A Primer on the ICAO Public Key Directory

White Paper

Version V1.5

Author:	Markus Hartmann, Stephan Körting, Olga Käthler
Date:	20/05/2009
Document ID:	Non
Confidentiality:	Public
Project or offer ID:	20013000

Table Of Contents

A Primer on the ICAO Public Key Directory

1 Summary

An electronic machine readable travel document (eMRTD), primarily the electronic passport (ePassport) will be of maximum use in facilitating international travel providing the introducing State considers how these electronic documents are validated at foreign borders. This is often overlooked by national authorities that introduce eMRTDs, mainly due to a lack of understanding the mechanisms of the underlying Public Key Infrastructure (PKI) and the central role of the ICAO Public Key Directory (PKD) in facilitating the validation process at international borders. This leads to the issuance of eMRTDs that cannot be electronically validated at foreign borders, thus loosing the main advantage of being electronically readable.

Without sharing critical information with other States via the ICAO PKD (or with huge efforts via bilateral agreements), an electronic MRTD has little or no benefit as compared to a non-electronic one.

➧ An ePassport issuer who participates in the ICAO PKD will:

- utilize eMRTD features
- save costs and efforts
- achieve the highest security

This document targets project managers of eMRTD projects and decision makers in eMRTD issuing agencies. It explains how eMRTDs can be electronically validated at international borders and why the ICAO PKD takes a central role in facilitating this process.

The section "Introduction to the ICAO Public Key Directory" gives an overview of the basic functionality of the document validation process via the ICAO Public Key Directory and explains the idea behind the established chain of trust.

The section "Benefits of the ICAO Public Key Directory " of this document describes why it is beneficial to a State issuing and validating eMRTDs.

The section "How to join the ICAO PKD" describes the steps necessary for joining the ICAO PKD.

1.1 A Note on Notations

Inserts

Background on technical concepts is provided in inserts. These concepts may be familiar to some readers and may be skipped by them without missing vital information from this document.

➧ Key statements are emphasized like this.

2 Introduction to the ICAO Public Key Directory

2.1 The Chain of Trust

Accepting a travel document as a token of identity at an international border requires three questions to be answered by the border control agent:

1. Does the document belong to the person providing it?
2. Is the document authentic and was it not falsified in any way?
3. Is the document rightfully issued by the proper authority entitled to issuing it?

Only after all three questions are answered positively, does the border control agent need to assess whether this document entitles its rightful bearer to enter the country.

The usual and well-known way of answering these questions by visually comparing the portrait photo with its owner and analyzing physical security features of the document found its electronic analogy in the world of eMRTD. The first question is additionally answered by a (possibly automated) comparison of the owner's face with the image stored inside the eMRTD. The second and third question can be answered in an automated process, proving at the same time the authenticity of the document and its rightful origin.

The aim behind this process is to provide a means of linking the document's validity and authenticity back to its issuing authority. To achieve this a chain of trust is established from the issuing authority to the document. Basically the border control system trusts in the authenticity of the chip's data because it trusts the security elements posted by a trustworthy authority. These security elements are trustworthy only if they are certified by the higher standing authority of the issuing State and if they are linked back to this authority.

Basically a chain of electronic certificates and signatures is created with one end securely anchored in the authority of the issuing State and the other end securely stored in the chip of the eMRTD. The anchor is called Country Signing Certificate Authority (CSCA). It issues certificates to security modules that are attached to the actual personalization of the eMRTD. These security modules are called Document Signers. These then create electronic signatures over the different data stored on the eMRTD's chip to be stored in the chip as the Document Security Object (SOD).

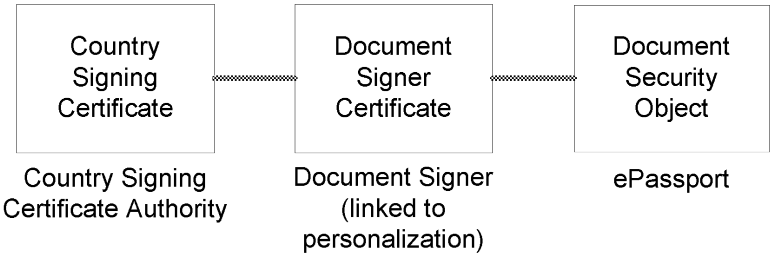

Country Signing Certificate
Document Signer Certificate
Document Security Object
Country Signing Certificate Authority
Document Signer (linked to personalization)
ePassport

Figure 1: The chain of trust

To validate an eMRTD at an international border the border control system retrieves the SOD from the eMRTD's chip. Its authenticity and by implication the authenticity of the eMRTD can be proven, if the signature checks against the document signer certificate and if the document signer certificate checks against the country signing certificate.

This validation requires three preconditions to be fulfilled:

1. The border control system must know the country signing certificate.
2. The border control system must know the document signer certificate.
3. The border control system must know if these certificates are still valid or whether they have been revoked and published in a Certificate Revocation List (CRL).

The distribution process of the necessary certificates and their revocation lists can be simplified using the ICAO PKD. This centralized directory acts as a broker where each participating State uploads document signer certificates and certificate revocation lists. Uploaded certificates and CRLs of all participating States can then be easily downloaded in one single transaction. The country signing certificates are exchanged bilaterally between States. Additionally States may publish a signed list of received CSCA certificates of other States (Master Lists) as well as CSCA Link Certificates within the ICAO PKD (cf. 3.2 and 3.3).

➠ Document Signer Certificates, Certificate Revocation Lists, CSCA Link Certificates and Master Lists are published in the ICAO PKD.

The responsibility for ICAO PKD lies by the ICAO PKD Board - a standing body installed by the *"Memorandum of Understanding Regarding Participation and Cost Sharing in the Electronic Machine Readable Travel Documents ICAO Public Key Directory"* (MoU). PKD Board Members are nominated by the participating States and appointed by the ICAO Council. The PKD Board may have up to fifteen Members. The MoU determines general rules and operational procedures for participation in the PKD.

For building and running of the validation service ICAO engaged Netrust, a Singapore based company. Netrust, acting as the PKD Operator, provides technical e-mail and phone support to all participating States. The main site of the PKD is placed in Singapore while the backup site is placed in Bangkok, as it has been shown on the figure 2.

ICAO PKD contains a "Write"-Directory for the upload of Master Lists, certificates and CRLs. After verification these are published within a "Read"-Directory, available for download by all global entities. The ICAO PKD participating States will receive a secure privileged access port for PKD download.

The root CSCA certificates of the States must be brought to ICAO headquarter in Montreal where they are imported securely to the ICAO site of the PKD (High Security Module, HSM) under the observation of the State's representatives and the senior security officials of ICAO.

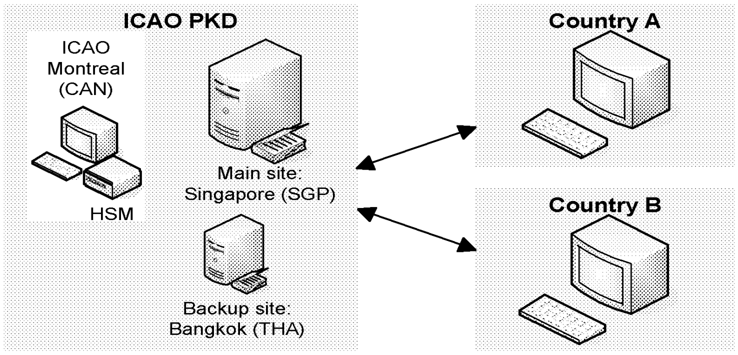


Figure 2: The PKD architecture

2.2 A closer Look

What is this public key cryptography anyway?

Public key cryptography is a core concept to almost any eGovernment activity, but the basic principles are often unclear to anyone but some technical staff. While the mathematics behind it may be quite frightening and are beyond the scope of this document, understanding the concepts may be very helpful to the reader.

All cryptography is based on the concept that a mathematic function takes a secret key (a number) and some input data and delivers a result, which has seemingly nothing to do with the input data. But using the mathematic function (or its inverse) again with the correct secret key restores the input data. Any other key will provide garbage.

Public key cryptography is based on some mathematic functions that have a rather uncommon behaviour: the key is actually a pair of numbers. Once the cryptographic function is used on some input data with one part of the key, the other part of the key is required to retrieve the original information. If one part of the key is then kept secret by its owner (the secret key) and the other part shared with other people (the public key), anything that is encrypted by the owner with the secret key can be decrypted by anyone that has access to his public key. It also works the other way around, anyone can encrypt data with the public key and the result can only be deciphered with the use of the secret key.

At first sight, the second approach is more pragmatic. Its use in encrypting messages that can only be read by the rightful recipient is quite obvious. But the first alternative has also a huge value. Encrypting a message with a secret key, which is known to only one person, proves its origin and authenticity to anyone. This is the core of this mathematical mystery called electronic signature.

To create an electronic signature a checksum (the hash value) is computed for the message to be signed. This hash value is generated in such a way that the smallest change in the message would create a completely different hash value. This hash value is then encrypted with the secret key of the message sender. Anyone who wants to validate the authenticity of the message needs to recalculate the hash value from the message, then decipher the hash value with the help of the sender’s public key and finally compare the two. If they match, the message was signed by the sender and has not been changed!

The certificates everyone talks about are a means of establishing trust between two parties that do not know each other by routing that trust through one or more intermediaries. In effect certificates are quite simply messages that contain the description of an identity, the public key of this identity and a signature by some party that may be trusted by others. The certificate signer vouches with his signature for the correct matching of identity and public key, just like an MRTD issuing authority vouches for the identity of the passport holder. So anyone trusting the certificate signer can also trust in the identity within the certificate.

3 ICAO PKD: how it works

3.1 Basic Functionality

Beside the bilateral exchange of the CSCA certificates, each State participating in the ICAO PKD is required to securely submit its CSCA certificate to ICAO. This represents the trust anchor for this States's eMRTD. After all formal participation procedures are complete, the document signer certificates and the revocation lists will be delivered to ICAO PKD. The authenticity of the DS certificates can now be verified using the public keys stored inside the CSCA certificates. The read-only version of ICAO PKD that contains validated document signer certificates and CRLs is accessible to all States, airlines and other entities for verification of eMRTDs. The border control system needs only to:

1. Retrieve data groups from the chip and check their integrity by comparison of their hash values with the values, stored in the document security object (SOD).
2. Verify the signature of the document security object.

The following figure shows how the different information required to validate an eMRTD in an automated process travels from its different points of origin to a border control station. Keep in mind that the actual validation process is then automated to the point where the border control agent only has to put the eMRTD on a reader and view the result.

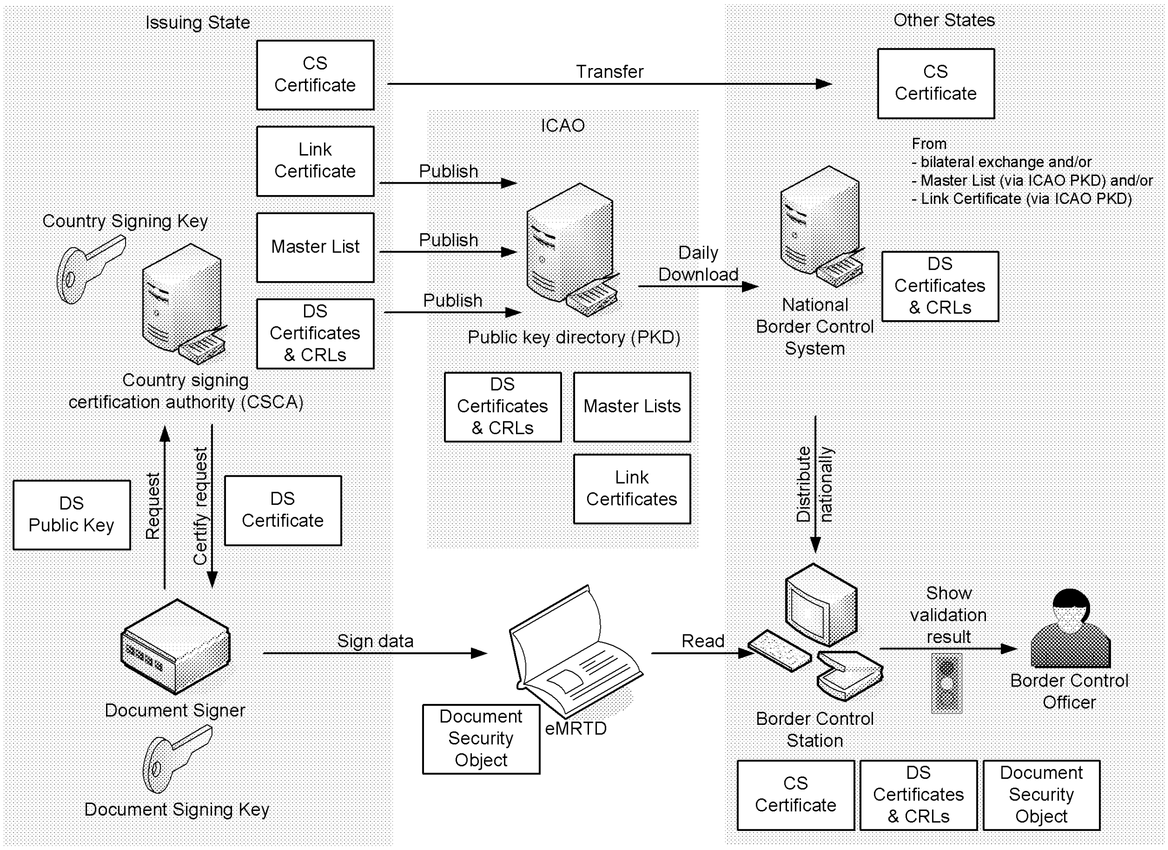


Figure 3: Chain of Trust from Issuer to Border Control

One way of signature verification is to download the corresponding DS certificate from the ICAO PKD, extract the DS public key and use it for verification, provided the check for any revocation against CRLs is carried out regularly. Due to the fact that currently most of the States issue eMRTDs with DS certificates stored inside of the SODs, the signature can be verified using the extracted DS certificate. The authenticity of this certificate can be proven by its verification with the corresponding CSCA link certificate from ICAO PKD.

Independent of the execution way of the SOD verification, the security of the chain of trust relies on the integrity and authenticity of the CSCA certificates. For the purpose of a better security protection of CSCA certificates, the ICAO PKD Board decided to additionally support an alternative method for CSCA certificate presentation (Master Lists, CSCA Link Certificates).

3.2 Master Lists to facilitate the Exchange of CSCA Certificates

A Master List is simply a signed list of certificates and is intended to mitigate the risk of substitution of a CSCA certificate by a rogue certificate and the addition of rogue certificates to a list of trustworthy CSCA certificates. A Master List enables the verification of documents of the States without diplomatic agreements for CSCA certificates distribution. The main idea of this approach is based on countersigning of the CSCA certificates of the issuing States by other States and distributing of the countersigned CSCA certificates via ICAO PKD.

More detailed, the ICAO PKD participating State may publish a list of received and validated CSCA certificates. The conditions of completion of this list depend on the diplomatic exchanges and verification processes of that State. The Master Lists will be available for download from the ICAO PKD in addition to the bilaterally exchanged certificates.

The following example on the figure 4 illustrates the process and advantage of Master Lists:

- State A exchanges CSCA certificates with States B, C and X via trusted channels.
- State A compiles, countersigns and publishes a Master List containing B, C, X and A.
- State X can download the Master List of A and retrieve the CSCA certificate of State C which State X can use, based on the State X decision to trust in the validity of the information provided by State A.

If other States also publish Master Lists via the ICAO PKD, a receiving State can align several Master Lists and thus validate their contents.

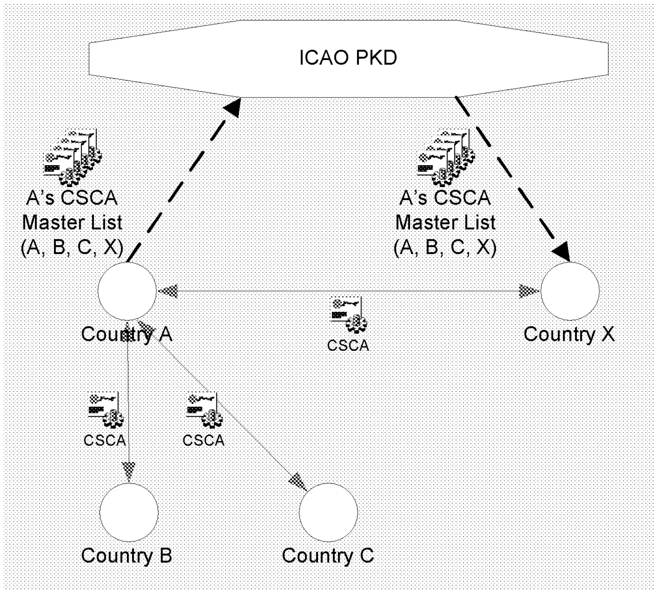

ICAO PKD
A's CSCA Master List (A, B, C, X)
A's CSCA Master List (A, B, C, X)
Country A
CSCA
Country X
CSCA
CSCA
Country B
Country C

Figure 4: Distribution of CSCAs via Master Lists

3.3 CSCA Link Certificates to facilitate the follow-up of CSCA Certificates

The CSCA link certificates provide a means of exchanging new CSCA certificates by simply signing it with the old CSCA keys. This means that the cumbersome secure exchange through administrative and diplomatic channels must only take place once with each State at the beginning of eMRTD cooperation in the field of border control.

CSCA link certificates are published to all States through the ICAO PKD.

3.4 Responsibilities of the participating States

Each participating State is required to provide the ICAO PKD with up-to-date certificates and certificate revocation lists. The exact manner of transmitting this information is specified in the PKD Interface Specification which is disclosed to participating States.

In detail the following data is to be provided by the participating State:

- Document signer certificates
- Certificate revocation lists
- CSCA Master List (optional)
- CSCA link certificates
- CSCA certificates (not published, but used by ICAO PKD for validation)

4 Benefits of the ICAO Public Key Directory

➧ Without the ability of validating the electronic data in an eMRTD at a foreign border, the travel document must be treated exactly as a non-electronically readable travel document and provides no added security.

Validation of an eMRTD obviously relies on ability of a border control system to verify the signature of the Document Security Object and thus to validate the certificate chain. Any State issuing travel documents carries the responsibility of ensuring that foreign border control agencies can validate the authenticity and integrity of these travel documents. Issuing eMRTDs without providing foreign border control agencies with the required information to validate this electronic information does not make any sense, since the border control agency is then forced to treat this eMRTD just like a non-electronic MRTD without any benefit of the electronic component to the border control agency and the document holder.

➧ ICAO PKD provides a fast and secure way for the electronic validation of eMRTDs.

ICAO PKD is a trustworthy directory to simplify the document validation process, at the same time increasing the security of an eMRTD. Freely downloadable DS certificates and CRLs save transaction time in the validation of the e-passport since it is not required to read the certificate from the chip and since the certificates may be checked against the issuing State's country signers in advance to be stored in the border control system as a "good"-list of document signer certificates. This is enhanced by the fact that the ICAO PKD will validate each certificate before it is published, thus offering a list of "good" certificates.

➧ Compromised or false certificates or keys are immediately detected through the ICAO PKD.

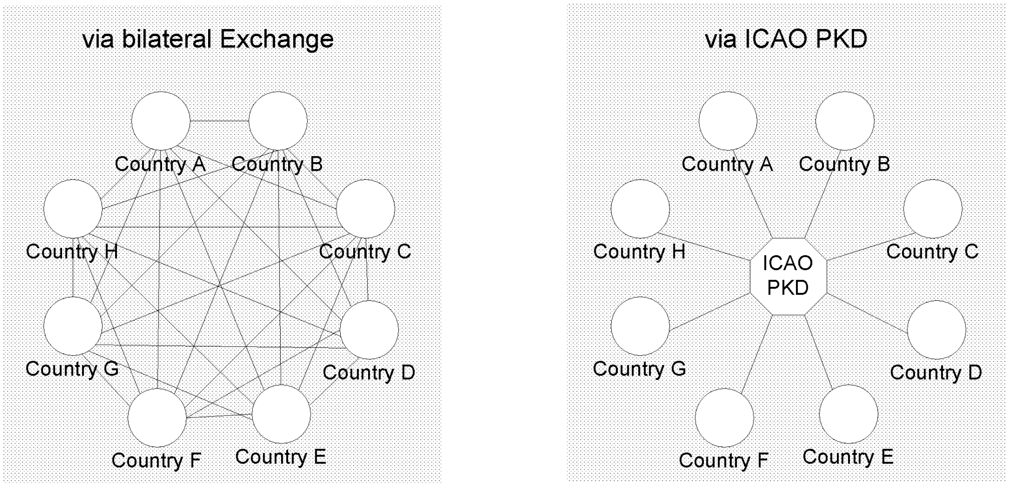
Keeping the certificate revocation lists up to date is another task of high importance to the security of the eMRTDs' validation process. These are used to inform anyone concerned of any security problem with a certificate or its creator. E. g. if a document signer is stolen, the thief would be able to create a valid SOD for a falsified eMRTD. By revoking the certificate of the stolen document signer this attempted fraud will be effectively countered.

It is the responsibility of the issuing State to publish the list of revoked certificates to all States. By publishing the CRL to the ICAO PKD this daily task can be met with very little effort.

➧ Participation in the ICAO PKD is a simple and cost-efficient means to provide other States with certificates and revocation lists for the validation of eMRTD.

One major challenge in the e-passport systems PKIs is the exchange of certificates and revocation lists between States. The following figure demonstrates the communications between States without and with the ICAO PKD:

Distribution of Certificates and CRLs



This example shows 8 states requiring 56 bilateral exchanges (left) or 2 exchanges with the PKD (right) to be up to date with certificates and CRLs. In case of 188 ICAO States 35,156 bilateral exchanges would be necessary while there are still 2 exchanges necessary with the PKD.

Figure 5: Required Number of Communications for distributing Certificates and CRLs

It is quite obvious that the efforts to establish and maintain individual interfaces to each State are prohibitively high. At the same time this procedure would be more error-prone and time-consuming during day to day operations.

➧ ICAO PKD Master Lists of CSCA certificates and CSCA Link Certificates can save a lot of bilateral diplomatic certificate exchanges.

As discussed above the CSCA Certificate plays the main role as the anchor of trust in the validation process of the ePassports. The Master List concept enables verification of the chain of trust even with States where there hasn't been any certificate exchange by diplomatic means. Publishing of the signed list of validated CSCA certificates in the ICAO PKD gives opportunity for an additional validation of already received certificates.

➧ A State participating in the ICAO PKD will facilitate international travelling for its citizens.

While the border control agencies profit from a widespread use of the ICAO PKD, the true benefit will be to the travelling citizens from participating States. In simplifying the eMRTD's validation process while at the same time enhancing its security and trustworthiness, crossing international borders will be quick, easy and hassle-free for the citizen. Travellers from States not participating in the ICAO PKD on the other hand may experience more time-consuming examinations of their travel documents due to the fact that the electronic chain of trust may be more difficult or even impossible to validate. A missing or out-of-date certificate revocation list may cast some doubt on the authenticity of even a perfectly valid eMRTD.

➧ By participating in the ICAO PKD an eMRTD issuing State will be able to share experiences with other States and benefit from their advice.

For the issuing State participation in the ICAO PKD and in the PKD Board also constitutes a forum to share experiences and advice with eMRTD issuing agencies from other States. eMRTD issuing and foreign States' trust in the issued eMRTDs may benefit from close cooperation with other States and the resulting exchange of information. In addition an in-depth knowledge of administrative, procedural and technical regulations gained through PKD Board work is beneficial to the smooth operation of national PKD based applications. Parties that take an active role in the PKD Board may initiate improvements of existing regulations or future developments.

➧ By utilizing the ICAO PKD in the border control agencies a State proactively contributes to international border security and to aviation security.

International travel and aviation provides huge benefits to the global community as well as to the individual States. At the same time increased international travel poses security threats at the borders as well as to air travel. Reliable and tamper-proof identification of travellers counters quite a number of security threats starting with compliance to national rules on who is allowed to come into the country, up to disallowing criminal elements to cross borders by assuming false identities.

➧ Participating in the ICAO PKD offers first-serve-access for the issuing State's border control agencies.

With respect to downloading document signer certificates and certificate revocation lists from the PKD, a participating State has the additional benefit of having download priority whenever excess demand creates a backlog.

5 Conclusion

➧ Issuing an eMRTD without participating in the ICAO PKD will be of little benefit.

States that do not join the ICAO PKD and yet issue eMRTDs risk:

- that their citizen's e-passport is not trusted at foreign borders;
- wasting efforts to establish interfaces for exchanging certificates and CRLs to all individual ICAO States instead of just one to the ICAO PKD;
- losing the additional security provided by ICAO PKD as an independent and trustworthy broker.

6 How to join the ICAO PKD

To join the ICAO PKD as an eMRTD issuer, the issuing State or entity must first submit a "Notice of Participation" to the ICAO Secretary General and then sign up with the PKD operator.

Joining the ICAO PKD is a quick process, participation being effective on the first day of the month following the sign up and payment of the Registration Fee.

Participating in the ICAO PKD requires payment of a one off Registration Fee and a recurring Annual Fee. The Annual Fees may be considered moderate and – since they are only raised to cover the cost of operation – may be expected to drop as the number of PKD Participants increases.

More details on joining the ICAO PKD are set forth in the *"Memorandum of Understanding (MoU) Regarding Participation and Cost Sharing in the Electronic Machine Readable Travel Documents ICAO Public Key Directory"* and the "PKD Procedures".

Support and additional advice can be requested by States issuing eMRTDs from the Implementation and Capacity Building Working Group via the ICAO Secretariat. This holds particularly true for any issues the issuing State may experience with PKI.

It is recommended to visit the PKD main page for further details and background information (http://www2.icao.int/en/MRTD/Pages/icaoPKD.aspx).

7 Glossary / Abbreviations

CA	Certificate Authority
Certificate	an electronic document establishing a digital identity by combining the identity name or identifier with the public key of the identity, a validity period and an electronic signature by a third party
Certificate Authority	a trusted third party that issues digital certificates for use by other parties
Certificate Revocation List	certificates whose validity is compromised for any reasons are published in a certificate revocation list rendering them useless.
CRL	Certificate Revocation List
CSCA	Country Signing Certificate Authority
eMRTD	electronic machine readable travel document, mostly the electronic passport.
PKD	Public Key Directory
PKI	Public Key Infrastructure
Public Key Directory	a broker service that publishes certificates and revocation lists for download
Public Key Infrastructure	An arrangement that binds public keys to their respective user identity by means of a certificate authority. By validating certificates a chain of trust is established that gives a proof of authenticity to the verifying agency.
SOD	Document Security Object

References

ICAO, Doc 9303, Machine Readable Travel Documents, part 1, 2006.

ICAO, Memorandum of Understanding (MoU) Regarding Participation and Cost Sharing in the Electronic Machine Readable Travel Documents ICAO Public Key Directory, 2008.

ICAO, PKD Procedures for the ICAO Public Key Directory, 2006.

ICAO, PKD Regulations for the ICAO Public Key Directory, 2007.

ICAO, TR, CSCA countersigning and Master List issuance, v.0.61, 2008.

Revision History

Version	Date	Alteration	Author
V1.0	03 Mar 2009	Final draft version issued to ICAO ICBWG and PKD Board for review	Markus Hartmann Stephan Körting Olga Käthler
V1.01	06 Mar 2009	First review	Dr. Eckart Brauer
V1.1	09 Mar 2009	Updated after first review	Markus Hartmann Stephan Körting Olga Käthler
V1.2	11 Mar 2009	Final review	Dr. Eckart Brauer
V1.3	07 May 2009	Final review for the ICB WG	Markus Hartmann
V1.4	12 May 2009	Final review after the 7th meeting of the PKD Board	Dr. Eckart Brauer
V1.5	20 May 2009	linguistic review before publication	PKD Board