TAG-MRTD/15
WP/4
28/4/04

**TECHNICAL ADVISORY GROUP ON
MACHINE READABLE TRAVEL DOCUMENTS**

Fifteenth Meeting

(Montreal, 17 to 21 May 2004)

Agenda Item 3: Report of the New Technologies Working Group
Agenda Item 3.1: Update on development of specifications for the use of PKI digital signatures for MRTDs

NEW TECHNICAL REPORT - PKI FOR MRTDs

(Presented by the New Technologies Working Group (NTWG) and
the Public Key Infrastructure (PKI) Task Force)

1. A paper proposing the use of a PKI scheme to secure electronic data on MRTDs was endorsed by TAG/14. It was recognized by the TAG that the paper limited itself to describing concepts involved in the use of a Public Key Directory run by ICAO and describing the roles of issuing and receiving States. Further work was needed to specify the scheme in sufficient detail to enable implementation. This further work has been undertaken by a PKI Task Force organized by the NTWG.

2. A new Technical Report has been prepared, providing, at a detailed technical level, specifications that can be used by issuing States to implement PKI in securing electronic data in their travel documents. The specified document security object, electronically signed by the issuing state, enables receiving States to verify the authenticity and integrity of the electronic data in the document's chip.

3. The Technical Report also specifies the requirements for states and organizations wanting to read electronic data and specifies a Public Key Directory that ICAO can implement. The report recommends that document signer public keys be stored on the MRTD chip itself, but this is optional. The Public Key Directory will provide a valuable service to the MRTD community even if the public key is included on the document's chip.

4. Furthermore the Technical Report provides specifications for additional optional security features that can be adopted to counter threats of eavesdropping and skimming of data from contactless chips. This additional security feature called 'basic access control' in the Technical Report can be adopted at the discretion of the issuing State.

5. A further optional additional security feature called “active authentication” is specified. The latter prevents chip substitution and could be adopted at unmanned controls were the MRTD is used as an electronic token to gain access.

6. The Technical Report has reached a stage of development and review when NTWG believe it offers sufficient detail for states to proceed with e-passports. However when implementations are made, issues will arise and there will be a need to keep the Report under review.

(2 pages)

7. The PKI scheme is designed to protect data written time of issue and not updated. A further challenge for NTWG will be to develop a globally interoperable PKI scheme that can accommodate additions to electronic data in the lifetime of the document. This work is beyond the scope of the present Task Force.

8. To supplement the Technical Report a “Frequently Asked Questions” document is provided in TAG-MRTD-WP/10. This has been prepared because of the technical nature of the PKI report itself. The questions were largely invented by Task Force members, and it is intended to update the document with genuine questions from the MRTD community as they arise.

9. ACTION BY THE TAG/MRTD

9.1 The TAG/MRTD is invited to endorse the Technical Report, “PKI for Machine Readable Travel Documents Offering ICC Read-only Access”, Version 1.0.

— END —