International Civil Aviation Organization

TAG-MRTD/19-WP/4
2/11/09
English Only

WORKING PAPER

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 2.4: Technical Report Supplemental Access Control

TECHNICAL REPORT SUPPLEMENTAL ACCESS CONTROL

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

1. INTRODUCTION

1.1 The Technical Report on "Supplemental Access Control" specifies an access control mechanism that is supplementary to Basic Access Control.

1.2 The specified access control mechanism is a framework that allows for various implementation options, e.g. mappings, algorithms, passwords, et cetera.

1.3 In the Technical Report choices for the implementation in Machine Readable Travel Documents are defined.

2. BACKGROUND

2.1 Doc 9303 Part 1 as well as Part 3, Volume 2, Section IV provides the specification of the OPTIONAL Basic Access Control mechanism, which protects the contents of the IC against skimming and eavesdropping.

2.2 For this purpose Basic Access Control enforces the Inspection System to authorize itself before granting access to the chip data and it establishes a secure (encrypted) communications channel.

2.3 The security provided by Basic Access Control is limited by the design of the protocol. The data that is used for the generation of the Basic Access keys are Document Number, Date of Birth, and Date of Expiry. As a consequence the resulting keys have a relatively low entropy.

2.4 Although Basic Access Control is OPTIONAL, due to its simplicity it turned out to be very successful and a vast majority of eMRTD issuing States have implemented it. Thus the Basic Access Control mechanism is now recognized as a RECOMMENDED feature for privacy protection.

2.5 Basic Access Control was specified in 2004, meaning that eMRTDs issued now with a validity period of 10 years near the end of their validity period are protected by a 15 years old privacy protection mechanism. Due to the ongoing increasing computer power, successful attacking eavesdropped communications will become more and more feasible during this time period. Therefore a work item on the development of an alternative to Basic Access Control was started.

2.6 This Working Paper introduces the Technical Report on “Supplemental Access Control”, being the result of this work.

3. SUPPLEMENTAL ACCESS CONTROL

3.1 Supplemental Access Control is based on the access control mechanism “Password Authenticated Connection Establishment” (PACE) as framework.

3.2 Similar to Basic Access Control PACE also enforces authorized access to the chip contents and establishes Secure Messaging between an MRTD chip and an inspection system. However, in the PACE protocol the entropy of the password(s) used to authenticate the inspection system has much less influence on the strength of the keys and can therefore be very low.

3.3 For globally interoperable machine readable travel documents two passwords have been defined:

a) Document Number, Date of Birth and Date of Expiry from the MRZ (similar to Basic Access Control);

b) A “Card Access Number” (CAN), which is a number printed on the data page or on the front side of an id-1 size MRTD. Since this CAN can be relatively short (6 digits generally are sufficient) it has the advantage that it can easily be typed in manually.

3.4 Although the cryptographic protocols differ, the inspection procedure when a MRTD with Supplemental Access Control is offered to an inspection system is similar to Basic Access Control. Optically or visually read information is used to derive a PACE Key to gain access to the chip and to set up a secure channel for communications between the MRTD chip and the inspection system.

4. PATENT CONSIDERATION

4.1 PACE allows for various implementation options, e.g. mappings, algorithms, passwords, et cetera. The technical report specifies a few options with respect to mappings. For one of these options a patent is pending.

4.2 The patent holder of this mapping has indicated that the patent application has mainly a protective character, and therefore the patent holder does not want this patent to be an obstacle to the definition of a password based authentication mechanism named PACE.

4.3 This statement of the patent holder is under consideration of the NTWG, which will result in a choice between a number of available solutions, as described in a separate Information Paper on this subject.

5. IMPLEMENTATION STRATEGY

5.1 A key consideration in the development has been preserving global interoperability. Therefore the PACE protocol is defined as being supplemental to Basic Access Control. It MAY be implemented in addition to Basic Access Control, but not instead of it.

5.2 Inspection Systems SHOULD implement and use PACE if provided by the MRTD chip.

5.3 Basic Access Control will remain the "default" access control mechanism for globally interoperable MRTDs as long as it provides sufficient security. Basic Access Control may however become deprecated in the future. Therefore in time PACE will become the default access control mechanism.

5.4 The approach described above allows for a gradual change over from BAC to PACE during of the next 10 to 20 years.

6. ACTION BY THE TAG/MRTD

6.1 The TAG/MRTD is invited to:

a) recognize the necessity to specify a access control mechanism supplementary to Basic Access Control;

b) mandate the NTWG to negotiate the solutions with respect to the mentioned patent consideration and incorporate the conclusion in the final version of the Technical Report;

c) approve the Technical Report "Supplemental Access Control" containing this specification for inclusion into Document 9303;

d) promote the implementation of "Supplemental Access Control" in eMRTDs and Inspection Systems within a period of 5 years from the date of this Working Paper.

— END —