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

NINETEENTH MEETING

Montréal, 7 to 9 December 2009

Agenda Item 2:   Activities of the NTWG
Agenda Item 2.13:   Technical Report LDS and PKI Maintenance

**TECHNICAL REPORT
LDS AND PKI MAINTENANCE**

(Presented by the New Technologies Working Group (NTWG))

1.   **INTRODUCTION**

1.1   The sixth edition of Doc 9303 Part 1, Volume 2, published in September 2006, and the third edition of Doc 9303 Part 3, Volume 2, contain the technical specifications of the Logical Data Structure (LDS) in Section III, and the Public Key Infrastructure (PKI) in Section IV.

1.2   Issues that arise within the scope of Doc 9303 are being addressed in the "Supplement to Doc 9303". The purpose of this Supplement is to provide guidance, advice, update, clarification and amplification to the Travel Document community to have timely and official direction with respect to the standard. The Supplement is being published on a regular base.

1.3   The purpose of this Information Paper is to inform the TAG/MRTD on the status with respect to the work that has been undertaken with respect to an evaluation of the present LDS and PKI specifications, which is planned to result in a Technical Report "LDS and PKI Maintenance".

2.   **BACKGROUND**

2.1   In its meeting in September 2008 in Bern, the NTWG discussed the roadmap for development of specifications for the next generation of Machine Readable Travel Documents.

2.2   It was decided to separate the discussions on new functionalities, resulting in a new version of the specifications, and a revision of the present specifications with respect to actuality and security.

2.3   The LDS and PKI specifications in the latest editions of Doc 9303 were developed in 2004. In the fast moving world of technology evolution and increasing computer power an evaluation of the specifications now, after five years, is a necessity to preserve the appropriate level of accuracy ands security.

3.   **TECHNICAL REPORT**

3.1   The results of the LDS and PKI evaluation will lead to a revision of the specifications in a Technical report "LDS and PKI Maintenance".

3.2   The following specifications are foreseen to be revised:

      a) LDS versioning;

      b) Certificate Profiles;

      c) Active Authentication.

3.3   The initial work on the technical specifications, based on an approved list of Work Items will be carried out within Task Force 5 of ISO/IEC JTC1 SC17 WG3.

3.4   The Technical Report is planned to be presented to the TAG/MRTD for approval in its twentieth meeting. To achieve this, review cycles will be carried out on drafts by the NTWG.

— END —