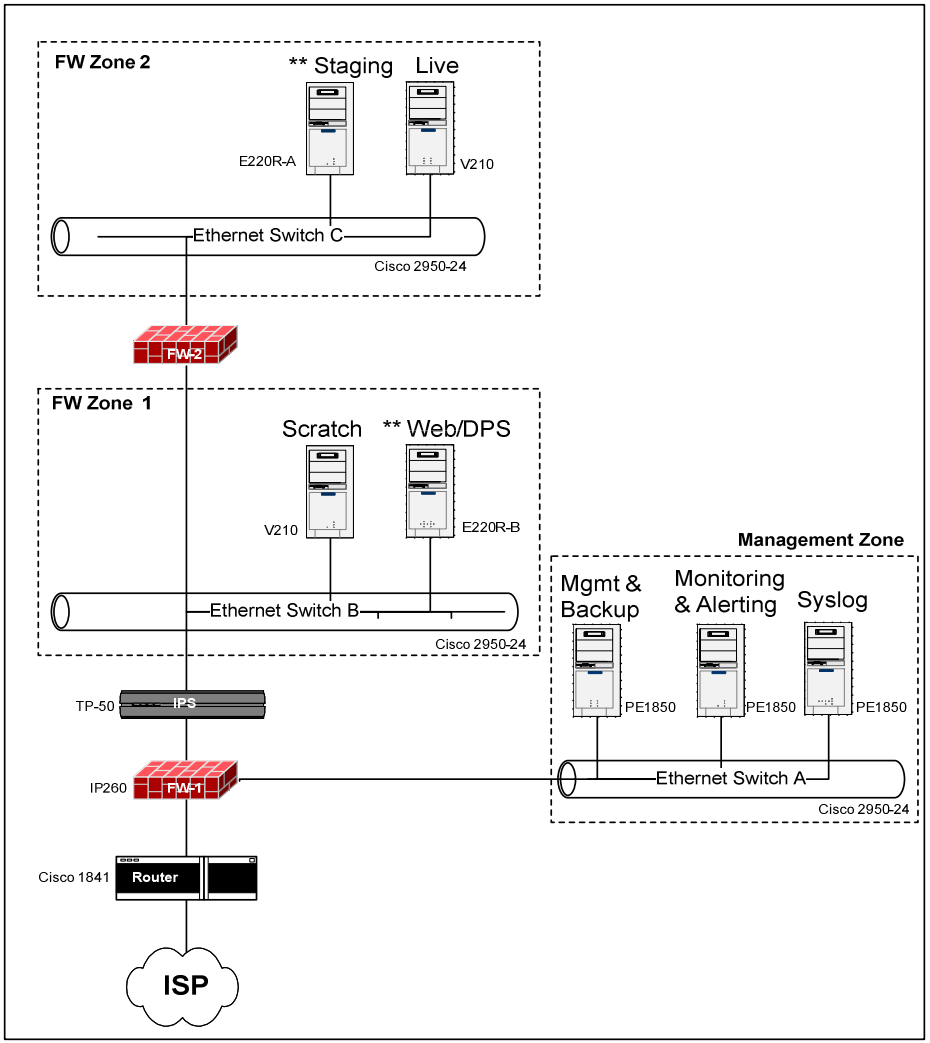
A Global Trust Exchange



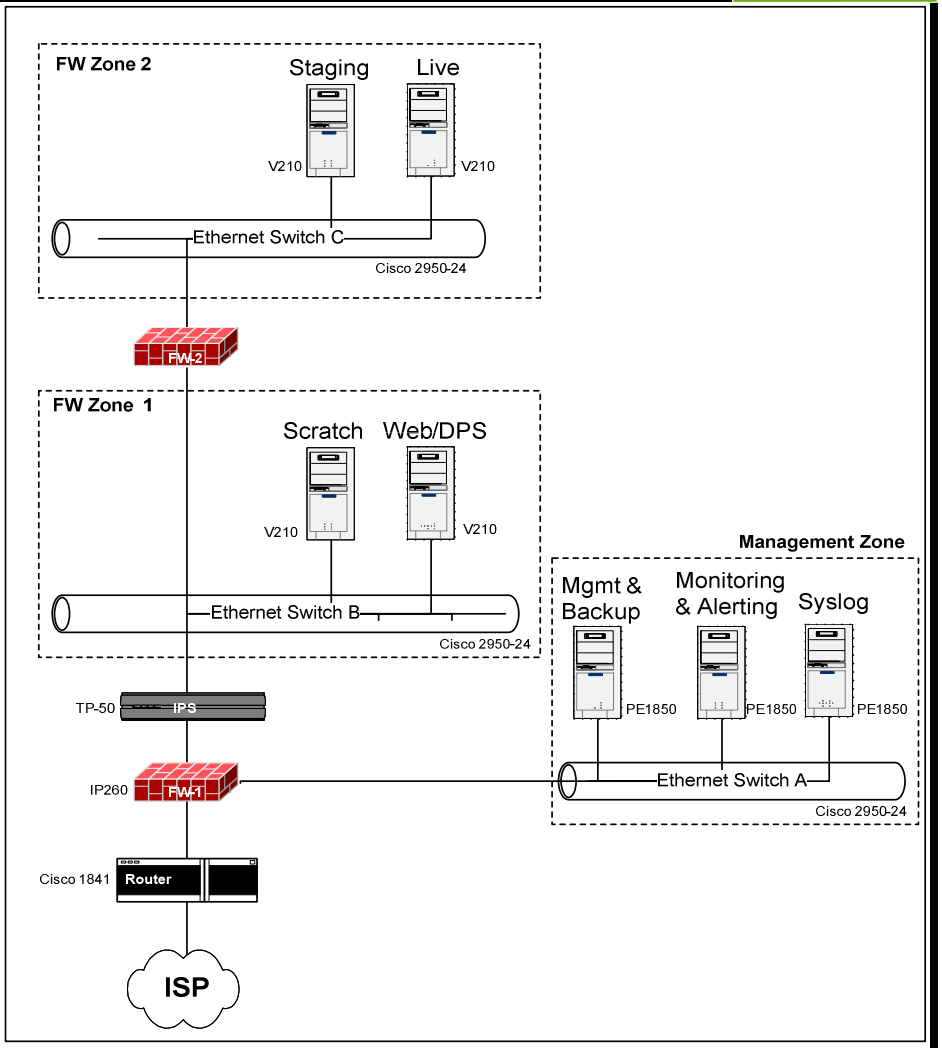
Current Services of the PKD

- Document Signers and CRLs of Participants
- CSCA Registry – Yellow Pages for the Passport Issuance Agency of the Participant
- CSCA Master List – List of CSCAs used by Participants
- Compliance website to check DSC/CRL/ML against Doc 9303

Architecture



ICAO PKD Operator DC - Singapore

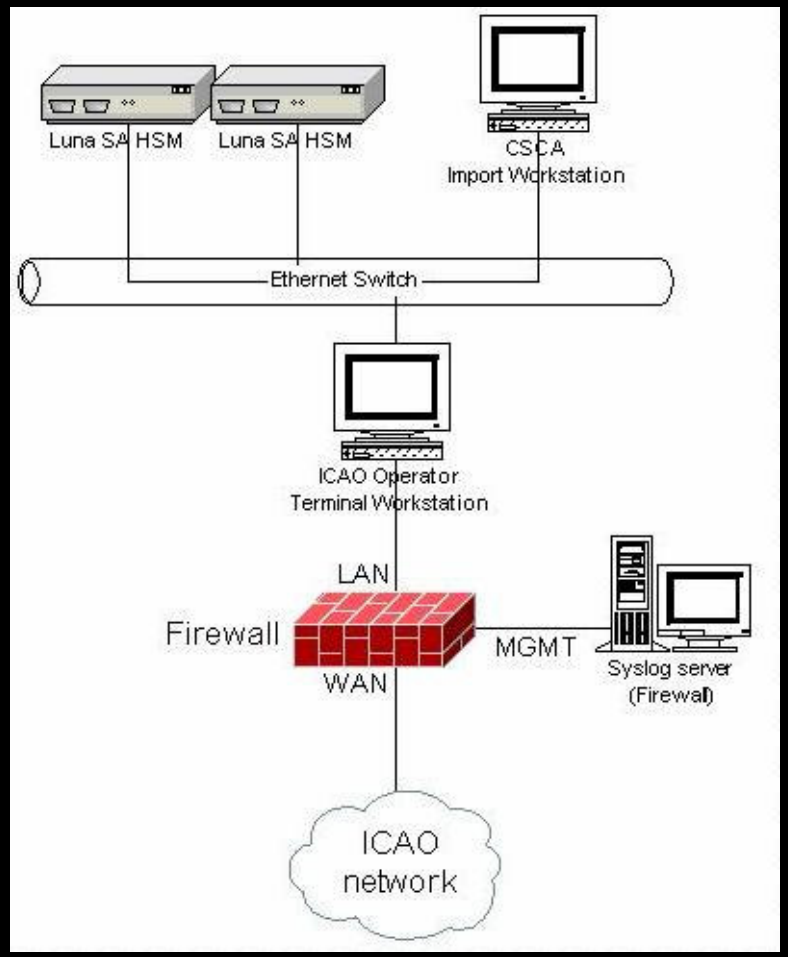


ICAO PKD Operator DC - Bangkok

PKD Architecture

- 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
- All other directory access requires VPN
- Download accessible through LDAP proxy servers only

PKD Architecture



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

Process Flow

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

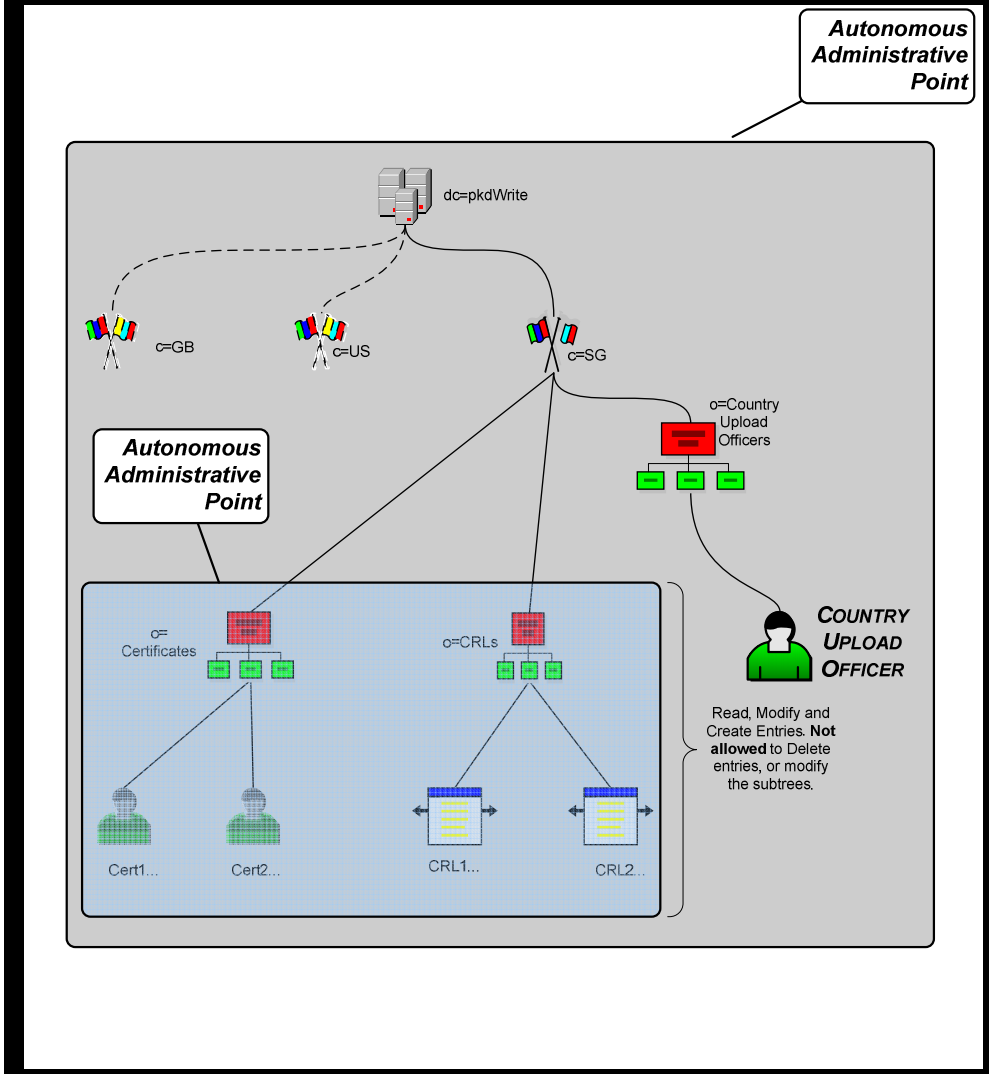
Import of CSCA

- Country sends Thumbprint through Email/Fax
- Representative carries CSCA. Country sends details of representative to ICAO for verification
- Personnel involved - Three Security Officers, one IS person, one Operator + Countryrepresentative

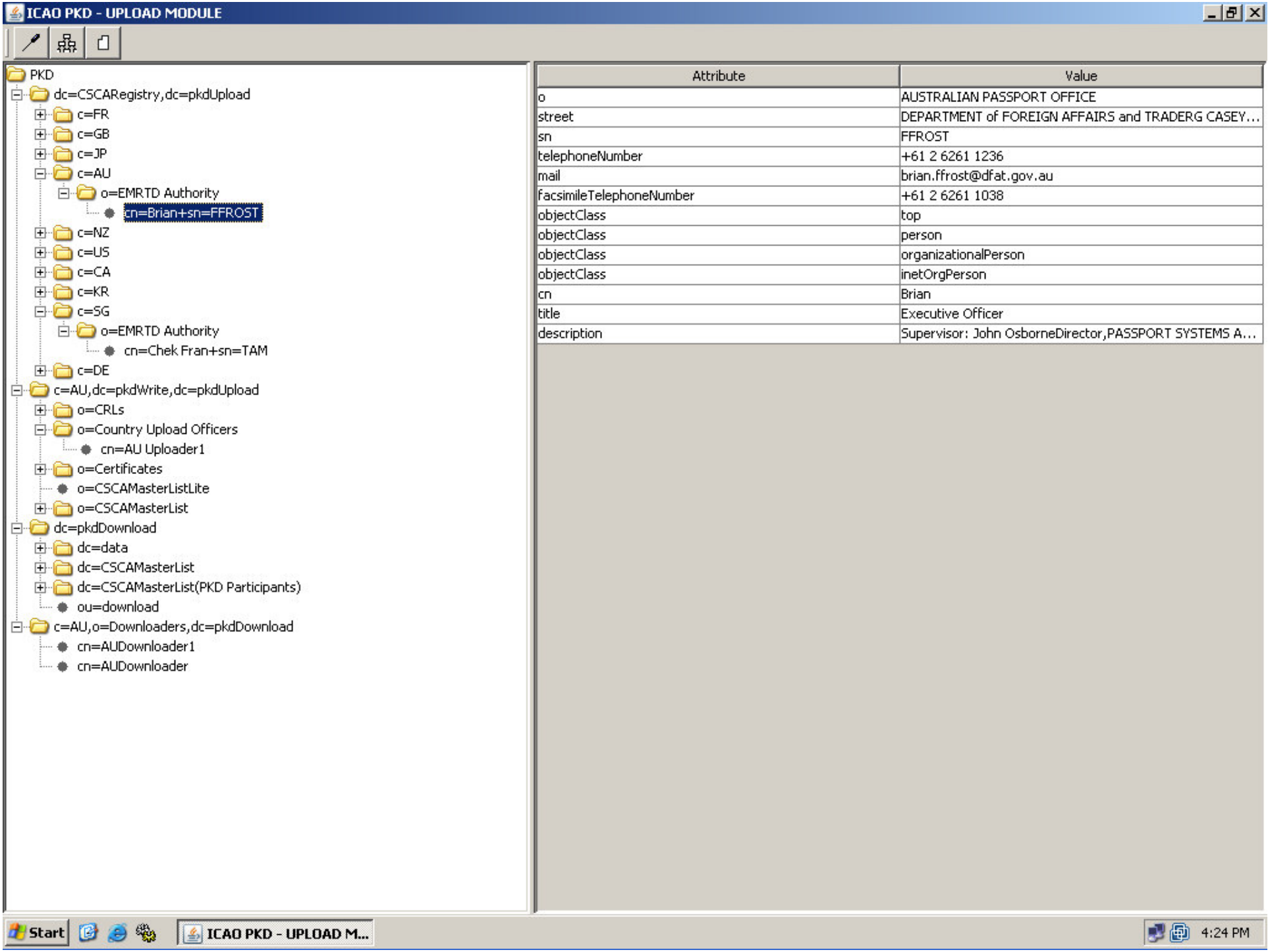
Upload by Participant

- **Authentication using 2-way SSL**
  - Country generates CSR. Sends to Netrust.
  - Netrust signs using a root used only for issuing credentials for PKD access.
  - SASL external mechanism.
- **Login monitored - each wrong login sends sms to 6 personnel within Netrust**
  - Details of account attempted and IP address of the user
- **If three attempts exceeded, account is locked out**

Upload by Participant



- **Access limited to creating entries in a restricted area**
  - Every entry created/modified is copied automatically to an archive system with date/time, creators name and modifiers name. Hence, an audit trail of the access (write only).
- **Read access for CSCA registery**


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

Verification and Approval

- **Monitoring engine**
  - Checks entries every hour
  - Checks the DN of the DSC/CRL and entry against interface specs
    - Participants will be using an automated solution. Error indicates a red flag.
    - Check if the country in the DN is the same as the tree.
  - Sends signed email to country acknowleding receipt
    - In house fraud can be detected.

Verification and Approval

➔ Approval

- Cool down period of 4 days between sending receipt email to country and approval - no cool down for CRL.
- Country can request to stop further processing of entry
- Request entered in system by ICAO operators
- Automatic email sent to countries regarding action taken

Publish to live

- Every 6 hours, an automatic batch examines all entries that are approved.
- Entries Copied to live, creates LDIF, calculates checksum.
- Email sent to country informing of entry in live.

Download

- **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.

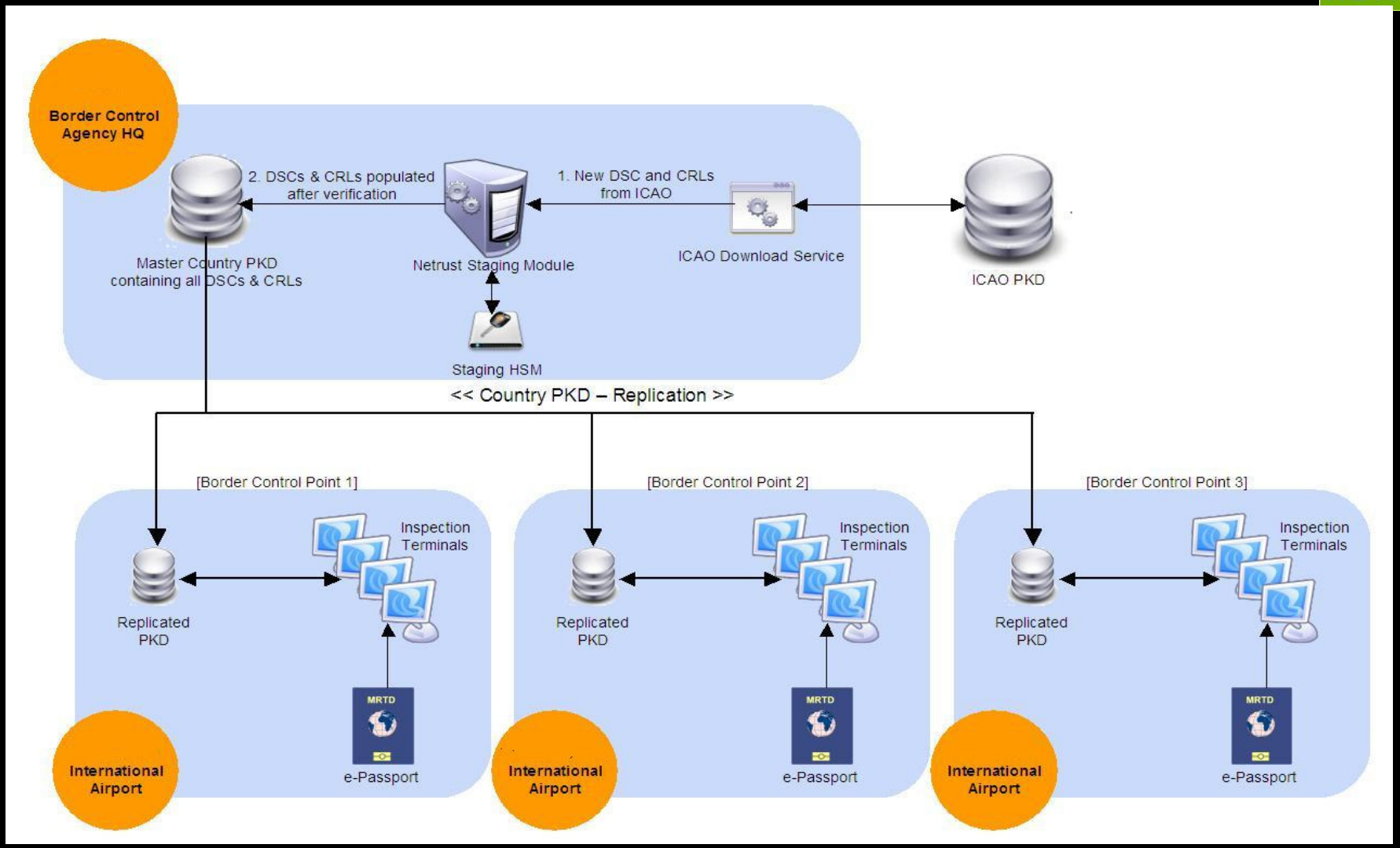
Download – non-participants

- **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**

DR planning

- **Scenario analysis of the impact of Disasters. Classified into three categories**
  - **OUTCON 1**
    - **Single component failure**
    - **No external impact**
    - **No loss of data integrity**
  - **OUTCON 2**
    - **Single component failure**
    - **Slight external impact**
    - **Possible loss of data integrity**
  - **OUTCON 3**
    - **Significant external impact**
    - **Possible service outage**
    - **Significant possibility of loss of data integrity.**

National PKD

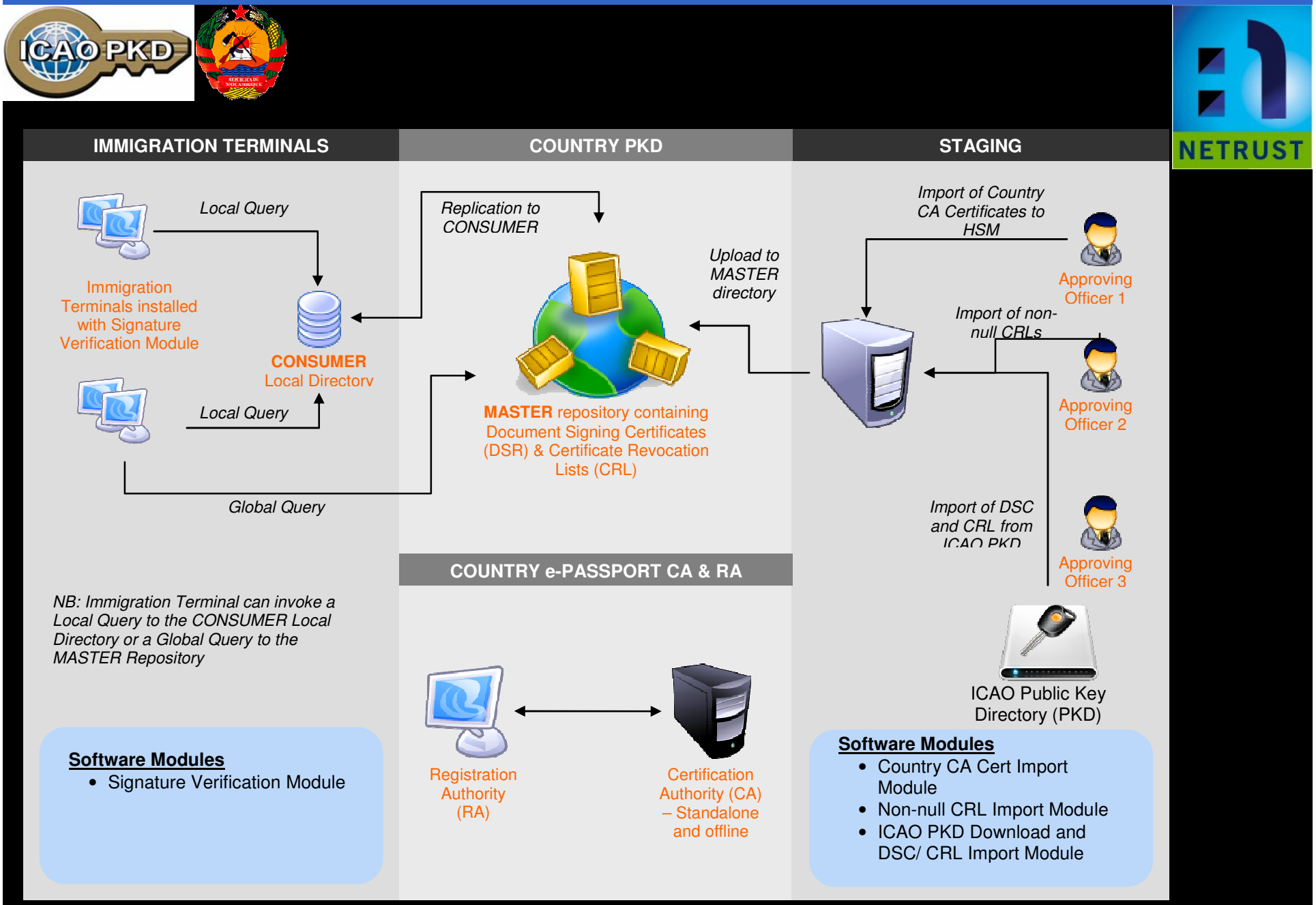


Trust Decisions

- **Other checks necessary at terminal**
  - DSC subject name and Issuer subject name belong to the same country as passport presented

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
- Secure import of DSCs/CRLs received through diplomatic means
- Harvesting of new DSCs from Passports for future decisions.


IMMIGRATION TERMINALS
COUNTRY PKD
STAGING
Local Query
Immigration Terminals installed with Signature Verification Module
CONSUMER
Local Directory
Local Query
Global Query
Replication to CONSUMER
MASTER repository containing Document Signing Certificates (DSR) & Certificate Revocation Lists (CRL)
Upload to MASTER directory
Import of Country CA Certificates to HSM
Approving Officer 1
Import of non-null CRLs
Approving Officer 2
Import of DSC and CRL from ICAO PKD
Approving Officer 3
ICAO Public Key Directory (PKD)
COUNTRY e-PASSPORT CA & RA
Registration Authority (RA)
Certification Authority (CA) – Standalone and offline
NB: Immigration Terminal can invoke a Local Query to the CONSUMER Local Directory or a Global Query to the MASTER Repository
Software Modules
Signature Verification Module
Software Modules
Country CA Cert Import Module
Non-null CRL Import Module
ICAO PKD Download and DSC/ CRL Import Module

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

Thank You

R Rajeshkumar
R.Rajeshkumar@netrust.net
Rajesh@netrust.net
RRaj88@gmail.com
Dy. CEO
Netrust Pte Ltd
http://www.netrust.net