International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/16
WP/10
13/9/05
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS

Sixteenth Meeting

(Montreal, 26 to 28 September 2005)

Agenda Item 2: Implementation of e-passports
Agenda Item 2.1: Progress and issues

PROPOSED DEVELOPMENT OF A TECHNICAL REPORT "PKI FOR MACHINE READABLE TRAVEL DOCUMENTS" – VERSION 2

(Presented by the New Technologies Working Group)

1. INTRODUCTION

1.1 At TAG-MRTD/15, the NTWG presented WP/4 (New Technical Report - PKI for MRTDs). This document invited the TAG-MRTD to endorse the Technical Report, "PKI for Machine Readable Travel Documents Offering ICC Read-only Access", Version 1.0. The TAG-MRTD endorsed this Technical Report.

1.2 A Version 1.1 of this Technical Report was prepared for publication, and published on the ICAO website in October 2004.

1.3 The Technical Report provides, at a detailed level, specifications that can be used by MRTD-issuing States to implement PKI in securing the authenticity and integrity of electronic data in their travel documents. It also specifies the requirements for States and organisations wanting to read and verify this data and specifies a PKD that ICAO can implement. The report also provides specifications for additional optional security features that can be adopted to counter threats of skimming and eavesdropping of data from contactless chips and the prevention of chip substitution.

1.4 The Technical Report has been incorporated into the sixth edition of Doc 9303 Part 1, Volume 2.

1.5 Issues, arising from implementation practices, that come within the scope of the Technical Report, e.g. the relevant part of the sixth edition of Doc 9303 Part 1, Volume 2, are being addressed in the "Supplement--9303". The purpose of this Supplement is to provide guidance, advice, update, clarification and amplification as a "bridge" between the formal drafting of Standards and Technical Reports and the needs of the Travel Document community to have timely and official direction to rely on. The Supplement is being published on a regular base.

2. BACKGROUND

2.1 Version 1.1 of the Technical Report, e.g. the relevant part of the sixth edition of Doc 9303 Part 1, Volume 2, is intentionally limited to MRTDs offering ICC *read-only* access. The chip should be locked after personalisation and no provisions have been specified to secure writing data to the chip after issuance of the MRTD. Future developments may lead to the need for specifying such provisions.

2.2 The specified measures concern the authenticity, integrity and protection of the Logical Data Structure (LDS), containing only the face being the *primary* biometric. Intentionally, in this version no provisions have been specified to secure additional *secondary* biometrics, such as finger and iris. States, wishing to incorporate these biometrics into their MRTDs in an interoperable way, will encounter the need for specifications.

2.3 The specified protocols, algorithms and recommended minimum key lengths are based on the state of technology at the time of writing the specifications, bearing in mind the validity periods for MRTDs of 5-10 years. Due to the rapid evolution of technology and computer power, it was foreseen that they need continuous evaluation, of which the results will be reflected in the Supplement.

2.4 The Technical Report "PKI for Machine Readable Travel Documents Offering ICC Read-only Access" and the Technical Report "Development of a Logical Data Structure (LDS) for Optional Capacity Expansion Technologies" are related. Changes and further development of the LDS need to remain in harmony with the appropriate security measures and therefore require evaluation of the PKI.

3. ACTION BY THE TAG/MRTD

3.1 The TAG/MRTD is invited to:

a) approve continuation of the on-going development of guidelines and standards being carried out by the NTWG in the area of securing electronic data in MRTDs and MRTD related systems;

b) decide that a Version 2 of the PKI Technical Report will be developed in which the resulting guidelines and standards will be specified, for subsequent consideration and adoption by the TAG-MRTD; and

c) decide that this Technical Report be guided by the suggested draft Table of contents in the Appendix to this Working Paper, including but not limited to the subject matter listed therein.

— — — — — — — —

APPENDIX

TECHNICAL REPORT "PKI FOR MACHINE READABLE TRAVEL DOCUMENTS – VERSION 2"

DRAFT TABLE OF CONTENTS

1. **INTRODUCTION**

1.1 Scope and purpose

1.2 Backwards compatibility

1.3 Relation to other documents

1.3.1 TR-PKI V1.1

1.3.2 Doc 9303, sixth edition

1.3.3 Supplement – 9303

1.3.4 Guide to Interfacing e-MRTDs and Inspection Systems

1.3.5 LDS

1.4 Assumptions

1.5 Terminology

1.5.1 Technical Report Terminology

1.5.2 CAs, Keys and Certificates

1.5.3 Abbreviations

2. **EVALUATION**

2.1 Passive Authentication

2.2 Basic Access Control

2.3 Active Authentication

2.4 Minimum key lengths

2.5 Recommended Algorithms

3. **SPECIFICATIONS**

3.1 Passive Authentication for Multiple Data Group Entrances

3.2 Extended Access Control

3.3 Chip contents updating

3.4 Authority Revocation List

4. **APPENDICES**

— END —