Achieving PKI Interoperability

Results of the JKS-IWG Interoperability project

Japan PKI Forum

Korea PKI Forum

PKI Forum Singapore

30 April 2002

Acknowledgements

This report is a collective effort and achievement of the individuals and organizations that volunteered their valuable time and resources contributing to the improved understanding and interoperability of PKI in Asia.

We wish to thank the following organizations and people for their valuable contributions to this work.

Contributing Writers

- Japan
  - Dr Satoru TEZUKA, Japan PKI Forum (PKI-J)
  - Hisanori MISHIMA, PKI-J
  - Shigeru KAMEDA, PKI-J
  - Ako MISHIO, PKI-J
  - Hiroyuki KUBO, PKI-J
  - Kiyoshi WATANABE, PKI-J
  - Hironobu GOSHIMA, PKI-J
  - Masaki SHIMAOKA, PKI-J
  - Satoshi TAKEMOTO, PKI-J
  - Shun NAGAKURA, PKI-J
- Korea
  - Jaeil LEE, Korea Information Security Agency(KISA)
  - Seok-Lae LEE, KISA
  - Bosung HWANG, KISA
  - Inkyoung JEON, KISA
  - Moonbo SHIM, KISA
  - Taewon PARK, KISA
  - Woncheol LEE, KISA
- Singapore
  - Meng Chow KANG
  - PKI Forum Singapore

Review Teams

- IWG Technical WG

1. Introduction

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. The Japan, Korea, Singapore Interoperability Working Group (JKS-IWG) of the ASIA PKI Forum (APKI-F) was conceived in June 2001 as a step towards achieving PKI interoperability in Asia.

JKS-IWG conducted an Interoperability Project to explore how the nationally certified Certification Authorities can be interoperable with each other. The goal of this project was to develop a test-bed framework and conduct the experiment, demonstrating an interoperable PKI framework.

This document presents the project overview, the experiment models, and the results of the JKS IWG Interoperability Experimental Project. It also includes recommendations on the way forward to achieve PKI interoperability in Asia and a “Recommended Technical Profile” for digital certificates.

2. Objective and Scope

2.1 Objective

The objective of this interoperability experiment, undertaken by members of the JKS-IWG, was to achieve PKI interoperability in Asia with recommended PKI specifications capable of supporting each participating country's operating conditions. This work is also aimed at providing a reference for future participants in the APKIF on the PKI implementation status in Asia.

2.2 Scope

Phase 1 of the JKS-IWG project focused on the following:

1. Interoperability of CA in the three countries proposed by respective representing IWG members;
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.

The JKS-IWG attempted to use a common business application for the interoperability test, but this was found to be infeasible due to the time and resource constraints involved in the project. Different applications were therefore used by each IWG member for the experiment.

3. JKS-IWG Structure and Organization

3.1 IWG Structure

The JKS-IWG organization structure is depicted in the figure below. It is managed through a central Management Committee, supported by the Japan, Korea and Singapore Interoperability Project Teams.

3.2 Participants

The cooperation between products and services vendors, CAs, and the PKI forums was necessary to conduct the project. The JKS-IWG group aimed to have certified-or–accredited-CA in each country involved, however the Japan CA was in the process of accreditation by the government when the project began. The project participants were:

Korea	Singapore	Japan
• Korea Information Security Agency • Korea Information Certificate Authority, Inc • Korea PKI Forum	PKI Forum Singapore	Japan PKI Forum

4. Project Overview and Experiment model

The experiment was conducted from the June 2001 to March 2002 with technical testing conducted from October 2001 to February 2002.

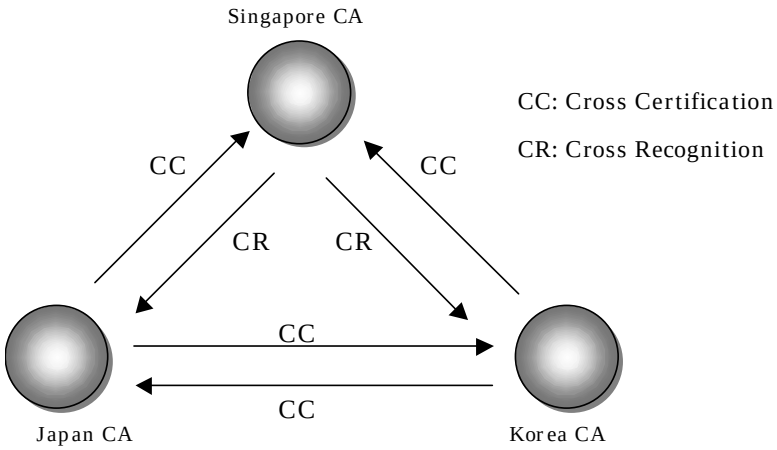
4.1 Project Overview

The project was conducted as follows:

1. Investigate and analyze technical and operational issues in each participating country;
2. Design an experimental model for PKI interoperability, addressing technical details as necessary;
3. Discuss and agree on the application software for the interoperability test;
4. Establish simulation centers and conduct the interoperability testing;
5. Review the progress in regular periods and produce a final report to document the result and recommendations.

4.2 CA-CA Interoperability Model

The following model describes the CA-CA relationship in this project. This is a hybrid model between the Cross Certification (CC) Model and Cross Recognition (CR) Model. This model was selected due to current constraints in respective country to support a common model such as Cross Certification, or Cross Recognition. The interoperability experiment proved that the hybrid model combining both CC and CR is a practical model that can be used in any physical implementation.



4.2.1 The CA-CA model between Singapore CA and Korea CA

Between the Singapore CA and Korea CA, the cross certification model and the cross recognition model are combined. Korea's CA issues a certificate upon receiving a request for a PKCS#10 cross certificate from Singapore's CA. Singapore, without issuing a cross certificate, displays the certificate issued by Korea's CA, and an end

entity trusts the certificate.

4.2.2 The CA-CA model between Singapore CA and Japan CA

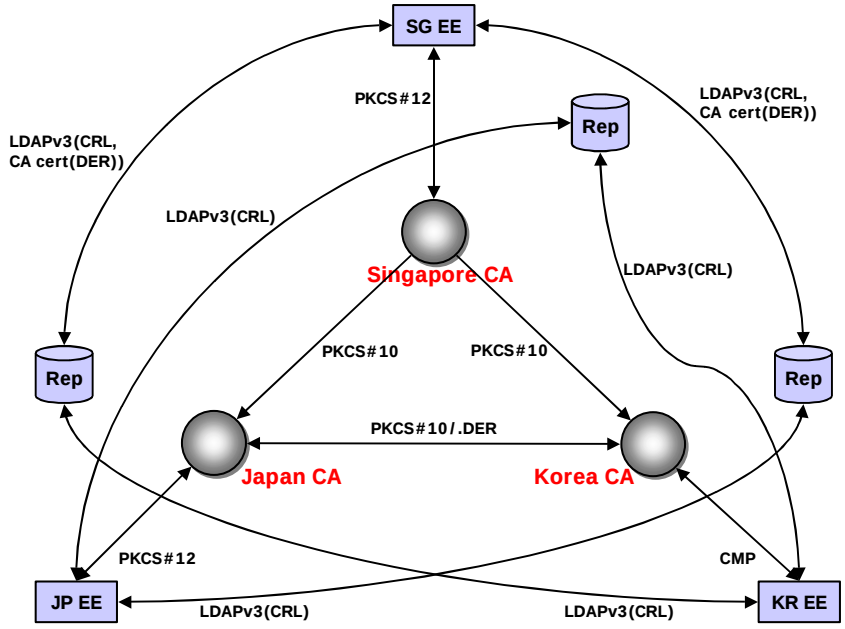
Between the Singapore CA and Japan CA, the same model of the Singapore and Korea CA are applied to the model between Singapore CA and Japan CA.

4.2.3 The CA-CA model between Korea CA and Japan CA

Between the Korea CA and Japan CA, the cross certification model are used. The one CA issues the PKCS#10 and cross certificate to the other CA.

4.3 Certificate Issuance and Directory Search Model

The following figure shows the data format and the flow of the certificate issuance and directory search.



4.3.1 CA-CA certificate issuance

Between the Singapore CA and Korea CA or Japan CA, the Singapore CA issues the PKCS#10 to the Korea and Japan CAs, and generate a cross certificate only for the reverse element of crossCertificatePair. Between Korea CA and Japan CA, the both CAs exchange the PKCS#10 data and then cross certificates each other.

4.3.2 CA-End Entity certificate issuance

In each PKI domain, Singapore and Japan decided to use the PKCS#12 data format for the end-entity certificate. Korea decided to use the CMP for the end-entity certificate.

4.3.3 Directory Search interface

For the directory interface, all repositories are to use LDAPv3 in order to maintain the interoperability.

4.4 Validation Models

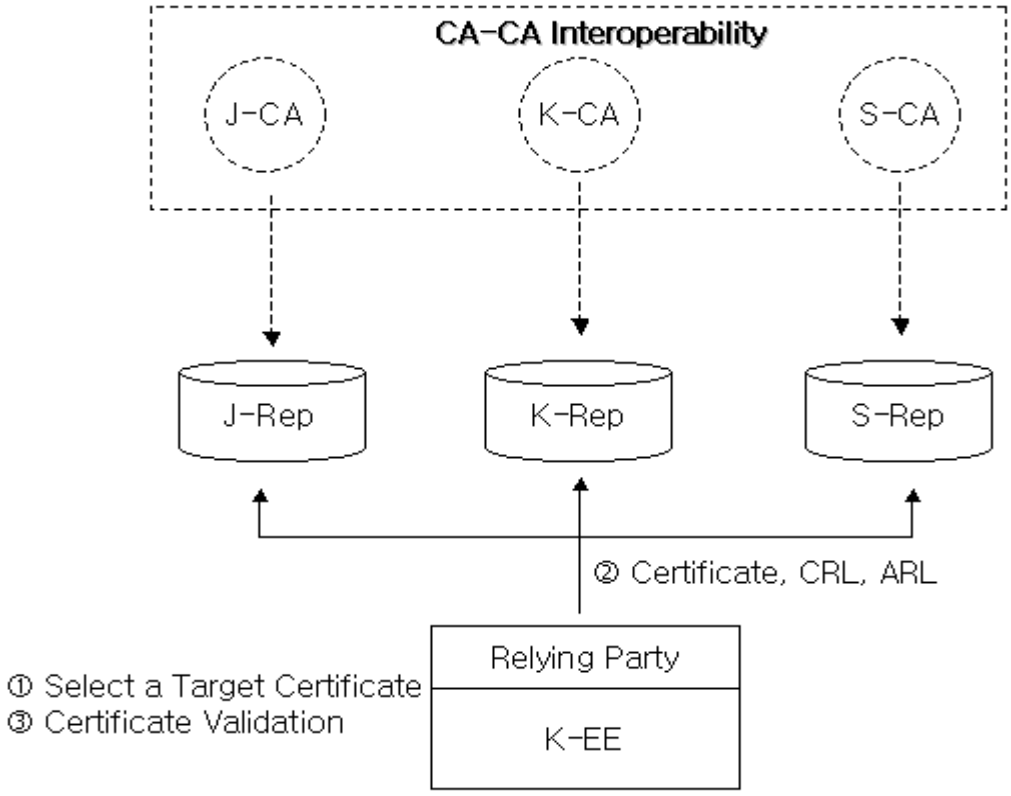
In this experiment, two validation models are used. One is the Validation Authority (VA) server-based model and the other is End Entity (EE) client side model.

4.4.1 Korea Validation Model

Korea implemented both EE validation, and VA model in the experiment.

EE Validation

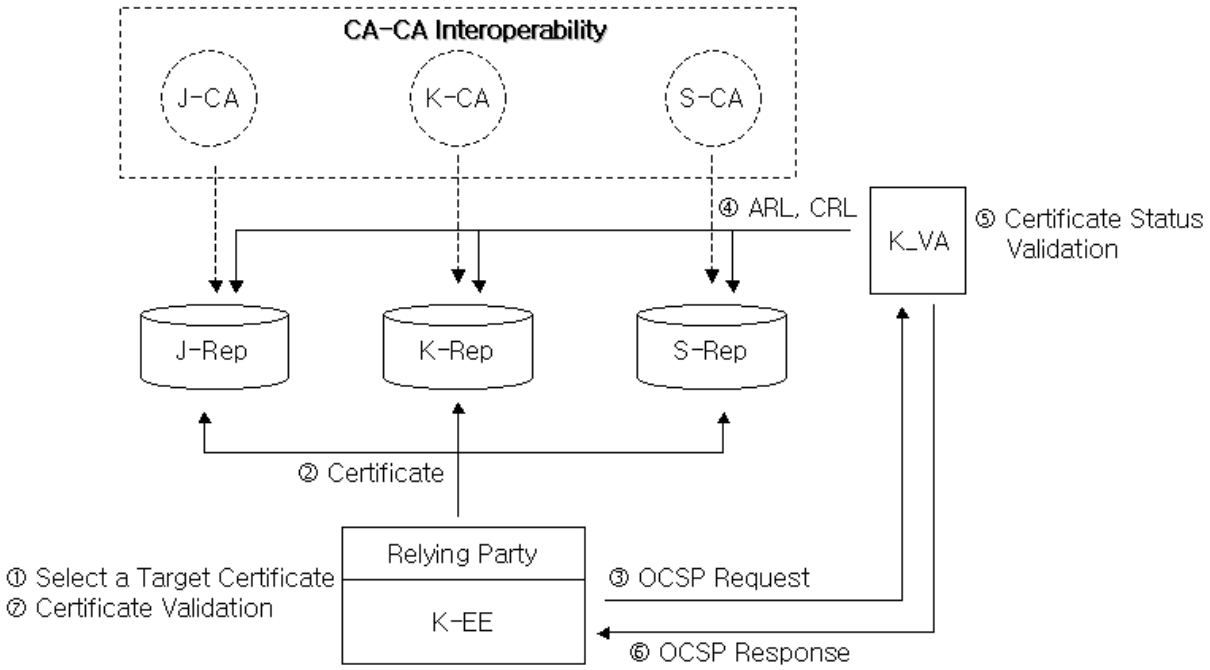
Relying party retrieves required information from each country's directory to verify the certificates, following the certificate path validation procedure stated in the RFC2459. When verifying the EE certificates from Japan and Singapore, cross certificates issued by Korea are used.



VA model

Korea VA has functions of OCSPv1(RFC 2560). So the relying party, as shown below, requests certificate status to VA after establishing the certificate path from each country's directory. Relying party verifies the certificate following the

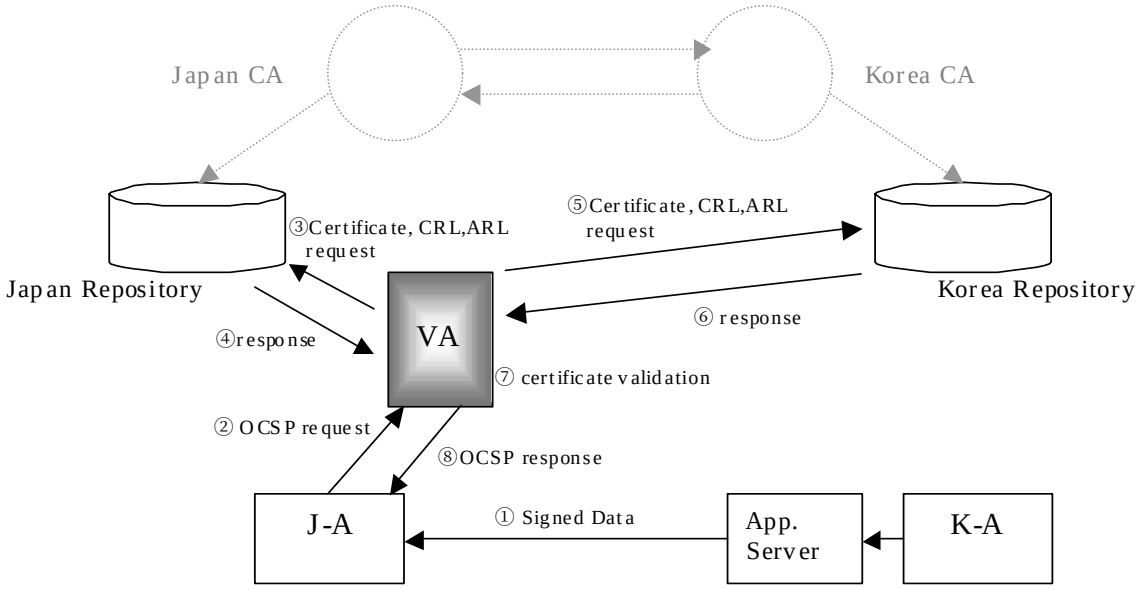
certificate path validation procedure in RFC2459 based on the status results.



4.4.2 Japan Validation Model

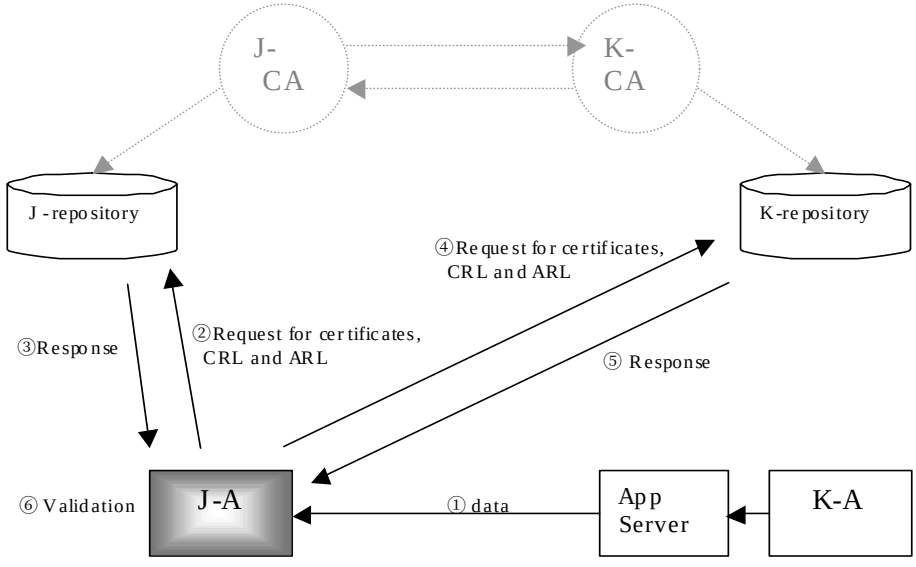
The validation process is different when the different trust model is achieved. In this experiment, the EE client changes the validation processes in different trust models. When Japanese and Korean users are the relying parties, the cross certification validation is processed. When Singaporean user is the relying party, the cross recognition validation is processed. The path validation algorithm conforms to the recommendations documented in RFC 2459.

The following figure shows the overview of the validation process when the VA is adopted between Korean and Japanese transactions (Cross Certification as trust model) for example:



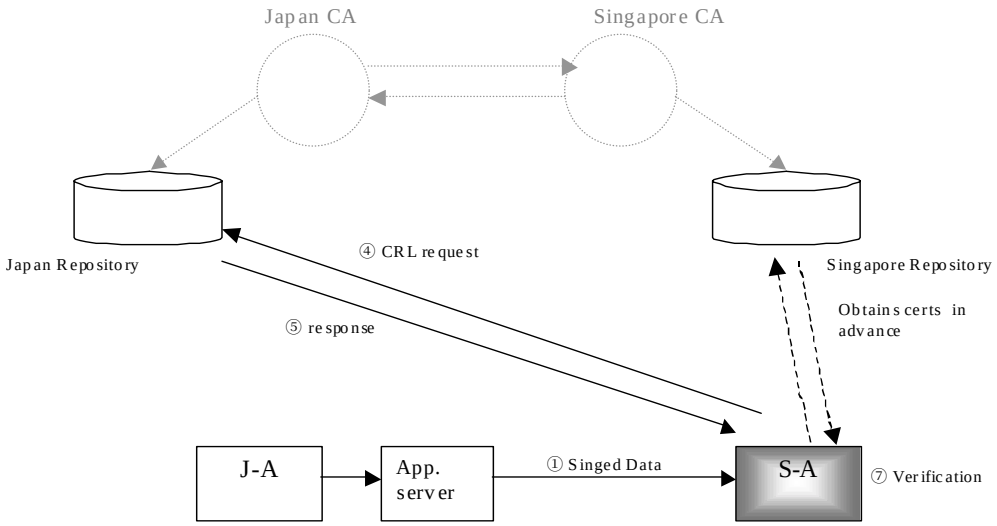
The communications between Japanese client and VA is OCSP, and the OCSP extensions for path validation requests/response are also developed. The LDAP v3 messages are used for communications between VA and repositories.

The following picture shows the overview of validation process in EE client model.



The communication between the End Entity client and repositories is LDAP v3.

When the Singaporean is the relying party, the following validation process is employed.



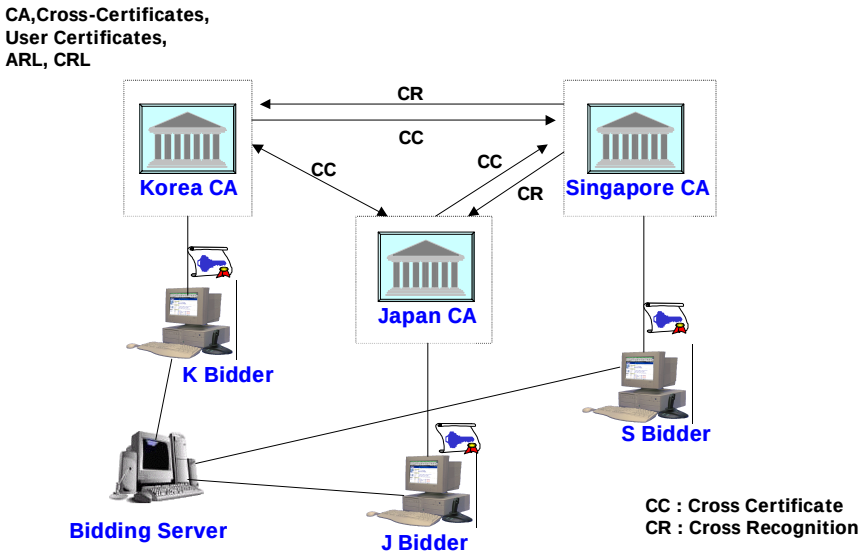
In the experiment, the VA was not involved in the transactions when the Singaporean EE client was the relying party. Only the EE client was able to do the transactions.

4.5 Application Model

JKS-IWG adopted two applications, e-bidding and e-procurement for the experiment.

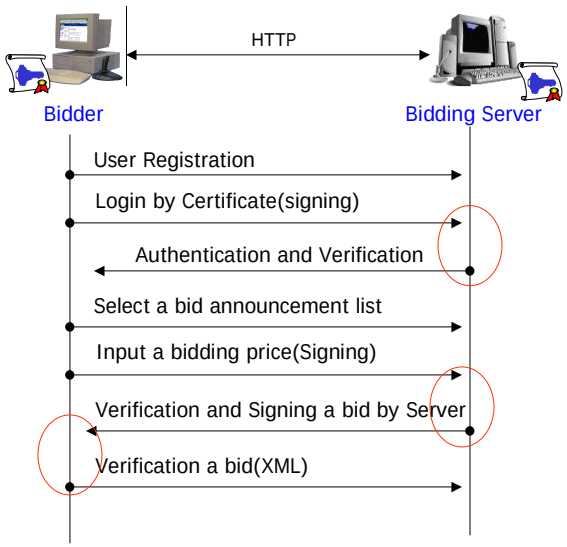
4.5.1 Korea Application

Korea adopted electronic bidding system.



Scenario is the electronic bidding system using web on the Internet. As depicted in the picture, users get certificates from their own country's CA. Between each country's CA, trust relationship of Cross Certification or Cross Recognition is established.

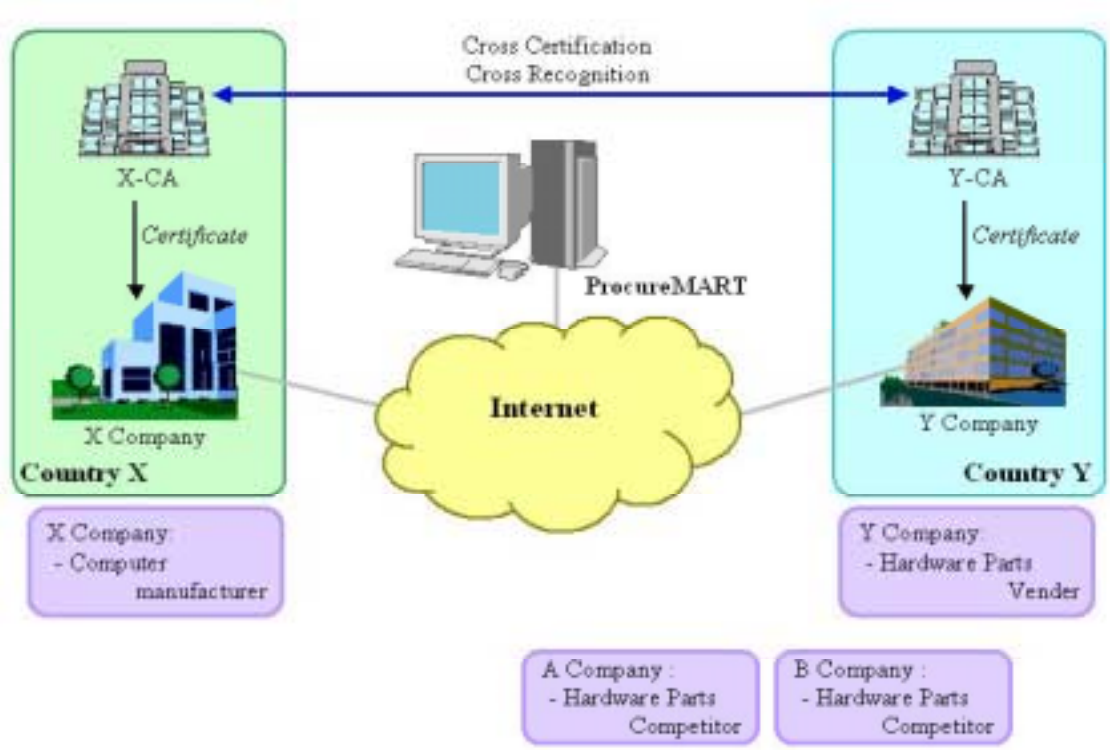
Business flow is as following.



1. User Registration
2. Login using certificate and the digital signature
3. Certificate verification and user authentication
4. Select a bid announcement list and join the bidding
5. Transmit bidding price with digital signature and encryption
6. Server verifies the user's digital signature and reply with receipt with digital signature
7. Verify the receipt

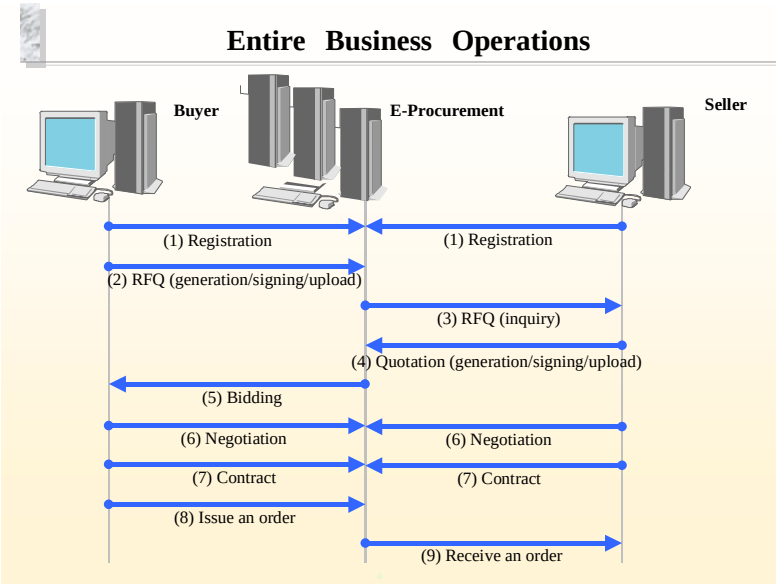
4.5.2 Japan Application

The Japan adopted the e-procurement system as the application model.



The scenario is a "business-to-business" (B2B) transaction conducted over the Internet using the procurement system. The figure above depicts that the Company X adopts X CA that issues certificates to the employees in Company X and the Company Y, typically located in foreign countries, adopts the Y CA that issues the certificates to the employees in Company Y. Between the two CA, the Cross Certification or Cross Recognition trust relationship is achieved.

The business flow is as follows:



1. User registration
2. Generation of Estimate Expense Sheet/Signing Signature/Upload (buyer)
3. Reference to Estimate Expense Sheet/Signature Validation (seller)
4. Generation of Reply Sheet/Signing Signature/Upload (seller)
5. Reference to Reply Sheet/Signature Validation/Estimation (buyer)
6. Generation of Contract Document/Signing Signature/Sending (buyer)
7. Reception of Contract Document/Signature Validation/Signing Signature/ Reply (seller)
8. Generation of Purchase Order/Signing Signature/Sending (buyer)
9. Reception of Purchase Order/Signature Validation/Acceptance Inspection (seller)

5. Experiment plan

5.1 Test plan

To test the aforementioned models, the JKS-IWG developed a specific test plan. The members developed three test scenarios to obtain the results; basic test, advanced test, and application test. In addition, for the test evidences, the members decided to collect several server data in order to backup the test result. The data include the CA system log, directory server log, VA server log, application server & client log.

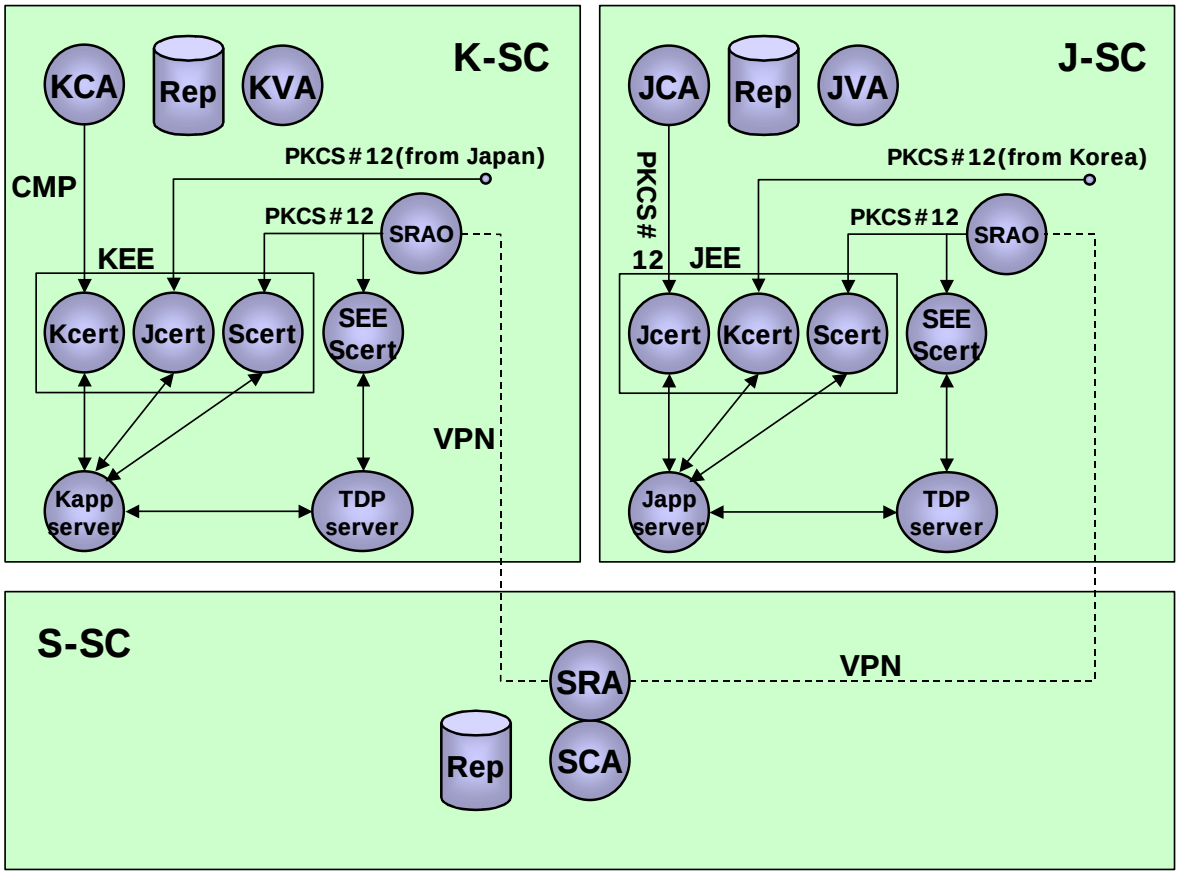
The test consists of into three phases, the basic test, the advanced test, and the application test.

Test Phase	Contents
Basic Test	Issue certificates
	Revoke certificates and issue CRL/ARL
	Update certificates
	Renew certificates
Advanced Test	Path Construction and Validation
	Key Changeover (Pending)
Application Test	Based on the business scenarios

The basic test was intended for the CA systems to check whether the systems can perform the certification-related functions necessary to construct the CA-CA models among the 3 parties. The advanced test was conducted to check whether the validation can be achieved with both VA server and End Entity client models. The application test was conducted based on several business scenarios. The detail test items and the experiment results are described in the Appendix 1 and 2.

5.2 Test environments in JKS-IWG experiment

JKS-IWG members established their own test environments. The following figure shows the overview of the test environment between three countries.



- K-SC: Korea Simulation Center, J-SC : Japan SC, S-SC : Singapore SC
- KCA: Korea CA Server, JCA : Japan CA Server, SCA : Singapore CA Server
- SRA: Singapore Registration Authority, SRAO : SRA Operator
- KEE: Korea End-Entity, JEE : Japan EE, SEE : Singapore EE
- CMP: Certificate Management Protocol
- Kcert: Certificate issued by Korea, Jcert : Certificate issued by Japan
- Scert: Certificate issued by Singapore
- KApp: Korea Application, JApp : Japan Application
- TDP: Transaction Delivery Platform
- VPN: Virtual Private Network

Korea and Japan provided the CA and End-Entity's application environments and Singapore provided the CA environment. At the Korea and Japan simulation centers, the Singapore RAO was established to issue the Singapore certificates remotely.

6. Experiment Results

JSK-IWG members have completed the interoperability experiment successfully. Details of the experiment results are described in Appendix 1 and 2. Main points on the test and results are summarized below.

6.1 Basic Test

The basic test includes issuance, update, revocation, and renewal for the cross certificate. The purpose of these tests was to check whether the cross certificate has been issued in compliant with the certificate profile, and the certificate request profile matches the certificate request. The test also validates the certificate published through confirmation with the directory servers. All of the tests corresponded with their purposes and successfully completed.

6.2 Advanced Test

The purpose of the advanced test was to check whether the EE is able to verify the certificate from a foreign CA. Path construction and validation tools developed in each country should be able to perform successfully for diverse types of the certificate. The test included path construction and path validation using invalid certificates such as the revoked certificates, expired certificates, and the certificates within which CertificatePolicies field was invalid. All of the tests corresponded with their purposes.

6.3 Application Test

The application used in this test has functions such as; automatic download and installation of client program using web interface, login procedure using certificate, certificate request and issuing function for a new user, certificate Import, set Trust Anchor, bidding and transmitting the bid with digital signature, verifying the bid results from server for the client. All of the tests corresponded with their purposes.

Appendix 1: Experiment Test Items

This section describes the details of test items for the basic, advanced, and application tests.

Test Items

1. Basic Test

The Basic Test includes the following four tests: the issuance, revocation, update, and renewal of the certification.

1.1 The certificate issuance includes the following test items:

Item No	Test Items	Result Confirmation Process
1	Issue Self-signed Certificate	Contents confirmation
2	Issue Certificate Request	Contents confirmation
3	Issue CrossCertificate	Contents confirmation
4	Issue CrossCertificatePair	Contents confirmation
5	Issue EE Certificate	Contents confirmation
6	*Issue Application Server Certificate(not tested actually)*	*Contents confirmation*
7	Issue VA Server Certificate	Contents confirmation

This test checked whether the CA systems can issue particular certificates to entities based on certificate profile. Item 6 was not conducted since, in design principle, the application server was not the one that checks the signature or/and certificates in the application model.

1.2 The certificate revocation test includes the following items:

Item No	Test Items	Result Confirmation Process
1	Issue CRL	Contents Confirmation
2	Issue ARL	Contents Confirmation

This test checked whether the CA systems can issue the CRL/ARL against particular entities based on certificate Profile.

1.3 The certificate update test includes the following item:

Item No	Test Items	Result Confirmation Process
1	Update CrossCertificate	Remove from repository and insert the new one.

This test extends the certificate period by issuing a new certificate.

1.4 The certificate renewal test includes the following items:

Item No	Test Items	Result Confirmation Process
1	Revocation Old CrossCertificate	Stored to repository
2	Re-issue CrossCertificate	Stored to repository

This test updates a certificate when non-key data is changed by issuing a new certificate.

2. Advance Test

The advance test is path construction and validation test. It checks whether particular validation processes can verify certificates based on the trust model between the subscriber and relying party. The VA can be used to check status of certificate by relying party.

The advance test includes the following items:

Item No	Test Items	Test Contents
1	Normal Test	It checks whether Certificate path construction and validation can be performed normally. Validation Model : EE Model or VA Model
2	Revoked Test	It checks whether Certificate path construction and validation cannot be performed because of including revoked certificate in Certificate path. Validation Model : EE Model or VA Model
3	Validity Test	It checks whether Certificate path construction and validation cannot be performed because of including expired certificate in Certificate path.
4	Policy Test	It checks whether Certificate path construction and validation cannot be performed because of the certificate including invalid policy OID in Certificate path.
5	Path Construction Test	It checks whether Certificate path construction and validation cannot be performed because path construction cannot be completed?.

In order to conduct the advanced test, it was necessary to prepare the following certificates.

	EE	Contents	Test Items
1	EE01	Valid EE	Normal Test
2	EE02	Revoked EE	Revoked Test
3	EE03	Expired EE	Validity Test
4	EE04	EE which a policy does not suit	Policy Test
5	EE05	EE which has not carried out cross Certificate(cross recognition)	Path Construction Test

3. Application Test: Japan

The application test was conducted amongst the application server, EE client holding each country's Certificate, using the application server, VA and J-EE in the Japan's Simulation Center, J-EE in Korea's Center, and J-EE in Singapore's Center. The business flows reflect the

application test scenarios, since the each flow has to be tested between the two parties. In addition, this test involves the VA and EE client as the validation entity as well.

Item No	Contents	Pattern
1	Test the entire business operations, by using buying side's certificates (in normal cases) and selling side's certificates (in normal cases). Validation Model: EE Model	1) buyer:J-EE(J) seller:J-EE(K) 2)buyer:J-EE(K) seller:J-EE(J) 3)buyer:J-EE(J) seller:J-EE(S) 4)buyer:J-EE(S) seller:J-EE(J)
2	Test the entire business operations, by using buying side's certificates (in normal cases) and selling side's certificates (in normal cases). Validation Model: VA Model.	1)buyer:J-EE(J) seller:J-EE(K) 2)buyer:J-EE(K) seller:J-EE(J) 3)buyer:J-EE(J) seller:J-EE(S) 4)buyer:J-EE(S) seller:J-EE(J)
3	Test the entire business operations, by using buying side's certificates (in normal cases) and selling side's certificates (in revoked-Cert cases). Validation Model: EE Model	1)buyer:J-EE(J) seller:J-EE(K) 2)buyer:J-EE(K) seller:J-EE(J) 3)buyer:J-EE(J) seller:J-EE(S) 4)buyer:J-EE(S) seller:J-EE(J)
4	Test the entire business operations, by using buying side's certificates (in normal cases) and selling side's certificates (in revoked-Cert cases). Validation Model: VA Model	1)buyer:J-EE(J) seller:J-EE(K) 2)buyer:J-EE(K) seller:J-EE(J) 3)buyer:J-EE(J) seller:J-EE(S) 4)buyer:J-EE(S) seller:J-EE(J)
5	Test the entire business operations, by using buying side's certificates (in revoked-Cert cases) and selling side's certificates (in normal cases). Validation Model: EE Model	1)buyer:J-EE(J) seller:J-EE(K) 2)buyer:J-EE(K) seller:J-EE(J) 3)buyer:J-EE(J) seller:J-EE(S) 4)buyer:J-EE(S) seller:J-EE(J)
6	Test the entire business operations, by using buying side's certificates (in revoked-Cert cases) and selling side's certificates (in normal cases). Validation Model: VA Model	1)buyer:J-EE(J) seller:J-EE(K) 2)buyer:J-EE(K) seller:J-EE(J) 3)buyer:J-EE(J) seller:J-EE(S) 4)buyer:J-EE(S)

		seller:J-EE(J)

4. Application Test: Korea

Electronic bidding using certificate from Korea, Japan, and Singapore user, and bidding server verifies the user's digital signature. Test scenario is similar to the CA-CA advance test.

Appendix 2: Experiment Test Results

This appendix describes the detail test results including the basic, advanced, and application tests.

Test Results

1. Basic Test: Japan

1.1 Certificate issuance

Test Items	Result
Issue self-signed certificate Issue End Entity certificate Issue VA certificate	O
Receive pkcs#10 Issue Cross Certificate to Korea CA Generate CrossCertificatePair and store it to Rep.	O
Issue Cross Certificate to Singapore CAs Generate CrossCertificatePair(only reverse elements) and store it to the Rep.	O
Receive the cross certification request Receive Cross Certificate to Japan CA by Korea	O
Receive the cross certification request	O

1.2 Certificate revocation

Test Items	Result
Issue CRL for Japan End-Entity	O
Issue ARL for cross certificate to Korea CA	O
Issue ARL for cross certificate to Singapore CA	O

1.3 Certificate update

Test Items	Result
update cross certificate to Korea CA generate new crossCertificatePairs (modify reverse element only)	O
update cross certificate to Singapore CA generate new crossCertificatePairs (modify reverse element only)	O

1.4 Certificate renewal

Test Items	Result
issue ARL renew a cross certificate to Korea CA generate new crossCertificatePairs (modify reverse element only)	O
issue ARL renew a cross certificate to Singapore CA generate new crossCertificatePairs (reverse element only)	O

2. Basic Test: Korea

2.1 Cross-Certificate Issuance

Test Items	Result
Create the key pair for cross-certificate Make PKCS#10	O
Issue self-signed certificate Send PKCS#10 Issue EE certificate	O
Receive PKCS#10 from Japan Issue and Send Cross Certificate to Japan	O
Receive PKCS#10 from Singapore Issue Cross Certificate to Singapore Generate CrossCertificatePair(only reverse elements) and store it Rep	O
Receive Cross Certificate from Japan Generate CrossCertificatePair and store it Rep	O

2.2 Cross-Certificate Update

Test Items	Result
Send PKCS#10 for update Delete CrossCertificatePair in Rep	O
Receive OJCS#10 from Japan Issue and Send Cross Certificate to Japan	O
Receive PKCS#10 from Singapore Issue Cross Certificate to Singapore Generate CrossCertificatePair(only reverse elements) and store it Rep	O
Receive Cross Certificate from Japan Generate CrossCertificatePair and store it Rep	O

2.3 Cross-Certificate Revocation

Test Items	Result
Revoke Cross Certificate to Japan Issue ARL	O
Revoke EE certificate Issue CRL	O
Revoke Cross Certificate to Singapore Issue ARL	O

2.4 Cross-Certificate renewal

Test Items	Result
Delete CrossCertificatePair for Japan in Rep Revoke the cross certificate to Japan Issue ARL Send PKCS#10 to Japan	O

Receive PKCS#10 form Japan Renew and send cross certificate to Japan Generate CrossCertificatePair and store it Rep	O
Delete CrossCertificatePair for Singapore in Rep Revoke the cross certificate Issue ARL	O
Receive PKCS#10 from Singapore Issue Cross Certificate to Singapore Generate CrossCertificatePair(only reverse elements) and store it Rep	O

3. Advance Test: Japan

3.1 Certificate check (path check)

Test patterns	Signer (Subscriber)	RP	Model	Result
(a)	J-User	K-User	EE	O
(b)	K-User	J-User	EE	O
(c)	K-User	J-User	VA	O
(d)	J-User	S-User	EE	O
(e)	S-User	J-User	EE	O
(f)	S-User	J-User	VA	x

3.2 Revocation (when the singer is revoked)

Test patterns	Signer (Subscriber)	RP	Model	Result
(a)	J-User	K-User	EE	O
(b)	K-User	J-User	EE	O
(c)	K-User	J-User	VA	O
(d)	J-User	S-User	EE	O
(e)	S-User	J-User	EE	O
(f)	S-User	J-User	VA	x

3.3 Validity check (when the certificate is expired)

Test patterns	Signer (Subscriber)	RP	Model	Result
(a)	J-User	K-User	EE	O
(b)	K-User	J-User	EE	O
(c)	K-User	J-User	VA	O
(d)	J-User	S-User	EE	O
(e)	S-User	J-User	EE	O
(f)	S-User	J-User	VA	O

3.4 Policy check (when the invalid policy ID is inserted)

Test patterns	Signer (Subscriber)	RP	Model	Result
(a)	J-User	K-User	EE	O
(b)	K-User	J-User	EE	O

(c)	K-User	J-User	VA	O
(d)	J-User	S-User	EE	O
(e)	S-User	J-User	EE	O
(f)	S-User	J-User	VA	O

4. Advance Test: Korea

4.1 Normal test

Signer	Cross Certificates Status	Model	Result
J-User	Normal	EE	O
		VA	
J-User	Revoked	EE	O
		VA	
S-User	Normal	EE	O
S-User	Revoked	EE	O

4.2 Revoke test (signer certificate is revoke)

Signer	Cross Certificates Status	Model	Result
J-User	Normal	EE	O
		VA	
J-User	Revoked	EE	O
		VA	
S-User	Normal	EE	O
S-User	Revoked	EE	O

4.3 Validity test (signer certificate is not valid)

Signer	Cross Certificates Status	Result
J-User	Normal	O
J-User	Revoked	O
S-User	Normal	O
S-User	Revoked	O

4.4 Policy test (signer certificate’s policy is not correct)

Signer	Cross Certificates Status	Result
J-User	Normal	O
J-User	Revoked	O
S-User	Normal	O
S-User	Revoked	O

5. Application test: Japan

5.1 Normal test

Buyer	Seller	Model	Result
J-User	K-User	EE	O

K-User	J-User	EE	O
J-User	S-User	EE	O
S-User	J-User	EE	O
J-User	K-User	VA	O
J-User	S-User	VA	x

5.2 Revoked (1) when the seller is revoked

Buyer	Seller	Model	Result
J-User	K-User	EE	O
K-User	J-User	EE	O
J-User	S-User	EE	O
S-User	J-User	EE	O
J-User	K-User	VA	O
J-User	S-User	VA	x

5.3 Revoked (2) when the buyer is revoked

Buyer	Seller	Model	Result
J-User	K-User	EE	O
K-User	J-User	EE	O
J-User	S-User	EE	O
S-User	J-User	EE	O
J-User	K-User	VA	O
J-User	S-User	VA	O

6. Application test: Korea

6.1 Normal test

Bidder	Cross Certificates Status	Result
J-User	Normal	O
J-User	Revoked	O
S-User	Normal	O
S-User	Revoked	O

6.2 Revoke test (signer certificate is revoke)

Bidder	Cross Certificates Status	Result
J-User	Normal	O
J-User	Revoked	O
S-User	Normal	O
S-User	Revoked	O

6.3 Validity test (signer certificate is not valid)

Bidder	Cross Certificates Status	Result
J-User	Normal	O
J-User	Revoked	O
S-User	Normal	O

S-User	Revoked	O

6.4 Policy test (signer certificate's policy is not correct)

Bidder	Cross Certificates Status	Result
J-User	Normal	O
J-User	Revoked	O
S-User	Normal	O
S-User	Revoked	O

[put the box for the OCSP test]

Note:

Test result symbols

O – Positive test result

X – Negative test result

Appendix 3: JKS IWG CA Certificate & CRL Profile

Experiment and Actual Certificate and CRL profiles among the three countries.
(M: Mandatory, --: Not-defined, O: Optional, C: Critical, NC: Non-Critical, X : Not recommended)

1. Japan (Experiment Profile)

1.1 Self-Signed Certificate

1.1.2 Self-Signed Certificate Basic Fields

Fields	Self	Type of ASN.1
Version	3 (0x2)	INTEGER
serialNumber	3223604 (0x313034)	INTEGER
signature	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)	OID
validity		
notBefore	010901000000Z	UTC TIME
notAfter	020101000000Z	UTC TIME
Issuer		
type	C=JP, O=Japan Certification Services, CN=Test Root CA	OID
value		UTF8String or PrintableString
subject		
type	C=JP, O=Japan Certification Services, CN=Test Root CA	OID
value		UTF8String or PrintableString
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1 (rsaEncryption)	OID
subjectPublicKey	Modulus (2048 bit): 00:b2:56:c6:92:e9:d2:76:fa:fe:3d:59:cc:5e:13:0f:53: 15:55:f9:68:94:92:28:50:b0:ec:d8:dd:6d:ad:c6:ab:47 :72:27:cf:90:24:1e:ae:2e:e4:af:c9:62:a8:71:53:84:cf: 13:6e:49:23:8b:9f:d2:0e:e2:e9:a7:11:9b:0b:ec:09:21: e9:62:a5:82:35:11:b1:99:88:ec:ae:c3:97:1c:37:17:07 :8a:e5:23:21:36:0d:3c:f0:46:f0:81:5d:a8:ab:27:04:9c :b8:e8:a8:df:bc:f8:45:22:d2:55:ec:82:17:0e:b0:25:84 :31:2d:ba:63:2d:aa:5e:08:65:22:71:c7:b3:8d:1f:4c:70 :70:71:05:6d:87:e7:ad:70:24:2b:96:51:67:18:59:78:f c:3c:8a:c0:2a:63:03:f4:e5:16:35:8f:7f:0d:65:e3:d5:3 8:0d:f9:c1:23:18:2e:f5:49:8b:b4:28:58:32:ee:66:27:e 2:b1:60:e1:5c:27:0f:f8:76:22:ae:a0:96:63:d9:8b:fa:1 c:2d:ab:22:af:33:d0:e2:7d:5f:ec:fe:3e:59:74:ef:3d:05 :95:ac:16:3c:72:ff:46:fa:c7:5c:d0:9a:50:62:95:9c:99: 0b:dd:f2:48:3b:0a:38:9a:92:cf:e4:01:de:02:2f:8f:fe:c 7:1d Exponent: 65537 (0x10001)	BIT STRING
issuerUniqueID		---
subjectUniqueID		---

1.1.3 Self-Signed Certificate Extension Fields

Fields			Type of ASN.1
authorityKeyIdentifier		NC	
keyIdentifier	8B:92:4B:C6:0D:6F:B1:35:E1:1F:6A:D3:98:59:05:78:A4:A2:20:B4		OCTETSTRING
subejctKeyIdentifier	8B:92:4B:C6:0D:6F:B1:35:E1:1F:6A:D3:98:59:05:78:A4:A2:20:B4	NC	OCTETSTRING
keyUsage	Key CertSign, cRLSign	C	BITSTRING
basicConstraints		C	
cA	TRUE		BOOLEAN
pathLenConstraints			INTEGER
cRLDistributionPoints		NC	
distributionPoint			
fullName	DirName:/C=JP/O=Japan Certification Services/CN=Test ROOT CA URI:ldap://j-re.apki-j-sim.jp/cn=Test%20ROOT%20CA,o=Japan%20Certification%20Services,c=JP		DN, URI

1.2 Cross Certificate

1.2.1 Cross Certificate Basic Fields

Fields	Self	Type of ASN.1
Version	3 (0x2)	INTEGER
serialNumber	0x313138 (3223864)	INTEGER
signature	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)	OID
validity		
notBefore	010901000000Z	UTC TIME
notAfter	020101000000Z	UTC TIME
Issuer		
type	C=JP, O=Japan Certification Services, CN=Test Root CA	OID
value		UTF8String or PrintableString
subject		
type	C=KR, O=KISA, OU=TestCA, CN=TestRootCA	OID
value		UTF8String or PrintableString
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1 (rsaEncryption)	OID

subjectPublicKey	Modulus (2048 bit): 00:be:dd:25:4b:4a:13:c6:03:e5:16:6c:8f:4a:d5:df:7a: 16:f3:80:d5:ed:6b:b7:ee:77:fa:16:d2:48:4b:34:3d:72: a2:5f:8f:dd:7e:a9:f0:9e:43:b1:19:2a:6c:5b:67:17:73: 55:fd:f9:c6:fb:ea:90:cf:32:26:db:5c:22:8a:9a:41:9f:c e:2d:7f:71:1b:db:65:c9:38:62:16:c0:21:4d:c6:69:d9: 88:e5:93:89:82:84:58:e8:ca:29:7e:a7:e1:d3:86:97:91 :46:c3:c7:de:a7:cf:46:55:82:56:ea:3d:75:5d:ee:40:83 :55:ed:f9:40:6d:cf:85:1e:47:2f:31:21:5e:af:bb:36:57: fc:1c:3b:1f:b0:f4:b0:66:c8:94:f2:ff:00:e1:1a:79:2d:3 2:6c:c1:f5:b6:0e:68:ba:34:66:ef:95:7c:1d:5f:3b:ce:df :11:b0:0c:fc:95:4e:48:25:48:96:db:06:e7:1f:d3:c4:41 :d1:be:e6:6f:e1:e3:cc:75:d7:a1:7e:2a:f7:e1:8f:c6:e7: bf:79:aa:99:c9:44:a2:26:f9:a6:fb:1e:56:56:34:31:f0:9 a:dc:bb:c8:4c:c4:64:01:6a:25:60:84:98:e4:b1:65:d9: 22:06:99:44:0f:2a:d7:a0:20:e5:e5:12:29:c1:a2:2c:d9: bd Exponent: 65537 (0x10001)	BIT STRING
issuerUniqueID		---
subjectUniqueID		---

1.2.2 Cross Certificate Extension Fields

Fields	Cross		Type of ASN.1
authorityKeyIdentifier		NC	
keyIdentifier	8B:92:4B:C6:0D:6F:B1:35:E1:1F:6A:D3:98:59 :05:78:A4:A2:20:B4		OCTETSTRING
subejctKeyIdentifier	CA:96:0B:4E:68:CA:4A:04:FE:E0:3E:0F:B1:F 9:78:A2:83:9D:18:0C	NC	OCTETSTRING
keyUsage	Key CertSign, cRLSign	C	BITSTRING
certificatePolicies		C	
policyIdentifier	0.2.440.20013.1.2001.1		OID
policyMappings		C	
issureDomainPolicy	0.2.440.20013.1.2001.1		
subjectDomainPolicy	1.2.410.200004.2.1		
basicConstraints		C	
cA	TRUE		BOOLEAN
cRLDistributionPoints		NC	
distributionPoint			
fullName	DirName:/C=JP/O=Japan Certification Services/CN=Test ROOT CA URI:ldap://j-re.apki-j-sim.jp/cn=Test%20ROO T%20CA,o=Japan%20Certification%20Service s,c=JP		DN, URI

1.3 End-Entity Certificate

1.3.1 End-Entity Certificate Basic Fields

Fields	Self	Type of ASN.1
Version	3 (0x2)	INTEGER
serialNumber	3223609 (0x313039)	INTEGER
signature	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)	OID
validity		
notBefore	010901000000Z	UTC TIME
notAfter	020101000000Z	UTC TIME
issuer		
type	C=JP, O=Japan Certification Services, CN=Test Root CA	OID
value		UTF8String or PrintableString
subject		
type	C=JP, CN=JPEE01	OID
value		UTF8String or PrintableString
subjectPublicKeyInfo		
algorithm	1.2.840.113549.1.1.1 (rsaEncryption)	OID
subjectPublicKey	Modulus (1024 bit): 00:de:59:6b:b0:38:3f:7b:9e:9d:c3:b0:42:f4:15:19:74: a3:84:25:f9:5e:4f:34:8b:d0:51:7b:72:9e:11:42:96:78: f1:68:0a:41:ef:e2:b4:7b:b3:5c:a1:d5:b3:bb:11:d1:b9: 6a:97:2f:91:46:1c:62:0d:51:39:e5:67:36:4a:32:4f:1d: 33:b9:66:bd:ec:be:58:06:71:bf:9c:7e:c3:dd:9e:4a:43: 5e:1d:b4:b7:03:a7:bb:b6:82:a3:ec:f7:30:4f:cf:f1:07:3 0:a0:d9:ed:02:3f:68:e2:6d:d2:70:a6:32:a3:4e:cb:d7:8 9:e3:d2:45:a5:7d:ee:5c:3f:b7 Exponent: 65537 (0x10001)	BIT STRING
issuerUniqueID		---
subjectUniqueID		---

1.3.2 End-Entity Certificate Extension Fields

Fields	EE		Type of ASN.1
authorityKeyIdentifier		NC	
keyIdentifier	8B:92:4B:C6:0D:6F:B1:35:E1:1F:6A:D3: 98:59:05:78:A4:A2:20:B4		OCTETSTRING
subejctKeyIdentifier	76:34:B1:87:9E:20:42:A4:C7:43:7A:84:4F :34:43:12:1A:01:53:D8	NC	OCTETSTRING
keyUsage	Digital Signature	C	BITSTRING
certificatePolicies		C	
policyIdentifier	0.2.440.20013.1.2001.1		OID
policyQualifiers			
explicitText	Explicit Text: Accredited under e-Signature Law(Japan)		VisibleString
cRLDistributionPoints		NC	
distributionPoint			

fullName	DirName:/C=JP/O=Japan Certification Services/CN=Test ROOT CA URI:ldap://j-re.apki-j-sim.jp/cn=Test%20ROOT%20CA,o=Japan%20Certification%20Services,c=JP		DN, URI

1.4 CRL/ARL

1.4.1 CRL/ARL Basic Fields

Fields	CRL/ARL	Type of ASN.1
version	2 (0x1)	INTEGER
signature	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)	OID
issuer		
type	C=JP, O=Japan Certification Services, CN=Test Root CA	OID
value		UTF8String or PrintableString
thisUpdate	011015135058Z	UTC TIME
nextUpdate	011017135058Z	UTC TIME
revokedCertificates		
serialNumber	3223857 (0x313131)	INTEGER
revocationDate	011015000000Z	UTC TIME

1.4.2 CRL/ARL Entry Extensions

Fields	CRL/ARL		Type of ASN.1
reasonCode	0	NC	ENUMERATED

1.4.3 CRL/ARL Extension Fields

Fields	CRL/ARL		Type of ASN.1
authorityKeyIdentifier		NC	
keyIdentifier	8B:92:4B:C6:0D:6F:B1:35:E1:1F: 6A:D3:98:59:05:78:A4:A2:20:B4		OCTETSTRING
cRLNumber	12855	NC	INTEGER
issuingDistributionPoint		C	
distributionPoint			
fullName	DirName:/C=JP/ O=Japan Certification Services/ CN=Test ROOT CA URI:ldap://j-re.apki-j-sim.jp/ cn=Test%20ROOT%20CA, o=Japan%20Certification%20Services, c=JP		DN, URI
onlyContainsUserCerts	TRUE(CRL)		BOOLEAN
onlyContainsCACerts	TRUE(ARL)		BOOLEAN

2. Korea (Experiment Profile)

2.1 Self-Signed Certificate

2.1.1 Self-Signed Certificate Basic Fields

Field	Generation	ASN.1 TYPE	Value
Version	M	INTEGER	V3(2)
SerialNumber	M	INTEGER	$0<n<2^{128}$
Signature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Validity			
NotBefore	M	UTC TIME	010901000000Z
NotAfter	M	UTC TIME	020101000000Z
Issuer			
Type	M	OID	C={KR, SG, JP}[1], O=XXXX, OU=XXXX, CN=XXXX
Value	M	UTF8String or PrintableString	
Subject			
Type	M	OID	C={KR, SG, JP}, O=XXXX, OU=XXXX, CN=XXXX
Value	M	UTF8String or PrintableString	
SubjectPublicKeyInfo			
Algorithm	M	OID	1.2.840.113549.1.1.1 rsaEncryption (2048bit)
SubjectPublicKey	M	BITSTRING	

2.1.2 Self-Signed Certificate Extension Fields

Field	Generation	ASN.1 TYPE	Value
authorityKeyIdentifier (non-Critical)			
KeyIdentifier	M	OCTETSTRING	Hash value of Issuer's public-key (SHA-1 160bit)
subjectKeyIdentifier (non-Critical)	M	OCTETSTRING	Hash value of subjectPublicKey (SHA-1 160bit)
keyUsage (Critical)	M	BITSTRING	KeyCertSign, cRLSign
CertificatePolicies			
PolicyIdentifier	--		
PolicyQualifiers			
PolicyQualifierId	--		
Qualifier			
CPSuri	--		
UserNotice			
NoticeRef			
Organization	--		
noticeNumber	--		
ExplicitText	--		
BasicConstraints (Critical)			
CA	M	BOOLEAN	TRUE

[1] ASN.1 type of Country is printableString. It is the same as that of the following.

CRLDistributionPoints (non-Critical)			
DistributionPoint			
FullName	M		(a) **URI**[2]

2.2 Cross-Certificate

2.2.1 Cross-Certificate Basic Fields

Field	Generation	ASN.1 TYPE	Value
Version	M	INTEGER	V3(2)
SerialNumber	M	INTEGER	$0<n<2^{128}$
signature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Validity			
NotBefore	M	UTC TIME	010901000000Z
NotAfter	M	UTC TIME	020101000000Z
Issuer			
Type	M	OID	C={KR, JP}, O=XXXX, OU=XXXX, CN=XXXX
Value	M	UTF8String or PrintableString	
Subject			
Type	M	OID	C={KR, SG, JP}, O=XXXX, OU=XXXX, CN=XXXX
Value	M	UTF8String or PrintableString	
SubjectPublicKeyInfo			
Algorithm	M	OID	1.2.840.113549.1.1.1 rsaEncryption (2048bit)
SubjectPublicKey	M	BITSTRING	

2.2.2 Cross-Certificate Extension Fields

Field	Generation	ASN.1 TYPE	Value
authorityKeyIdentifier (non-Critical)			
keyIdentifier	M	OCTETSTRING	Hash value of Issuer's public-key (SHA-1 160bit)
subjectKeyIdentifier (non-Critical)	M	OCTETSTRING	Hash value of subjectPublicKey (SHA-1 160bit)
keyUsage (Critical)	M	BITSTRING	KeyCertSign, cRLSign
certificatePolicies (Critical)			
policyIdentifier	M	OID	
PolicyQualifiers			
policyQualifierId	--		
Qualifier			
cPSuri	--		
UserNotice			
NoticeRef			
organization	--		
noticeNumber	--		
explicitText	--		

[2] DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be the same value.

PolicyMappings (non-Critical)			
issureDomainPolicy	M		
subjectDomainPolicy	M		
BasicConstraints (Critical)			
CA	M	BOOLEAN	TRUE
CRLDistributionPoints (non-Critical)			
DistributionPoint			
fullName	M		(b) **URI**[3]

2.3 End-Entity Certificate

2.3.1 End-Entity Certificate Basic Fields

Field	Generation	ASN.1 TYPE	Value
Version	M	INTEGER	V3(2)
serialNumber	M	INTEGER	$0<n<2^{128}$
Signature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Validity			
NotBefore	M	UTC TIME	010901000000Z
NotAfter	M	UTC TIME	020101000000Z
Issuer			
Type	M	OID	C={KR, SG, JP}, O=XXXX, OU=XXXX, CN=XXXX
Value	M	UTF8String or PrintableString	
Subject			
Type	M	OID	C={KR, SG, JP}, O=XXXX, OU=XXXX, CN=XXXX
Value	M	UTF8String or PrintableString	
SubjectPublicKeyInfo			
Algorithm	M	OID	1.2.840.113549.1.1.1 rsaEncryption (1024bit)
SubjectPublicKey	M	BITSTRING	

2.3.2 End-Entity Certificate Extension Fields

Field	Generation	ASN.1 TYPE	Value
authorityKeyIdentifier (non-Critical)			
KeyIdentifier	M	OCTETSTRING	Hash value of Issuer's public-key (SHA-1 160bit)
subjectKeyIdentifier (non-Critical)	M	OCTETSTRING	Hash value of subjectPublicKey (SHA-1 160bit)
keyUsage (Critical)	M	BITSTRING	digitalSignature
certificatePolicies (non-Critical)			
policyIdentifier	M	OID	
PolicyQualifiers			
policyQualifierId	--		
Qualifier			
CPSuri	--		

[3] DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be the same value.

UserNotice			
NoticeRef			
organization	--		
noticeNumber	--		
explicitText	M	VisibleString	
subjectAltName (non-Critical)	O	Rfc822name	[4]
CRLDistributionPoints (non-Critical)			
DistributionPoint			
FullName	M		(c) **URI** [5]

2.4 CRL/ARL Profile

2.4.1 CRL Basic Fields

Field	generation	ASN.1 TYPE	Value
version	M	INTEGER	V2(1)
signature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Issuer			
type	M	OID	C={KR, SG, JP}, O=XXXX, OU=XXXX, CN=XXXX
vale	M	UTF8String or PrintableString	
thisUpdate	M	UTC TIME	
nextUpdate	M	UTC TIME	ThisUpdate + 7days
RevokedCertificates			
serialNumber	M	INTEGER	
revocationDate	M	UTC TIME	

2.4.2 CRL Extension Fields

FIELD	Generation	ASN.1 TYPE	Value
AuthorityKeyIdentifier (non-Critical)			
keyIdentifier	M	OCTETSTRING	Hash value of Issuer's public-key (SHA-1 160bit)
cRLNumber (non-Critical)	M	INTEGER	
IssuingDistributionPoint (Critical)			
DistributionPoint			
fullName	M		(d) **URI**[6]
onlyContainsUserCerts	M	BOOLEAN	TRUE

2.4.3 CRL Entry Extensions

FIELD	Generation	ASN.1 TYPE	Value
ReasonCode (non-Critical)	M	ENUMERATED	

[4] Depends on the Korean Certificate Profile requirement.
[5] DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be the same.
[6] DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be the same value.

2.4.4 ARL Basic Fields

Field	generation	ASN.1 TYPE	Value
Version	M	INTEGER	V2(1)
Signature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Issuer			
type	M	OID	C={KR, SG, JP}, O=XXXX, OU=XXXX, CN=XXXX
vale	M	UTF8String or PrintableString	
thisUpdate	M	UTC TIME	
nextUpdate	M	UTC TIME	ThisUpdate + 7days
RevokedCertificates			
serialNumber	M	INTEGER	
revocationDate	M	UTC TIME	

2.4.5 ARL Extension Fields

FIELD	Generation	ASN.1 TYPE	Value
AuthorityKeyIdentifier (non-Critical)			
keyIdentifier	M	OCTETSTRING	Hash value of Issuer's public-key (SHA-1 160bit)
cRLNumber (non-Critical)	M	INTEGER	
IssuingDistributionPoint (Critical)			
DistributionPoint			
fullName	M		(e) **URI**[7]
OnlyContainsCACerts	M	BOOLEAN	TRUE

2.4.6 ARL Entry Extensions

FIELD	Generation	ASN.1 TYPE	Value
reasonCode (non-Critical)	M	ENUMERATED	

[7] DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be the same value.

3. Singapore (Experiment & Actual Profile)

3.1 Self-Signed Certificate

3.1.1 Self-Signed Certificate Basic Field

Field	Self	ASN.1 TYPE	NOTE
Version	M	INTEGER	V3
SerialNumber	M	INTEGER	$0<n<(2^{32}-1)$
Signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity	M		
notBefore	M	UTC TIME	
notAfter	M	UTC TIME	
Issuer	M		
type	M	OID	
value	M	UTF8String or PrintableString	
subject	M		
type	M	OID	
value	M	UTF8String or PrintableString	
subjectPublicKeyInfo	M		
algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
subjectPublicKey	M	BIT STRING	
issuerUniqueID	--	---	
subjectUniqueID	--	---	

3.1.2 Self-Signed Certificate Extension Field

Field	Self		ASN.1 TYPE	NOTE
AuthorityKeyIdentifier	M	NC		
KeyIdentifier	M		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit)
AuthCertIssuer	O		DirectoryName	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
AuthCertSerialNumber	O		INTEGER	
SubejctKeyIdentifier	M	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit)
KeyUsage	M	NC	BIT STRING	Certificate Signing, Off-line CRL Signing, CRL Signing
ExtendedKeyUsage	--			
PrivateKeyUsagePeriod	--			
CertificatePolicies	--			
PolicyIdentifier	--			
PolicyQualifiers	--			
PolicyQualifierId	--			
Qualifier	--			
CPSuri	--			
UserNotice	--			
NoticeRef	--			
Organization	--			
noticeNumber s	--			

ExplicitText	--		VisibleString	
policyMappings	--			
IssureDomainPolicy			OID	
SubjectDomainPolicy			OID	
SubjectAltName	--	--		
IssuerAltName	--	--		
BasicConstraints	M	C		
CA	M		BOOLEAN	
pathLenConstraints	O		INTEGER	
NameConstraints	--			
permittedSubtrees				
Base			GeneralName	
Minimum				
Maximum				
excludedSubtrees				
base			GeneralName	
minimum				
maximum				
policyConstraints	--			
cRLDistributionPoints	M	NC		
DistributionPoint	M			
fullName	M		URI	
nameRelativeToCRLIssuer	--			
ReasonFlags	--			
cRLIssuer	--			
subjectDirectoryAttributes	--			
AuthorityInfoAccess	--			
accessMethod	--			
accessLocation	--			

3.2 CA Certificate

3.2.1 CA Certificate Basic Field

Field	Cross	ASN.1 TYPE	NOTE
Version	M	INTEGER	V3
SerialNumber	M	INTEGER	$0<n<(2^{32}-1)$
Signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity	M		
NotBefore	M	UTC TIME	
NotAfter	M	UTC TIME	
Issuer	M		
Type	M	OID	
Value	M	UTF8String or PrintableString	
Subject	M		
Type	M	OID	
Value	M	UTF8String or PrintableString	
subjectPublicKeyInfo	M		
Algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
SubjectPublicKey	M	BIT STRING	

IssuerUniqueID	--	---	
SubjectUniqueID	--	---	

3.2.2 CA Certificate Extension Field

Field	Cross		ASN.1 TYPE	NOTE
AuthorityKeyIdentifier	M	NC		
KeyIdentifier	M		OCTET STRING	The hash value of Issuer's pubic key (SHA-1 160bit)
AuthCertIssuer	O		DirectoryName	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
AuthCertSerialNumber	O		INTEGER	
SubejctKeyIdentifier	M	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit)
KeyUsage	M	NC	BIT STRING	Certificate Signing, Off-line CRL Signing, CRL Signing
ExtendedKeyUsage	--			
PrivateKeyUsagePeriod	--			
CertificatePolicies	--			
PolicyIdentifier	--		OID	
PolicyQualifiers	--			
PolicyQualifierId	--			
Qualifier	--			
CPSuri	--			
UserNotice	--			
NoticeRef	--			
Organization	--			
noticeNumber S	--			
ExplicitText	--		VisibleString	
policyMappings	--			
IssureDomainPolicy	--		OID	
SubjectDomainPolicy	--		OID	
SubjectAltName	--			
IssuerAltName	--			
BasicConstraints	M	C		
CA	M		BOOLEAN	
pathLenConstraints	--		INTEGER	The Cross Certificate must not be set.
nameConstraints	--			
permittedSubtrees	--			
base	--		GeneralName	
minimum	--			
maximum	--			
excludedSubtrees	--			
base	--		GeneralName	
minimum	--			
maximum	--			
PolicyConstraints	--			
cRLDistributionPoints	M	NC		
DistributionPoint	M			
FullName	M		URI	
nameRelativeToCRLIssuer	--			
ReasonFlags	--			
CRLIssuer	--			

subjectDirectoryAttributes	--			
AuthorityInfoAccess	--			
accessMethod	--			
accessLocation	--			

3.3 User Certificate

3.3.1 User Certificate Basic Field

Field	EE	ASN.1 TYPE	NOTE
Version	M	INTEGER	V3
SerialNumber	M	INTEGER	$0<n<(2^{32}-1)$
Signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity	M		
NotBefore	M	UTC TIME	
NotAfter	M	UTC TIME	
Issuer	M		
Type	M	OID	
Value	M	UTF8String or PrintableString	
Subject	M		
Type	M	OID	
Value	M	UTF8String or PrintableString	
SubjectPublicKeyInfo	M		
Algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
SubjectPublicKey	M	BIT STRING	
IssuerUniqueID	--	---	
SubjectUniqueID	--	---	

3.3.2 User Certificate Extension Field

Field	EE		ASN.1 TYPE	NOTE
AuthorityKeyIdentifier	M	NC		
KeyIdentifier	M		OCTET STRING	The hash value of Issuer's pubic key (SHA-1 160bit)
AuthCertIssuer	O		DirectoryName	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
AuthCertSerialNumber	O		INTEGER	
SubejctKeyIdentifier	M	NC	OCTET STRING	The value of the Subject's public key (SHA-1 160bit)
KeyUsage	M	NC	BIT STRING	Digital Signature, Key Encipherment
ExtendedKeyUsage	--			
PrivateKeyUsagePeriod	--			
CertificatePolicies	M	NC		
PolicyIdentifier	M		OID	
PolicyQualifiers	--			
PolicyQualifierId	--			
Qualifier	--			
CPSuri	--			
UserNotice	--			
NoticeRef	--			

Organization	--			
noticeNumber S	--			
ExplicitText	--		VisibleString	
policyMappings	--			
IssureDomainPolicy			OID	
SubjectDomainPolicy			OID	
SubjectAltName	--			
IssuerAltName	--			
BasicConstraints	M	NC		
End-Entity	M		BOOLEAN	
pathLenConstraints	M		INTEGER	
nameConstraints	--			
permittedSubtrees				
Base			GeneralName	
Minimum				
Maximum				
excludedSubtrees				
Base			GeneralName	
Minimum				
Maximum				
PolicyConstraints	--			
cRLDistributionPoints	M	NC		
DistributionPoint	M			
FullName	M		URI	
nameRelativeToCRLIssuer	--			
ReasonFlags	--			
CRLIssuer	--			
subjectDirectoryAttributes	--			
AuthorityInfoAccess	--			
accessMethod	--			
accessLocation	--			

3.4 CRL Profile

3.4.1 CRL Basic Field

Field	CRL	ASN.1TYPE	NOTE
version	M	INTEGER	V2
sigature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
issuer	M		
type	M	OID	
vale	M	UTF8String or PrintableString	
thisUpdate	M	UTCTime	
nextUpdate	M	UTCTime	
revokedCertificates	M		
serialNumber	M	INTEGER	
revocationDate	M	UTCTime	

3.4.2 CRL Extension Field

Field	CRL	ASN.1TYPE	NOTE
issureAltName	--		

authorityKeyIdentifier	M	NC		
keyIdentifier	M		OCTET STRING	The hash value of Issuer's public Key (SHA-1 160bit)
authorityCertIssuer	O		UTF8String (DirectoryName)	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
authorityCertSerialNumber	O		INTEGER	
cRLNumber	M	NC	INTEGER	2.5.29.20 (CRL Number)
deltaCRLIndicator	--			
baseCRLNumber	--			
issuingDistributionPoint	--			
distributionPoint	--			When CRLDP is set, the this field must be set as well and the same value is used.
fullName	--		URI	
nameRelativeToCRLIssuer	--			
onlyContainsUserCerts	--		BOOLEAN	
OnlyContainsCACerts	--		BOOLEAN	
onlySomeReasons	--			
indirectCRL	--			

3.4.3 Entry Extension Field

Field	CRL		ASN.1TYPE	NOTE
reasonCode	M	NC	ENUMERATED	
HoldInstructionCode	--			
invalidityDate	--			
certificateIssuer	--			

3.5 ARL Profile

3.5.1 ARL Basic Field

Field	ARL	ASN.1TYPE	NOTE
Version	M	INTEGER	V2
Sigature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Issuer	M		
Type	M	OID	
Vale	M	UTF8String or PrintableString	
thisUpdate	M	UTCTime	
nextUpdate	M	UTCTime	
revokedCertificates	M		
serialNumber	M	INTEGER	
revocationDate	M	UTCTime	

3.5.2 ARL Extension Field

Field	ARL		ASN.1TYPE	NOTE
IssureAltName	--			
authorityKeyIdentifier	M	NC		

KeyIdentifier	M		OCTET STRING	The hash value of Issuer's public Key (SHA-1 160bit)
authorityCertIssuer	O		UTF8String (DirectoryName)	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
authorityCertSerialNumber	O		INTEGER	
CRLNumber	M	NC	INTEGER	2.5.29.20 (CRL Number)
deltaCRLIndicator	--			
baseCRLNumber	--			
issuingDistributionPoint	M	C		2.5.29.28
distributionPoint	M			When CRLDP is set, the this field must be set as well and the same value is used.
FullName	M		URI	
nameRelativeToCRLIssuer	O			
onlyContainsUserCerts	--		BOOLEAN	
OnlyContainsCACerts	M		BOOLEAN	
onlySomeReasons	--			
IndirectCRL	--			

3.5.3 Entry Extension Field

Field	ARL		ASN.1TYPE	NOTE
ReasonCode	M	NC	ENUMERATED	
HoldInstructionCode	--			
invalidityDate	--			
certificateIssuer	--			

4. Japan (Actual Certificate Profile)

4.1 Self-Signed Certificate

4.1.1 Self-Signed Certificate Basic Field

Field	Self	ASN.1 TYPE	NOTE
Version	M	INTEGER	V3(2)
SerialNumber	M	INTEGER	$0<n<2^{128}$
Signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity	M		
NotBefore	M	UTC TIME	
NotAfter	M	UTC TIME	
Issuer	M		
Type	M	OID	
Value	M	UTF8String or PrintableString	
Subject	M		
Type	M	OID	
Value	M	UTF8String or PrintableString	
SubjectPublicKeyInfo	M		
Algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
SubjectPublicKey	M	BIT STRING	
IssuerUniqueID	--	---	
SubjectUniqueID	--	---	

4.1.2 Self-Signed Certificate Extension Field

Field	Self		ASN.1 TYPE	NOTE
AuthorityKeyIdentifier	M	NC		
KeyIdentifier	M		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit)
AuthCertIssuer	O		DirectoryName	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
AuthCertSerialNumber	O		INTEGER	
SubejctKeyIdentifier	M	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit)
KeyUsage	M	C	BIT STRING	key CertSign, cRLSign
ExtendedKeyUsage	--			
PrivateKeyUsagePeriod	--			
CertificatePolicies	O	C		
PolicyIdentifier	O		OID	
PolicyQualifiers	--			
PolicyQualifierId	--			
Qualifier	--			
CPSuri	--			
UserNotice	--			
NoticeRef	--			
Organization	--			
noticeNumber S	--			
ExplicitText	--		VisibleString	

policyMappings	--			
IssureDomainPolicy			OID	
SubjectDomainPolicy			OID	
SubjectAltName	O	NC		
IssuerAltName	O	NC		
BasicConstraints	M	C		
CA	M		BOOLEAN	
PathLenConstraints	O		INTEGER	
nameConstraints	--			
PermittedSubtrees				
Base			GeneralName	
Minimum				
Maximum				
ExcludedSubtrees				
Base			GeneralName	
Minimum				
Maximum				
PolicyConstraints	--			
CRLDistributionPoints	M	NC		
DistributionPoint	M			
FullName	M		URI	
nameRelativeToCRLIssuer	--			
ReasonFlags	--			
CRLIssuer	--			
subjectDirectoryAttributes	--			
AuthorityInfoAccess	O	NC		
AccessMethod	O			
AccessLocation	O			

4.2 CA Certificate

4.2.1 CA Certificate Basic Field

Field	Cross	ASN.1 TYPE	NOTE
Version	M	INTEGER	V3(2)
serialNumber	M	INTEGER	$0<n<2^{128}$
signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
validity	M		
notBefore	M	UTC TIME	
notAfter	M	UTC TIME	
issuer	M		
type	M	OID	
value	M	UTF8String or PrintableString	
subject	M		
type	M	OID	
value	M	UTF8String or PrintableString	
subjectPublicKeyInfo	M		
algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
subjectPublicKey	M	BIT STRING	
issuerUniqueID	--	---	

subjectUniqueID	--	---	

4.2.2 CA Certificate Extension Field

Field	Cross		ASN.1 TYPE	NOTE
AuthorityKeyIdentifier	M	NC		
KeyIdentifier	M		OCTET STRING	The hash value of Issuer's pubic key (SHA-1 160bit)
AuthCertIssuer	O		DirectoryName	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
AuthCertSerialNumber	O		INTEGER	
SubejctKeyIdentifier	M	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit)
KeyUsage	M	C	BIT STRING	Key CertSign, cRLSign
ExtendedKeyUsage	--			
PrivateKeyUsagePeriod	--			
CertificatePolicies	M	C		
PolicyIdentifier	M		OID	
PolicyQualifiers	--			
PolicyQualifierId	--			
Qualifier	--			
CPSuri	--			
UserNotice	--			
NoticeRef	--			
Organization	--			
noticeNumber s	--			
ExplicitText	--		VisibleString	
policyMappings	M	NC		
IssureDomainPolicy	M		OID	
SubjectDomainPolicy	M		OID	
SubjectAltName	--			
IssuerAltName	--			
BasicConstraints	M	C		
CA	M		BOOLEAN	
pathLenConstraints	--		INTEGER	The Cross Certificate must not be set.
nameConstraints	O	C		
permittedSubtrees	O			
base	O		GeneralName	
minimum	--			
maximum	--			
excludedSubtrees	O			
base	O		GeneralName	
minimum	--			
maximum	--			
policyConstraints	O	C		
cRLDistributionPoints	M	NC		
DistributionPoint	M			
fullName	M		URI	
nameRelativeToCRLIssuer	--			
ReasonFlags	--			
cRLIssuer	--			
subjectDirectoryAttributes	--			
AuthorityInfoAccess	O	NC		
accessMethod	O			

accessLocation	O			

4.3 User Certificate

4.3.1 User Certificate Basic Field

Field	EE	ASN.1 TYPE	NOTE
Version	M	INTEGER	V3(2)
SerialNumber	M	INTEGER	$0<n<2^{128}$
Signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity	M		
NotBefore	M	UTC TIME	
NotAfter	M	UTC TIME	
Issuer	M		
Type	M	OID	
Value	M	UTF8String or PrintableString	
Subject	M		
Type	M	OID	
Value	M	UTF8String or PrintableString	
subjectPublicKeyInfo	M		
Algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
subjectPublicKey	M	BIT STRING	
IssuerUniqueID	--	---	
SubjectUniqueID	--	---	

4.3.2 User Certificate Extension Field

Field	EE		ASN.1 TYPE	NOTE
AuthorityKeyIdentifier	M	NC		
KeyIdentifier	M		OCTET STRING	The hash value of Issuer's pubic key (SHA-1 160bit)
AuthCertIssuer	O		DirectoryName	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
AuthCertSerialNumber	O		INTEGER	
SubejctKeyIdentifier	M	NC	OCTET STRING	The value of the Subject's public key (SHA-1 160bit)
KeyUsage	M	C	BIT STRING	digitalSignature
ExtendedKeyUsage	--			
PrivateKeyUsagePeriod	--			
CertificatePolicies	M	NC		
PolicyIdentifier	M		OID	
PolicyQualifiers	O			
PolicyQualifierId	--			
Qualifier	--			
CPSuri	--			
UserNotice	--			
NoticeRef	--			
Organization	--			
noticeNumber s	--			
ExplicitText	O		VisibleString	

policyMappings	--			
IssureDomainPolicy			OID	
SubjectDomainPolicy			OID	
SubjectAltName	O	NC		
IssuerAltName	--			
BasicConstraints	--			
CA	--		BOOLEAN	
pathLenConstraints	--		INTEGER	
nameConstraints	--			
permittedSubtrees				
base			GeneralName	
minimum				
maximum				
excludedSubtrees				
base			GeneralName	
minimum				
maximum				
policyConstraints	--			
cRLDistributionPoints	M	NC		
DistributionPoint	M			
fullName	M		URI	
nameRelativeToCRLIssuer	--			
ReasonFlags	--			
cRLIssuer	--			
subjectDirectoryAttributes	--			
AuthorityInfoAccess	O	NC		
accessMethod	O			
accessLocation	O			

4.4 CRL Profile

4.4.1 Basic Field

Field	CRL	ASN.1TYPE	NOTE
Version	M	INTEGER	V2(1)
Sigature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Issure	M		
Type	M	OID	
Vale	M	UTF8String or PrintableString	
ThisUpdate	M	UTCTime	
NextUpdate	M	UTCTime	
RevokedCertificates	M		
SerialNumber	M	INTEGER	
RevocationDate	M	UTCTime	

4.4.2 Extension Field

Field	CRL		ASN.1TYPE	NOTE
issureAltName	--			
authorityKeyIdentifier	M	NC		
keyIdentifier	M		OCTET STRING	The hash value of Issuer's public Key (SHA-1 160bit)

authorityCertIssuer	O		UTF8String (DirectoryName)	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
authorityCertSerialNumber	O		INTEGER	
cRLNumber	M	NC	INTEGER	
deltaCRLIndicator	--			
baseCRLNumber	--			
issuingDistributionPoint	M	C		
distributionPoint	M			When CRLDP is set, the this field must be set as well and the same value is used.
fullName	M		URI	
nameRelativeToCRLIssuer	O			
onlyContainsUserCerts	M		BOOLEAN	
OnlyContainsCACerts	--		BOOLEAN	
onlySomeReasons	--			
indirectCRL	--			

4.4.3 Entry Extension Field

Field	CRL		ASN.1TYPE	NOTE
reasonCode	M	NC	ENUMERATED	
HoldInstructionCode	--			
invalidityDate	--			
certificateIssuer	--			

4.5 ARL Profile

4.5.1 Basic Field

Field	ARL	ASN.1TYPE	NOTE
Version	M	INTEGER	V2(1)
Sigature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Issure	M		
Type	M	OID	
Vale	M	UTF8String or PrintableString	
ThisUpdate	M	UTCTime	
NextUpdate	M	UTCTime	
revokedCertificates	M		
serialNumber	M	INTEGER	
revocationDate	M	UTCTime	

4.5.2 Extension Field

Field	ARL		ASN.1TYPE	NOTE
IssureAltName	--			
authorityKeyIdentifier	M	NC		

KeyIdentifier	M		OCTET STRING	The hash value of Issuer's public Key (SHA-1 160bit)
authorityCertIssuer	O		UTF8String (DirectoryName)	When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa.
authorityCertSerialNumber	O		INTEGER	
CRLNumber	M	NC	INTEGER	
deltaCRLIndicator	--			
baseCRLNumber	--			
issuingDistributionPoint	M	C		
distributionPoint	M			When CRLDP is set, the this field must be set as well and the same value is used.
FullName	M		URI	
nameRelativeToCRLIssuer	O			
onlyContainsUserCerts	--		BOOLEAN	
OnlyContainsCACerts	M		BOOLEAN	
onlySomeReasons	--			
IndirectCRL	--			

4.5.3 Entry Extension Field

Field	ARL		ASN.1TYPE	NOTE
ReasonCode	M	NC	ENUMERATED	
HoldInstructionCode	--			
InvalidityDate	--			
CertificateIssuer	--			

5. Korea (Actual Profile)

5.1 Self-Signed Certificate

5.1.1 Self-Signed Basic Field

FIELD	Generation	ASN.1 TYPE	Value
Version	M	INTEGER	V3(2)
SerialNumber	M	INTEGER	$0<n<2^{160}$
Signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity			
NotBefore	M	UTC TIME	
NotAfter	M	UTC TIME	
Issuer			
Type	M	OID	If the value is impossible to express in printable string, then UTF8 String is used,
Value	M	UTF8String or PrintableString	
Subject			
Type	M	OID	If the value is impossible to express in printable string, then UTF8 String is used,
Value	M	UTF8String or PrintableString	
subjectPublicKeyInfo			
Algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
subjectPublicKey	M	BIT STRING	
Issuer Unique ID	X		
Subject Unique ID	X		

5.1.2 Self-Signed Extension Field

FIELD	Generation	ASN.1 TYPE	Value
AuthorityKeyIdentifier(non-Critical)			
KeyIdentifier	M	OCTET STRING	Hash Value of Issuer's public key (SHA1-160bit)
SubjectKeyIdentifier(non-Critical)			
KeyIdentifier	M	OCTET STRING	Hash Value of Subject's public key (SHA1-160bit)
KeyUsage (Critical)	M	BIT STRING	KeyCertSign, cRLSign
Private Key Usage Period(non-critical)	X		
CertificatePolicies(both)			
PolicyIdentifier	M		
Policy Mappings (non-Critical)	O		
SubjectAltName (non-Critical)	M	UTF8String	Directory Name
IssuerAltName (non-Critical)	O	UTF8String	Directory Name In actual certificate, we use this field mandatory

SubjectDirectory Attributes (non-Critical)	X		
NameConstraints (Critical)	O		I
Extended Key Usage (both)	O		
BasicConstraints(Critical)			
CA	M	BOOLEAN	TRUE
pathLenConstraint	M	INTEGER	1
PolicyConstraints(Critical)			
requireExplicitPolicy	O	INTEGER	0
cRLDistributionPoints (non-Critical)			
DistributionPoint			
FullName	M		URI:ldap://Host Name:PORT/CRL DN
AuthorityInformation Access(non-Critical)	O		

5.2 CA Certificate

5.2.1 Basic Field

FIELD	Generation	ASN.1 TYPE	Value
Version	M	INTEGER	V3(2)
SerialNumber	M	INTEGER	$0<n<2^{160}$
Signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity			
NotBefore	M	UTC TIME	
NotAfter	M	UTC TIME	
Issuer			
Type	M	OID	If the value is impossible to express in printable string, then UTF8 String is used,
Value	M	UTF8String or PrintableString	
Subject			
Type	M	OID	If the value is impossible to express in printable string, then UTF8 String is used,
Value	M	UTF8String or PrintableString	
subjectPublicKeyInfo			
Algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
subjectPublicKey	M	BIT STRING	
Issuer Unique ID	X		
Subject Unique ID	X		

5.2.2 Extension Field

FIELD	Generation	ASN.1 TYPE	Value
AuthorityKeyIdentifier(non-Critical)			
KeyIdentifier	M	OCTET STRING	Hash Value of Issuer's public key (SHA1-160bit)
SubjectKeyIdentifier(non-Critical)			
KeyIdentifier	M	OCTET STRING	Hash Value of Subject's public key (SHA1-160bit)
KeyUsage (Critical)	M	BIT STRING	KeyCertSign, cRLSign
Private Key Usage Period(non-critical)	X		
CertificatePolicies(both)			
PolicyIdentifier	M		
Policy Mappings (non-Critical)	O		
SubjectAltName (non-Critical)	M	UTF8String	Directory Name
IssuerAltName (non-Critical)	O	UTF8String	Directory Name In actual certificate, we use this field mandatory
SubjectDirectory Attributes (non-Critical)	X		
NameConstraints (Critical)	O		I
Extended Key Usage (both)	O		
BasicConstraints(Critical)			
CA	M	BOOLEAN	TRUE
pathLenConstraint	M	INTEGER	0
PolicyConstraints(Critical)			
requireExplicitPolicy	O	INTEGER	0
cRLDistributionPoints (non-Critical)			
DistributionPoint			
FullName	M		URI:ldap://Host Name:PORT/CRL DN
AuthorityInformation Access(non-Critical)	O		

5.3 User Certificate

5.3.1 Basic Field

FIELD	Generation	ASN.1 TYPE	Value
Version	M	INTEGER	V3(2)
serialNumber	M	INTEGER	$0<n<2^{160}$
Signature	M	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity			
notBefore	M	UTC TIME	
notAfter	M	UTC TIME	
Issuer			
Type	M	OID	If the value is impossible to express in printable string, then UTF8 String is used,
Value	M	UTF8String or PrintableString	
Subject			
Type	M	OID	If the value is impossible to express in printable string, then UTF8 String is used,
Value	M	UTF8String or PrintableString	
subjectPublicKeyInfo			
Algorithm	M	OID	1.2.840.113549.1.1.1 (rsaEncryption)
subjectPublicKey	M	BIT STRING	
Issuer Unique ID	X		
Subject Unique ID	X		

5.3.2 Extension Field

FIELD	Generation	ASN.1 TYPE	Value
AuthorityKeyIdentifier(non-Critical)			
KeyIdentifier	M	OCTET STRING	Hash Value of Issuer's public key (SHA1-160bit)
SubjectKeyIdentifier(non-Critical)			
KeyIdentifier	M	OCTET STRING	Hash Value of Subject's public key (SHA1-160bit)
KeyUsage (Critical)	M	BIT STRING	KeyCertSign, cRLSign
Private Key Usage Period(non-Critical)	X		
CertificatePolicies(both)			
PolicyIdentifier	M		
Policy Mappings (-)	-		
SubjectAltName (non-Critical)	M	UTF8String	Directory Name
IssuerAltName (non-Critical)	O	UTF8String	Directory Name In actual certificate, we use this field mandatory
SubjectDirectory Attributes (non-Critical)	X		
NameConstraints(-)	-		I
Extended Key Usage (both)	O		
BasicConstraints (Critical)	X		0
PolicyConstraints (-)	-		
cRLDistributionPoints (non-Critical)			
DistributionPoint			
FullName	M		URI:ldap://Host Name:PORT/CRL DN
AuthorityInformation Access(non-Critical)	O		

5.4 CRL Profile

5.4.1 Basic Field

Field	Generation	ASN.1 TYPE	Value
version	M	INTEGER	V2(1)
sigature	M	OID	1.2.840.113549.1.1.5 sha1WithRSAEncryption
Issure	M		
Type	M	OID	
Vale	M	UTF8String or PrintableString	If the value is impossible to express in printable string, then UTF8 String is used,
thisUpdate	M	UTCTime	
nextUpdate	M	UTCTime	
revokedCertificates	M		
User Certificates	M	INTEGER	If there is no revoked certificates, this filed isn't used
RevocationDate	M	UTCTime	
CRLEntryExt	M		

5.4.2 Extension Field

FIELD	Genearation	ASN.1 TYPE	Value
AuthorityKeyIdentifier(non-Critical)			
KeyIdentifier	M	OCTET STRING	Hash Value if Issuer's public-key(SHA1-160bit)
Issue Alt Name (non-Critical)	O		
CRLNumber (non-Critical)	M	INTEGER	
IssuerDistribution Point(Critical)	O		

5.4.3 Entry Extension Field

FILED	Generation	ASN.1 TYPE	Value
reasonCode (critical)	M	ENUMERATED	
HoldInstructionCode (non-Critical)	O		
Invalidity Date (non-Critical)	O		
Certificate Issuer (Critical)	O		

Appendix 4: Recommended Certificate and CRL profile.

(M: Mandatory, ---: Not-defined, O: Optional, C: Critical, NC: Non-Critical, JP/J: Japan, KR/K: Korea, SG/S: Singapore)

1. Self-Signed Certificate.

1.1 Basic Fields

Fields	JP	KR	SG	Type of ASN.1	Evaluation	Note
version	M	M	M	INTEGER	Common	v3(2)
serialNumber	M	M	M	INTEGER	Common See Note	J: Up to 16 octets (JCSI Profile) K: Up to 16 octets for generation and up to 20 octets for processing. S: There is especially such a requirement identified
signature	M	M	M	OID	Common	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
validity	M	M	M		Common	
notBefore	M	M	M	UTC TIME		
notAfter	M	M	M	UTC TIME		
issuer	M	M	M		Common	
Type	M	M	M	OID		
Value	M	M	M	UTF8String or PrintableString		PrintableString is used for Country attribute
subject	M	M	M		Common	
Type	M	M	M	OID		
Value	M	M	M	UTF8String or PrintableString		PrintableString is used for Country attribute.
subjectPublicKeyInfo	M	M	M		Common	
Algorithm	M	M	M	OID		1.2.840.113549.1.1.1 (rsaEncryption)
subjectPublicKey	M	M	M	BIT STRING		2048 bit
issuerUniqueID	---	---	---	---	Common	
subjectUniqueID	---	---	---	---	Common	

1.2 Extension Fields

	Fields	JP		KR		SG		Type of ASN.1	Evaluation	Note
	AuthorityKeyIdentifier	M	NC	M	NC	M	NC		Common	
	KeyIdentifier	M		M		M		OCTETSTRING		The hash value of Issuer's pubic key (SHA-1 160bit: The 1st calculation method in RFC2459 ch.4.2.1.2)
	AuthCertIssuer	O		O		O		directoryName		When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa
	AuthCertSerialNumber	O		O		O		INTEGER		
	SubejctKeyIdentifier	M	NC	M	NC	M	NC	OCTET STRING	Common	The value of the Subject's public key (SHA-1 160bit: The 1st calculation method in RFC2459 ch. 4.2.1.2)
	KeyUsage	M	C	M	C	M	NC	BIT STRING	Different	keyCertSign, cRLSign J,K: This extension appears as a critical extension. S: This extension appears as a non-critical extension. RFC2459: When used, this extension SHOULD be marked critical.
	ExtendedKeyUsage	—	—	—	—	—	—		Common	
	PrivateKeyUsagePeriod	—	—	—	—	—	—		Common	
	CertificatePolicies	O	C	M	C	—	—		Different	J: This extension appears as a critical extension when used. In the requirement of Japanese GPKI, this filed MUST NOT appear. K: This extension must appear as critical. S: Not-defined
	PolicyIdentifier	O		M		—		OID		
	PolicyQualifiers	—		O		—				JS: Not-defined K: Generation of this field is optional.
	CPSuri	—		O		—		IA5String		JS: Not-defined K: Generation of this field is optional.
	UserNotice	—		—		—				
	NoticeRef	—		—		—				
	ExplicitText	—		—		—				
	PolicyMappings	—	—	—	—	—	—		Common	
	IssureDomainPolicy	—		—		—				
	SubjectDomainPolicy	—		—		—				
	SubjectAltName	O	NC	O	NC	—	—		Different	J: In the requirement of Japanese GPKI, this filed MUST NOT appear. K: This extension can be used when indicating other names of subject organization S: Not-defined

	IssuerAltName	O	NC	O	NC	—	—		Different	J: In the requirement of Japanese GPKI, this filed MUST NOT appear. K: This extension can be used when indicating other names of issuer organization S: Not-defined

	BasicConstraints	M	C	M	C	M	NC		Different	JK: This extension appears as a critical extension. S: This extension appears as a non-critical extension. RFC2459: MUST appear as a critical extension
	CA	M		M		M		BOOLEAN		TRUE
	PathLenConstraints	O		—		O		INTEGER		JS: Using this extension is optional K : Self-signed certificate has no limit for path length.
	NameConstraints	—	—	—	—	—	—		Common	
	PermittedSubtrees	—		—		—				
	Base	—		—		—		GeneralName		
	Minimum	—		—		—		INTEGER		
	Maximum	—		—		—		INTEGER		
	ExcludedSubtrees	—		—		—				
	Base	—		—		—		GeneralName		
	Minimum	—		—		—		INTEGER		
	Maximum	—		—		—		INTEGER		
	PolicyConstraints	—	—	—	—	—	—		Common	
	RequireExplicitPolicy	—		—		—				
	InhibitPolicyMapping	—		—		—				
	CRLDistributionPoints	M	NC	M	NC	M	NC		Common	
	DistributionPoint	M		M		M				
	FullName	M		M		M		directoryName or URI		J : DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be th must be the same value K : DistributionPoint names must have at least one name value same as that in CRL/ARL, to avoid substitution attack.
	nameRelativeToCRLIssuer	—		—		—				
	ReasonFlags	—		—		—				
	CRLIssuer	—		—		—				
	subjectDirectoryAttributes	—	—	—	—	—			Common	
	AuthorityInfoAccess	—	—	—	—	—	—		Common	
	AccessMethod	—		—		—				
	AccessLocation	—		—		—				

2. Cross Certificate.

2.1 Basic Fields

Fields	JP	KR	SG	Type of ASN.1	Evaluation	Note
Version	M	M		INTEGER	Common	v3(2)
SerialNumber	M	M		INTEGER	Common See Note	J: up to 16 octets (JCSI Profile) K: Up to 16 octets for generation and up to 20 octets for processing S: There is not specified
Signature	M	M		OID	Common	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity	M	M			Common	
NotBefore	M	M		UTC TIME	Common	
NotAfter	M	M		UTC TIME	Common	
Issuer	M	M			Common	
Type	M	M		OID	Common	
Value	M	M		UTF8String or PrintableString	Common	PrintableString is used for Country attribute.
Subject	M	M			Common	
Type	M	M		OID	Common	
Value	M	M		UTF8String or PrintableString	Common	PrintableString is used for Country attribute.
subjectPublicKeyInfo	M	M			Common	
Algorithm	M	M		OID	Common	1.2.840.113549.1.1.1 (rsaEncryption)
SubjectPublicKey	M	M		BIT STRING	Common	2048 bit
IssuerUniqueID	---	---		---	Common	
SubjectUniqueID	---	---		---	Common	

2.2 Extension Fields

	Fields	JP		KR		SG	Type of ASN.1	Evaluation	Note
	authorityKeyIdentifier	M	NC	M	NC			Common	
	KeyIdentifier	M		M			OCTETSTRING		The hash value of Issuer's pubic key (SHA-1 160bit: The 1st calculation method in RFC2459 ch.4.2.1.2)
	AuthCertIssuer	O		O			directoryName		When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa
	authCertSerialNumber	O		O			INTEGER		
	subejctKeyIdentifier	M	NC	M	NC		OCTETSTRING	Common	The value of the Subject's public key (SHA-1 160bit: The 1st calculation method in RFC2459 ch. 4.2.1.2)
	KeyUsage	M	C	M	C		BITSTRING	Common	keyCertSign, cRLSign
	ExtendedKeyUsage	—	—	—	—			Common	
	privateKeyUsagePeriod	—	—	—	—			Common	
	CertificatePolicies	M	C	M	C			Different	J,K: This extension must appear as a critical.
	policyIdentifier	M		M			OID		
	policyQualifiers	—		O					J: Not-defined K: Generation of this field is optional.
	CPSuri	—		O					J: Not-defined K: Generation of this field is optional.
	userNotice	—		O					J: Not-defined K: Generation of this field is optional.
	noticeRef	—		—					
	explicitText	—		O			K : BMPString		J: Not-defined K: Using this extension is optional. When it appears, BMPString will be used to represent 2 byte characters.
	PolicyMappings	M	NC	M	NC			Common	
	issureDomainPolicy	M		M					
	subjectDomainPolicy	M		M					
	SubjectAltName	—	—	O	NC			Different	J: Not-defined K: This extension can be used when indicating other names of subject organization
	IssuerAltName	—	—	O	NC			Different	J: Not-defined K: This extension can be used when indicating other names of issuer organization

	Fields	JP		KR		SG	Type of ASN.1	Evaluation	Note
	BasicConstraints	M	C	M	C			Different	
	CA	M		M			BOOLEAN		
	PathLenConstraints	—		O			INTEGER		K: This extension can be used to avoid unexpected extension of cross certification.
	NameConstraints	O	C	O	C			Common	
	PermittedSubtrees	O		O					
	Base	O		O			GeneralName		
	Minimum	—		—			INTEGER		
	Maximum	—		—			INTEGER		
	ExcludedSubtrees	O		O					
	Base	O		O			GeneralName		
	Minimum	—		—			INTEGER		
	Maximum	—		—			INTEGER		
	PolicyConstraints	O	C	O	C			Common	
	requireExplicitPolicy	O		O					
	inhibitPolicyMapping	O		O					
	CRLDistributionPoints	M	NC	M	NC			Common	
	DistributionPoint	M		M					
	FullName	M		M			directoryName or URI		J : DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be the same value. K : This DistributionPoint names must have at least one name value same as that in CRL/ARL, to avoid substitution attack.
	nameRelativeToCRLIssuer	—		—					
	ReasonFlags	—		—					
	CRLIssuer	—		—					
	subjectDirectoryAttributes	—	—	—	—			Common	
*	AuthorityInfoAccess	—	—	—	—			Common	
	AccessMethod	—		—					
	AccessLocation	—		—					

3. End-Entity Certificate

3.1 Basic Fields

Fields	JP	KR	SG	Type of ASN.1	Evaluation	Note
Version	M	M	M	INTEGER	Common	v3(2)
SerialNumber	M	M	M	INTEGER	Common see Note	J: up to 16 octets (JCSI Profile) K: Up to 16 octets for generation and up to 20 octets for processing S: There is especially no regulation about a value.
Signature	M	M	M	OID	Common	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
Validity	M	M	M		Common	
NotBefore	M	M	M	UTC TIME	Common	
NotAfter	M	M	M	UTC TIME	Common	
Issuer	M	M	M		Common	
Type	M	M	M	OID	Common	
Value	M	M	M	UTF8String or PrintableString	Common	PrintableString is used for Country attribute.
Subject	M	M	M		Common	
Type	M	M	M	OID	Common	
Value	M	M	M	UTF8String or PrintableString	Common	PrintableString is used for Country attribute.
subjectPublicKeyInfo	M	M	M		Common	
Algorithm	M	M	M	OID	Common	1.2.840.113549.1.1.1 (rsaEncryption)
SubjectPublicKey	M	M	M	BIT STRING	Common	1024 bit
IssuerUniqueID	---	---	---	---	Common	
SubjectUniqueID	---	---	---	---	Common	

3.2 Extension Fields

	Fields	JP		KR		SG		Type of ASN.1	Evaluation	Note
	authorityKeyIdentifier	M	NC	M	NC	M	NC		Common	
	keyIdentifier	M		M		M		OCTETSTRING		The hash value of Issuer's pubic key (SHA-1 160bit: The 1st calculation method in RFC2459 ch.4.2.1.2)
	authCertIssuer	O		O		O		directoryName		When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa
	authCertSerialNumber	O		O		O		INTEGER		
	subejctKeyIdentifier	M	NC	M	NC	M	NC	OCTETSTRING	Common	The value of the Subject's public key (SHA-1 160bit: The 1st calculation method in RFC2459 ch. 4.2.1.2)
	KeyUsage	M	C	M	C	M	NC	BITSTRING	Different	J : digitalSignature K : digitalSignature, nonRepudiation J,K: This extension appears as a critical extension. S: This extension appears as a non-critical extension. RFC2459: When used, this extension SHOULD be marked critical.
	extendedKeyUsage	—	—	—	—	—	—		Common	
	privateKeyUsagePeriod	—	—	—	—	—	—		Common	
	certificatePolicies	M	NC	M	C	—	—		Different	J: This extension appears as a non-critical extension. K: This extension must appear as critical. S: Not-defined
	policyIdentifier	M		M		—		OID		
	policyQualifiers	O		O		—				S: Not-defined JK: Generation of this field is optional.
	CPSuri	—		O		—				J,S: Not-defined K: Generation of this field is optional.
	userNotice	O		O		—				S: Not-defined J,K: Generation of this field is optional.
	noticeRef	—		—		—				
	explicitText	O		O		—		J : VisibleString K : BMPString		S: Not-defined J, K: Using this extension is optional. When it appears, Japan uses VisibleString, but Korea uses BMPString to represent 2 byte characters.
	policyMappings	—	—	—	—	—			Common	
	issureDomainPolicy	—		—		—				

	subjectDomainPolicy	—		—		—				
	subjectAltName	O	NC	M	NC	—	—		Different	J: In the requirement of Japanese GPKI, this filed MUST NOT appear. K: This extension must appear to indicate personal identifier. S: Not-defined
	IssuerAltName	—	—	O	NC	—	—		Different	J: In the requirement of Japanese GPKI, this filed MUST NOT appear. K: This extension can be used when indicating other names of issuer organization

	Fields	JP		KR		SG		Type of ASN.1	Evaluation	Note
	BasicConstraints	—	—	—	—	M	NC		Different	JK: Not-defined S: MUST appear RFC2459: This extension SHOULD NOT appear in end entity certificates.
	CA	—		—		M		BOOLEAN		
	pathLenConstraints	—		—		O		INTEGER		JK: Not-defined S: Generation of this field is optional.
	NameConstraints	—	—	—	—	—	—		Common	
	permittedSubtrees	—		—		—				
	Base	—		—		—				
	Minimum	—		—		—				
	Maximum	—		—		—				
	excludedSubtrees	—		—		—				
	Base	—		—		—				
	Minimum	—		—		—				
	Maximum	—		—		—				
	PolicyConstraints	—	—	—	—	—	—		Common	
	requireExplicitPolicy	—		—		—				
	inhibitPolicyMapping	—		—		—				
	cRLDistributionPoints	M	NC	M	NC	M	NC		Common	
	distributionPoint	M		M		M				
	FullName	M		M		M		directoryName or URI		J : DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be the same value. K : This DistributionPoint names must have at least one name value same as that in CRL/ARL, to avoid substitution attack.
	nameRelativeToCRLIssuer	—		—		—				
	ReasonFlags	—		—		—				
	CRLIssuer	—		—		—				
	SubjectDirectoryAttributes	—	—	—	—	—			Common	
	AuthorityInfoAccess	O	NC	M	NC	—	—		Different	JK: Generation of this field is optional. S: Not-defined

	AccessMethod	O		M		—		OID : id-ad-caIssuers		~~J~~K: Generation of this field is optional. K : This extension must be used to aid the certificate path construction. S: Not-defined
	AccessLocation	—		M		—		URI		K : The matching repository location will be described J,S: Not-defined

4. CRL & ARL

4.1 CRL/ARL Basic Field

Fields	JP	KR	SG	Type of ASN.1	Evaluation	Note
version	M	M	M	INTEGER	Common	v2(1)
signature	M	M	M	OID	Common	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
issuer	M	M	M		Common	
type	M	M	M	OID		
value	M	M	M	UTF8String or PrintableString		PrintableString is used for Country attribute.
thisUpdate	M	M	M	UTC TIME	Common	
nextUpdate	M	M	M	UTC TIME	Common	J: thisUpdate + 7days K: CRL update period varies according to CA's practice.
revokedCertificates	M	M	M		Common	
serialNumber	M	M	M	INTEGER		
revocationDate	M	M	M	UTC TIME		

4.2 CRL/ARL Entry Extensions

Fields	JP		KR		SG		Type of ASN.1	Evaluation	Note
reasonCode	M	NC	M	NC	M	NC	ENUMERATED	Common	
holdInstructionCode	—	—	—	—	—	—	OID	Common	
invalidityDate	—	—	O	NC	M	NC	GeneralizedTime	Different	J: Not-defined K: Generation of this field is optional. S: MUST appear
certificateIssuer	—	—	—	—	—	—		Common	

4.3 CRL/ARL Extension Fields

Fields	JP		KR		SG		Type of ASN.1	Evaluation	Note
authorityKeyIdentifier	M	NC	M	NC	M	NC		Common	
keyIdentifier	M		M		M		OCTETSTRING		The hash value of Issuer's pubic key (SHA-1 160bit: The 1st calculation method in RFC2459 ch.4.2.1.2)
authorityCertIssuer	O		O		O		UTF8STRING (DirectoryName)		When AuthCertIssuer is used, AuthCertSerialNumber must be set as well. Vise versa
authorityCertSerialNumber	O		O		O		INTEGER		
cRLNumber	M	NC	M	NC	M	NC	INTEGER	Common	
deltaCRLIndicator	—	—	–	–	—	—		Common	
baseCRLNumber	—		–		—				
issuingDistributionPoint	O	C	O	C	—	—		Different	S: Not-defined J,K: Generation of this field is optional. J: Under Japan's GPKI requirements, this field MUST appear.
distributionPoint	M		O		—				S: Not-defined J: MUST appear K : Generation of this field is optional
FullName	M		O		—		DirectoryName or URI		J : DistributionPoint of issuingDistributionPoint in CRL/ARL and CRLDP must be the same value. K : When this extension appears, DistributionPoint names must have at least one name value same as DistributionPoint names under processing to avoid substitution attack.. S: Not-defined J: MUST appear
nameRelativeToCRLIssuer	O		–		—				
OnlyContainsUserCerts	M(CRL)		O(CRL)		—		BOOLEAN		S: Not-defined J: MUST appear. K: When the issuer issues ARL and CRL separately, this extension can be used to distinguish them.
OnlyContainsCACerts	M(ARL)		O(ARL)		—		BOOLEAN		S: Not-defined J: MUST appear K: When the issuer issues ARL and CRL separately, this field can be used to distinguish them.
OnlySomeReasons	—		–		—				
IndirectCRL	—		–		—				