International Civil Aviation Organization

INFORMATION PAPER

TAG-MRTD/18-IP/1
22/4/08
English only

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 2.1: Logical Data Structure and Security Framework

LOGICAL DATA STRUCTURE AND SECURITY FRAMEWORK

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, contains 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 the sixth edition 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 roadmap for the developments to be undertaken to realize the next generation of specifications for the Logical Data Structure and the Security Framework for electronic Machine Readable Travel Documents (LDS & PKI Version 2).

2. BACKGROUND

2.1 In its 16th meeting in September 2005 the TAG-MRTD approved two Working Papers, covering LDS & PKI Version 2. These Working Papers are WP/21 - ‘Second edition of Technical Report on development of a Logical Data Structure (LDS) for optional capacity expansion technologies on MRTDs’ and WP/10 - ‘Proposed development of a Technical Report “PKI for Machine Readable Travel Documents” – Version 2’.

2.2 It was anticipated that these second versions of the Technical Reports would be released in the year 2010.

2.3 It was recognized that LDS & PKI specifications are closely related and therefore the specifications need to be developed in a harmonized way.

3. PRESENT STATUS

3.1 At its meeting in February 2008 in Christchurch, the NTWG discussed the roadmap for the development of specifications for the next generation of Machine Readable Travel Documents.

3.2 Based on the necessity of harmonization between the specifications for the Logical Data Structure and the Security Framework, it was acknowledged that the work should result into one Technical Report, covering both.

3.3 A preliminary list of Work items for the Technical Report is provided under section 4 of this Information Paper, and consists of Work Items defined in the TAG_16 Working Papers 10 and 21, as well as additional Work Items. NTWG recognized the necessity for guidance from member States with respect to this list; the topics to be covered by specifications need to be defined within the NTWG and TAG-MRTD.

3.4 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.

3.5 The Technical Report is planned to be presented to the TAG for approval in 2011. To achieve this, review cycles will be carried out on drafts by the NTWG.

4. ROADMAP

4.1 The following table provides the LDS and PKI topics presented at TAG_16 and their logical relationship, plus additional Work Items. The items are sub-divided into maintenance of existing specifications and new specifications to be developed.

LDS	PKI
TAG_16 WP	
Maintenance	
	Evaluation: Passive Authentication • Effective use at inspection points • Certificate exchange • Life cycle time
	Evaluation: Basic Access Control • Life cycle time • Future alternative
	Evaluation: Active Authentication • Life cycle time • Chip Authentication alternative
	Evaluation: Algorithms & Key lengths • Life cycle time
Compatibility with changes in related standards	
Preserving interoperability	Backwards compatibility
New	
Accommodation of multiple applications • Travel functionality • ID-functionality	
Accommodation of chip update after issuance • Travel records • Visa	Chip contents updating • Travel records • Visa
	Extended Access Control • Global use • Chip Authentication without Terminal Authentication • Authorized chip update
	Passive Authentication for Multiple Data Group Entrances • Verifying parts of a Data Group
Additional	
Maintenance	
	Evaluation: Certificate Profiles • Consider relaxation of the extension, assigned MANDATORY and MUST NOT
New	
	CSCA countersigning • CSCA Master List in progess
	Multi application use of id cards • Consequences for Doc 9303 Part 3

— END —