INFORMATION PAPER

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS (TAG-MRTD)

EIGHTEENTH MEETING

Montréal, 5 to 8 May 2008

Agenda Item 2: Implementation of the Public Key Directory
Agenda Item 2.3: ICAO PKD Update

ICAO PKD UPDATE

Presented by the ICAO PKD Board

1.   INTRODUCTION

1.1   The ICAO PKD commenced operating in March 2007, just over one year ago, to promote the global interoperability of a validation system for electronic travel documents.

1.2   The ICAO PKD was created at the request of ICAO Contracting States by ICAO Council and operates under the authority of the "Memorandum of Understanding (MoU) Regarding Participation and Cost Sharing in the Electronic Machine Readable Travel Documents ICAO Public Key Directory".

1.3   The ICAO PKD Board is the standing body responsible for the ICAO PKD, appointed by ICAO Council. The ICAO Secretariat provides audited financial statements for, and administrative and operational support to, the ICAO PKD and to the ICAO PKD Board. The operator of the ICAO PKD, to be selected by the PKD Board, will be contracted by ICAO to deliver the validation system.

2.   ICAO PKD PARTICIPATION

2.1   The ICAO PKD has grown to nine participants - Australia, Canada, Germany, Japan, New Zealand, Republic of Korea, Singapore, United Kingdom and the United States of America. France is expected to complete participation formalities shortly.

3.   MODIFIED APPROACH TO THE VALIDATION OF E-MRTDS

3.1   During 2007 the PKD Board accepted a European proposal for adoption of an alternative scheme for validating electronic travel documents. The scheme is the subject of TAG/MRTD 18 WP/xx.

3.2   The proposed modified approach supports two, alternative methods for validating electronic travel documents using the ICAO PKD. The current scheme of validation achieved by comparison of the validated DSC in the PKD with the DSC read from the chip will continue. Under the modified scheme, validation of the DSC read from the chip will also be able to be achieved against a CSCA obtained from a Masterlist available from the ICAO PKD. Both schemes will rely on certificate revocation checks, also available through the ICAO PKD.

3.3   The strength of the modified approach is simplified validation, for those States able to adopt the modified scheme, and a stronger regime for all participants for establishing the credentials of the providers of CSCA certificates, the highest level of trust in the system, via the CSCA 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.

4.   ICAO PKD – OTHER DEVELOPMENTS

4.1   The ICAO PKD Board has implemented operational procedures including:

- *ICAO PKD Board Rules of Procedure*
- *ICAO PKD Procedure for Handling Operational Complaints*
- *Procedures for Proposing Amendments to the ICAO PKD MoU*
- *ICAO PKD Rules and Procedure for Updating the PKD Fee Schedule*

4.2   A sound technical and administrative foundation has been established. The focus of future work to develop the ICAO PKD will be to increase participation by improving the service offered by the ICAO PKD. This will be achieved by reducing the cost of participation and developing business processes that make the exchange of PKI certificates and revocation lists more effective and efficient.

4.3   The 2007 ICAO Assembly urged all ICAO ePassport issuing States to join the ICAO PKD. The 2008 ICAO FAL/P recently approved adoption of a "Recommended Practice" at paragraph 3.9.1 in Chapter 3 of Annex 9 that "Contracting States issuing, or intending to issue ePassports and/or; implementing at border control automated checks on ePassports; should join the ICAO Public Key Directory (PKD)."

4.4   Current information on the ICAO PKD, participant contacts and the current fee schedule as well as copies of the MoU, PKD technical documents and the PKD Board's procedural documents are available at the PKD web page on the ICAO MRTD website at: http://mrtd.icao.int/content/view/47/251/

5.   ACTION BY THE TAG/MRTD

5.1   The TAG/MRTD is invited to note progress in establishing the ICAO PKD to support a globally interoperable scheme for the validation of eMRTDs.

— END —