# Implementation of the Public Key Directory


**Ross Greenwood**

2007 Chairperson ICAO PKD Board

Australian Passport Office


**TAG/MRTD 18**

**18th Meeting of the Technical Advisory Group on Machine Readable Travel Document**

# Today's presentation

- Provide the TAG with a brief update on the ICAO PKD
- Seek TAG approval to amend 9303 consistent with WP14 proposal on CSCA Master Lists

# PKD Update

- PKD commenced operations in March 2007
- Growing participation - global coverage:
  - Japan, Republic of Korea & Singapore
  - United States and Canada
  - Germany and United Kingdom *(and soon to be joined by France)*
  - Australia and New Zealand

# PKD Governance

- Comprehensive up to date technical and other information on the PKD is available at:

http://www.mrtd.icao.int/content/view/47/251/

- Documents available for download include the PKD Board's:
  - Rules of Procedure
  - complaints handling arrangements
  - procedures for setting fees
  - procedures for amending the PKD Memorandum of Understanding.

# PKD Registration Fee

- Registration Fee (a one time fee payable after notices of participation are lodged)
  - Currently USD85,000
  - ICAO Council are expected to consider a PKD Board proposal to amend the PKD MoU to reduce the fee to **USD25,000** in June 2008
  - The PKD Board has also recommended that excess payments of Registration Fees will be credited against future year annual fees
  - See PKD webpage for details

# PKD Annual Fee

- Annual Fee (a fee paid annually by all **active** PKD participants, payable after certificate uploads commence)
  - 2008 Annual Fee is **USD100,000**
  - Annual Fees are expected to reduce in 2009 and subsequent years as participation grows and because the establishment costs of the ICAO PKD have been met
  - The annual fee is applied on a pro rata basis
  - Credits on excess annual fee collections are applied to future year's liabilities
  - See *ICAO PKD Rules and Procedure for Updating the PKD Fee Schedule* document available from PKD webpage for details

# PKD – The Future

The PKD Board's priorities for the future are:

- to improve the PKD's business processes and
- further reduce the cost of participation, in order to
- attract new participants, in order to
- better support the PKD's objective to implement a globally interoperable system to support ePassport validation.

# CSCA countersigning and Master List issuance

- In September 2007 the PKD Board accepted a European Union proposal for adopting a modified approach to ePassport validation and distribution of CSCA Certificates.
- WG3/TF5 have subsequently developed the Technical Report before the TAG at the request of the NTWG, after a request from the PKD Board.

# Validation Under The Modified Approach

The modified approach, if adopted by the TAG will mean that in future there will be **two**, alternative methods for validating ePassports using the ICAO PKD:

1. The current scheme: comparison of the validated DSC in the PKD with the DSC read from the chip together with a check for any revocation against CRLs; both the DSC and the CRLs are uploaded after verification by ICAO against the CSCA.

or

2. The modified scheme: verify the DSC read from the chip with the CSCA certificates, together with a check for any revocation against CRLs verified with the CSCA certificates; the PKD supports distribution of CSCA certificate by publishing CSCA Master Lists.

# Features of the Modified Approach

- The strength of the modified approach is simplified validation, for those States able to adopt the new validation method, and simplified management of the exchange of CSCAs via the Master Lists.

- The modified approach will 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 (i.e. a passport issuance IT system issue) or
  - to rely on DSC comparison and a CRL check as the validation method (i.e. a border control IT system issue)

- The PKD Board and NTWG have endorsed the Technical Report as providing a sound technical foundation for implementing the CSCA Master List concept

# Next Steps

Subject to TAG approval:

- Develop a business process framework to support the compilation and exchange of Master Lists and CSCA revocations to achieve the modified approach to ePassport validation
- Redesign the ICAO PKD to accept CSCA Master Lists
- States to compile and exchange Master Lists
- Upload Master Lists to ICAO PKD
- Make Master Lists available for download

# Action required of TAG?

The TAG is invited to:

1. Approve the Technical Report – CSCA Countersigning and Master List Issuance for inclusion in Document 9303; and
2. Note that further work to develop business processes to support ePassport validation and to manage the exchange of certificates and revocation lists is required, and will be undertaken by the PKD Board and the NTWG.

# Questions?

# Question

- Will the Master List replace bilateral exchange of Certificates (eg by Diplomatic means)?

- No, The Master List approach is intended to support but not to replace bilateral distribution of self-signed certificates.

# Question

- How will Master Lists be exchanged between member states?
- Master Lists will be uploaded to the ICAO PKD, and will be available through a new PKD download process (with a policy on access to be determined by the PKD Board).
- States outside the ICAO PKD may also exchange Master Lists on a bilateral basis.

# Question

- How will Certificate Revocation be managed for CSCAs in a Master List?

- The use of CRLs is already defined in Document 9303. The Master List technical report describes technical aspects of CRL management. The PKD Board will be developing business processes and protocols to ensure that revocations of CSCAs, if they occur, are available immediately via the PKD. The PKD Board will seek NTWG advice (from WG3/TF5) as and if required in developing the policy and protocols.

# Question

- How has the solution evolved since the initial discussion?
- The original proposal suggested a process of countersigning keys issued by other CAs known as “Cross Certification” based on the X509 standard.
- This approach raised “trust” issues. The Master List concept was developed to ensure the benefits of simplified exchange of CSCAs was maintained in a scheme with no implied trust.