付録 1

PKI コンポーネント間接続に関する標準

付録 1-1

相互接続インターフェース仕様

CA-CA Interoperability

Interface Specification

- Table of Contents -

- List of Figures –

- List of Tables -

- Trademarks, Registered Trademarks -

1. Introduction

This specification describes a minimum set of interfaces to the JHKST (Japan / Hong Kong, China / Korea / Singapore / Chinese Taipei) PKI Model needed by the Certification Authority, application developers, and the end-entity users to interconnect one another. In 2002, Korea, Singapore, and Japan developed the PKI model, so called a hybrid PKI model between Cross Certification and Cross Recognition. In 2003, Japan, Hong Kong China, and Chinese Taipei experimented the PKI model in a similar fashion. This specification is written, based on the results of the experiments and the final report, by the Interoperability Working Group (IWG) of Asia PKI Initiative.

The specification includes the certificate and CRL profile, directory profiles for multiple PKI domains' interoperability, with greater harmony with the Internet Engineering Task Force (IETF) Public Key Infrastructure, ITU-T Recommendation, and other standard documents. The specification establishes a profile that is a largely subset of the PKI profile in IETF in order to help maintain the interoperability in multiple PKI domain environments. All of the other technical details are also referred from the documents published by standardization organizations.

The specification is still generic in a sense that potential PKI designers still can customize this specification for their specific needs. However, in order to make interoperable environments in multiple PKI domains, this specification suggests the recommended profiles and procedure.

It is important that the JHKST PKI model be compatible as much as possible with PKI efforts established in other activities conduced and hope that the JHKST PKI model could be used as a reference model for PKI initiatives in Asia regions.

A final report in 2001 experiment can be found at the PKI-J web page:

http://www.japanpkiforum.jp/E/index.htm

2. References

[x500]	ITU-T Recommendation X.500 – Information technology – Open Systems Interconnection – The Directory: Overview of concepts, models and services, 2001
[x501]	ITU-T Recommendation X.501 – Information technology – Open Systems Interconnection – The Directory: Models, 2001
[x509]	ITU-T Recommendation X.509 – Information technology –Open Systems Interconnection – The Directory: Authentication Framework, 1997
[x520]	ITU-T Recommendation X.520 – Information technology – Open Systems Interconnection – The Directory: Selected attribute types, 2001
[x521]	ITU-T Recommendation X.521 – Information technology – Open Systems Interconnection – The Directory: Selected object classes, 2001
[x690]	ITU-T Recommendation X.690 – Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 1998
[2251]	Lightweight Directory Access Protocol (v3) Internet Request For Comments 2251 December 1997
[2252]	Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions. Internet Request For Comments 2252 December 1997
[2253]	Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names Internet Request For Comments 2253 December 1997
[2254]	The String Representation of LDAP Internet Request For Comments 2254 December 1997
[2255]	The LDAP URL Format Internet Request For Comments 2255 December 1997
[2256]	A Summary of the X.500 (96) User Schema for use with LDAPv3 Internet Request For Comments 2256 December 1997
[2279]	UTF-8, a transformation format of ISO 10646 Internet Request For Comments 2279 January 1998
[2396]	Uniform Resource Identifiers (URI): Generic Syntax Internet Request For Comments 2396 August 1998
[2459]	Internet X.509 Public Key Infrastructure Certificate and CRL Profile Internet Request For Comments 2459 January 1999
[2559]	Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2 Internet Request For Comments 2559 April 1999
[2560]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP Schema Internet Request For Comments 2560 June 1999.
[2587]	Internet X.509 Public Key Infrastructure LDAPv2 Schema Internet Request For Comments 2587 June 1999
[3280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile Internet Request For Comments 3280 April 2002
[p10]	PKCS 10: Certification Request Syntax Version 1.0, 1993
[p12]	PKCS 12 v1.0: Personal Information Exchange Syntax, 1999

3. Symbols and Abbreviations

ARL	Authority Revocation List
ASN.1	Abstract Syntax Notation One
B2B	Business to Business
BER	Basic Encoding Rules
CA	Certification Authority
CRL	Certificate Revocation List
CC	Cross Certification
DAP	Directory Access Protocol
DER	Distinguished Encoding Rules
DIT	Directory Information Tree
DN	Distinguished Name
EE	End entity
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKCS	Public Key Cryptograph Standard
RDN	Relative Distinguished Name
RA	Registration Authority
SCA	Subordinate CA
VA	Validation Authority

4. CA-CA Model

The PKI technology develops several CA-CA models in which the relying party can trust the information and digital certificates signed by other parties in multiple PKI domains. It is unlikely that end-entity transactions can be accomplished with the PKI applications without considering the PKI CA-CA model. After evaluating several possibilities, the IWG employs two major models, Cross Certification and Cross Recognition.

4.1 Overview

This section describes a CA-CA model. The CA-CA model used in this experiment is shown below.

4.1.1 Cross Certification (CC)

The concept of Cross Certification is that a CA publishes a certificate to another CA. There are two kinds of Cross Certification. One is “Mutual Cross Certification”. The other is “Unilateral Cross Certification”. These are described below.

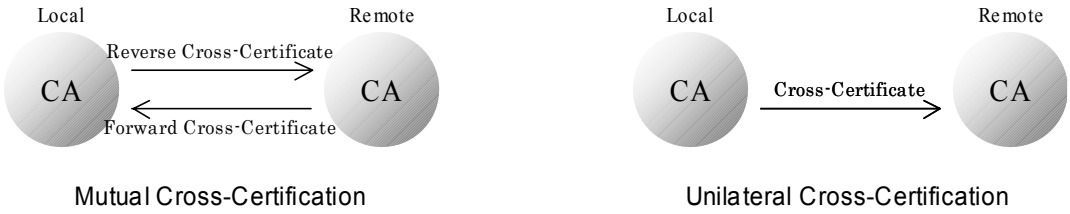

Fig. 1 Cross Certification (Mutual CC, Unilateral CC)

Mutual Cross Certification is the case where one CA publishes a certificate to the other, and vice versa. The relationship of “Cross Certification” is shown at the left of the Fig. 1. Unilateral Cross Certification is the case where one CA publishes a certificate only to a remote CA. The model “Unilateral Cross Certification” is used when adopting a hybrid model and when a CA publishes a certificate to a subordinate CA.

In multiple PKI domains environment, especially in international context, it is more suitable for each party to use the Mutual CC model when the Cross Certification model is employed.

4.1.2 Cross Recognition (CR)

Cross Recognition is a concept considered by APEC TEL WG, and is defined as follows:

> *An interoperability arrangement in which a relying party in one PKI domain can use authority information in another PKI domain to authenticate a subject in the other PKI domain, and vice-versa.* [1]

An example of application for Cross Recognition is "Web browser model". Web browser has a lot of certificates as a trusted list. An example of the method to establish Cross Recognition is that a relying party stores the trust anchor certificates into application, decides whether to accept the sender's certificate or not, and validates the certificate based on the trust anchor information as user-acceptable trust point[2]. The Cross Recognition covers a concept of the acceptance framework on how the relying party can decide to accept the trust anchor certificate of the other parties. However, this is out of scope in this document.

4.2 IWG Architecture

IWG Architecture is constituted on the basis of the following concepts:

- For Cross Certification, Root CAs publish cross certificates each other.
- For Cross Recognition, an EE trusts the Root CA of the other domain based on the EE decision (Presumably, some information is given in advance to evaluate the trust relationship.)
- The Root CAs have zero or more subordinate CAs.

Therefore, IWG Architecture becomes the following models.

[1] ACHIEVING PKI INTEROPERABILITY (http://www.apectelwg.org/apecdata/telwg/eaTG/eatf06.doc)
[2] It is expected that the sender's CP OID or/and the relying party' CP OID are set as user_initial_policy_set in order to validate the certificate path in CR model.

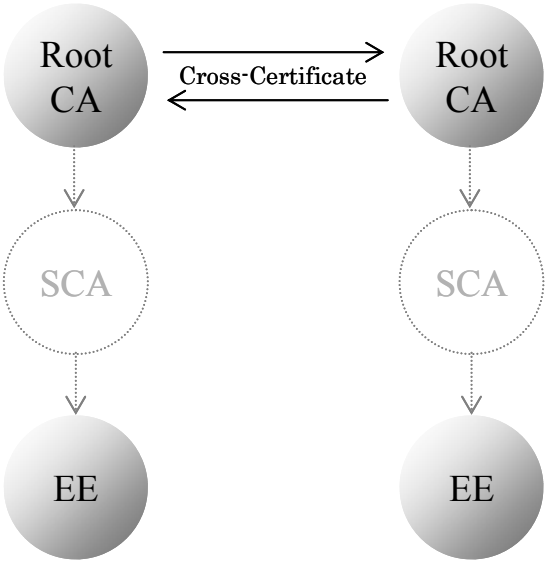

Fig. 2 Cross Certification (IWG Architecture)

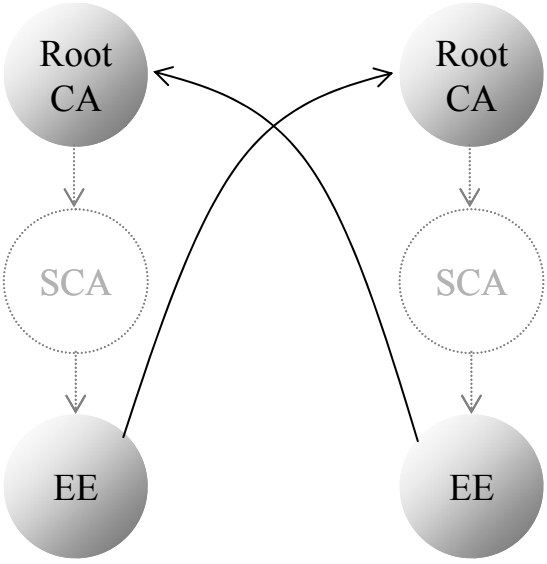

Fig. 3 Cross Recognition (IWG Architecture)

With our experience, the government-initiated architectures tend to employ the CC model (Bridge CA model as well) and Business-to-Business oriented architectures employ the CR or Web model. It is suggested that it is preferable for CA systems and end-entity applications to handle the two models used in the multiple PKI domains.

4.3 Policy Structure Consideration

In the multiple PKI domains environment, it is imperative to establish, evaluate, agree upon, and check the certificate policies and their mappings in consistent manners. IWG architecture assumes that the multiple domains establish solid certificate policies and agree upon between the CAs, or such policies are evaluated by some trusted audited organization. It is highly expected that a valid policy path should be constructed in the certificate path and validated in the relying party applications. Even the CR model should provide some mechanisms to notify the information of certificate policies to help the EE decision and the option to check the valid policy.

5. Interface of PKI Components

5.1 PKI Components

The following figure shows the PKI components in the IWG architecture. There is a minimum set of the PKI components interfaces to be agreed upon between involved parties. Typically, the internal CA-RA-EE interfaces are not important for the multiple domains environment. Rather, the CA-CA interface and the EE-Repository interface are important and have to be agreed. The solid line is the interface to other domains, and the broken line is out of scope.

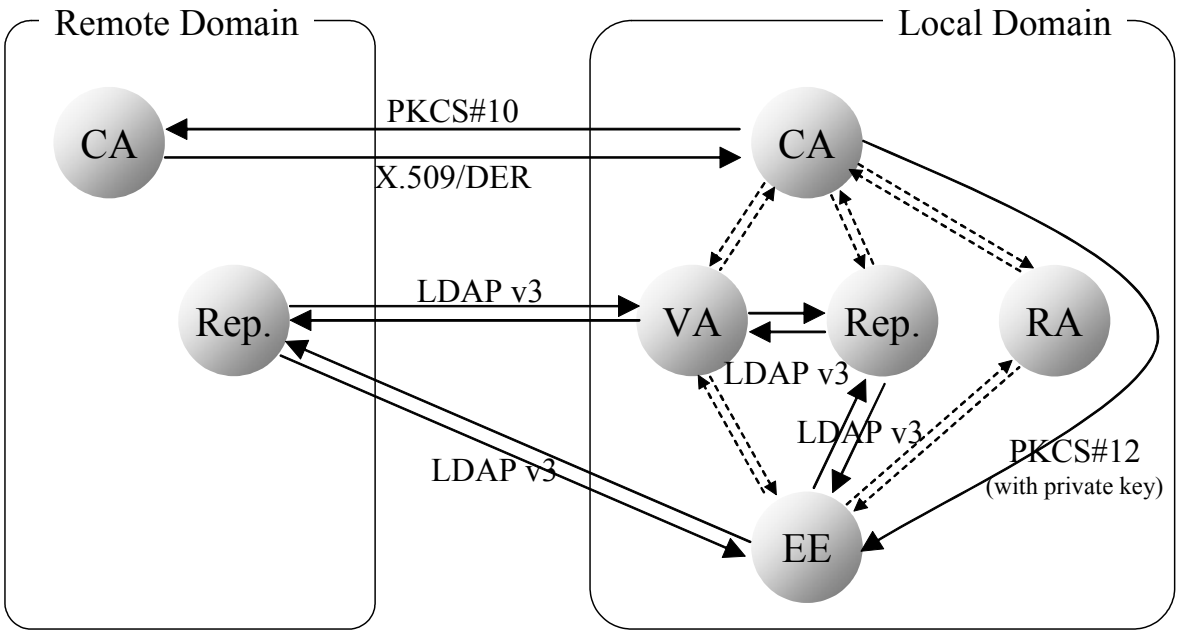

Fig. 4 PKI Components

Here is the summary of the PKI components interfaces that be agreed. For the certificate profile, the detail will be described later.

Content	Interface
Certificate profile	X.509(97) v3[x509], RFC3280[3280]
Certificate encoding format	DER[x690]
CRL profile	X.509(97) v3, RFC3280
CRL encoding format	DER
Cross-Cert request format	PKCS#10[p10]
Cross-Cert response format.	X.509/DER
The method to sends the fingerprint.	E-Mail
POP (proof of possession)	Verification of digital signature on certificate request format

Table. 1 CA-CA interface

Content	Interface
EE Certificate response format	PKCS#12[p12] (Private-key included)

Table. 2 CA-EE interface

Content	Interface
Repository access protocol (e.g., LDAPv2, LDAPv3, DAP)	LDAPv3[2251]

Table. 3 End Entity-Repository interface and VA-Repository interface

Content	Interface
EE-VA access protocol	OPTIONAL
Role of VA	Certificate Validation Server (Path Construction, Path Validation)

Table. 4 End Entity-VA interface

Content	Interface
Certificate path validation method	RFC3280
Certificate validation entity	VA, EE

Table. 5 End Entity-End Entity interface

6. Profile

The certificate and crl/arl profile is based on the X.509 and RFC 3280 standards. The RFC 3280 provides the information on the details of the data fields and format and the guidance on the choices of the fields, and the values in each field. The IWG creates a profile that is a great harmony with the standards and that is more specific to the choice of the data values and fields to maintain the interoperability in multiple PKI domains. The profile contains the basic and extension fields. The basic fields are needed to set the value in mandatory fashion. An extension can be non-critical or critical. If an extension is critical and an application does not recognize or cannot process that extension, the application must reject any transaction. The handling of the criticality follows the RFC 3280.

6.1 Policy of Designing Certificate/CRL Profiles

- Certificate/CRL profile is based on rfc3280 and X.509 (97).
- The profile is primarily designed for the digital signature usage for document exchange applications and for the secure email usage of EE.
- This profile includes the new fields of RFC3280, even not defined.
- The local encryption algorithm and private extensions of each country are not used. Currently IWG members agree upon only the SHA-1 for hash algorithm. Other choices can always be considered.
- The character set in Certificate/CRL must be within the range of PrintableString. (Multi-byte code is out of scope in this experiment.)
- xxxConstraint extensions MAY be used in the test environments. However in the real usage, complex xxxConstraint extensions are recommended not to use.
- Some parts are based on the present implementation and the limitations of the application such as Microsoft® Windows® operating systems and etc.

6.2 CA Certificate Profile

There are 4 types of the CA certificates, Root CA certificate, Self-issued, Subordinate CA certificate, and Cross certificate. In the experiment, to simplify the certificate hierarchy, the subordinate CA was excluded. Therefore the following profile shows only the ROOT CA's self-signed certificate and CC (cross certification) certificate. The subordinate CA certificate profile will be defined in the future. This will be more or less

a similar set of the Cross certificate fields without the policy mapping extension field.

6.2.1 ROOT CA Certificate Profile

The ROOT CA's self-signed certificate is used for signing other CA certificates, self-issued certificate, cross certificate, and its subordinate CA certificate. The ROOT CA certificate will be used to provide the public key of the trust anchor and the initial information of the certificate path processing.

Certificate Basic field

FIELD	NOTE
version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 2 (v3).
serialNumber (Mandatory)	unique integer. Up to 20 octets.
Signature (Mandatory)	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
issuer (Mandatory)	X.500 DN. Although DN is generally encoded by UTF8STRING, according to description of the X.520(2001), Country attribute is encoded by PrintableString.
Validity (Mandatory)	UTC TIME
subject (Mandatory)	X.500 DN. And see issure.
subjectPublicKeyInfo (Mandatory)	1.2.840.113549.1.1.1 (rsaEncryption) CA: 2,048bit
issureUniqueID (not used)	
subjectUniqueID (not used)	

Certificate Extension field

FIELD	NOTE
authorityKeyIdentifier (optional, non-critical)	**keyID(Mandatory):** The hash value of Issuer's public key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2.

	authorityCertIssuer(optional): DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
subjectKeyIdentifier (Mandatory, non-critical)	The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage (optional, critical)	When used, keyCertSign and cRLSign should be included at least.
extKeyUsage (not used)	
privateKeyUsagePeriod (not used)	
certificatePolicies (optional, critical)	When used, policyID MUST be present.
policyMappings (not used)	
subjectAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
issureAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
subjectDirectryAttributes (not used)	
basicConstraints (Mandatory, critical)	cA=TRUE pathLen=optional (INTEGER)
nameConstraints (not used)	
policyConstraints (not used)	
cRLDistributionPoints (optional, non-critical)	directoryName, URI
authorityInfoAccess (optional, non-critical)	If the PKI domain uses OCSP, this field will be used.
inhibitAnyPolicy (not used)	
freshestCRL (not used)	
subjectInfoAccessSyntax (not used)	

6.2.2 CC Certificate

The CC certificate is a certificate, issued by the issuer domain to the subject domain. The CC certificate represents the subject domain policy is equivalent to the issuer domain policy. The certificate is allowed to use constraint-related extensions such as basic constraints, policy constraints, and name constraints. However, extreme cautions must be required in order to design such extensions in multiple PKI domains. IWG profile currently requires only the basic constraint as a mandatory field in CA certificates.

Certificate Basic field

the same as ROOT CA Certificate

Certificate Extension field

About certificatePolicies, the critical-flag can be set as "non-critical", considering the implementation of the present application (e.g. Microsoft® Windows® 2000 operating system or earlier etc). However, it is necessary to check the policy in the path processing.

FIELD	NOTE
authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2 **authorityCertIssuer(optional):** DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
subjectKeyIdentifier (Mandatory, non-critical)	The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage (Mandatory, critical)	keyCertSign, cRLSign
extKeyUsage (not used)	
privateKeyUsagePeriod (not used)	

certificatePolicies (Mandatory, ether critical or non-critical[3])	policyID MUST be present.
policyMappings (Mandatory, non-critical)	
subjectAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
issureAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
subjectDirectryAttributes (not used)	
basicConstraints (Mandatory, critical)	cA=TRUE pathLen=optional (INTEGER)
nameConstraints (optional, critical)	
policyConstraints (optional, critical)	If the PKI domain wants to strictly validate of certificate policies, this field will be set as requireExplicitPolicy=0.
cRLDistributionPoints (Mandatory, non-critical)	"distPoint.fullname" must contain URI (port number, attribute: Mandatory binary option: optional[4])
authorityInfoAccess (not used)	If the PKI domain uses OCSP, this field will be used.
inhibitAnyPolicy (not used)	
freshestCRL (not used)	
subjectInfoAccessSyntax (not used)	

6.2.3 SubCA Certificate

The SubCA certificate is a certificate, issued by the CA to the subordinate CA.

Certificate Basic field

the same as ROOT CA Certificate

[3] It must be verified of a policy by the case of non-critical as well as the case of critical.
[4] ldap://hostname[:portnumber]/dn?attr[;binary]

Certificate Extension field

About certificatePolicies, the critical-flag can be set as "non-critical", considering the implementation of the present application (e.g. Microsoft® Windows® 2000 operating systems or earlier etc). However, it is necessary to check the policy in the path process.

FIELD	NOTE
authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2 **authorityCertIssuer(optional):** DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
subjectKeyIdentifier (Mandatory, non-critical)	The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage (Mandatory, critical)	keyCertSign, cRLSign
extKeyUsage (not used)	
privateKeyUsagePeriod (not used)	
certificatePolicies (Mandatory, ether critical or non-critical [5])	policyID MUST be present.
policyMappings (Mandatory, non-critical)	
subjectAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
issureAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
subjectDirectryAttributes (not used)	
basicConstraints (Mandatory, critical)	cA=TRUE pathLen=optional (INTEGER)

[5] It must be verified of a policy by the case of non-critical as well as the case of critical.

nameConstraints (optional, critical)	
policyConstraints (not used)	
cRLDistributionPoints (Mandatory, non-critical)	"distPoint.fullname" must contain URI (port number, attribute: Mandatory binary option: optional[6])
authorityInfoAccess (not used)	If the PKI domain uses OCSP, this field will be used.
inhibitAnyPolicy (not used)	
freshestCRL (not used)	
subjectInfoAccessSyntax (not used)	

6.3 EE Certificate Profile

The EE Certificate is used by individual or the electric ID to identify the entity for certain transactions. The issuer and subject name in the certificate is the DN for a corresponding entry in the directory.

The common fields of the EE Certificate are specified in "6.3.1". The following sections, "6.3.2" and "6.3.3" specify the differences from "6.3.1" for individual applications.

6.3.1 Common EE Profile

Certificate Basic field

the same as ROOT CA Certificate

Certificate Extension field

About certificatePolicies, critical-flag can be set to non-critical in consideration of the present application implementation (e.g. windows2000 or earlier etc). However, it is necessary to validate of a policy also the same as the case of critical.

FIELD	NOTE
authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's public key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2

[6] ldap://hostname[:portnumber]/dn?attr[;binary]

	authorityCertIssuer(optional): DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
subjectKeyIdentifier (Mandatory, non-critical)	The hash value of Issuer's public key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage (Mandatory, critical)	Please see 6.3.2 and 6.3.3 about a value.
extKeyUsage (not used)	
privateKeyUsagePeriod (not used)	
certificatePolicies (Mandatory, ether critical or non-critical [7])	policyID MUST be present.
policyMappings (not used)	
subjectAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used. And see 6.3.3.
issureAltName (optional, non-critical)	If the PKI domain wants to include email address or etc in the certificate, this field will be used.
subjectDirectryAttributes (not used)	
basicConstraints (optional, critical)	It recommends that CAs don't include a this field.
nameConstraints (not used)	
policyConstraints (not used)	
cRLDistributionPoints (Mandatory, non-critical)	"distPoint.fullname" must contain URI (port number, attribute: Mandatory binary option: optional[8])
authorityInfoAccess (not used)	If the PKI domain uses OCSP, this fieldwill be used.

[7] It must be verified of a policy by the case of non-critical as well as the case of critical.
[8] ldap://hostname[:portnumber]/dn?attr[;binary]

inhibitAnyPolicy (not used)	
freshestCRL (not used)	
subjectInfoAccessSyntax (not used)	

6.3.2 Identification Certificate (digital signature)

Certificate Extension field

keyUsage (Mandatory, critical)	digitalSignature (, nonRepudiation)

6.3.3 Secure E-Mail Certificate (data Encipherment and digital signature)

Certificate Extension field

keyUsage (Mandatory, critical)	keyEncipherment, dataEncipherment
subjectAltName (Mandatory, non-critical)	If the PKI domain wants to include multi byte code or email address or etc in the certificate, this field will be used.

6.4 ARL/CRL Profile

Authority Revocation List (ARL) and Certificate Revocation List (CRL) are used to check whether a certificate in the certification path has not been revoked or not. This profile distinguishes the ARL and CRL in order for the CA to customize their revocation policy. This design policy suggests that the IWG profile accepts the CA revocation information in the CRL, which primarily includes the EE revocation information. In addition, IWG profile accepts the separate/multiple CRL distribution policy based on the revocation reasons and serial number, for instance. This is up to the decision of the CA issuing policy. The application should handle the revocation policy of the CA.

6.4.1 Common ARL/CRL Profile

ARL/CRL Basic field

FIELD	NOTE
Version (Mandatory)	Since extension field appears in this profile, the value MUST be set to 1 (v2).
signature (Mandatory)	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
issure (Mandatory)	X.500 DN. Although DN is generally encoded by UTF8STRING, according to description of the

	X.520(2001), Country attribute is encoded by PrintableString.
thisUpdate (Mandatory)	UTCTIME
nextUpdate (Mandatory)	UTCTIME
revokedCertificates (Mandatory)	

ARL/CRL EntryExtensions

FIELD	NOTE
ReasonCode (Mandatory, non-critical)	
holdInstructionCode (not used)	
invaliditydDate (optional, non-critical)	GeneralizedTime
CertificateIssuer (not used)	

ARL/CRL Extensions

FIELD	NOTE
authorityKeyIdentifier (Mandatory, non-critical)	**keyId(Mandatory):** The hash value of Issuer's pubic key (SHA1 160bit). The 1st calculation method in RFC3280 ch.4.2.1.2 **authorityCertIssuer(optional):** DN **authCertSerialNum(optional):** INTEGER When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa.
issureAltName (not-used)	
cRLNumber (Mandatory, non-critical)	unique integer. up to 20 octets.
deltaCRLIndicator (optional, critical)	If the PKI domain wants to use dCRL, this field will be used.
issuingDistributionPoint	Please see 6.5.4 about a value.
freshestCRL (optional, non-critical)	If the PKI domain wants to use dCRL, this field will be used.
crlScope (not-used)	

6.5 Interoperability consideration (Certificate & CRL)

6.5.1 Encoding rules of DirectoryName

Although DN is generally encoded by UTF8STRING, according to description of the X.520(2001), Country attribute is encoded by PrintableString.

6.5.2 basicConstraints in EE certificate

According to the description of X.690(97), “The encoding of a set value or sequence value shall not include an encoding for any component value which is equal to its default value.”. Therefore, basicConstraint MUST NOT appear in the EE certificate.

6.5.3 The escape method to describe the LDAPURI in case that "comma character" is included in RDN value (e.g. value of cRLDP.distname.fullname etc.)

Since "comma character (,)" is used as a delimiter character of RDN in DN, cautions are needed when the comma character is included in RDN value. (Of course, there are characters that must take care about as well.)

In order to change the DN into the URI, it is necessary to make the DN “string representation” first using the method described by RFC2253. Since "comma character" is used as a delimiter character at this time, it is necessary to be escaped. Four kinds of methods exist. For example, assume “country name=AA, organization name=ABC Co., Ltd.”, it is as follows.

1. o=ABC Co.¥2C Ltd.,c=AA
2. o=ABC Co.¥2c Ltd.,c=AA
3. o=ABC Co.¥, Ltd.,c=AA
4. o=”ABC Co., Ltd.”,c=AA

And it is as follows when above four are URI.

1'. ldap://example.tld/o=ABC%20Co.%5C2C%20Ltd.,c=AA
2'. ldap://example.tld/o=ABC%20Co.%5C2c%20Ltd.,c=AA
3'. ldap://example.tld/o=ABC%20Co.%5C,%20Ltd.,c=AA
4'. ldap://example.tld/o=%22ABC%20Co.,%20Ltd%22,c=AA

The special character including "comma character" can be used by being escaped escaping as mentioned above. If you use it, you should test carefully in advance.

6.5.4 Value of cRLDistributionPoints and issuingDistributionPoints

Four kinds of publication policies of CRL are considered.

CA publishes only one (FULL) CRL (no ARL)

iDP -- Optional (critical/non-critical)
- distPoint -- Optional
  - fullName -- Optional
- nameRelativeToCRLIssuer -- not defined
- onlyContainsUserCerts -- forbidden to use
- onlyContainsCACerts -- forbidden to use
- onlySomeReasons -- forbidden to use
- indirectCRL -- not defined

CA publishes separate CRLs (no ARL)

iDP -- Mandatory (critical)
- distPoint -- Mandatory
  - fullName -- Mandatory
  - nameRelativeToCRLIssuer -- not defined
- onlyContainsUserCerts -- forbidden to use
- onlyContainsCACerts -- forbidden to use
- onlySomeReasons -- forbidden to use
- indirectCRL -- not defined

CA publishes one CRL and one ARL

iDP -- Mandatory (critical)
- distPoint -- Optional
  - fullName -- Optional
  - nameRelativeToCRLIssuer -- not defined
- onlyContainsUserCerts -- Mandatory in CRL
- onlyContainsCACerts -- Mandatory in ARL
- onlySomeReasons -- forbidden to use
- indirectCRL -- not defined

CA publishes separate CRLs and ARL

iDP -- Mandatory (critical)
- distPoint -- Mandatory

fullName -- Mandatory

nameRelativeToCRLIssuer -- not defined

onlyContainsUserCerts -- Mandatory in CRL

onlyContainsCACerts -- Mandatory in ARL

onlySomeReasons -- forbidden to use

indirectCRL -- not defined

APPENDIX OCSP responder

Certificate Basic field

the same as ROOT CA Certificate

Certificate Extension field

extKeyUsage (Optional, non-critical)	OCSPSigning
To-be-defined [TBD]	TBD

6.6 Repository Profile

To store the certificate and crl/arl information in repository, IWG profile employs the LDAP directory. IWG profile will use LDAP v3, primarily to use the referral function to fetch the certificates and crls/arls in multiple PKI domains enviroment. To simplify the directory operations, no replication and integrated-directory environments are considered. The profile suggests that the referral is a focal function in order to access to the information in other domains.

6.6.1 DIT

DIT structure in each country is not specified. This specification only mandates that the DN in a certificate should be corresponding to the structure of the DN in DIT.
A sample DIT is following.

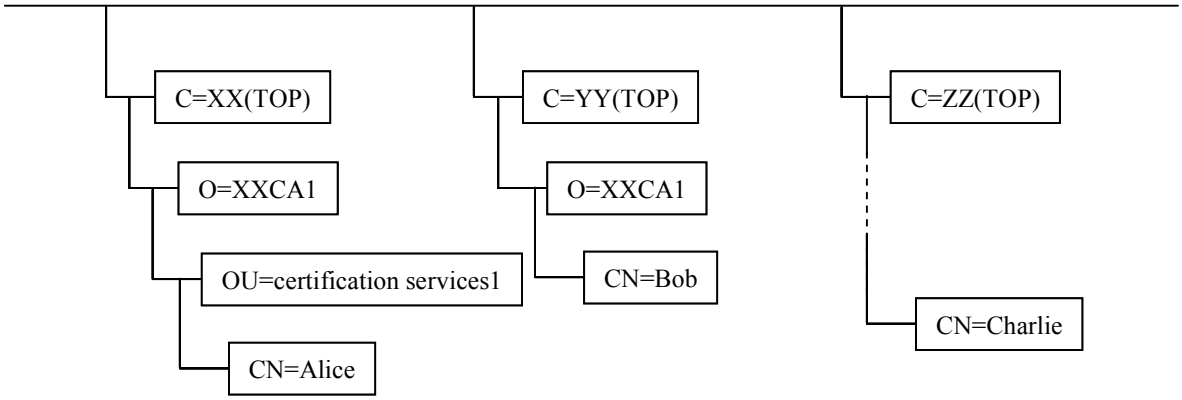

Fig. 5 sample DIT Tree (3 parties) in one directory

In Fig. 5, the “c=XX” entry, appropriate subordinate entry, and the referral should be defined. Note: in real usage, c=XX will not likely be used for the actual referral entry, since there is no such a representative directory server. The O or OU entry is the most likely.

6.6.2 Schema (objectclass, attribute)

No base objectclasses are described currently. Objectclass and attribute of each entry MUST be compliant with X.520, X.521, X.509, RFC2256, RFC2587, RFC2798, and other standard documents.

(1) CA

Objectclass and attribute

For the CA, the following object classes MUST be used.

- pkiCA (2.5.6.21) or certificationAuthority (2.5.6.16)

```
pkiCA     OBJECT-CLASS     ::= {
    SUBCLASS OF     {top}
    KIND                auxiliary
    MAY CONTAIN     {cACertificate |
                        certificateRevocationList |
                        authorityRevocationList |
                        crossCertificatePair }
    ID      joint-iso-ccitt(2) ds(5) objectClass(6) pkiCA(22)}

cACertificate       ATTRIBUTE   ::=   {
        WITH SYNTAX     Certificate
        EQUALITY MATCHING RULE      certificateExactMatch
        ID   joint-iso-ccitt(2) ds(5) attributeType(4) cACertificate(37) }

crossCertificatePairATTRIBUTE::={
    WITH SYNTAX     CertificatePair
    EQUALITY MATCHING RULE certificatePairExactMatch
 ID joint-iso-ccitt(2) ds(5) attributeType(4) crossCertificatePair(40)}

certificateRevocationListATTRIBUTE::={
                WITH SYNTAX   CertificateList
                EQUALITY MATCHING RULE certificateListExactMatch
            ID joint-iso-ccitt(2) ds(5) attributeType(4)
                certificateRevocationList(39)}

authorityRevocationListATTRIBUTE::={
                WITH SYNTAX     CertificateList
                EQUALITY MATCHING RULE certificateListExactMatch
            ID joint-iso-ccitt(2) ds(5) attributeType(4)
                authorityRevocationList(38)}
```

(2.5.6.16 NAME 'certificationAuthority' SUP top AUXILIARY
MUST (authorityRevocationList $ certificateRevocationList $
cACertificate) MAY crossCertificatePair)

(2) End Entity

No base objectclass is described currently.

Objectclass and attribute

For the EE, the following object classes MUST be used.

- pkiUser (2.5.6.21) or inetOrgPerson (2.16.840.1.113730.3.2.2)

pkiUser OBJECT-CLASS ::= {
SUBCLASS OF {top}
KIND auxiliary
MAY CONTAIN {userCertificate}
ID id-oc-pkiUser }

userCertificate ATTRIBUTE ::= {
WITH SYNTAX
Certificate
EQUALITY MATCHING RULE
certificateExactMatch
ID id-at-userCertificate}

(2.16.840.1.113730.3.2.2
NAME 'inetOrgPerson'
SUP organizationalPerson
STRUCTURAL
MAY (
audio $ businessCategory $ carLicense $ departmentNumber $
displayName $ employeeNumber $ employeeType $ givenName $
homePhone $ homePostalAddress $ initials $ jpegPhoto $
labeledURI $ mail $ manager $ mobile $ o $ pager $
photo $ roomNumber $ secretary $ uid $ userCertificate $
x500uniqueIdentifier $ preferredLanguage $
userSMIMECertificate $ userPKCS12
)

)

(3) CRLDP

Objectclass and attribute

For the CRLDP, the following object class MUST be used.

- cRLDistributionPoint (2.5.6.19)

```
cRLDistributionPoint        OBJECT-CLASS        ::= {
        SUBCLASS OF             { top }
        KIND                        structural
        MUST CONTAIN            { commonName }
        MAY CONTAIN             {  certificateRevocationList
| authorityRevocationList |      deltaRevocationList }
        ID
    id-oc-cRLDistributionPoint }
```

(4) Referral

Objectclass and attribute

For the Referral, the following object class MUST be used.

- Referral (2.16.840.1.113730.3.2.6)

```
( 2.16.840.1.113730.3.2.6
    NAME 'referral'
    DESC 'named subordinate reference object'
    STRUCTURAL
    MUST ref )

( 2.16.840.1.113730.3.1.34
    NAME 'ref'
    DESC 'named reference - a labeledURI'
    EQUALITY caseExactMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15
    USAGE distributedOperation )
```