# Asia PKI Interoperability Guideline

# (Version 1.0)

## March, 2004

**Asia PKI Forum**
**Interoperability Working Group**

## Preface

This document is the recommended design for the interoperable PKI framework in Asian countries and areas, which is the result of extensive researches and works by the members of Interoperability Working Group (IWG) in Asia PKI Forum.

We thank to the following contributed authors.

China PKI Forum ---------- Jiajun Ning (Mr.)
Chinese Taipei PKI Forum -------- Eho-Cheng Lo, Frank (Mr.)
Hong Kong, China PKI Forum --- Vinci Wong (Mr.)
Japan PKI Forum ---------- Hisanori Mishima (Mr.), Main Author, Editor
Korea PKI Forum ---------- Jeun, In Kyoung (Ms.)
PKI Forum Singapore ---------- Evelyn Ong (Ms.)
Macau Post ---------- Sun Kuan Ieong, Gregory (Mr.)


### Acknowledgement

Almost all parts of "Part II Technical part" owe to the results of JKST PKI INTEROPERABILITY PROOF EXPERIMENT conducted by JKST IWG team (Japan PKI Forum, Korea PKI Forum, PKI Forum Singapore and Chinese Taipei PKI Forum).


March, 2004

# Contents


**PREFACE** ..... **2**

**PART I INTRODUCTION** ..... **5**

**1. OVERVIEW** ..... **5**
**2. GLOSSARY** ..... **6**
**3. PURPOSE** ..... **8**
**4. OBJECTIVES** ..... **9**
**5. ORGANIZATION OF THE DOCUMENT** ..... **10**
**6. SCOPE** ..... **11**
**7. REGULATION** ..... **12**

**PART II TECHNICAL PART** ..... **13**

**1. TRUST MODEL** ..... **13**
*1.1 Cross Certification (CC)* ..... *13*
*1.2 Cross Recognition (CR)* ..... *14*
**2. PKI COMPONENT INTERFACES** ..... **15**
*2.1 PKI Components* ..... *15*
**3. CERTIFICATE AND CRL PROFILE** ..... **17**
*3.1 Policy of Designing Certificate/CRL Profiles* ..... *17*
*3.2 CA Certificate Profile* ..... *17*
*3.2.1 ROOT CA Certificate Profile* ..... *17*
*3.2.2 CC Certificate* ..... *19*
*3.2.3 SubCA Certificate (for the future reference)* ..... *20*
*3.3 EE Certificate Profile* ..... *21*
*3.3.1 Common EE Profile* ..... *21*
*3.3.2 Identification Certificate (digital signature)* ..... *22*
*3.3.3 Secure E-Mail Certificate (data Encipherment and digital signature)* ..... *23*
*3.4 ARL/CRL Profile* ..... *23*
*3.4.1 ARL/CRL Basic field* ..... *23*
*3.4.2 ARL/CRL EntryExtensions* ..... *23*
*3.4.3 ARL/CRL Extensions* ..... *23*
*3.4.4 Value of cRLDistributionPoints and issuingDistributionPoints* ..... *24*
*3.5 Interoperability consideration (Certificate & CRL)* ..... *25*
*3.5.1 Encoding rules of DirectoryName* ..... *25*
*3.5.2 basicConstraints in EE certificate* ..... *25*
*3.5.3 Escape method in the LDAPURL* ..... *26*
*3.6 APPENDIX OCSP responder* ..... *26*
**4. REPOSITORY** ..... **27**
*4.1 Repository Profile* ..... *27*
*4.2 DIT* ..... *27*
*4.3 Schema (objectclass, attribute)* ..... *27*
**5. CERTIFICATE VALIDATION (FUTURE WORK)** ..... **30**
**6. ADDITIONAL AREAS FOR THE PKI INTEROPERABILITY (FUTURE PLAN)** ..... **31**

**PART III POLICY PART** ..... **32**

**APPENDIX 1 PATH PROCESSING GUIDELINE FOR IMPLEMENTATION AND TESTING (FUTURE WORK)** ..... **33**

**APPENDIX 2 ACTUAL CERTIFICATE AND CRL PROFILES BEING USED IN ASIA** ..... **34**

**APPENDIX 3 JKS/T, JT/KS, JH PKI INTEROPERABILITY PROOF EXPERIMENT .....40**

**APPENDIX 4 CHINA, CHINESE TAIPEI, HONG KONG, CHINA AND MACAO CHINA PKI INTEROPERABILITY PROOF EXPERIMENT .....41**

# Part I Introduction

## 1. Overview

PKI (Public Key Infrastructure) is an important enabling technology for secure online transactions, especially for cross border trade. PKI promotes secure transactions in terms of confidentiality and integrity protection, and provide a trust infrastructure to enable non-repudiation of transactions and messages in the Internet environment where business is conducted between business entities and individuals.

The recent PKI initiatives in various countries in Asia, such as the establishment of certification framework, legislation of digital signature, and development of national PKI projects with different solutions and products, shape the national PKI structures at the domestic levels, and could potentially bring about economic impact across the region in varying degrees.

In terms of the promotion of global PKI framework, however, there is a need to ensure that parties in different PKI domains can interoperate. In this regard, it is necessary for cross border working initiatives to be formed to ensure that the different PKI structures and practices are examined and deliberated to develop a mutually agreed inter-working PKI framework at the regional and subsequently, international levels. Interoperability Working Group (IWG) of Asia PKI Forum (APKI-F) was conceived in March 2002 as a step towards achieving PKI interoperability in Asia.

APKI-F, IWG started the discussion of how to design an interoperable PKI specification. We learned from various experiences in IWG member's countries and areas, and also learned from the experiences of the proof experiment for PKI interoperability. Especially two results of preceded experiments of PKI interoperability which are conducted by, Japan-Korea-Singapore-Chinese Taipei-Hong Kong, China and China-Chinese Taipei-Hong Kong, China.

## 2. Glossary

| | |
|---|---|
| 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 |

## 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. Purpose

The very purpose of this guideline is viewed in both functional and business aspects. From functional view, “PKI Interoperability” means the ability of separate PKI-enabled systems or services to be linked together and then work as well as operate as if they were a single entity. For electronic commerce, “PKI Interoperability” could be treated as “to be able to do secure and trusted business” without ad hoc and proprietary integrations. To maintain the neutrality and to ensure the usability, this guideline is only intended to provide a referential roadmap for interested parties to achieve PKI interoperability within different scenarios and scales from Asian perspective.

In view of this, the document is to deliver the recommended PKI-related specifications for the construction of interoperable PKI in Asia.

Specifically, the trust of PKI is valid within a "PKI domain" which is consisted of a CA (which issues certificates) and EEs (which trust and use the certificates). It means that the trust is not valid outside of this PKI domain.

On the contrary, there are many CAs in Asia, which have already started their operations. In case of conducting a cross-border electronic commerce, these CAs have to be operating interoperably, and the certificates issued by those CAs have to be trusted each other.

In order to achieve this interoperable situation, both CAs have to agreed to accept common specification, harmonize their certificate profiles each other.

This document provides a recommended profile for this interoperability.

## 4. Objectives

Thinking of PKI interoperability as a set of levels, such as policy, legal framework, technology and application, makes itself a challenging but achievable endeavor and ambition. To realize the above purpose, the information contained in this guideline is to facilitate interested CAs to attain the objectives of mutually/multilaterally negotiating an understanding and of reaching the agreement on PKI trust model, component interfaces, certificate/CRL profiles, repository, certificate validation and policy mapping.

## 5. Organization of the Document

This document is organized into three parts.
Part I provides an introduction of this document (for example, overview, purposes, scope, regulation, glossary).
Part II is a main part of this document. This part provides detail of technical specifications.
Part III provides policy aspect of PKI : for example, a policy mapping issue between different CAs which are operated based on different PKI policies (CP and CPS).

(but it does not appear at first version).

Part II technical part is consisted of;

1. Trust Model : architectures of CA to CA connections : how one CA trusts the other CA.
2. PKI component interfaces : interfaces for PKI components ; CA to CA, CA to EE, repository to EE and VA, EE to VA, EE to EE.
3. Certificate and CRL Profile : the detail specification for Certificates and CRL based on RFC3280 and X.509.
4. Repository : Repository profiles, DIT, schema.
5. Certificate Validation : validation methods for certificate such that EE based model, VA based model and OCSP.
6. Additional areas for the PKI interoperability : other technical topics for PKI interoperability will be provided in this section. The noticing topics are following;

CA key update / Handling encryption Certificate / Necessity of issuing a certificate on a Repository / Attributes of a subordinate CA certificate in stored entry / URL description of access methods / Referral implementation / Application interoperability related issues / Common API of PKCS#11 profile. Of course, there may be more additional topics.

## 6. Scope

This document presents trust models, interfaces for PKI components, profiles for Certificates and CRLs, Repositories and Cerfificate Validation methods.

1. Interoperability of CA in different PKI domains;
2. Establishment of a trust model to enable interoperability;
3. Documentation of participating CA' s certificate profile, and interfaces to key infrastructure components (such as CA, LDAP, VA, and RA facilities);
4. Certificate profile.

Policy issues (mapping policy for different PKI demains) are provided in the future work.

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.

## 7. Regulation

This document is opened to all members of Asia PKI forum, and allowed to use freely.

This document is a recommendation, not an obligation (That is why we named this document as a "Guideline", not a "Standard"). The specification described in this document is examined and verified with proof experiments. Therefore in case of constructing a cross-border PKI interoperability system, this guideline is highly recommended to adopt.

# Part II Technical Part

## 1. Trust 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.

### 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.

## 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.

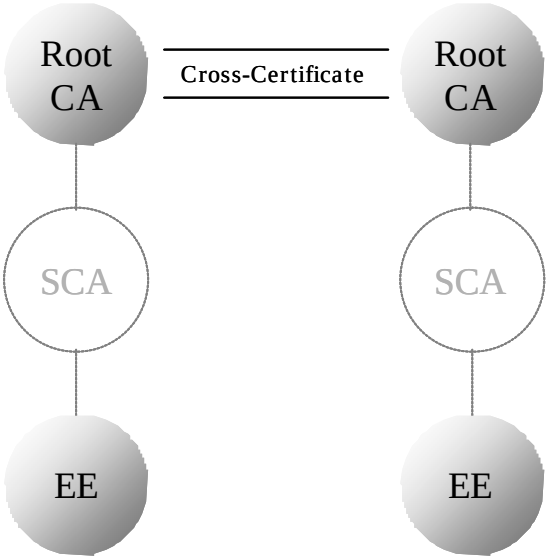
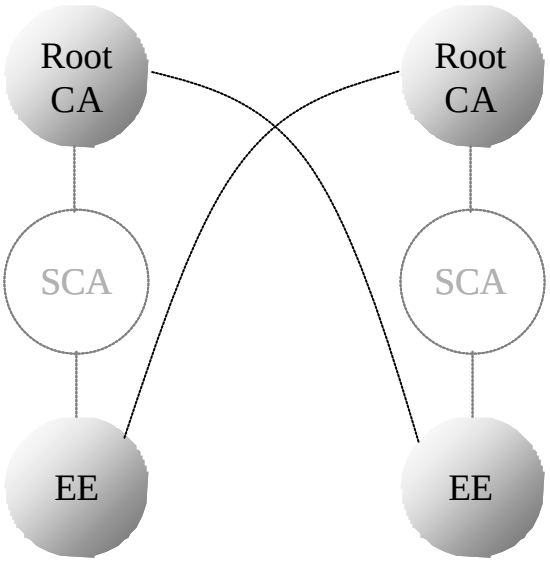



Fig. 2 Cross Certificate




Cross Recognition

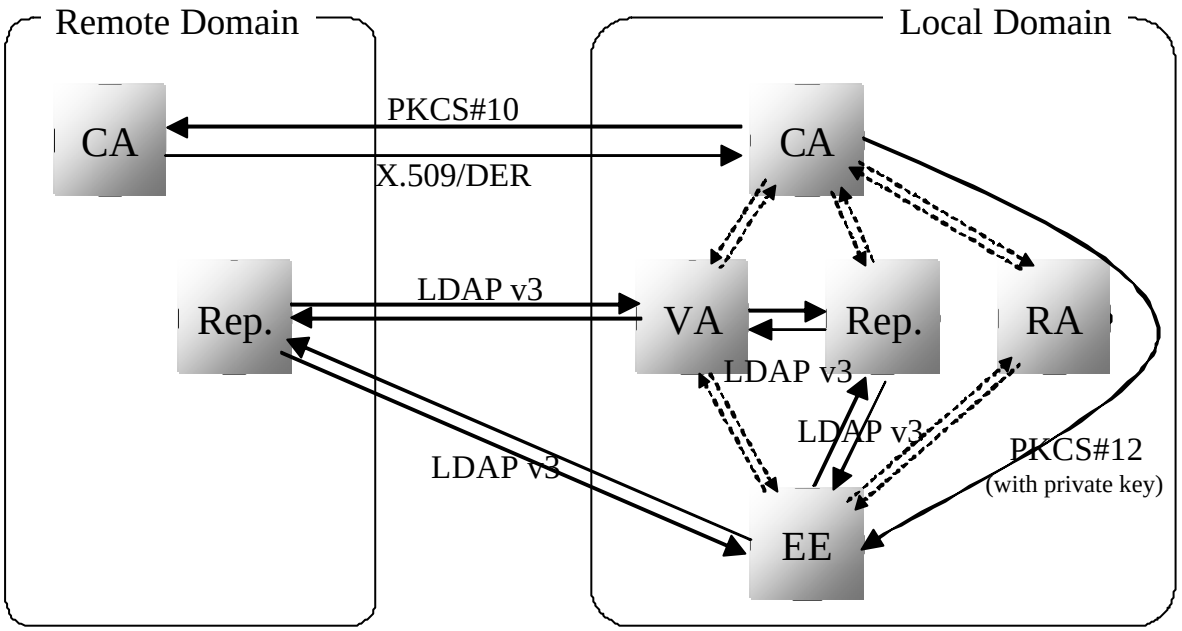
[1] ACHIEVING PKI INTEROPERABILITY (http://www.apectelwg.org/apecdata/telwg/eaTG/eatf06.doc)

[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.

## 2. PKI component interfaces

### 2.1 PKI Components

The following figure shows the PKI components in the APKI-F, 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 scope




of this guideline, and the broken line is out of scope.

Fig. 3 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

## 3. Certificate and CRL 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. APKI-F, 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.

### 3.1 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 APKI-F,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.

### 3.2 CA Certificate Profile

There are 4 types of the CA certificates, Root CA certificate, Self-issued, Subordinate CA certificate, and Cross certificate. For the simplification of the certificate hierarchy, the subordinate CA was excluded in this document. 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.

#### 3.2.1 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.

(1) Certificate Basic field

| FIELD | NOTE |
|---|---|

| | |
|---|---|
| version<br>(Mandatory) | Since extension field appears in this profile, the value MUST be set to 2 (v3). |
| serialNumber<br>(Mandatory) | unique integer. Up to 20 octets. |
| Signature (Mandatory) | 1.2.840.113549.1.1.5<br>(sha1WithRSAEncryption) |
| issuer<br>(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<br>(Mandatory) | UTC TIME |
| subject<br>(Mandatory) | X.500 DN. And see issuer. |
| subjectPublicKeyInfo<br>(Mandatory) | 1.2.840.113549.1.1.1 (rsaEncryption)<br>CA: 2,048bit |
| issuerUniqueID<br>(not used) | |
| subjectUniqueID<br>(not used) | |

(2) Certificate Extension field

| FIELD | NOTE |
|---|---|
| authorityKeyIdentifier<br>(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.<br>**authorityCertIssuer(optional):** DN<br>**authCertSerialNum(optional):** INTEGER<br>When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa. |
| subjectKeyIdentifier<br>(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<br>(optional, critical) | When used, keyCertSign and cRLSign should be included at least. |
| extKeyUsage (not used) | |
| privateKeyUsagePeriod<br>(not used) | |
| certificatePolicies<br>(optional, critical) | When used, policyID MUST be present. |
| policyMappings (not used) | |
| subjectAltName<br>(optional, non-critical) | If the PKI domain wants to include email address or etc in the certificate, this field will be used. |
| issuerAltName<br>(optional, non-critical) | If the PKI domain wants to include email address or etc in the certificate, this field will be used. |
| subjectDirectryAttributes<br>(not used) | |
| basicConstraints | cA=TRUE |

| | |
|---|---|
| (Mandatory, critical) | pathLen=optional (INTEGER) |
| nameConstraints<br>(not used) | |
| policyConstraints<br>(not used) | |
| cRLDistributionPoints<br>(optional, non-critical) | directoryName, URI |
| authorityInfoAccess<br>(optional, non-critical) | If the PKI domain uses OCSP, this field will be used. |
| inhibitAnyPolicy (not used) | |
| freshestCRL (not used) | |
| subjectInfoAccessSyntax<br>(not used) | |

### 3.2.2 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. The profile of this guideline currently requires only the basic constraint as a mandatory field in CA certificates.

(1) Certificate Basic field

Same as ROOT CA Certificate

(2) 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<br>(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<br>**authorityCertIssuer(optional):** DN<br>**authCertSerialNum(optional):** INTEGER<br>When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa. |
| subjectKeyIdentifier<br>(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<br>(not used) | |

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

### 3.2.3 SubCA Certificate (for the future reference)

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

(1) Certificate Basic field

Same as ROOT CA Certificate

(2) 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<br>(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<br>**authorityCertIssuer(optional):** DN<br>**authCertSerialNum(optional):** INTEGER<br>When AuthCertIssuer is used, AuthCertSerialNum |

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

| | |
|---|---|
| | 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 [4]) | 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. |
| issuerAltName (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<br>pathLen=optional (INTEGER) |
| nameConstraints (optional, critical) | |
| policyConstraints (not used) | |
| cRLDistributionPoints (Mandatory, non-critical) | “distPoint.fullname” must contain URI<br>ldap://hostname[:portnumber]/dn?attr[;binary]<br>(port number, attribute: Mandatory<br>binary option: optional) |
| authorityInfoAccess (not used) | If the PKI domain uses OCSP, this field will be used. |
| inhibitAnyPolicy (not used) | |
| freshestCRL (not used) | |
| subjectInfoAccessSyntax (not used) | |

### 3.3 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 "3.3.1". The following sections, “3.3.2” and “3.3.3” specify the differences from “3.3.1” for individual applications.

#### 3.3.1 Common EE Profile

(1) Certificate Basic field

the same as ROOT CA Certificate

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

(2) 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<br>**authorityCertIssuer(optional):** DN<br>**authCertSerialNum(optional):** INTEGER<br>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 3.3.20 and 3.3.3 about a value. |
| extKeyUsage (not used) | |
| privateKeyUsagePeriod (not used) | |
| certificatePolicies (Mandatory, ether critical or non-critical [5]) | 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 3.3.3. |
| issuerAltName (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<br>ldap://hostname[:portnumber]/dn?attr[;binary]<br>(port number, attribute: Mandatory<br>binary option: optional) |
| authorityInfoAccess (not used) | If the PKI domain uses OCSP, this fieldwill be used. |
| inhibitAnyPolicy (not used) | |
| freshestCRL (not used) | |
| subjectInfoAccessSyntax (not used) | |

### 3.3.2 Identification Certificate (digital signature)

(1) Certificate Extension field

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

| | |
|---|---|
| keyUsage (Mandatory, critical) | digitalSignature (, nonRepudiation) |

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

(1) Certificate Extension field

| | |
|---|---|
| keyUsage (Mandatory, critical) | keyEncipherment, dataEncipherment |
| subjectAltName<br>(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. |

## 3.4 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, the profile of this guideline 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.

### 3.4.1 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) |
| 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. |
| thisUpdate (Mandatory) | UTCTIME |
| nextUpdate (Mandatory) | UTCTIME |
| revokedCertificates (Mandatory) | |

### 3.4.2 ARL/CRL EntryExtensions

| FIELD | NOTE |
|---|---|
| ReasonCode<br>(Mandatory, non-critical) | |
| holdInstructionCode<br>(not used) | |
| invalidityDate<br>(optional, non-critical) | GeneralizedTime |
| CertificateIssuer (not used) | |

### 3.4.3 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<br>**authorityCertIssuer(optional):** DN<br>**authCertSerialNum(optional):** INTEGER<br>When AuthCertIssuer is used, AuthCertSerialNum must be set as well. Vise versa. |
| issuerAltName (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 3.4.4 about a value. |
| freshestCRL (optional, non-critical) | If the PKI domain wants to use dCRL, this field will be used. |
| crlScope (not-used) | |

### 3.4.4 Value of cRLDistributionPoints and issuingDistributionPoints

The value of issuingDistributionPoints changes according to the CRL publication policy. This profile allows CA to have the partitioned CRL distribution policy. There are four types of publication policies of CRL that considered.

(1) CA publishes one full CRL
(2) CA publishes partitioned CRLs only
(3) CA publishes one complete CRL and one complete ARL
(4) CA publishes partitioned CRLs, and one complete ARL or partitioned ARLs

This profile defines the following three terms to avoid the confusion on the CRL distribution terms.

1. Full CRL is a CRL that lists all revoked certificate including the all EE and CA certificates
2. Complete CRL(ARL) is a CRL that lists all revoked certificates within two given scopes. One is the set of the certificates covered by the CRL that contains all the EE certificates only. The other is the set of the certificates covered by the CRL that contains all the CA certificates only.
3. Partitioned CRL is a partition of a full CRL or complete CRL(ARL), partition with some kinds of the criteria such as the range of the certificate serial number or some other ad hoc range. These criteria depend on the CA policy. The CA makes sure that the union of the full set of the partitioned CRL should be equivalent to a full CRL. This profile assumes that the partitioned CRL must be published at the locations of the cRLDistributionPoint.DistributionPoint.fullName and issuingDistributionPoint.distributionPoint.fullname fields.

The values of issuingDistributionPoints are as follows.

(1) 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

(2) 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

(3) 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

(4) 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

### 3.5 Interoperability consideration (Certificate & CRL)

#### 3.5.1 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.

#### 3.5.2 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.

### 3.5.3 Escape method in the LDAPURL

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.

## 3.6 APPENDIX OCSP responder

(1) Certificate Basic field

Same as ROOT CA Certificate

(2) Certificate Extension field

| | |
|---|---|
| extKeyUsage<br>(Optional, non-critical) | OCSPSigning |
| To-be-defined [TBD] | TBD |

## 4. Repository

### 4.1 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.

### 4.2 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.

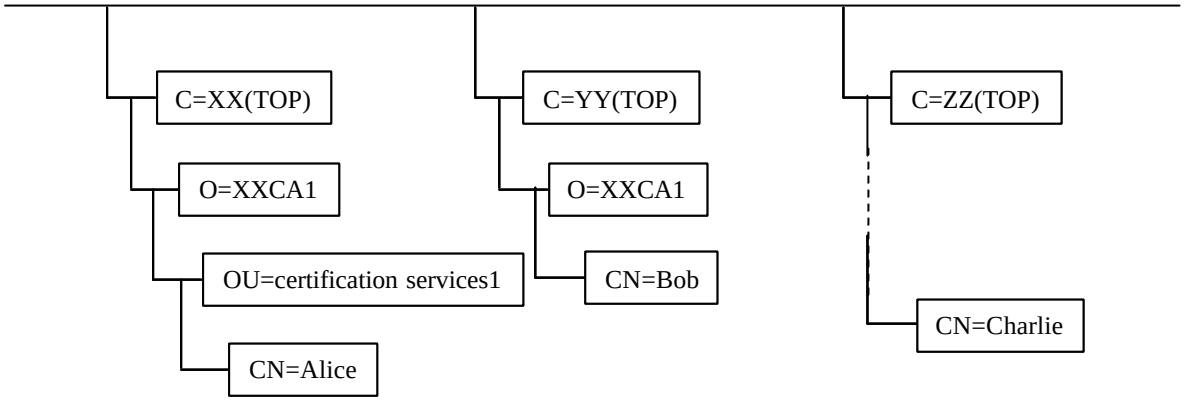



Fig. 2 sample DIT Tree (3 parties) in one directory

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.

### 4.3 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 (2.5.6.22) 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 )
```

## 5. Certificate Validation (future work)

***This part will be replaced for the "Path Processing Guideline" in the future.***

## 6. Additional areas for the PKI interoperability (future plan)

Topics for discussion (candidates)

- Qualified Certificate based on RFC3039
- CA key update
- Handling encryption Certificate
- Necessity of issuing a certificate on a Repository
- Attributes of a subordinate CA certificate in stored entry
- URL description of access methods
- Referral implementation
- Application interoperability related issues
- Common API of PKCS#11 profile

Asia PKI Forum will consider Qualified Certificate Profile as an additional research area for the PKI interoperability in Asia. Qualified Certificate Profile is defined in Directive 1999/93/EC of the European Parliament on a community framework for electronic signatures and RFC 3039. Due to the importance of the EUQC certificate profile, member countries might start to consider how EUQC certificate profile can benefit local PKI development, as well as PKI interoperability between Asia and Europe.

## Part III Policy Part (future plan)

In this section we discuss a policy mapping issue between different CAs which are operated based on different PKI policies (CP and CPS). At first we have to identify what is the problem, and then we have to decide the discussion items.

# Appendix 1 Path Processing Guideline for Implementation and Testing (future work)

## Appendix 2 Actual Certificate and CRL profiles being used in Asia
**(update March 31, 2004)**

There are many licensed and accredited CA in Asia. The followings are the list of CAs and their Web site. As for the Certificate and CRL profiles, please refer to their CP/CPS.

1. China
2. Chinese Taipei
3. Hong Kong, China
4. India
5. Japan
6. Korea
7. Macao, China
8. Malaysia
9. Singapore
10. Thailand

### 1. China

According to "China Information Security Year book 2002-2003", China PKI Forum, there are 69 CAs in Mainland China.

1.1 Central ordinary cities (4 CA)

(1) BJCA (Beijing Certificate Authority)
http://www.bjca.org.cn
(2) SHECA (Shanghai Electronic Certificate Authority Center Co.,Ltd.)
http://www.sheca.com/php/index.php
(3) TJCA (Tianjin CA)
http://www.etcj.net/ca
(4) CQ CA (Chong Qing Certificate Authority Center)
http://www.cqca.net

1.2 Local government CA (23 prefectures, 5 municipalities, 2 liberties)

Jilin CA, SXCA(Shanxi), SDCA(Shandong), HNCA(Henan), Shanxi CA, AHCA (Anhui), FJCA (Fujian), SZCA(Shenzhen), HBCA (Hubei), NET CA(Guangdong Electronic Certificate Authority), etc.

1.3 Commercial CA

(1) CTCA (China Telecommunications Corporation)
http://www.chinatelecom.com.cn/
(2) CFCA (China Financial Certification Authority)
http://www.cfca.com.cn/
(3) iTruschina CO., Ltd.
http://www.itrus.com.cn/
(4) TrustAsia China Ltd

etc.

## 2. Chinese Taipei

2.1 Government CA

(1) GRCA (Government Root CA)
http://grca.nat.gov.tw
(2) MOICA (Ministry of Interior)
http://moica.nat.gov.tw/html/index.htm
(3) MOEACA (Ministry of Economic Affairs)
http://moeaca.nat.gov.tw/
(4) GCA (Government Certificate Authority)
http://www.pki.gov.tw/
(5) GTestCA
http://gtestca.nat.gov.tw/

2.2 Commercial CA

(1) TWCA (TaiCA)
http://www.taica.com.tw/
(2) ChungHwa Telecom
http://www.cht.com.tw/
(3) HiTRUST (Taiwan)
http://www.hitrust.com.tw/hitrustexe/frontend/default_tw.asp
(4) Chief Telecom
http://www.chiefca.com.tw/

2.3 Approved CPS List (March 15, 2004)

| | Name of Approved CPS | Approval date | CA (or CA Owner) | Website |
|---|---|---|---|---|
| 1 | SETCo. CA CPS | 2002.08.14 | TWCA.com | http://www.taica.com.tw |
| 2 | Government Root CA (GRCA) CPS | 2002.08.15 | RDEC | http://grca.nat.gov.tw |
| 3 | HiTrust VTNCPS | 2002.10.18 | HiTrust | http://www.hitrust.com.tw/ |
| 4 | Taiwan Financial CA (TFCA) CPS | 2002.10.30 | TWCA.com | http://www.taica.com.tw |
| 5 | Taiwan Financial Policy CA (TFPCA) CPS | 2002.10.31 | TWCA.com | http://www.taica.com.tw |
| 6 | Taiwan-CA.com Inc. CPS | 2002.11.04 | TWCA.com | http://www.taica.com.tw |
| 7 | Government CA (GCA)CPS | 2002.12.12 | RDEC | http://gca.nat.gov.tw/ |
| 8 | HiTrust(FinancialXML Certificate )CPS | 2002.12.19 | HiTrust | http://www.hitrust.com.tw/repository |
| 9 | Taiwan Financial User CA (TFUCA) CPS | 2003.01.13 | TWCA.com | http://www.taica.com.tw |
| 10 | Chunghwa Telecom PKI (ePKI) CPS | 2003.02.10 | Chunghwa Telecom | http://epki.com.tw |

| | | | | |
|---|---|---|---|---|
| 11 | MOEA CA CPS | 2003.03.18 | MOEA | http://moeaca.nat.gov.tw/ |
| 12 | Chief Global Certification Services CPS | 2003.03.21 | Chief Telecom | http://www.chiefca.com.tw/repository.php |
| 13 | Financial Information Service Co., Ltd CPS | 2003.03.28 | Financial Information Service Co., Ltd | http://www.taica.com.tw |
| 14 | Ministry of Interior CA CPS | 2003.04.03 | Ministry of Interior | http://moica.nat.gov.tw |
| 15 | Taiwan Commercial Root CA CPS | 2003.05.14 | HiTrust | https://www.hitrust.com.tw/repository/TCRCA |
| 16 | Healthcare CA CPS | 2003.06.06 | Department of Health | http://hca.doh.gov.tw |
| 17 | GCA CPS | 2003.07.22 | RDEC | http://www.pki.gov.tw |
| 18 | XCA CPS | 2004.02.04 | RDEC | http://xca.nat.gov.tw/ |
| 19 | Taiwan Bridge CA CPS | 2004.03.02 | MOEA | http://www.bca.org.tw |

**3. Hong Kong, China**

(1) eGov : Electronic Submission of Forms
http://www.info.gov.hk/digital21/eform/english/links.html
(The list of all CA which are available for eGov application.)
(2) HongKong Post
http://www.hongkongpost.com/
(3) Digi-Sign Certification Services Limited
http://www.info.gov.hk/digital21/eform/english/links.html
(4) HiTRUST.COM Inc., Ltd.
http://www.hitrust.com.hk/home/index.htm
(5) JETCO
http://www.jetco.com.hk/
=> Digi-Sign succeeded the role.

**4. India**

Licensed CAs in India

(1) TCS-CA (Tata Consultancy Services)
http://www.tcs-ca.tcs.co.in/index.jsp
(2) SafeScrypt Ltd.
http://www.safescrypt.com/
(3) IDRBT-CA (Institute for Development and Research in Banking Technology)
http://www.idrbt.ac.in/
(4) NIC-CA (National Informatics Centre)
http://home.nic.in/

**5. Japan**

5.1 Government PKI (1 BCA + 14 Ministry CAs)

(1) GPKI Bridge CA
http://www.gpki.go.jp/cpcps/index.html
(2) Cabinet Office
http://www.shinsei.cao.go.jp/ninshoukyoku.html
(3) NPA (National Police Agency)
http://www.shinsei.npa.go.jp/ca/ninshokyoku_top.html
(4) FSA (Financial Services Agency)
http://annai.fsa.go.jp/annai/contents/e7.html
(5) MPHPT (Ministry of Public Management, Home Affairs, Posts and Telecommunications)
http://www.soumu.go.jp/kyoutsuu/ninshoukyoku.html
(6) MOJ (Ministry of Justice Japan)
http://shinsei.moj.go.jp/certification/certification_top.html
(7) MOF (Ministry of Finance Japan)
http://www.shinsei.mof.go.jp/ninshoukyoku_detail.htm
(8) MECSST (Ministry of Education, Culture, Sports, Science and Technology)
https://shinsei-cert.mext.go.jp/guide/ninsyo/index.html
(9) MHLW (Ministry of Health, Labour and Welfare)
http://hanyous.mhlw.go.jp/shinsei/crn/html/CRNSecurity.html#ninshou
(10) MAFF (Ministry of Agriculture, Forestry and Fisheries of Japan)
http://www.maff.go.jp/denmado/ninsyo/ninsyogaiyou.html
(11) METI (Ministry of Economy, Trade and Industry)
http://www.meti.go.jp/application/ninsho/index.htm
(12) MLIT (Ministry of Land, Infrastructure and Transport)
http://www.goa.mlit.go.jp/mlitca/
(13) MOE (Ministry of the Environment)
http://www.env.go.jp/envca/ninshoukyoku_detail.html
(14) JDA (Japan Defense Agency)
(not open)
(15) MOFAJ (Ministry of Foreign Affairs of Japan)
(not open)

5.2 Accredited Private CA Services (11 CAs)

(1) JCSI
http://www.jcsinc.co.jp/
(2) Commercial Registration CA
http://www.moj.go.jp/ONLINE/CERTIFICATION/
(3) NDN (Nihon Denshi Ninsho Co., Ltd.)
http://www.ninsho.co.jp/index.html
(4) NTT medias Co., Ltd.
http://www.nttms.co.jp/
(5) TOiNX
http://www.toinx.co.jp/
(6) Cyber Wave Japan
http://www.cwj.jp/
(7) TEIKOKU DATABANK Ltd.
http://www.tdb.co.jp/
(8) SECOM Co., Ltd.
http://www.secomtrust.net/

(9) Japan Net
http://www.japannet.jp/
(10) All Japan Federation of Certified Social Insurance Labour Consultant Associations
http://www.shakaihokenroumushi.jp/
(11) The Japan Chamber of Commerce and Industry
http://www.jcci.or.jp/

**6. Korea**

(1) KISA (Korea Certification Authority Central)
http://www.rootca.or.kr/
The list of CPS, Cert, ASL/ARL;
http://www.rootca.or.kr/eng/cert_en/cert_list_en.html
(2) KICA (Korea Information Certificate Authority)
http://www.kica.or.kr/index.jsp
(3) KOSCOM (Korea Securities Computer Corp.)
http://www.koscom.co.kr/main/index.jsp
(4) KFTC (Korea Financial Telecommunications & Clearings institute)
http://www.kftc.or.kr/
(5) NCA (National Computerization Agency)
http://sign.nca.or.kr/
(6) KTNET
http://www.ktnet.co.kr/
(7) CrossCert
http://www.crosscert.com/

**7. Macao, China**

(1) eSignTrust (Macao Post Certification Services)
http://www.esigntrust.com/chi/html/pki.html

**8. Malaysia**

(1) Digicert Sdn. Bhd.
http://www.digicert.com.my/
(2) MSC Trustgate.com SDN BHD
http://www.msctrustgate.com/

**9. Singapore**

(1) Netrust
http://www.netrust.com.sg/
(2) TrustAsia
http://www.trustasia.com/

**10. Thailand**

(1) Thai Digital ID
http://www.thaidigitalid.com/indexeng.html

(2) Acerts

http://www.acerts.net/mainframe/mainframe.php?p_lang=eng

## Appendix 3 JKS/T, JT/KS, JH PKI Interoperability Proof Experiment

- Achieving PKI Interoperability 2003, Results of the JKST-IWG Interoperability project
- IWG Recommended Profiles
- CA-CA Interoperability Interface Specification for experiment
- Certificate Path Processing Implementation Guideline
- Certificate Path Processing Guideline
- Certificate Path Processing Guideline
- PKCS #11 Testing

# Appendix 4 China, Chinese Taipei, Hong Kong, China and Macao China PKI Interoperability Proof Experiment