# ICAO Directory Specifications

Version 1.0

November 25, 2004

# Table of Contents

# Chapter 1 Overview

## 1.1 Purpose

ICAO (International Civil Aviation Organization) is working on specifications of the electronic passport. They finished defining the concept of common directory (Public Key Directory: it is referred as ICAO-PKD hereafter) but they have not completed detailed specifications for practical use. Therefore, this document is to define detailed specifications for implementation of ICAO-PKD.

The current relevant specification of ICAO is described in TECHNICAL REPORT "*PKI for Machine Readable Travel Document offering ICC Read-Only Access Version 1.1* (Date: October 01, 2004)" (it is referred as ICAO TECHNICAL REPORT). This document is based on ICAO TECHNICAL REPORT.

## 1.2 Glossary

ICA TECHNICAL REPORT uses key words below: “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED” and “MAY”.

These key words are defined in RFC2119as described in the table 1.2-1 (Terms defined in RFC2119).

Table 1.2-1 Terms defined in RFC2119

| Terms | Meaning |
|---|---|
| MUST | Absolute requirement of the specification |
| REQUIRED | |
| SHALL | |
| MUST NOT | Absolute prohibition of the specification |
| SHALL NOT | |
| SHOULD | The full implications must be understood and carefully weighed before choosing a different course. |
| RECOMMENDED | |
| SHOULD NOT | The full implications must be understood and carefully weighed before choosing a different course. |
| NOT RECOMMENDED | |

With regard to these terms, in order to define the difference between the statements originally in ICAO TECHNICAL and those newly added to this document, the former has (*originally stated*) at the end of the statement and the latter has (*newly stated*).

Statements using one of the terms above in ICAO TECHNICAL REPORT:

Example: It is reccomended that - - - (*originally stated*).

Statements (using one of the terms above) appearing newly in this document:

Example: CRL distribution points should be - - - (*newly stated*).

The abbreviations used in this document are shown in the table 1.2-2 “Abbreviations” below.

Table 1.2-2 Abbreviations

| Abb. | Formal nomenclature | Description |
|---|---|---|
| CSCA | Country Signing CA | The certification authority of each country to realize the electronic passport |
| DS | Document Signer | The person who issues the electronic passport |
| CA | Certification Authority | |
| CRL | Certificate Revocation List | |
| ICAO | International Civil Aviation Organization | |
| PKD | Public Key Directory | |

## 1.3 Overall Picture

An electronic passport has an IC chip embedded in it and the IC chip carries electronic data including the face photo, finger prints and so on. In order to assure that the electronic data in it are genuine and have not been altered, digital signature should be attached.

The figure 1.3-1 shows the system architecture of the electronic passport: from issuance to validation.

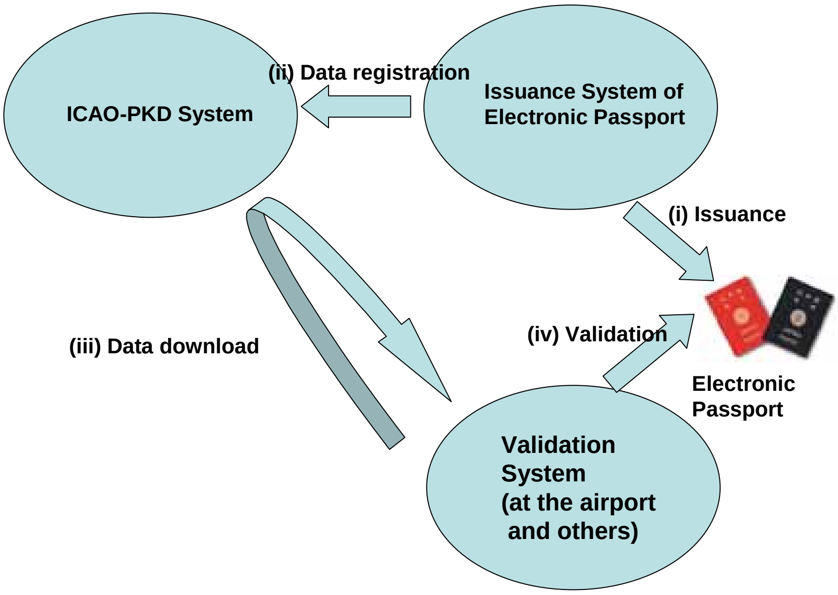

Fig. 1.3-1 System Architecture (Issuance to Validation)

(i) An electronic passport is issued by the electronic passport issuance system.

(ii) The data required to validate the electronic passport is genuine are registered in the ICAO-PKD system.

(iii) The validation system installed at the airport or others downloads the registered data from ICAO-PKD.

(iv) The passport is validated by the downloaded data when the passport is submitted for inspection of entry into, and departure from, the country.

The details of the electronic passport issuance system, ICAO-PKD system and validation system will be described in the subsequent pages.

(1) Electronic passport issuance system

The electronic passport issuance system consists of CSCA and the passport-issuing system.

The CSCA certificate is used as signature for DS Certificate and Certificate Revocation List (CRL).

The DS Certificate is used to sign the electronic data stored in the IC chip of the electronic passport.

CRL stores the information about revocation of CSCA Certificate or DS Certificate.

The figure 1.3-2 shows the process of issuance of the electronic passport.

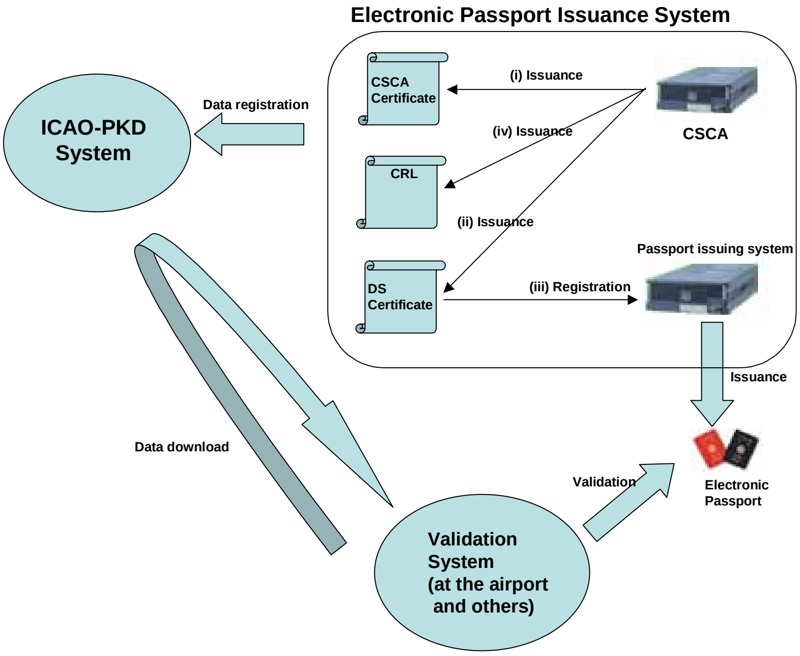

Fig 1.3-2 Outline of Electronic Passport Issuance System

(i) CSCA issues CSCA Certificate (self-signed certificate).

(ii) CSCA issues DS Certificate.

(iii) DS Certificate is registered in the passport issuing system to be used for signature of the electronic passport.

(iv) CSCA issues CRL.

(2) ICAO-PKD System

The ICAO-PKD system consists of a common registration directory and a common reference directory.

The data stored in the common registration directory are copied in the common reference directory after the validity of data is confirmed, so that the data can be referred for inspection of entry into, and departure from, the country.

Figure 1.3-3 shows the flow of data storage, validation and registration of ICAO-PKD.

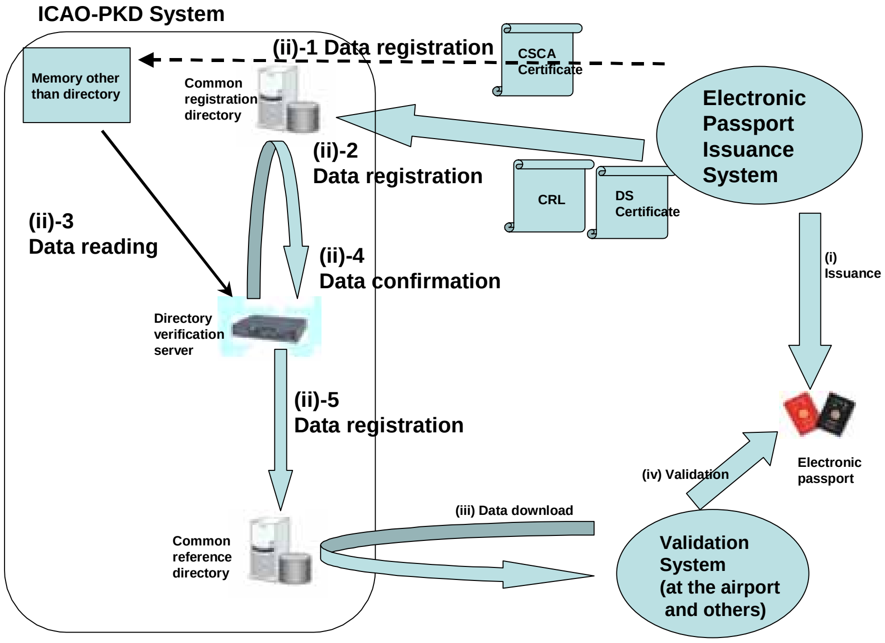

Fig 1.3-3 Flow of data storage, validation and registration of ICAO-PKD

(ii)-1 CSCA Certificate is stored off-line in the media other than the directory of ICAO-PKD.

(ii)-2 DS Certificate and CRL are transmitted by LDAP protocol (specified in RFC2251 to 2256), which is a standard used to make an access to the directory. The transmission data are encrypted through SSL server authentication.

(ii)-3 The directory validation server reads CSCA that is stored as described in (ii)-1 above.

(ii)-4 In order to confirm that the certificate and CRL data stored in (ii)-2 are genuine, digital signature of CSCA Certificate is verified.

(ii)-5 After validation, the data are stored in the common directory (public directory) that is downloaded from the country validation system.

(3) Validation system

When a country validates an electronic passport, there are three ways of taking the data for validation as described below:

- Make an access to ICAO-PKD whenever validation is required,
- The validation system entirely downloads the data from ICAO-PKD regularly, or
- The country downloads the entire data from ICAO-PKD regularly.

ICAO TECHNICAL REPORT recommended that the entire directory should be downloaded everyday (*originally stated*).

If it is selected to make an access to ICAO-PKD whenever it is required, the system performance may be degraded because of too many accesses. Therefore, it should not be selected to make an access to ICAO-PKD whenever validation is required (*newly stated*).

The remaining two ways will be described below.

■ In case that the validation system entirely downloads the data from ICAO-PKD regularly:

The validation system registers CSCA Certificate that was exchanged with another country. The system downloads DS Certificate and CRL from ICAO-PKD to validate the signature against the registered CSCA Certificate. The system checks whether the electronic passport is signed by the correct DS Certificate, and whether the signed DS Certificate is registered in CRL.

In this way, the validation system at an airport or other facility can identify the person by inspection surely and safely.

The figure 1.3-4 shows the individual download model to illustrate the flow of operations by the validation system.

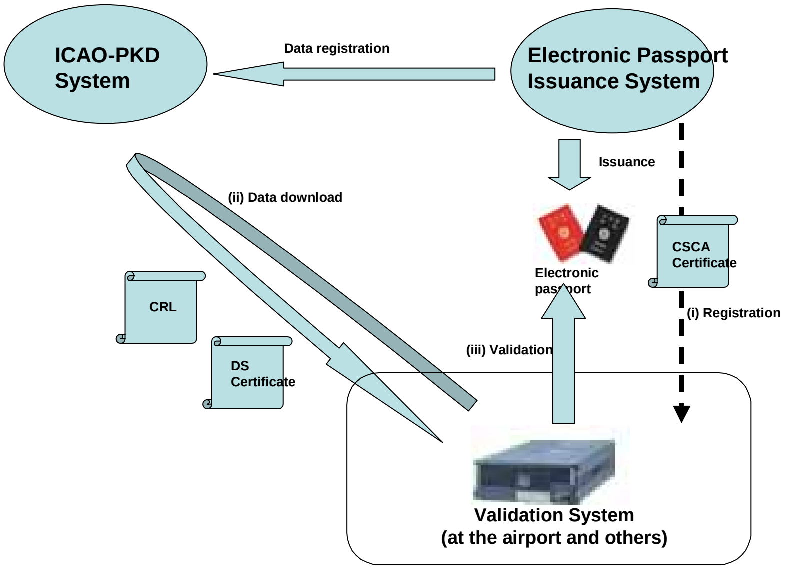

Fig. 1.3-4 Individual Download Model

(i) A country obtains safely CSCA Certificate of another country by the diplomatic means between the two countries in advance and registers it in the validation system.

(ii) The validation system downloads DS Certificate and CRL from ICAO-PKD.

(iii) The system checks the electronic passport against the data described in (i) and (ii) above.

■ In case that the country entirely downloads the data from ICAO-PKD regularly:

In this model (each country downloads the data at one location), each country builds up a local directory server and operate local PKD.

Figure 1.3-5 shows the flow of operations of Local PKD Model.

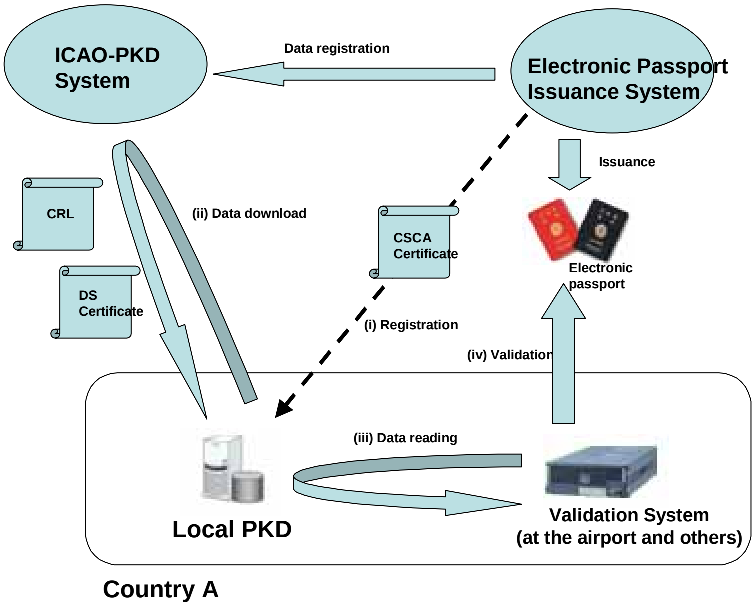

Fig. 1.3-5 Local PKD Model

(i) A country securely obtains CSCA Certificate of another country by the diplomatic means between the two countries in advance and registers it in the local PKD.

(ii) The local PKD downloads DS Certificate and CRL from ICAO-PKD.

(iii) The validation system reads the data required for validation from the local PKD.

(iv) The system checks the electronic passport against the data described in (iii) above.

## 1.4 Preconditions for estimation of performance

There are some variable elements when we estimate performances related to ICAO-PKD.

The preconditions we used for estimation are shown in the figure 1.4-1 "Preconditions for estimation".

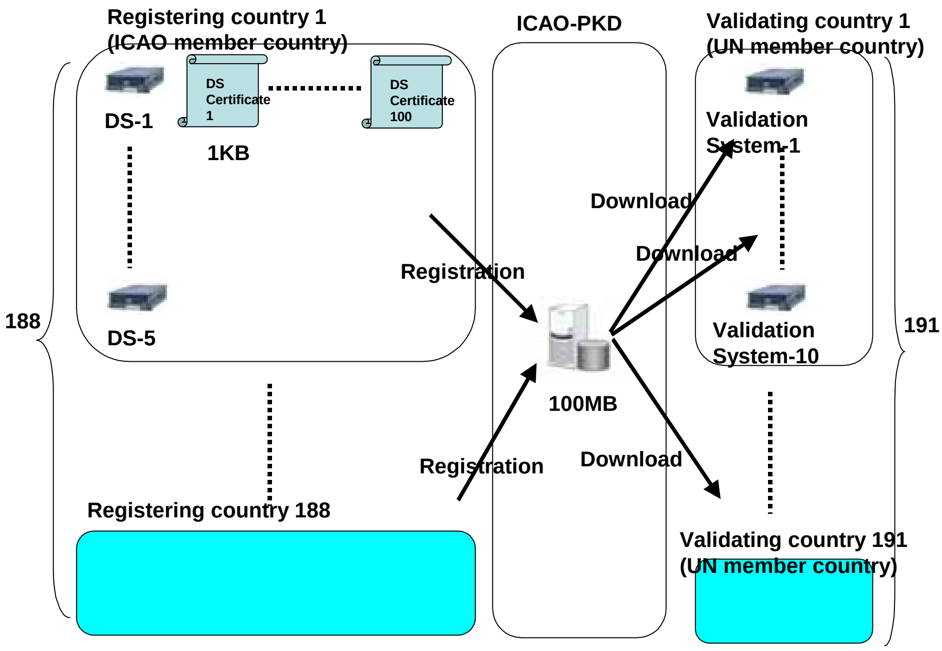

Fig. 1.4-1 Preconditions for Estimation

- Assuming the validation system of each country entirely downloads the data at ten sites.
- Assuming all 188 member countries of ICAO-PKD will register their data in ICAO-PKD.
- Assuming all 191 member countries of UN will acquire the data from ICAO-PKD.
- The number of DS Certificates controlled by one Document Signer becomes variable, depending on renewal interval and expiration date. We use a few conditions for calculation and finally concluded the total number of DS Certificates will be 100, considering some margin.

  For the detail, refer to the section 2.2.1 "Performance of Common Registration Directory".
- Assuming one country has five Document Signers.

- Assuming the data size (DS Certificate or CRL) on the directory is approximate 1KB.
- Assuming the size of the directory of ICAO-PKD is approximate 100MB.
- Registration of DS Certificate should be done by addition.
- It is assumed that access from each country is not concentrated.
- Assuming the LDAP protocol is used for access to ICAO-PKD.

Note)

ICAO TECHNICAL REPORT mentioned “PKD is set up as X.500 directory". On the other hand, the directory update mentioned “the LDAP protocol is used". They are contradicting to each other. This document assumes ICAO-PKD uses the LDAP protocol for data transfer.

# Chapter 2 Requirements for Public Key Directory and Proposals

Requirements for ICAO-PKD and relevant proposals cover the items below:

- Internal systems of the server
- PKD system
- Coordination between servers
- Coordination between clients and servers
- Interface for update
- Interface for reference
- Operation

## 2.1 Internal systems of the server

With regard to the directory profile in the server, it is necessary to configure a directory information tree without contradictions for all entries included in ICAO-PKD. In order to realize this, the items below will be examined with the way of storing the entity data configuring ICAO-PKD being considered.

- Tree configuration
- Schema

### 2.1.1 Tree configuration

ICAO TECHNICAL REPORT mentioned the attributes below should be used (*originally stated*).

It also mentioned that a country may add serial number (*originally stated*).

- country (country code with one or two letters)
- organization
- organizational-unit
- common name
- serial number

However, ICAO TECHNICAL REPORT did not stipulate the tree configuration including the structure.

Considering the attributes described above, we made an example of director configuration as shown in the figure 2.1.1-1. The data stored in ICAO-PKD and required for inspection of a person at entry into or departure from a country are DS Certificate and CRL (*newly stated*).

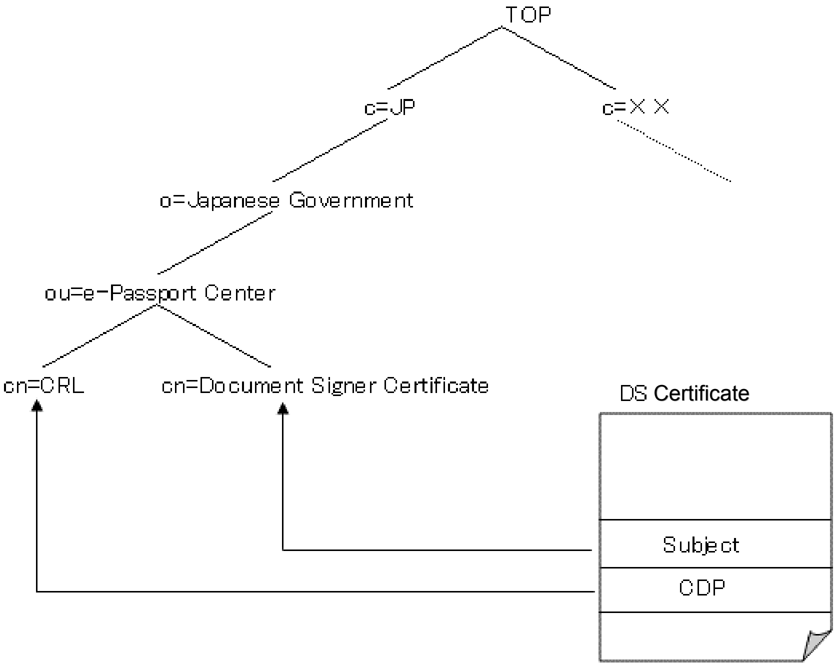

Fig. 2.1.1-1 Example of Directory Configuration

As the figure 2.1.1-1 “Example of Directory Configuration” shows, DS Certificate contains Subject and CRL distribution point (CDP). Subject has the person’s DN in it and CDP has DN of CRL in it. This way, you can use the DN as a key word to obtain required information.

If a country wants to have Document Signer for each state, the directory configuration will be like an example described in the figure 2.1.1-2 “Example of Directory Configuration, Hierarchical Type”.

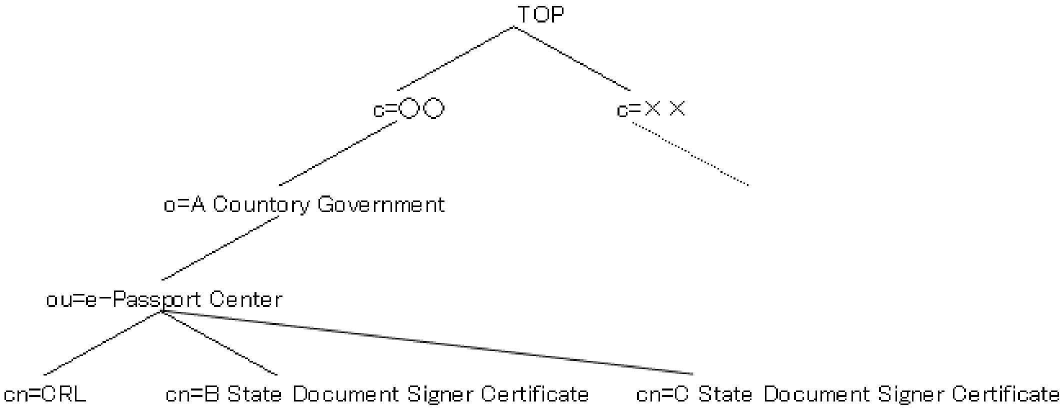
TOP
c=○○
c=××
o=A Countory Government
ou=e-Passport Center
cn=CRL
cn=B State Document Signer Certificate
cn=C State Document Signer Certificate

Fig. 2.1.1-2 Example of Directory Configuration, Hierarchical Type

ICAO-PKD should create an entry of a country. The procedure should be as follows: when ICAO-PKD receives an application to new registration from a country, ICAO-PKD creates an entry (using a country code [two letter] of ISO 3166). For the procedure of notification of a new entry of a country, refer to the section 2.6 "Operation".

For the configuration below the entry of a country, each country may want to configure it according to its needs. So, it is preferable to let each country configure it freely. For example, as the table 2.1.1-1 "Identity Attribute Type and Attributes for Each Layer" shows, each entry uses layers, object classes and attributes (*newly stated*).

Table 2.1.1-1 Identity Attribute Type & Attributes for Each Layer

| Layer | Identity Attribute | Minimum Length | Maximum Length | Possible Attributes (Example) |
|---|---|---|---|---|
| First Layer | c | 2 | 2 | Country code of ISO 3166 (two letters)<br>Example: "JP" |
| Second Layer | o | 1 | 64 | The name of the government is stored.<br>Example : "Japanese Government" |
| Third Layer | ou | 1 | 64 | The issuing administration is stored.<br>Example: "e-Passport Center" |
| Fourth Layer | cn | 1 | 64 | The name of DS Certificate is stored.<br>Example: "Document Signer Certificate"<br>The name of CRL is stored.<br>Example: "CRL" |

To specify a CRL distribution point, there are two ways; to specify either URL or DN where CRL can be obtained.

Examples URL: ldaps://***/cn=CRL,…
DN: cn=CRL,…

There may be a case in which a country downloads the entire data and sets up its own directory servers for operation. In that case, CRL distribution points should be described in a relative way. Therefore, CRL distributions points should be in the style of DN (*newly stated*).

### 2.1.2 Schema

ICAO TECHNICAL REPORT did not specify object classes and attributes to be used.

In this section, the result we studied about attributes to be used for DN will be described.

It should be noted that the character code of the information stored in ICAO-PKD should be within the scope defined by Printable String so that ICAO-PKD can be used throughout the world (*newly stated*).

The object classes are used to establish DN that specify either DS Certificate or CRL.

#### (1) Country

For the object class that configures an entry indicating a country, the country object class specified in RFC2256 is used. The c attribute that is indispensable for the country object class is used (c attribute is specified in RFC2256). For this attribute, two-letter country code (ISO 3166) is used.

The definition of the country object class is described in the table 2.1.2-2 “Definition of country Object Class”.

The definition of c attribute is described in RFC2256.

Table 2.1.2-2 Definition of country Object Class

| | |
|---|---|
| [Object Class Name] | country |
| [Object Identifier] | joint-iso-itu-t(2) ds(5) objectClass(6)<br>country(2) |
| [Type] | Structure type |
| [Attribute to be supported by ICAO-PKD] | c |

(2) Organization

For the object class that configures an entry indicating an organization, the organization object class specified in RFC2256 is used. The o attribute that is indispensable for the organization object class is used (o attribute is specified in RFC2256).

The definition of the organization object class is described in the table 2.1.2-3 “Definition of organization Object Class”.

The definition of o attribute is described in RFC2256.

Table 2.1.2-3 Definition of organization Object Class

| | |
|---|---|
| [Object Class Name] | organization |
| [Object Identifier] | joint-iso-itu-t(2) ds(5) objectClass(6)<br>organization(4) |
| [Type] | Structure type |
| [Attribute to be supported by ICAO-PKD] | o |

(3) Organizational Unit

For the object class that configures an entry indicating an organizational unit, the organizationalUnit object class specified in RFC2256 is used. The ou attribute that is indispensable for the organizationalUnit object class is used (ou attribute is specified in RFC2256).

The definition of the organizationalUnit object class is described in the table 2.1.2-4 “Definition of organizationalUnit Object Class”.

The definition of ou attribute is described in RFC2256.

Table 2.1.2-4 Definition of organizationalUnit Object Class

| | |
|---|---|
| [Object Class Name] | organizationalUnit |
| [Object Identifier] | joint-iso-itu-t(2) ds(5) objectClass(6) organizationalUnit(5) |
| [Type] | Structure type |
| [Attribute to be supported by ICAO-PKD] | ou |

(4) DS Certificate

For the object class that configures an entry indicating DS Certificate, either one of the inetOrgPerson object class specified in RFC2256, the pkiUser object class specified in RFC2587 or the device object class specified in RFC2256 is used.

The cn attribute and sn attribute that are indispensable for the inetOrgPerson object class are used (cn and sn attributes are specified in RFC2256). In addition to those, an arbitrary attribute, userCertificate (specified in RFC2256), is used to store the certificate.

Since the pkiUser object class is auxiliary type, it may be used in combination with another object class of structure type.

In case that the device object class is used, an optional attribute, serialNumber attribute (specified in RFC2256) can be used by using it in combination with the pkiUser object class described above.

The definition of the inetOrgPerson object class is described in the table 2.1.2-5 “Definition of inetOrgPerson Object Class”.

The definition of the pkiUser object class is described in the table 2.1.2-6 “Definition of pkiUser Object Class”.

The definition of the device object class is described in the table 2.1.2-7 “Definition of device Object Class”.

Table 2.1.2-5 Definition of inetOrgPerson Object Class

| | |
|---|---|
| [Object Class Name] | inetOrgPerson |
| [Object Identifier] | 2.16.840.1.113730.3.2.2 |
| [Type] | Structure type |
| [Attribute to be supported by ICAO-PKD] | cn<br>sn<br>userCertificate |

Table 2.1.2-6 Definition of pkiUser Object Class

| | |
|---|---|
| [Object Class Name] | pkiUser |
| [Object Identifier] | joint-iso-itu-t(2) ds(5) attributeType(4) pkiUser(21) |
| [Type] | Auxiliary type |
| [Attribute to be supported by ICAO-PKD] | userCertificate |

Table 2.1.2-7 Definition of device Object Class

| | |
|---|---|
| [Object Class Name] | device |
| [Object Identifier] | joint-iso-itu-t(2) ds(5) attributeType(4) device (14) |
| [Type] | Structure type |
| [Attribute to be supported by ICAO-PKD] | cn<br>serialNumber |

(5) CRL, ARL and Certificate

There are two ways of specifying the location where CRL and ARL are stored as described below:

- Use of CRL Distribution Point in the extension area of Certificate
- Use of the object class where CA Certificate is stored

For the use of Certificate's CRL Distribution Point in the extension area, ICAO TECHNICAL REPORT mentioned it is optional. If this extension area is not used, the object class where CA Certificate is stored will be used. On the other hand, ICAO TECHNICAL REPORT said CSCA Certificate is not stored in the directory. Therefore, a vacant Certificate object class should be used.

Though ICAO TECHNICAL REPORT said link certificate can be used, it did not mention anything about storage in the directory. In conclusion, we think the link certificate can be stored in the directory.

■ In case of using CRL Distribution Point in the extension area of Certificate

For the object class that configures an entry indicating CRL and ARL, the cRLDistributionPoint object class specified in RFC2587 is used. The cn attribute that is indispensable for cRLDistributionPoint object class is used. In addition to that, an arbitrary attribute, certificateRevocationList (specified in RFC2256), is used to store the CRL. An arbitrary attribute, authorityRevocationList (specified in RFC2256), is used to store the ARL.

The definition of the cRLDistributionPoint object class is described in the table 2.1.2-8 "Definition of cRLDistributionPoint Object Class".

The definitions of attributes, certificateRevocationList and authorityRevocationList are described in RFC2256.

Table 2.1.2-8 Definition of cRLDistributionPoint Object Class

| | |
|---|---|
| [Object Class Name] | cRLDistributionPoint |
| [Object Identifier] | joint-iso-itu-t(2) ds(5) objectClass(6)<br>cRLDistributionPoint(19) |
| [Type] | Structure type |
| [Attribute to be supported by ICAO-PKD] | cn<br>certificateRevocationList<br>authorityRevocationList |

■ In case of registering the link certificate, or in case of storing it in the object class where CA Certificate is stored:

For the object class that configures an entry indicating the link certificate, the pkiCA object class specified in RFC2587 is used. An arbitrary attribute, cACertificate (specified in RFC2256), is used to store the link certificate.

An arbitrary attribute, certificateRevocationList (specified in RFC2256), is used to store the CRL. An arbitrary attribute, authorityRevocationList (specified in RFC2256), is used to store the ARL.

Since the pkiCA object class is auxiliary type, it may be used in combination with another object class of structure type.

The definition of the pkiCA object class is described in the table 2.1.2-9 "Definition of pkiCA Object Class".

The definitions of attributes, cACertificate, certificateRevocationList and authorityRevocationList are described in RFC2256.

Table 2.1.2-9 Definition of pkiCA Object Class

| | |
|---|---|
| [Object Class Name] | pkiCA |
| [Object Identifier] | joint-iso-itu-t(2) ds(5) attributeType(4)<br>pkiCA(22) |
| [Type] | Auxiliary type |
| [Attribute to be supported by ICAO-PKD] | cACertificate<br>certificateRevocationList<br>authorityRevocationList |

CRL has two pieces of information; one is invalidation of the certification authority (i.e. CSCA) and the other is invalidation of end entity certificate (i.e. DS Certificate).

There are two types of CRL operation as described below:

- CRL (invalidation information of end entity certificate) and ARL (invalidation information of certification authority) are controlled separately.
- CRL has both pieces of the information above.

We consider that ICAO-PKD should not decide on one of them but support both of them (*newly stated*).

There is a special way of CRL (invalidation information of end entity certificate) issuance: it issues only differential information called delta CRL. The delta CRL is effective to save time because the entire CRL data do not have to be acquired every time. ICAO THECHNICAL REPORT recommended that the entire data should be downloaded every time because ICAO-PKD is small in size (*originally stated*). This way, we consider we should not use the delta CRL (*newly stated*).

## 2.2 PKD System

In this section, ICAO-PKD system is reviewed from the viewpoints below:

- Performance of Common Registration Directory
- Performance of Common Reference Directory
- Availability
- Network Security

### 2.2.1 Performance of Common Registration Directory

Though ICAO TECHNICAL REPORT mentioned nothing specific about the performance of common registration directory, we think that it should be able to maintain enough response even when accesses from member countries are made intensively (*newly stated*).

(1) Estimate of capacity of the directory

ICAO TECHNICAL REPORT took up three types of operation life cycle in Annex F. We used them to calculate the maximum number of DS Certificates that can be controlled.

Example 1: The update interval and validity period are shown below:

Table 2.2.1-1 Update Interval & Validity Period for Example 1

| | |
|---|---|
| Update interval of DS Certificate | 1 month |
| Validity period of passport | 5 years |
| Validity period of DS Certificate | 5 years and 1 month |
| Update interval of CSCA Certificate | 3 years |
| Validity period of CSCA Certificate | 8 years and 1 month |

The figure 2.2.1-1 illustrates how DS Certificate is updated with one month interval. As the figure shows clearly, while the first DS Certificate is valid (five years and one month) 61 DS Certificates will be issued (12 x 5 + 1).

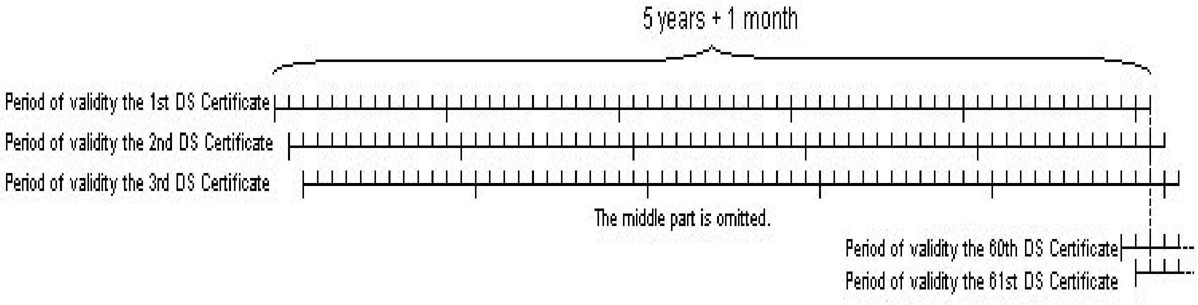
5 years + 1 month
Period of validity the 1st DS Certificate
Period of validity the 2nd DS Certificate
Period of validity the 3rd DS Certificate
The middle part is omitted.
Period of validity the 60th DS Certificate
Period of validity the 61st DS Certificate

Fig. 2.2.1-1 Update Interval of DS Certificate

Example 2: The update interval and validity period for are shown below:

Table 2.2.1-2 Update Interval & Validity Period for Example 2

| | |
|---|---|
| Update interval of DS Certificate | 2 months |
| Validity period of passport | 10 years |
| Validity period of DS Certificate | 10 years and 2 months |
| Update interval of CSCA Certificate | 4 years |
| Validity period of CSCA Certificate | 14 years and 2 months |

If it is calculated similarly to the example 1, 61 DS Certificates will be issued (6 x 10 + 1) while the first DS Certificate is valid (ten years and two month).

Example 3: The update interval and validity period for are shown below:

Table 2.2.1-3 Update Interval & Validity Period for Example 3

| | |
|---|---|
| Update interval of DS Certificate | 3 months |
| Validity period of passport | 10 years |
| Validity period of DS Certificate | 10 years and 3 months |
| Update interval of CSCA Certificate | 5 years |
| Validity period of CSCA Certificate | 15 years and 3 months |

If it is calculated similarly to the example 1, 41 DS Certificates will be issued (4 x 10 + 1) while the first DS Certificate is valid (ten years and three months).

Considering the three examples above, the total number of DS Certificates to be issued is assumed to be 100 at maximum (with a margin).

ICAO TECHNICAL REPORT mentioned that a country which issues many electronic passports may two or more DS keys (*originally stated*). Considering this, we assume there are five Document Signers in a country.

We assume the data size (DS Certificate or CRL) on the directory is approximate 1KB.

The number of entries: the number of CRL + (the number of DS) x (the number
of controlled DS Certificate) = 1 + 5 x 100 = 501

The data size of a country: (the number of entries) x the data size   500KB

The size of Directory: (the number of member countries) x (the number of
entries) x the data size
= 188 x 501 x 1KB   100MB

ICAO TECHNICAL REPORT mentioned the size of Directory is 15 to 20MB.

This size was obtained when the number of DS in a country was assumed to be one.

The number of entries: the number of CRL + (the number of DS) x (the number
of controlled DS Certificate) = 1 +1 x 100 = 101

The size of Directory: (the number of member countries) x (the number of
entries) x the data size
= 188 x 101 x 1KB   19MB

Since ICAO TECHNICAL REPORT said a country that issues many electronic passports may two or more DS keys (*originally stated*), we assume the size of Directory is approximate 100MB.

(2) Estimate of performance

According to ICAO TECHNICAL REPORT, CRL should be written in the common registration directory within 90 days ordinarily and within 48 hours in case of emergency. It is not probable that all the member countries start writing the data in the common registration directory all at once. However, if they write the data all together within 48 hours, the number of accesses to be made in one hour will be as follows.

The number of simultaneous accesses: (the number of member countries of

ICAO) / 48 hours 8

The data to be written in the common registration directory are either DS Certificate or CRL. In the section 2.7.1 “Viewpoint from ICAO”, writing of the data of DS Certificate should be ‘addition’ while that of CRL is ‘overwriting’. Thus, one access size should be 1KB because writing does not deal with all the data but only update data.

In conclusion, the performance required for the common registration directory of ICAO-PKD is as follows.

The size of Directory: 100MB

The number of simultaneous accesses: 8 (accesses/hour)

The size of one access: 1KB (data writing)

Response time: a few seconds or less

ICAO should decide the server configuration to meet the requirements above (*newly stated*).

### 2.2.2 Performance of Common Reference Directory

Though ICAO TECHNICAL REPORT mentioned nothing specific about the performance of common reference directory, we think that it should be able to maintain enough response even when accesses from member countries are made intensively (*newly stated*). This review is based on the result described in the section 2.2.1 “Performance of Common Registration Directory”.

With regard to the system that downloads the entire data, ICAO TECHNICAL REPORT did not clarify whether a country should download the data at a representative point or each one of the validation systems should download the data individually. If the former is selected, traffic will be reduced.

Therefore, it is preferable that a country should download the entire data at one point. It is also preferable that repository using LDAP server in accordance with PKD should be used.

However, because it is not specified that a country should download the data at a representative point, we should assume the maximum load. Thus, we assume all the countries (UN members) with 10 validation systems each for calculating simultaneous accesses. However, because they make accesses for download everyday, accesses will be dispersed. Now, we calculate how many accesses may be made per minute.

The number of simultaneous accesses: (the number of UN member countries) x (the number of validation systems in a country)/(24 hours x 60 minutes)

= 191 x 10/(24 x 60) 2

When the entire download is selected, search from the top of the hierarchical structure cannot be done. Search should be done for each country.

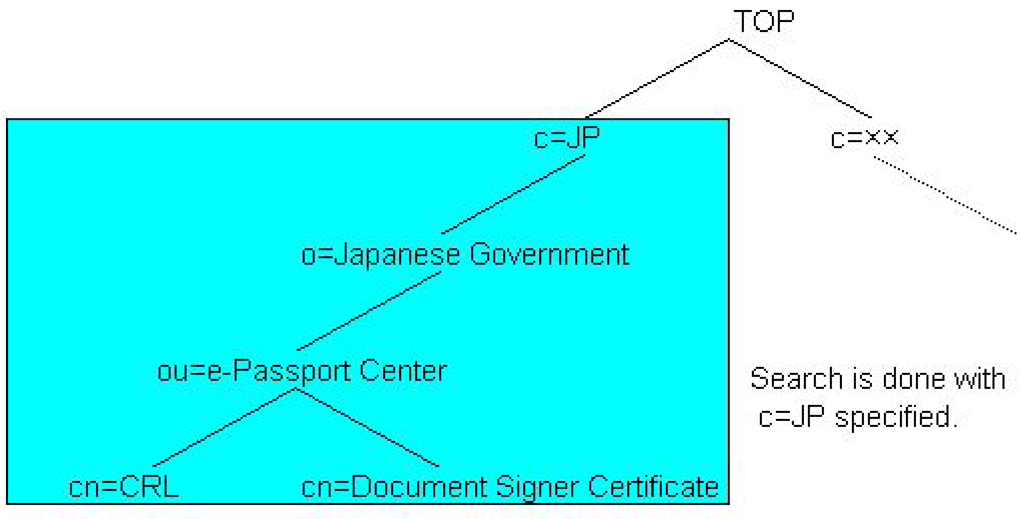
TOP
c=JP
c=xx
o=Japanese Government
ou=e-Passport Center
cn=CRL
cn=Document Signer Certificate
Search is done with c=JP specified.

Fig. 2.2.2-1 Scope of Download by One Operation

For example, if USA has DS for each state, the total number of DS should be 5,000 because we assume one DS has 100 certificates and USA has 50 states. Considering margin, the number of certificates should be 10,000. Since one certificate is assumed to be 1KB, the maximum download size with one operation should be 10MB (*newly stated*).

We have to consider the total size of download for ICAO-PKD, and it should be 100MB with one access.

In conclusion, the requirements for the common reference directory of ICAO-PKD are as follows:

The size of Directory: 100MB

The number of simultaneous accesses: 2 (accesses/minute)

The size of one access: 100MB (data reading)

Response time: a few minutes or less

The server configuration should be decided to meet the requirements above (*newly stated*).

### 2.2.3 Availability

Because every member country of ICAO makes access for update or reference at any time, the system must be available 24 hours a day, everyday. Thus, availability must be studied to meet this requirement (*newly stated*).

### 2.2.4 Network Security

Because ICAO-PKD is public to the Internet, threats from the network including security hole attacks and denial of service (DoS) attacks (*newly stated*).

## 2.3 Link among Servers

ICAO TECHNICAL REPORT did not specify the link among servers of ICAO-PKD. In order to secure sufficient performances and availability of the common registration directory and common reference directory, ICAO-PKD should be composed of several servers. The configuration diagram is shown in the figure 2.3.1 “System Configuration” (*newly stated*).

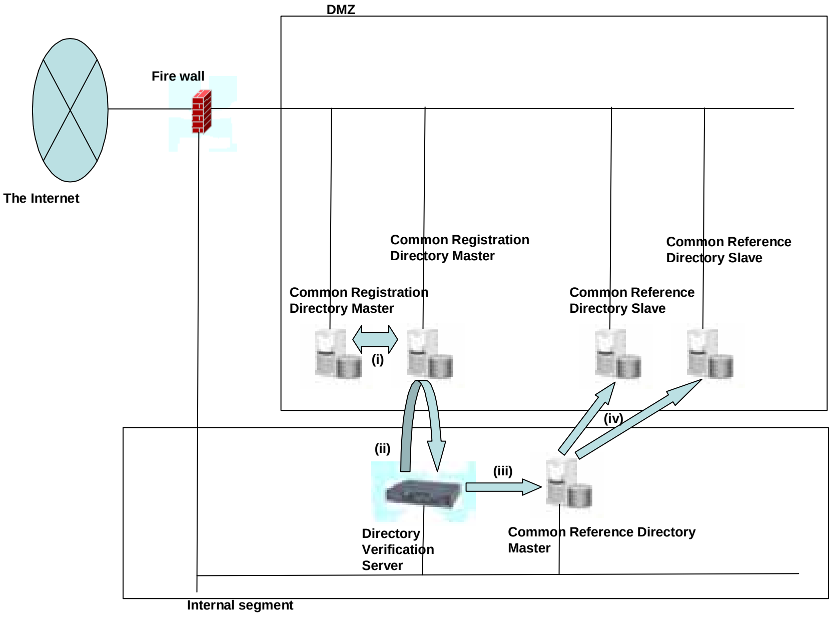
DMZ
Fire wall
The Internet
Common Registration Directory Master
Common Reference Directory Slave
Common Registration Directory Master
Common Reference Directory Slave
(i)
(iv)
(ii)
(iii)
Directory Verification Server
Common Reference Directory Master
Internal segment

Fig. 2.3.1 System Configuration

(i) Because writings are done to the common registration directory simultaneously, the configuration should have multi-master data replication.

(ii) DS Certificates and CRLs registered in the common registration directory should be checked to see if they are signed by the CSCA of the issuing country.

(iii) If signature validation successfully passed, the DS Certificate and CRL should be registered in the common reference directory.

In order to execute processing described in (ii) and (iii) above, the common registration directory and the common reference directory have their own servers (physically separated).

(iv) Because readings are done to the common reference directory simultaneously, the configuration should have data replication by master-slave link.

Writing to the common reference directory should be confined to the validation server.

To do so, there should be the master server of the common reference directory to do writing to the internal segment, and the slave server should be installed to DMZ.

In this way, if load to the common reference directory increases, you can increase servers.

## 2.4 Communication between Client and Server

Assuming that ICAO-PKD is the server and the servers of member countries (for upload and download) are the clients, we will examine the link between the clients and the server from the viewpoints below.

- LDAP protocol
- SSL

### 2.4.1 LDAP Protocol

In this section, LDAP protocol of ICAO-PKD is reviewed from the viewpoints below:

- Version
- Port number
- Operations of LDAP to be supported

#### (1) Version

Though ICAO TECHNICAL REPORT did not specify the version of LDAP protocol, we think the latest version of LDAP should be used for an access to ICAO-PKD.

The LDAPv3 should be used for an access to ICAO-PKD (*newly stated*).

It should be considered that LDAPv2 can be used in case of absolute necessity (*newly stated*).

However, if an access is made by LDAPv2, the parameter for the version of BindRequest should have 2. Furthermore, in case of LDAPv2, any attribute options including ";binary" should not be used.

#### (2) Port Number

Though ICAO TECHNICAL REPORT did not specify the port number for LDAP protocol, it specified the server authentication by SSL shall be done (*originally states*).

Therefore, an access should be made by LDAPS protocol. The port number should 636 in that case (*newly stated*).

#### (3) Operations of LDAP Supported

Though ICAO TECHNICAL REPORT did not specify operations of LDAP to be supported, we think the LDAP operations below that are specified in RFC1777 and RFC2251 should be supported (*newly stated*).

- Bind Request / Response
- Unbind Request / Response
- Search Request

- Search ResEntry / ResDone / ResRef (only for LDAPv3)
- Search Response (only for LDAPv2)
- Modify Request / Response
- Add Request / Response
- Delete Request / Response
- ModifyDN Request / Response (only for LDAPv3)
- ModifyRDN Request / Response (only for LDAPv2)

### 2.4.2 SSL

In this section, SSL communication of ICAO-PKD is reviewed from the viewpoints below:

- Version
- Handshake protocol
- Algorithm to be used
- Server certificate

(1) Version

Though ICAO TECHNICAL REPORT did not specify the version of SSL communication to be supported, we think TLS specified in RFC2246 based on the latest version of SSL (3.0) (*newly stated*).

(2) Handshake Protocol

Though ICAO TECHNICAL REPORT did not specify the handshake protocol of SSL communication to be supported, we think the handshake protocol specified in RFC2246 should be used (*newly stated*). Client authentication (one of the options) should not be used (*newly stated*).

Figure 2.4.2 shows the sequence of handshake protocol.

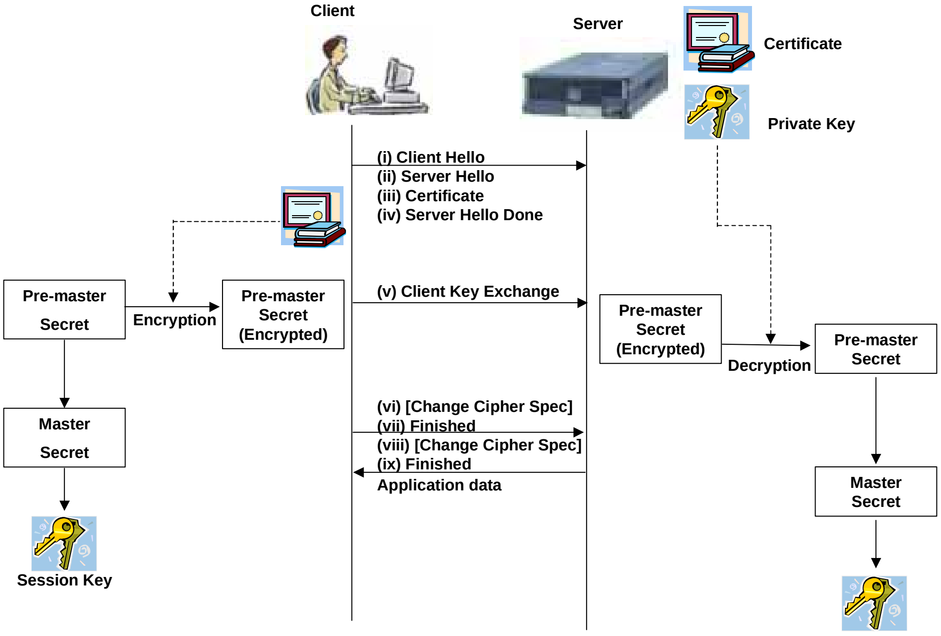

Fig. 2.4.2 Sequence of Handshake Protocol

The sequence of handshake protocol is described below:

(i) Client Hello

It notifies communication start to the server. The list of algorithms of encryption and compression that a client can use will be sent out.

Refer to the paragraph (3) below for the algorithms to be used.

(ii) Server Hello

The algorithms of encryption and compression to be used should be decided and the decision will be notified to the client. The algorithms are selected among the algorithms sent by the client.

Refer to the paragraph (3) below for the algorithms to be used.

(iii) Certificate

The server certificate including the list of certificates (certificate chain) up to the route CA will be sent out.

Refer to the paragraph (4) below for the certificates to be used.

(iv) Server Hello Done

The end of a series of messages starting from Server Hello will be notified to the client.

(v) Client Key Exchange

The information (called pre-master secret) to create the session key which is used for encryption will be created and sent to the server after the information being encrypted. The public key contained in the server certificate will be used for encryption of the pre-master secret.

(vi) [Change Cipher Spec]

The client creates the master secret from the pre-master secret and then create the session key from the mater secret.

Then, the information that cipher algorithms are ready will be notified to the server. Change Cipher Spec is not a part of the handshake protocol but an independent protocol (Change Cipher Spec Protocol).

(vii) Finished

It notifies the server that exchange of keys and authentication are finished successfully. The exchanged session key is used for encryption of the messages before transmitting them.

(viii) [Change Cipher Spec]

The server uses its own secret key to decrypt the pre-master secret after it receives the pre-master secret from the client. The server creates the master secret from the pre-master secret, and then creates the session key (common key) from the mater secret. This session key will be the same one as that was created by the client.

Then, the information that cipher algorithms are ready will be notified to the client. Change Cipher Spec is not a part of the handshake protocol but an independent protocol (Change Cipher Spec Protocol).

(ix) Finished

It notifies the server that exchange of keys and authentication are finished successfully. The exchanged session key is used for encryption of the messages before transmitting them.

After this step, the application data will be sent/received in the encrypted form.

(3) Algorithms Used

Because ICAO TECHNICAL REPORT did not specify the algorithms to be used for SSL communication, we will describe what we reviewed below.

The table 2.4.2-1 shows the list of Cipher Suites used for TLS (the cipher suites are specified by RFC2246).

Table 2.4.2-1 Cipher Suites for TLS

| Cipher Suites | Export-able | Key Exchange | Cipher | Hash |
|---|---|---|---|---|
| TLS_NULL_WITH_NULL_NULL | * | NULL | NULL | NULL |
| TLS_RSA_WITH_NULL_MD5 | * | RSA | NULL | MD5 |
| TLS_RSA_WITH_NULL_SHA | * | RSA | NULL | SHA |
| TLS_RSA_EXPORT_WITH_RC4_40_MD5 | * | RSA_EXPORT | RC4_40 | MD5 |
| TLS_RSA_WITH_RC4_128_MD5 |  | RSA | RC4_128 | MD5 |
| TLS_RSA_WITH_RC4_128_SHA |  | RSA | RC4_128 | SHA |
| TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 | * | RSA_EXPORT | RC2_CBC_40 | MD5 |
| TLS_RSA_WITH_IDEA_CBC_SHA |  | RSA | IDEA_CBC | SHA |
| TLS_RSA_EXPORT_WITH_DES40_CBC_SHA | * | RSA_EXPORT | DES40_CBC | SHA |
| TLS_RSA_WITH_DES_CBC_SHA |  | RSA | DES_CBC | SHA |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA |  | RSA | 3DES_EDE_CBC | SHA |
| TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA | * | DH_DSS_EXPORT | DES40_CBC | SHA |
| TLS_DH_DSS_WITH_DES_CBC_SHA |  | DH_DSS | DES_CBC | SHA |
| TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA |  | DH_DSS | 3DES_EDE_CBC | SHA |
| TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA | * | DH_RSA_EXPORT | DES40_CBC | SHA |
| TLS_DH_RSA_WITH_DES_CBC_SHA |  | DH_RSA | DES_CBC | SHA |
| TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA |  | DH_RSA | 3DES_EDE_CBC | SHA |
| TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA | * | DHE_DSS_EXPORT | DES40_CBC | SHA |
| TLS_DHE_DSS_WITH_DES_CBC_SHA |  | DHE_DSS | DES_CBC | SHA |
| TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA |  | DHE_DSS | 3DES_EDE_CBC | SHA |
| TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA | * | DHE_RSA_EXPORT | DES40_CBC | SHA |
| TLS_DHE_RSA_WITH_DES_CBC_SHA |  | DHE_RSA | DES_CBC | SHA |
| TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA |  | DHE_RSA | 3DES_EDE_CBC | SHA |
| TLS_DH_anon_EXPORT_WITH_RC4_40_MD5 | * | DH_anon_EXPORT | RC4_40 | MD5 |
| TLS_DH_anon_WITH_RC4_128_MD5 |  | DH_anon | RC4_128 | MD5 |
| TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA |  | DH_anon | DES40_CBC | SHA |
| TLS_DH_anon_WITH_DES_CBC_SHA |  | DH_anon | DES_CBC | SHA |
| TLS_DH_anon_WITH_3DES_EDE_CBC_SHA |  | DH_anon | 3DES_EDE_CBC | SHA |

The table 2.4.2-2 shows the list of Cipher Suites that are added by RFC3268 to the Cipher Suites (Addition) used for TLS.

Table 2.4.2-2 Cipher Suites for TLS (Addition)

| Cipher Suites | Key Exchange |
|---|---|
| TLS_RSA_WITH_AES_128_CBC_SHA | RSA |
| TLS_DH_DSS_WITH_AES_128_CBC_SHA | DH_DSS |
| TLS_DH_RSA_WITH_AES_128_CBC_SHA | DH_RSA |
| TLS_DHE_DSS_WITH_AES_128_CBC_SHA | DHE_DSS |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DHE_RSA |
| TLS_DH_anon_WITH_AES_128_CBC_SHA | DH_anon |
| TLS_RSA_WITH_AES_256_CBC_SHA | RSA |
| TLS_DH_DSS_WITH_AES_256_CBC_SHA | DH_DSS |
| TLS_DH_RSA_WITH_AES_256_CBC_SHA | DH_RSA |
| TLS_DHE_DSS_WITH_AES_256_CBC_SHA | DHE_DSS |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA | DHE_RSA |
| TLS_DH_anon_WITH_AES_256_CBC_SHA | DH_anon |

The algorithm set names below should not be used because they are for the case in which cipher is not used.

TLS_NULL_WITH_NULL_NULL
TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA

We think the set names below should not be used because they receive the attack called Meet-in-the-middle. This attack is known to aim at the weak point of Diffie Hellman. The sets below use key exchange by Diffie Hellman algorithm without authentication (it means the counterpart of communication is not authenticated).

TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5
TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_WITH_DES_CBC_SHA
TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
TLS_DH_anon_WITH_AES_128_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA

We also think that the set names below should not be used because it is pointed out that MD5 of hash algorithm has a few vulnerable points (*newly stated*).

TLS_RSA_WITH_NULL_MD5
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
TLS_DH_anon_WITH_RC4_128_MD5

We also think the set name below should not be used because exportable cipher suites are vulnerable (*newly stated*).

TLS_NULL_WITH_NULL_NULL
TLS_RSA_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_anon_EXPORT_WITH_RC4_40_MD5

We also think the set name below should not be used because DES ciphers are vulnerable (*newly stated*).

TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_DSS_WITH_DES_CBC_SHA
TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DH_RSA_WITH_DES_CBC_SHA
TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA

TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA

TLS_DH_anon_WITH_DES_CBC_SHA

(4) Recommended Cipher Suites

In conclusion, the figure 2.4.2-3 shows the cipher suites that should be used for TLS.

Table 2.4.2-3 Cipher Suites that should be used for TLS

| Cipher Suites | Key Exchange | Cipher | Hash |
|---|---|---|---|
| TLS_RSA_WITH_RC4_128_SHA | RSA | RC4_128 | SHA |
| TLS_RSA_WITH_IDEA_CBC_SHA | RSA | IDEA_CBC | SHA |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | RSA | 3DES_EDE_CBC | SHA |
| TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA | DH_DSS | 3DES_EDE_CBC | SHA |
| TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA | DH_RSA | 3DES_EDE_CBC | SHA |
| TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA | DHE_DSS | 3DES_EDE_CBC | SHA |
| TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA | DHE_RSA | 3DES_EDE_CBC | SHA |
| TLS_RSA_WITH_AES_128_CBC_SHA | RSA | AES_128_CBC | SHA |
| TLS_DH_DSS_WITH_AES_128_CBC_SHA | DH_DSS | AES_128_CBC | SHA |
| TLS_DH_RSA_WITH_AES_128_CBC_SHA | DH_RSA | AES_128_CBC | SHA |
| TLS_DHE_DSS_WITH_AES_128_CBC_SHA | DHE_DSS | AES_128_CBC | SHA |
| TLS_DHE_RSA_WITH_AES_128_CBC_SHA | DHE_RSA | AES_128_CBC | SHA |
| TLS_RSA_WITH_AES_256_CBC_SHA | RSA | AES_256_CBC_SHA | SHA |
| TLS_DH_DSS_WITH_AES_256_CBC_SHA | DH_DSS | AES_256_CBC_SHA | SHA |
| TLS_DH_RSA_WITH_AES_256_CBC_SHA | DH_RSA | AES_256_CBC_SHA | SHA |
| TLS_DHE_DSS_WITH_AES_256_CBC_SHA | DHE_DSS | AES_256_CBC_SHA | SHA |
| TLS_DHE_RSA_WITH_AES_256_CBC_SHA | DHE_RSA | AES_256_CBC_SHA | SHA |

(5) Server Certificate

ICAO TECHNICAL REPORT mentions that the server certificate shall be obtained from a commercial party in order to use SSL communication. However, it did not refer to whom it should be obtained from.

For the basis of selection for CA (certification authority) providers, there is audit of WebTrust for Certification Authorities sponsored by AICPA (American Institute of Certified Public Accountants). In selecting CA for the server certificate, the CA should pass the audit of WebTrust for Certification Authorities or equivalent (*newly stated*).

## 2.5 Interface for Update

In this section, Interface for Update of ICAO-PKD is reviewed from the viewpoints below:

- Security
- Operations of LDAP to be supported

### 2.5.1 Security

According to ICAO TECHNICAL REPORT, communication security depends on LDAP protocol which shall be used as the standard for making an access to Directory (*originally stated*). The transmission data shall be encrypted by authentication of the server through SSL (*originally stated*).

In this way LDAPS protocol is used.

According to ICAO TECHNICAL REPORT, access to the common registration directory shall be restricted to ICAO member countries. However, it does not specify access control clearly. So, we think the access control described in the figure 2.5.1-1 “Access Control of Common Registration Directory (draft)” can be applied.

Table 2.5.1-1 Access Control of Common Registration Directory (draft)

| Proposals | Merits | Demerits |
|---|---|---|
| Authentication by ID/password | Easy to handle because only ID/password should be notified. | ID/password may be leaked out. |
| Authentication of certificate by SASL | Safer than ID/password. | It is not clear who issues the certificate. |

Because ID/password may be leaked out, it is preferable to establish authentication of certificate by SASL (refer to RFC2222) (*newly stated*).

Regarding who issues the certificate of SASL, there are three possibilities: ICAO-PKD, certificate authorities recommended by ICAO or each country. In case each country issues the certificate, there are two possible cases: CSCA or a different certification authority issues it.

Table 2.5.1-2 Issuer of SASL Certificate (Proposal)

| Proposal | Merit | Demerit |
|---|---|---|
| ICAO issues it. | It can be operated under the unified security standard. | ICAO will have cost increase. |
| CA recommended by ICAO issues it. | It can be operated under the unified security standard. | — |
| Each country issues it. | Operation will be easier. | Security of each country's communication depend on the security level of the CA. |

In conclusion, it is preferable that CA recommended by ICAO should issue the certificate if authentication of certificate by SASL is used (*newly stated*).

### 2.5.2 LDAP Operations Supported

The common registration directory will be updated by additions from ICAO member countries. So, the LDAP operations below should be supported (*newly stated*).

**BindRequest**

It is authorized for connection.

BindRequest parameters are as follows:

| | |
|---|---|
| Version | 3 |
| Name | Identification of user |
| authentication.sasl | “LDAP_SASL_EXTERNAL” |

**Bind Response**

It should be in accordance with the definitions in RFC2251 4.2.3.

**Unbind Request / Response**

It should be in accordance with the definitions in RFC2251 4.3.

**Search Request**

It should be in accordance with the definitions in RFC2251 4.5.1.

**SearchResEntry / ResDone / ResRef**

It should be in accordance with the definitions in RFC2251 4.5.2 and 4.5.3.

**Modify Request / Response**

It should be in accordance with the definitions in RFC2251 4.6.

**Add Request/Response**

It should be in accordance with the definitions in RFC2251 4.7.

**Delete Request/Response**

It should be in accordance with the definitions in RFC2251 4.8.

**Modify DN Request/Response**

It should be in accordance with the definitions in RFC2251 4.9.

## 2.6 Interface for Reference

In this section, Interface for Reference of ICAO-PKD is reviewed from the viewpoints below:

- Security
- Operations of LDAP to be supported

### 2.6.1 Security

According to ICAO TECHNICAL REPORT, communication security depends on LDAP protocol which shall be used as the standard for making an access to Directory (*originally stated*). The transmission data shall be encrypted by authentication of the server through SSL (*originally stated*).

In this way LDAPS protocol is used.

According to ICAO TECHNICAL REPORT, access to the common reference directory is restricted to reading. ICAO TECHNICAL REPORT stipulates that an access for reading to ICAO-PKD shall not be restricted to member countries (*originally stated*). Therefore, the common reference directory should allow reading after anonymous connection (*newly stated*).

### 2.6.2 LDAP Operations to be Supported

The common reference directory is read by member countries. So, to the common reference directory, addition, update and deletion should not be done except by the validation server which updates the common reference directory from the common registration directory in ICAO-PKD. So, the LDAP operations below should be supported (*newly stated*).

**BindRequest**

It is authorized for connection.

BindRequest parameters are as follows:

| | |
|---|---|
| Version | 3 |
| Name | “” (letter string with the length being 0) |
| authenticaton.simple | “” (letter string with the length being 0) |

**Bind Response**

It should be in accordance with the definitions in RFC2251 4.2.3.

**Unbind Request / Response**

It should be in accordance with the definitions in RFC2251 4.3.

**Search Request**

It should be in accordance with the definitions in RFC2251 4.5.1.

**SearchResEntry / ResDone / ResRef**

It should be in accordance with the definitions in RFC2251 4.5.2 and 4.5.3.

It is possible to make unlimited connection by specifying 0 (zero) to sizelimit and timelimit (they are internal parameters for search) when connected from each country.

With regard to sizelimit of the common reference directory, the maximum download size is assumed to be 10MB for one operation. Refer to the section 2.2.2 “Performance of Common Reference Directory”.

With regard to timelimit, the time to allow all the data to be downloaded should be decided (*newly stated*).

## 2.7 Operations

In this section, operations of ICAO-PKD system are reviewed from the viewpoints below:

- Viewpoints from ICAO
- Viewpoints from issuing countries (writing)
- Viewpoints from validating countries (download)

### 2.7.1 Viewpoints from ICAO

(1) In case of registration of a new country to ICAO-PKD

When a new country is registered in ICAO-PKD, the data of the country with the tree configuration specified by the new country should be created (*newly stated*). The data should be two-letter country code of ISO 3166.

Because search from the top of the hierarchical structure of ICAO-PKD cannot be done, search should be done for each country. So, the member countries should know what countries are registered. To meet this purpose, when ICAO-PKD has a new country registered, it should disclose the information of the country on the web (*newly stated*).

When ICAO-PKD receives Country Signing CA Certificate from a new country, the procedure should be decided to have enough security as described below (*newly stated*).

- ICAO-PKD receives Country Signing CA Certificate in a safe way (ex. by e-mail or LDAP service).
- ICAO-PKD receives the finger print (message digest) of Country Signing CA Certificate via another route.
- The finger print (message digest) is checked whether it is the same as that on the Country Signing CA Certificate that was received earlier.

After ICAO-PKD confirms the Country Signing CA Certificate is genuine, it shall control it safely in accordance with HSM (Hardware Security Module) of the Common Criteria Protection Profile with EAL 4+ SOF-High (*originally stated*).

(2) Registration to Common Registration Directory

ICAO-PKD needs to confirm that the contents of DS Certificate and CRL are genuine when they are written in the common registration directory, and then ICAO-PKD discloses them to the common reference directory. The DS Certificate and CRL are issued by a country and they are signed by the Country Signing CA

Certificate of the issuing country. Therefore, ICAO-PKD checks DS Certificate and CRL (written in the common registration directory) against the Country Signing CA Certificate stored in HSM. And only when it is genuine, it should be disclosed to the common reference directory (*newly stated*).

For applications by a member country about addition/update of Country Signing CA Certificate, they are treated in the same way as that described in the paragraph (1) "In case of registration of a new country to ICAO-PKD" (*newly stated*).

(3) Deletion of Certificate

With regard to treatment of expired Country Signing CA Certificate, there are two possible ways: each country deletes it and ICAO-PKD deletes it. In case that each country deletes it: deletion by a vicious third person may not be prevented if the deletion from the common registration directory causes it to be deleted from the common reference directory. Therefore, it is possible for a country to ask for deletion of an expired certificate. However, the true purpose of treatment of expired certificates is to reduce unnecessary data in ICAO-PKD. Therefore, it is recommended that expired Country Signing CA Certificate should be deleted by ICAO-PKD (*newly stated*).

For expired DS Certificates of member countries, ICAO should check them periodically and delete them if they are really expired (*newly stated*).

Automatic deletion of the certificate from the common reference directory when the certificate is deleted from the common registration directory should not be implemented because there may be deletion by a vicious third person. Thus, ICAO-PKD should delete the certificate from the common registration directory independently of deletion of the certificate from the common reference directory (*newly stated*).

It is assumed that if DS Certificate is not stored in IC passport (SOD), the validation system may obtain DS Certificate from ICAO-PKD. In such case, the validation system will be unable to validate the signature of SOD. DS Certificate should be stored in ICAO-PKD until it is expired even when it lost validity (*newly stated*).

CRL should be overwritten by the member country for update (*newly stated*).

DS Certificate should be updated by additional entries specified by the member country for update (*newly stated*).

(4) Restoration by Backup

ICAO-PKD should automatically back up both the common registration directory and the common reference directory everyday (*newly stated*).

ICAO-PKD should also back up the entire system periodically (every three months) so that it can restore the system in case of trouble (*newly stated*).

(5) Trouble Shooting

The common registration directory and the common reference directory are required to be available 24 hours a day, everyday. Therefore, it is necessary to have contingency plans by installing the system monitoring device to monitor the operations all the time, so that restoration can be done immediately when a trouble occurs (*newly stated*).

ICAO-PKD validates the signs on Country Signing CA Certificate before disclosing the data from the common registration directory to the common reference directory. If the validation finds the sign is not that of the Country Signing CAA of the issuing country, it should be considered that a vicious third person tried to register invalid DS Certificate or CRL. In that case, the invalid DS Certificate or CRL should be stored in the file as evidence, and then it should be deleted from the common registration directory (*newly stated*). Because the common registration directory has access control by SASL authentication for each country, the fact that an invalid DS Certificate or CRL was written in the common registration directory suggests that the public key to be used for SASL authentication of the country had been stolen. Therefore, the certificate to be used for authentication should be made invalid and a new certificate should be issued for SASL authentication (*newly stated*).

### 2.7.2 Viewpoints from Issuing Countries (Writing)

(1) In case of registration of a new country to ICAO-PKD

When a country joins in ICAO-PKD for the first time, the issuing country should inform the data about country and organization in the directory's tree structure to ICAO-PKD, and have the user created by ICAO-PKD; the user is to access to the entry of the country and the organization and the common registration directory (*newly stated*).

The issuing country should design the layers below the organization and create an entry to store DS Certificate and CRL in the common registration directory (*newly stated*).

The issuing country sends Country Signing CA Certificate to ICAO-PKD. For the procedure to be used in this case, the procedure specified by "Viewpoint of ICAO" should be followed.

Besides the operation of ICAO-PKD, two countries send Country Signing CA Certificate by diplomatic channel if they have diplomatic relations.

ICAO TECHNICAL REPORT mentions that two countries exchange the certificate and CRL by using the existing route (i.e. e-mail, LDAP service and so on).

The possible transmission ways are listed below (*newly stated*).

Plan 1: transmission by the embassy

Plan 2: direct transmission

These two plans can be decided between two countries for implementation.

The method of transmission is more important and the possible methods are listed below.

Plan 1: encrypted data are sent by e-mail.

Plan 2: encrypted data are stored in the media (i.e. FD) and the media are transmitted.

Plan 3: the data are stored in the media with the password and the media are transmitted.

One of these methods should be selected.

(2) Registration to Common Registration Directory

An issuing country should upload the certificate in the common registration directory immediately when it issues DS Certificate. The issuing country shall update CRL with an interval of at least 90 days (*originally stated*).

(3) Trouble Shooting

The issuing country shall issue CRL immediately when the Document Signer secret key is compromised, and register it in ICAO-PKD within 48 hours (*originally stated*).

The issuing country shall issue CRL immediately when the Country Signing CA secret key is compromised, and register it in ICAO-PKD within 48 hours (*originally stated*).

Besides the operation of ICAO-PKD, two countries send CRL by diplomatic channel if they have diplomatic relations.

### 2.7.3 Viewpoints from Validating Countries (download)

(1) Initial Operation

The validating country needs to know the country information (c=xx) registered in ICAO-PKD when it downloads the information from ICAO-PKD because it cannot search from the top of the hierarchical structure. The validating country searches the country information (c=xx) registered in ICAO-PKD from the web (*newly stated*).

Besides the operation of ICAO-PKD, two countries receive Country Signing CA Certificate by diplomatic channel if they have diplomatic relations. For the way of receiving the certificate, the procedure described in the paragraph “Viewpoint of Issuing Countries (Writing)” should be used.

(2) Operation of Download

A validating country downloads the entire data of ICAO-PKD everyday. The validating country should download the entire data at one point in the country if possible, and it should disclose the data to the directory server (*newly stated*).

It is not recommended that making access to ICAO-PKD whenever required without downloading the data in advance from ICAO-PKD, because it impose a lot of loads (traffics) to the system (*newly stated*).

(3) Trouble Shooting

If the validating country fails to download the data due to time out, it should make a report to ICAO-PKD. ICAO-PKD investigates the state of loads on the common reference directory, and it adds a server if necessary (*newly stated*).