International Civil Aviation Organization

WORKING PAPER

TAG-MRTD/16
WP/24
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

ADOPTION OF DRAFT REGULATIONS VERSION 1.4 FOR THE ICAO PUBLIC KEY DIRECTORY (PKD)

(Presented by the Secretariat)

1. SUMMARY

1.1 This Working Paper presents the first working draft of regulations necessary for the participation in PKD by States and for the operation of the PKD by ICAO. These Regulations, if adopted, will provide basic guidance and understanding of PKD operations to all States. Action by the TAG/MRTD is in paragraph 4.

2. BACKGROUND

2.1 States planning to participate in the PKD require interface and data architecture specifications and other technical documentation to enable them to implement systems and software to upload their own certificates and access the entire directory.

2.2 In addition States, and all potential Users of the PKD, require a set of PKD Regulations which clearly set out what the PKD is intended to do, how the PKD will operate in terms of update frequency, response time to action requests, limitations of liability regarding the various entities involved with the PKD, fees and participation payment requirements, and other aspects of the PKD operation.

2.3 ICAO project staff developed draft versions of the PKD Regulations in the summer of 2005. This work was scrutinized carefully and edited, in August 2005, by the PKD Overview Group (OG), consisting of four technical experts appointed by the NTWG. The result was Version 1.4, which was recommended by the OG as the version that should be put to the TAG/MRTD for consideration and approval as the first published draft.

3. IMPACT ON PKD IMPLEMENTATION AND ON OTHER RELATED PROGRAMS

3.1 Adoption of the current Draft of the PKD Regulations is of fundamental importance to the implementation and operation of the PKD. Together with the PKD Draft MOU for participating States, it will be used as a design guide by the PKD implementation Contractor regarding crucial elements such as priorities for different service requests, response times, bandwidth requirements, and other functional characteristics of the PKD.

3.2 The Regulations also address the collection of fees and actions to be taken in the event of overdue payments.

3.3 Furthermore, regulations are necessary as a guide to the development of detailed operating procedures for the PKD.

3.4 The PKD regulations are important for the PKD, which is in turn essential for the operation of the proposed ICAO PKI infrastructure. It is necessary for the issuance of e-passports containing RF computer chips, biometric and other holder information, and the application of digital signatures for authentication of the data stored.

4. ACTION BY THE TAG/MRTD

4.1 The TAG-MRTD is invited to:

a) recommend that the Draft PKD Regulations Version 1.4 be adopted by ICAO as the first published draft of these Regulations;

b) agree that the adopted Draft regulations be circulated to all interested States for review and suggestions, and be used as a guide to States' development of systems and procedures to interface and operate with the PKD; and

c) note that the publication of revisions and amendments as deemed necessary be henceforth managed by the ICAO PKD Program Office under the guidance and acknowledgement of the PKD Advisory Group to be formed by the TAG/MRTD.

— — — — — — — —

THE ICAO PUBLIC KEY DIRECTORY (PKD)

DRAFT REGULATIONS

VERSION 1.4

AUGUST 4, 2005

Release Control

Release	Date	Description
1.1	07-13-2005	First draft of PKD regulations from D Clark
1.2	07-20-2005	Revised draft based on ICAO internal review
1.3	07-22-2005	Further revisions from initial review of the PKD OG Committee.
1.4	08-04-2005	First released draft resulting from edits, additions and clarifications by the OG

Release Notes

Version 1.1

Initial regulations text developed by D Clark.

Version 1.2

Revisions based on inputs and comments from various ICAO representatives, including ATB, TCB, Procurement, and others.

Version 1.3

Further revisions based on input from some members of the NTWG-appointed PKD Overview group.

Version 1.4

Final revisions and first released draft of Regulations resulting from specific reviews and recommendations of the PKD Overview Group, consisting of Alan Bennett (Australia), Robert Carter (UK), Rich Martin (USA), and Jun Ono (Japan).

Table of Contents

Section 1 - Authority

1.1 These regulations are issued by the ICAO PKD Program Office pursuant to (TAG minutes, Council resolutions, etc.) – to be completed

Section 2 - Definitions

2.1 "PKD" means the Public Key Directory. This directory contains Document signing certificates and Certificate Revocation Lists as defined below.

2.2 "**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 upload of digital signing key certificates.

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

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

2.5 "**ICAO PKD Program Office**" means the ICAO organizational entity, currently the ATB, which is responsible for supervision and management of the ICAO PKD Operations Office as well as for the overall ICAO PKD Program.

2.6 "**PKD Advisory Group**" means that group to be appointed by the TAG/NTWG which is ultimately responsible for recommending to TAG/NTWG, regulations, procedures, fees, and other aspects of the PKD. The PKD Advisory Group has no authority over ICAO, but the ICAO PKD Program 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 vital that this group be established and in place prior to the completion of the detail design of the ICAO PKD service.

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

2.8 "**PKD READ Directory**" is the read-only PKD directory containing all document signing certificates and CRL's. This directory cannot be modified by participating States.

2.9 “**ICAO**” as used herein means the International Civil Aviation Organization headquartered in Montreal, Canada.

2.10 ***“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.

2.11 ***“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}).

2.12 “***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.

2.13 ***“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.

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

2.15 ***“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).

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

Section 3 - General Provisions

3.1 The Public Key Directory shall be accessible 24 hours per day, 7 days per week.

3.2 Only Participating States shall have PKD access for certificate update purposes.

3.3 All entities shall have open access to the PKD for download without pre-registration or sign-on. However, entities other than participating States may have restrictions imposed on the frequency of downloads requested daily.

3.4 All participating States shall also have access to the PKD for queries of individual certificates or CRLs..

3.5 Technical support shall be available to participating States on a 24 hour per day, 7 days per week basis, by web access and by telephone. The PKD technical support website will contain extensive FAQ and other information in the 6 official ICAO languages, and telephone and email locations for direct operator support in at least 2 languages, one being English.

3.6 Technical support for all non-participating entities shall be restricted to access to the PKD technical support website. Access to direct operator technical support by email or telephone is not an obligation of the PKD Operator or the Participating States, and may be made available as an option to non-participating entities on a fee-for-service basis by the PKD Operator. Such arrangements will be made with the consent of the ICAO PKD Program Office and the PKD Advisory Group.

Section 4 – Registration - Information Requirements

4.1 Only States issuing e-passports, or about to issue e-passports, will register and participate in the PKD.

4.2 States wishing to participate will advise the ICAO PKD Program Office of their intent to do so in writing, duly signed by a senior government official or ICAO delegate.

4.3 Information to be provided will consist of at least the following components:

4.3.1 The designation of the single officer or organizational entity within the State, the "***e-passport Authority***" (EPA) of the State, who will be the main officer responsible for all State Document Signer Certificates (C_{DS}) forwarded to the PKD. This designation must include the name, title, location, position of the person primarily responsible in the State, along with the information of his or her designated senior officer

4.3.2 The designation of the State's ICAO PKI ***Country Signing CA*** (CSCA), including the name, position, office, title, and contact information regarding the State's CSCA.

4.3.3 The designation of one or more sending locations that will be sending certificates from the State CIL's of the State.

4.3.4 A statement of the total number of all passports issued in the last 12 months by the State, and the total number of all passports presently in circulation by the

State. This information will be updated annually.

4.3.5 A statement of the estimated number of Document Signer Certificates (C_{DS}) and CRL sets, including null CRL's that will be issued by the State each year.

4.3.6 A certificate representing the ***Country Signing CA Certificate*** (C_{CSCA}) distributed securely by diplomatic courier or equivalent, and containing the CSCA's Public Key for verification of Document Signer Certificates (C_{DS}) regularly sent by the States' EPA and CILs. This may be sent later, at systems integration time but prior to e-passport issuance by the participating State. C_{CSCA} ‘s shall be securely stored only at the ICAO Operations Office.

Section 5 – Registration - Setup and Integration Process

5.1 Upon provision and review of all of the above information, the ICAO PKD program Office shall arrange for the participating State to carry out and implement the following items:

5.1.1 A ***Memorandum of Understanding*** (MOU) to be signed between ICAO and the State substantively in the form as that attached to these regulations. This MOU will at a minimum include the following terms, among others:

5.1.1.1 **Limitation of Liability.** The MOU will set out the procedures and conditions under which the ICAO PKD will accept and perform due diligence reviews on State-supplied certificates, and upload them into the PKD Directory, and the State will accept these procedures and conditions as satisfactory and sufficient to keep the ICAO PKD Program Office, the ICAO PKD Operations Office, and the PKD Operator free of liability regarding certificate content on the PKD. Likewise, the MOU will specify that the PKD Operator, but not ICAO, will have responsibility for data protection, data integrity, and availability of the PKD in accordance with the contract between ICAO and the PKD Operator.

5.1.1.2 **Fee Schedules and Payments.** The MOU will designate the fee schedules appropriate to the 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. The State will agree in the MOU to abide by all such fee schedules and payment terms and conditions, including redress actions for late payments or other default.

5.1.2 **Registration and Setup Fees.** The State shall make the appropriate registration fee payment in full before any work commences between the ICAO PKD Operations Office, the PKD Operator, and the State to integrate the State and its certificates into the PKD.

5.1.3 **Scheduling Commencement of Setup**. Upon signing of the MOU and State payment of the registration and setup fees, the State shall specify a date within the 12 month period thereafter when it wishes to actively commence integration testing of its certificate issuance process with the ICAO PKD Operations Office and with the PKD Operator. Prior to that the State shall have access to all ICAO PKD Technical Specifications, including PKD Interface Specifications, access to a PKD Operator-provided proxy PKD test bed facility, and some limited technical assistance from the PKD Operator as specified in the ICAO contract with the PKD Operator, to aid the State in designing and integrating an ICAO PKI certificate generation and issuance facility within the State. Technical cooperation and support for final integration testing shall commence on the integration test date specified by the State.

5.1.4 **Responsibility for Integration**. The design and implementation of software and computer systems to integrate a State's e-passport certificate issuance requirements into the PKD are the sole responsibility of the participating State. Limited design support services and test bed facilities are provided by the PKD Operator for assistance in this regard, as part of the setup fee, but are not warranted. Any additional PKD Operator technical services beyond those defined in the contract with the PKD Operator, whether for initial design and development or for final setup integration, can be accommodated as a matter of separate contract arrangements between the State and the PKD Operator, without any obligation or involvement of, or warranty by, the ICAO PKD Program Office.

5.1.5 **Commencement of Annual Operational Fees.** Annual operational fees shall first become collectible from the State upon final written acceptance of the setup process by the State and by the ICAO PKD Program Office regarding integration of the State's certificates into the PKD; this is not to be later than 90 days after commencement of setup integration as above except as otherwise agreed between the State and the ICAO PKD Program Office in exceptional circumstances.

Section 6 - PKD Upload

6.1 New Document Signer Certificates (C_{DS}) and Certificate Revocation Lists (CRL's) will be forwarded by a State CIL electronically to the ICAO PKD Operations Office in a form provided by the PKD Interface Specifications. Communication shall be protected by a secure connection. Each C_{DS} shall be forwarded 90 days in advance but not less than 30 days except in the case of unusual or urgent situations. CRL's, including null CRL's as stated in the PKI technical report, shall be forwarded on a timely basis.

6.2 Upon receipt, the ICAO PKD Operations Office shall automatically send a systems-level acknowledgement of each message. A separate application-level custom receipt shall be sent to the participating State EPA.

6.3 The ICAO PKD Operations Office shall carry out appropriate certificate verification, and shall upload the certificate to the PKD READ Directory update queue, in a normal time period of 24 hours but not to exceed 72 hours after receipt.

6.4 Successful C_{DS} and CRL upload shall be confirmed by another application-level notification to the State's EPA.

6.5 The new certificate will be available after the next version update of the PKD READ directory from the batched update queue of new certificates, not to be later than 12 hours after posting to the queue by the ICAO PKD Operations Office.

Section 7 - PKD Download

7.1 A PKD download is a file transfer of a complete copy of the latest version of the PKD READ Directory in existence at any time. It is expected that Participating States will download on a daily basis.

7.2 All entities can access the PKD READ Directory and request a download. The access shall not require any sign-on or permission-based methodology. Requesting sites that represent participating States shall be given download priority if bandwidth limitations and excess demand create a backlog situation at any time. Registered participating States shall have a unique access capability designed in the architecture.

7.3 Download requests by Non-participating entities shall be subject to prior acceptance of ICAO's Terms and Conditions, to be displayed on the screen as appropriate.

7.4 As part of the access protocol, the recipient will be directed to a related website or other PKD data area where data integrity checks are provided for each download version, also protected by secure communications.

Section 8 - PKD Query

8.1 A query is a request for an individual C_{DS} on the PKD READ Directory. This is a more customary application request made of an LDAP Directory, to find and verify a certificate reference contained on a document (in this case, an e-passport), and to obtain the appropriate public key to verify the digital signature.

8.2 Only registered participating States will have query capability.

8.3 Queries will take lower precedence than any download request, but will have a design maximum wait time of x minutes (tbd).

8.4 All PKD READ Directory query communications will be protected by secure communications.

8.5 Any query restrictions to be imposed on any participating State will be negotiated and agreed with that State and approved by the PKD Advisory Group representing all participating States.

Section 9 - Fee Collections

9.1 Fees will be proposed by the ICAO PKD program Office in consultation with the PKD Operator, and will be endorsed by the PKD Advisory Group representing all participating States.

9.2 Fee schedules and PKD cash flow will be reviewed annually, or more frequently as required by circumstances. Any surplus will remain to the credit of a PKD reserve, or be used to credit fee accounts, as may be decided by the ICAO PKD Program Office and the PKD Advisory Group.

9.3 Fees will be collected by the PKD Operator, who will maintain an invoicing, accounts payable, and account reporting and control system on behalf of the ICAO. Participating States will set up their own invoicing and payment mechanisms appropriate for that State, as specified in their specific MOU

9.4 All fees collected will be deposited to an account that is used to pay all ICAO PKD Program and PKD Operator PKD costs in accordance with the provisions of the ICAO contract with the PKD Operator.

9.5 It is expected that the accounts of the PKD service shall be audited annually..

Section 10 - Complaints

10.1 Documented and substantiated complaints may be made by participating States only. All operational complaints and issues are expected to go through the PKD Operator helpdesk. Procedures will be developed that detail the hierarchical structure to support the remediation of any complaints.

10.2 All non operational complaints should be kept confidential.

10.3 The entity to which complaints are made shall promptly address each complaint. If discussions or a satisfactory outcome is not received in a timely manner, not more than 30 days in each case, then the complaining party may take the complaint to the next higher complaint level as defined by the complaints procedures document.

10.4 None of the PKD Operator, the ICAO Operations Office, the ICAO PKD Program Office, or the PKD Advisory Group has any obligation to agree with or accommodate any complaint once all PKD authority levels have reviewed the complaint without finding merit in it.

Section 11 - Confidentiality

11.1 All PKD READ Directory information is, by its nature, open to the public.

11.2 Information pertaining to participating States, such as State EPA and CIL information, fees and schedules and the status of individual State accounts, State upload frequencies and timing, and all such information outside of the strict contents of the PKD READ Directory shall be considered confidential and protected by ICAO and the PKD Operator.

Section 12 - Reports

12.1 The ICAO PKD Operations Office and the PKD Operator will produce appropriate statistics and other operating reports on a state by state basis restricted to such state. These reports will be on various statistics and measurements, such as technical and operational response times, update frequencies by countries, query and download access requests by entity, and many other statistics. Additionally, this information may be aggregated (not specifying participating states) and used in support of existing and proposed changes to architectures, technical support resources, ICAO operational staffing, and other matters, but kept strictly confidential.

12.2 The PKD Operator, on behalf of the ICAO PKD Program Office, the PKD Advisory Group and all participating States, shall produce regular financial reports showing aggregate accounting summaries by State and overall. These will show regular accounting results but also special cost accounting statistics measuring net fees paid for services provided, as detailed by a number of factors such as by Tier level, by certificate issued, and by other criteria. These statistics will be used to analyze and support fee changes as appropriate.

Section 13 - Adoption of PKD Procedures and Interface specifications

13.1 The ICAO PKD Program Office and the PKD Operator will develop and maintain detailed procedures that will describe the specific operation of the PKD and the operational interfaces of participating States. It is required that this operational procedures be published for review within the TAG/NTWG community.

13.2 The ICAO PKD Program Office and the PKD Advisory Group may, from time to time, amend these regulations.

Section 14 Final Provisions

14.1 Requests for amendments to these regulations may be submitted to the ICAO PKD Program Office and to the PKD Advisory Group, for review as determined by the PKD Advisory Group on the merits of the proposal.

14.2 These regulations and procedures shall be made electronically available to the public website.

— END —