International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/16
WP/26
13/9/05
English only

TECHNICAL ADVISORY GROUP ON MACHINE READABLE TRAVEL DOCUMENTS

Sixteenth Meeting

(Montreal, 26 to 28 September 2005)

Agenda Item 4: Implementation of the Public Key Directory

PKD MEMORANDUM OF UNDERSTANDING TO BE SIGNED BETWEEN ICAO AND PARTICIPATING STATES INDIVIDUALLY

(Presented by the Secretariat)

1. INTRODUCTION

1.1 During its 175th Session, the Council approved the establishment of a Public Key Directory (PKD), a database of public keys that is essential for the successful and secured, worldwide implementation and interoperability of electronic passports under the supervision of ICAO on a cost-recovery basis.

1.2 In addition, the Council requested the Secretariat to develop a template text of the formal arrangement between ICAO and the States willing to participate in the PKD system [Participation Agreement or Memorandum of Understanding (MoU)], which will be discussed during the coming Session. This MoU will legally support formal arrangements between ICAO and each PKD Participating State in regards to the PKD system. A separate agreement will be signed with each Participating State and ICAO, and will solely bind the signing State concerned. ICAO Contracting States that are not involved with the PKD system will not be financially or legally bound in any way in relation to this system.

2. CONTENTS OF THE MOU

2.1 Some highlights of the MoU, which is attached to this working paper, include, *inter alia*, the following:

2.1.1 A clause envisaging that the contract to be concluded between ICAO and the selected contractor is to be entered into on behalf of, and as mandatory of, the e-passport issuing States. Such contract will, *inter alia*, explicitly exclude ICAO from liability of any kind arising out of or in connection with the performance of the contract. It will also contain a provision on indemnification for the benefit of ICAO, according to which the Contractor is obliged to save and hold harmless ICAO, its officials and employees from claims of any kind or nature in relation to the operation of the PKD, including demands or claims made by third parties. The said contract will also contain a clause pertaining to ICAO's privileges and immunities, as well as a disclaimer clause according to which ICAO shall not be held liable in the event the PKD System were not viable for the operator from a commercial point of view.

2.1.2 Regarding ICAO Secretariat liability, the MoU includes, *inter alia*, the following:

a) a clause releasing ICAO from any liability that may arise in regard to the interoperability of a public key with a chip. A notice containing this and similar disclaimers will be posted on the PKD web site that will be used for downloading the public keys;

b) a clause holding jointly and severally liable all e-passport issuing States participating in the constitution of the PKD for all expenses related to the implementation and operation of the system, for the period established in the contract signed with with ICAO with the vendor chosen, and relieving the Organization of any financial or legal liability that may arise in relation to this project;

c) a clause by which e-passport issuing States assume full responsibility for any claim that may arise due to the use of e-passports related technology, and relieving the Organization of any financial or legal liability that may arise in relation to this project; and

d) a clause holding jointly and severally liable participating e-passport issuing States for any expenses or damages ICAO may incur due to any third party claims arising in relation to the PKD project.

2.1.3 Regarding the PKD Participating State, the MoU includes, *inter alia*, the following:

a) a clause that the Public Key Directory will be built and operated on a cost-recovery basis, including all costs incurred by ICAO in organizing, implementing and performing the functions related to the PKD, and that it will be fully supported by contributions and fees from Participating States;

b) a clause that the Participating State will abide by the PKD Regulations as approved by the TAG/MRTD at its 16th Meeting; and

c) a clause that, regarding payments for participating in the PKD system, each Participating State will negotiate and specify all the necessary administrative arrangements to allow its participation in the PKD system.

2.1.4 Regarding liability and other claims arising when valid passport with authentic information are not accepted due to an error, or in the event an invalid or fraudulent passport were accepted by airlines by error, these will usually dealt with by airlines and governments through administrative processes. It should be mentioned that these liabilities or claims exist today when airlines

or authorities examine conventional passports and the introduction of more sophisticated passports and reading systems will not change this situation.

2.1.5 Regarding ICAO Secretariat functions, the MoU describes functions such as overseeing implementation of the procedures, rules and regulations developed by the TAG/MRTD expert group, implementing any updates as may be provided from time to time, and updating the schedule of the user fees as may be required. In performing these functions, the Secretariat will benefit from the advice of the TAG/MRTD group of experts.

2.1.6 Regarding the interoperability of the public keys, each Participating State is responsible for the proper functioning of the public keys that it issues, in authenticating the respective passport to which they relate. Regarding the global interoperability, this is to be achieved by the operation of the PKD system itself.

3. ACTION BY THE TAG/MRTD

3.1 The TAG/MRTD is invited to:

a) to review the attached draft of the MoU; and

b) to make any pertinent comments and suggestions for inclusion in the final draft of the MoU to be presented to the Council in the coming Session.

— — — — — — — —

APPENDIX

Memorandum of Understanding (MoU)
between
the International Civil Aviation Organization
and State [formal name]
regarding Participation in the Public Key Directory (PKD)"

Draft version 1.1

27 September 2005

Whereas the ICAO Council during its 175th Session 31 May 2005 confirmed the development of a Public Key Directory under the supervision of ICAO;

Whereas the PKD Regulations have been approved by the Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD) during its 16th meeting, held in Montreal on 27 and 28 September 2005;

Whereas the ICAO Secretary General has selected and entered into contract negotiations with Netrust as the chosen PKD supplier.

IT IS AGREED AS FOLLOWS:

State [formal name], hereafter referred to as State [abbreviated name], hereby agrees to participate in the Public Key Directory as established in this MoU.

1. Definitions

For the purpose of this Agreement:

1. **"PKD"** means the Public Key Directory. This directory contains Document Signer Certificates (C_{DS})and Certificate Revocation Lists (CRLs) as defined below.

2. "**Participating State**" means a State that is or will soon be issuing e-passports and has registered with ICAO as a participant in the PKD for the uploading of digital signing key certificates.

3. "**Non-participating Entities**" means those States or other organizations or individuals who wish to have access to information in the PKD READ Directory.

4. "**ICAO PKD Operations Office**" means the PKD office staffed and managed by ICAO that carries out verification, due diligence, and updating of Document Signer Certificates (C_{DS}) forwarded from States to the PKD READ Directory.

5. "**ICAO PKD Programme Office**" means the ICAO organizational entity, currently the Air Transport Bureau (ATB), which is responsible for the supervision and management of the ICAO PKD Operations Office, as well as for the overall ICAO PKD Programme.

6. "**PKD Advisory Group**" means that group to be appointed by the TAG/MRTD which is ultimately responsible for recommending to the TAG/NTWG, regulations, procedures, fees, and other aspects of the PKD. The PKD Advisory Group has no authority over ICAO, but the ICAO PKD Programme Office manages and operates the Public Key Directory for the Participating States within the regulations and guidelines agreed upon by the PKD Advisory Group. It is essential that this group be established and in place prior to the completion of the detailed design of the ICAO PKD service..

7. "**PKD Operator**" means the commercial entity or contractor that has been contracted by ICAO to carry out the complete technical operations of the PKD, as well as fee collection and accounting for the PKD, in accordance with the contract entered into between ICAO and the PKD Operator in this regard.

8. "**PKD READ Directory**" is the read-only PKD directory containing all Document Signer Certificates and CRLs. This directory cannot be modified by Participating States.

9. "**ICAO**" means the International Civil Aviation Organization headquartered in Montreal, Canada.

10. ***"Document Signer Certificate"*** (C_{DS}) means a PKI certificate that contains a Public Key (and other information) that must be used to decrypt and verify a digital signature on an e-passport.

11. ***"Country Signing CA Certificate"*** (C_{CSCA}) means a PKI certificate containing a Public Key (and other information) that must be used to decrypt and verify a digital signature on a Document Signer Certificate (C_{DS}).

12. "***Certificate Issuing Location***" (CIL) means a location which is designated by a Participating State as one which will send the Document Signer Certificates (C_{DS}), duly signed by the CSCA, to the ICAO PKD.

13. ***"Country Signing CA"*** (CSCA) means that Certificate Authority in a Participating State which is responsible for managing the Country Signing CA Certificate (C_{CSCA}) that is used to sign all State Document Signer Certificates (C_{DS}). The CSCA is the highest trust authority in the Participating State with regard to the ICAO PKI infrastructure.

14. "***e-passport Authority***" (EPA) means the main organizational entity and officer of a Participating State responsible for all State Document Signer Certificates (C_{DS}) forwarded to the PKD.

15. ***"CRL"*** means Certificate Revocation List, used by States to revoke certificates issued by them, or to signify positively that no such revocations exist for their certificates (null CRLs).

16. ***"LDAP***" means Lightweight Directory Access Protocol, a PKI technology directory protocol which is the basis for the PKD.

2. **Objective**

2.1 The objective of this Agreement is to set out the conditions and requirements for the establishment and participation of a **State** in the ICAO Public Key Directory.

3. **PKD Rules and Regulations**

3.1 The PKD Rules and Regulations approved by the TAG/MRTD during its 16th meeting, held in Montreal on 27 and 28 September 2005, and their amendments shall be considered as an integral part of this Agreement.

4. **Participation**

4.1 Participation in the PKD shall be open to all Contracting States, subject to their meeting the conditions laid down in Article 4.2.

4.2 The following conditions are to be met by States willing to participate in the PKD…

5. **Authorization to enter into Contractual Agreement on behalf of the State**

5.1 **[State]** authorizes ICAO to enter into a contract agreement with the selected PKD Operator on behalf of, and as mandatory of, **[State]**. Such contract will, *inter alia*, explicitly exclude ICAO from liability of any kind arising out of or in connection with the performance of the contract. It will also contain a provision on indemnification for the benefit of ICAO, according to which the PKD Contractor is obliged to save and hold harmless ICAO, its officials and employees from claims of any kind or nature in relation to the operation of the PKD, including demands or claims made by third parties.

5.2 The contract mentioned in Article 5.1 will also contain a clause pertaining to ICAO's privileges and immunities, as well as a disclaimer clause according to which ICAO shall not be held liable in the event the PKD System is not viable for the operator from a commercial point of view.

6. **Cost Principle**

6.1 The PKD shall be established, operated and maintained on a cost-recovery basis, to be financed by voluntary contributions and fees as approved by the TAG/MRTD during its 16th Meeting and which are found in Attachment XX, from Participating States that produce e-passports and wish to transmit their country public keys as established in the PKD Rules & Regulations for uploading into the Directory.

6.2 All costs incurred by ICAO in organizing and performing the functions related to the PKD will also be borne by Participating States.

6.3 ICAO shall establish a separate special account for the receipt and distribution of contributions and assessments related to this issue.

6.4 The initial investments, costs and expenses necessary for the establishment of the PKD System, will be borne by the PKD Operator with eventual reimbursement from contributions and fees from Participating States.

7. **System Design**

7.1 The System Design and Technical Specifications for the establishment, development and operation of the PKD is set out in Annex....and is an integral part of his Agreement.

8. **Obligations of Parties**

8.1 The [State] undertakes to comply and conform at all times with the requirements set out in this MoU, the PKD Rules and Regulations and the Technical Specifications as amended from time to time.

9. **PKD Operational Concept**

9.1 The PKD Operator will be solely responsible for the performance of the system.

9.2 The verification function to be performed by the ICAO Operations Office, which will be located in ICAO Headquarters, consists of the following: each public key that is sent from a Participating State to ICAO will be “wrapped” in a package of data known as a certificate. The certificate itself will be digitally signed, and the signature will be encrypted. ICAO’s task will involve decryption of this digital signature using the State’s country-signing key and recomputing it to verify that the certificate is authentic and unaltered. All Country Signing Certificate Authority (CA) Certificates will be physically located in these facilities. Subsequently, ICAO staff will upload the public key, in the same form as it was received, into the main directory. The design and operational plan for the PKD call for the involvement of more than one person in these procedures, in order to minimize errors and optimize data security.

9.3 The ICAO PKD Programme Office will oversee the implementation of the procedures, rules and regulations developed by the TAG/MRTD expert group, implement any updates as may be provided from time to time, and update the schedule of the user fees as may be required. In performing these functions, the PKD Programme Office will benefit from the advice of the TAG/MRTD group of experts.

9.4 Regarding the interoperability of the public keys, [State] is solely responsible for the proper functioning of the public key that it issues, in authenticating the respective passport to which they relate.

10. **Liability**

10.1 ICAO is released from any liability that may arise in regard to the interoperability of a public key with a chip [what chip? Perhaps need to be more specific]. A notice containing this and similar disclaimers will be posted on the PKD web site that will be used for downloading the public keys.

10.2 **[State]** and all Participating States shall be held jointly and severally liable for all expenses related to the implementation and operation of the system, for the period established in the contract signed by ICAO with the PKD Operator, relieving the Organization of any financial and/or legal liability that may arise in relation to this project. [State] reserves the right to claim to the other Participating States their respective portion.

10.3 **[State]** and all Participating States assume full responsibility for any claim that may arise due to the use of e-passports-related technology, and relieving the Organization of any financial and/or legal liability that may arise in relation to this project.

10.4 **[State]** and all Participating States shall be held jointly and severally liable for any expenses or damages ICAO may incur due to any third party claims arising in relation to the PKD project. [State] reserves the right to claim to the other Participating States their respective portion.

10.5 The PKD Operator will have sole responsibility for data protection, data integrity, and availability of the PKD in accordance with the contract entered into between ICAO and the PKD Operator.

11. **Fee Schedules and Payments**

11.1 The fee schedules to be paid by **[State]** and the terms and conditions under which fee payments are required, when they are due, and the actions that may take place in the event of overdue payment of fees are found in Attachment. **[State]** hereby agrees to abide by all such fee schedules and payment terms and conditions, including redress for late payments or other defaults.

11.2 A schedule of state sign-up fees and annual user fees will be calculated taking into account the total estimated cost for a five-year operation, including the costs to ICAO, the number of countries expected to sign up in each of the five years, and the number of passports in circulation in each country.

11.3 These fees will be revised every …by the PKD Operator in conjunction with the ICAO PKD Programme Office, with the input from the PKD Operation Office. The resulting new schedule of fees will be communicated to Participating States in due time and form and will be considered part of this MoU.

11.4 Participating States will be required to pay sign-up fees and annual user fees in advance of depositing their keys in the system.

11.5 None of the Participating States shall be liable for any damage or loss of any kind arising from or in relation to failures and/or omissions in the provision, operation and maintenance of the PKD System.

11.6 Notwithstanding the previous paragraph, **[State]** shall, jointly and/or severally, indemnify and hold harmless, and defend, at its expense, ICAO, its officials, agents, servants and employees, from and against all suits, claims, demands and liability of any kind, including their costs and expenses, arising out of or in relation to the establishment, provision, operation and maintenance of the PKD System.

12. **Facilities and Personnel required**

12.1 The facilities and personnel required by the ICAO PKD Programme Office and the ICAO Operations Office for the purpose of providing, operating and maintaining the PKD System are listed in Annex..... to this Agreement.]

13. **Obligations of the PKD Operator**

13.1 The **PKD Operator** shall establish, operate (administer) and maintain the PKD System in accordance with the Technical Specifications set out in Attachment.....

14. **Amendments**

14.1 This MoU may be amended by an instrument in writing signed by duly authorized representatives of both parties.

15. **Settlement of Disputes**

15.1 Any dispute relating to the application or interpretation of this Agreement which cannot be settled by negotiation between the parties involved shall, upon request by any of the parties, be referred to the Council of ICAO for its recommendation. The decision of the Council shall be final and binding on the parties involved.

— END —