



ePassport PKI Validation & the ICAO PKD

Ross Greenwood
Chairman 2007 PKD Board
Australian Passport Office

The Third Symposium and Exhibition on ICAO MRTDs, Biometrics and Security Standards

The Border Clearance Process

Step # 1 - confirm identity

- 1 Integrity of issue process?
 - 2 Genuine passport?
 - 3 Passport unaltered?
 - 4 Passport lost/stolen/cancelled?
 - 5 Genuine holder?
-

Step # 2 – decide whether the passenger can enter

- 6 Intentions of passport holder?
- 7 Entry criteria met?
- 8 “Alerts”?



ePassports in the Border Clearance Process

Step # 1 - confirm identity

1 Integrity of issue process?

2 Genuine passport?

3 Passport unaltered?

4 Passport lost/stolen/cancelled?

5 Genuine holder?

PKI Validation

Biometric
Comparisons

Step # 2 – decide whether the passenger can enter

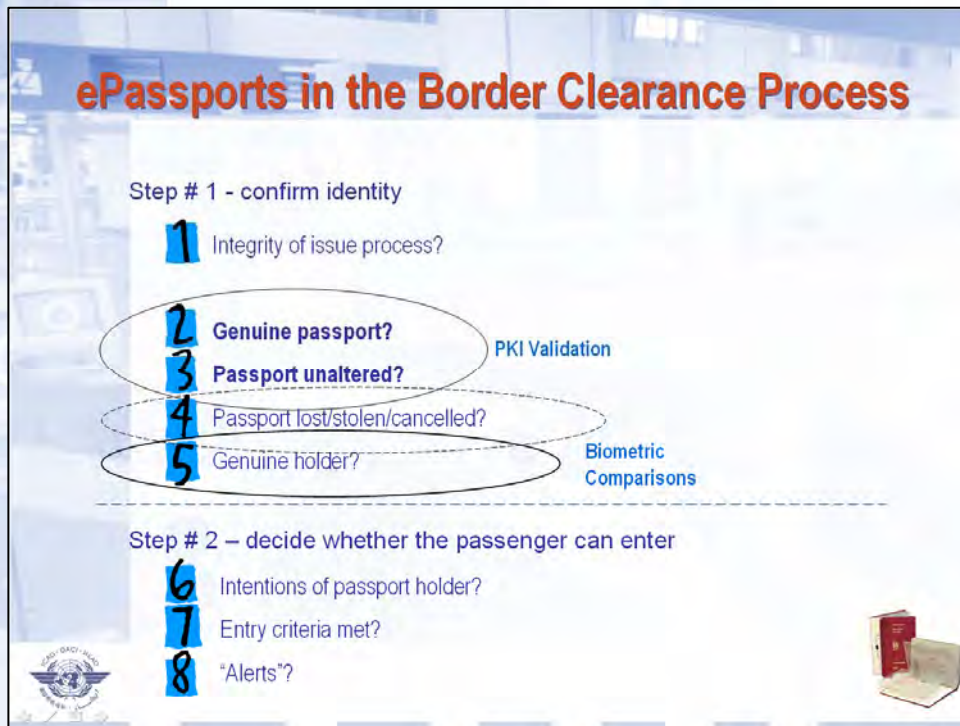
6 Intentions of passport holder?

7 Entry criteria met?

8 “Alerts”?



ePassports in the Border Clearance Process



➤ the benefits of PKI validation (and checks of lost/stolen passports, and biometric comparisons) are maximised in fully integrated solutions where all ePassport holders are examined (eg Smartgate) but

➤ significant benefits can still be obtained from cheaper, less integrated, risk based approaches – eg PKI validation (and checks of lost/stolen passports and photos on chips) of ePassport holders referred to secondary examination



The ICAO PKD – Recent Developments

In their meeting in Singapore on 10 September 2007 the PKD Board:

- Provisionally accepted a European proposal for a modified approach to ePassport validation using cross-signed country certificates.
 - It is expected this agreement, once confirmed, will allow Germany to join the PKD and that other European countries will follow their lead.
 - The agreement maintains backwards compatibility for those countries that have invested in the current scheme.
 - With increased membership the ICAO PKD will become more attractive as a one-stop shop to obtain public key certificates and revocation lists.
- Reduced registration and annual fees.
 - The revised one-off registration fee will be in the range of USD15-25,000.
 - Annual fees for the remainder of 2007 have been waived.
 - Annual fees for 2008 will be set to meet operational costs (current estimate is USD25,000 with 20 participating States).
- Confirmed Governance arrangements.
 - The PKD Board exercises financial and operational oversight.
 - A dedicated staff member has been recruited in ICAO in Montreal.
 - The ICAO PKD accounts are subject to audit and will in future be published.
 - ICAO will commence negotiating the operational contract with the operator shortly.



A Modified Approach – Improving the ICAO PKD

The compromise agreement that has been reached, which remains subject to confirmation by the parties to the discussion is that:

- the new CSCA cross certificates should be introduced into the ICAO PKD along with the one way web of trust advocated in the European proposal. The CSCA cross certificates would also be available for download from the PKD with CSCA continuing to be exchanged by diplomatic means, to achieve cross-certification.
- CRLs and DSCs will continue to be loaded to the ICAO PKD as a mandatory requirement. In future this will be the primary and preferred distribution method for CRLs.
- inclusion of DSC on the chip in all ePassports will be mandatory.



Validation Under the Modified Approach

The proposed modified approach will support two, alternative methods for validating ePassports using the ICAO PKD. Either:

- comparison of the DSC in the PKD with the DSC read from the chip together with a check for any revocation against CRLs (ie the current scheme) or
- check of the CSCA cross certificates against the DSC read from the chip, together with a check for any revocation against CRLs.

The modified approach will therefore be backwards compatible for those States that have relied, or are relying in their current planning, on the current PKD specification and have as a result decided either:

- not to include the DSC on the chip in their ePassport (ie a passport issuance IT system issue) or
- to rely on DSC comparison and a CRL check as the validation method (ie a border control IT system issue).

Implementing the modified approach will require amendment to 9303 and all of the current PKD documentation. The NTWG and ISO will commence work on the changes as soon as the agreement is confirmed.



A new Fee Structure

Summary

Incentives for immediate membership.

- Removal of early participant penalty in registration fee structure.
- Removal of annual fee bias against large State participation.
- New Registration Fee = US\$15~25,000
- Estimated New Annual Fee = US\$25,000* in 2008

* -subject to membership growing to 20 participants & confirmation of the terms of the operational contract



Further information:

For information on the ICAO PKD visit -

<http://mrtd.icao.int/content/view/47/251/>

or e-mail the Chairman of the ICAO PKD Board -

ross.greenwood@dfat.gov.au

For a guide to ePassport design & production issues visit -

http://www.apec.org/content/apec/publications/all_publications/committee_on_trade.html

