付録 2

PKI アプリケーションに関する標準

付録 2-1

パス検証テストガイドライン

JKST-IWG

Path Processing Testing Guideline

Ver 1.0

Mar 07, 2003

- CHANGES -

Version	Date	Comments	Detail
1.0	20030228	Published	First Edition

- Table of Contents -

1 Introduction

1.1 Background

The Interoperability Working Group (IWG), formed by Japan, Korea, and Singapore members, completed the multi PKI domains interoperability experiment[1]. In the experiment, the IWG established a CA-CA model with the Certificate and CRL and LDAP schema profile[2] to be interoperable each other.

Even though the different policies and trust models exist in each nation, the IWG successfully finished the interoperability tests and obtained some levels of confidence that an emerging framework could be possible. Trust models could be absorbed and/or coexist if a certificate and its chains are processed at the agreeable ways.

One of the lessons learnt from the project was that there are few frameworks, criteria, and even guidelines that all parties could be able to agree upon in terms of path processing test suites to evaluate the results each other. This difficulty stems largely from the fact that different PKI vendors have different testing methods and different PKI domains have different requirements in their own trust models.

In the multi PKI domain interoperability (especially different vendors in different countries involved), when no levels of conformance are guaranteed in terms of path processing, it would be difficult to ensure a Relying Party application in one country will validate the certificate and its path in the same way that the other does in other countries, and it would be hard to achieve the reliable infrastructure where secure business transactions are conducted.

Therefore, common agreeable test suites and the guideline should be created as criteria to check and verify the path processing logic in applications for the PKI environments, where the multiple CA topology and trust models could

---

[1] Achieving PKI Interoperability
Results of the JKS-IWG Interoperability project
http://www.japanpkiforum.jp/shiryou/IPA/final.pdf

[2] Achieving PKI Interoperability
Results of the JKS-IWG Interoperability project
Recommendations on Technical Certificate Profile
http://www.japanpkiforum.jp/shiryou/IPA/final_2pdf.pdf

coexist.

1.2 Objectives

The objective of this document is to test the path validation processing logic in the Relying Party (RP) application and certificate-issuance capabilities in the Certification Authority (CA) application. With this guideline, potential PKI users and service providers can evaluate applications, especially the RP application in the path processing logic function, which is crucial and critical to the trustworthiness of the PKI operations in business environments. By developing this document, the IWG will facilitate the CA-CA interoperability in multiple domains so as to ensure that each relying party can validate the certificates in the same fashion each other.

1.3 Intended Audience

This guideline is developed for the application vendors, PKI users, and service provides who actually uses the PKI applications for their businesses to ensure that the targeted applications can validate the certificates followed by the requirements derived from the IWG certificate and CRL profile.

2 Path Processing Test Pattern

2.1 Test Framework

2.1.1 Test Design Fundamental

This document is developed based on the path processing logic of RFC3280[3] specification, a subset of X.509[4] standard, test reference 'Conformance Testing of Relying Party Client Certificate Path Processing Logic'[5], and the requirements derived from the standards and IWG Certificate and CRL Profile.

---

[3] RFC3280
Internet X.509 Public Key Infrastructure: Certificate and CRL Profile
http://www.ietf.org/rfc/rfc3280.txt

[4] ITU-T RECOMMENDATION X.509 | ISO/IEC 9594-8:
"INFORMATION TECHNOLOGY - OPEN SYSTEMS INTERCONNECTION
- THE DIRECTORY: PUBLIC-KEY AND ATTRIBUTE CERTIFICATE FRAMEWORKS"

[5] Conformance Testing of Relying Party Client Certificate Path Processing Logic, 2001 v1.07
http://csrc.nist.gov/pki/testing/x509paths.html

The specifications and requirements are used as a basis for test items necessary to evaluate the RP applications for targeted PKI architectures and services.

With the specifications and requirements, this guideline has two features:

1) Test is categorized more from the PKI user side.
2) Test can be used combining several test models.

The test is categorized based on the users' and service providers' perspectives rather than application developers' perspectives. The test is structured, more considering the PKI service environment for the users/service provider to evaluate the application easier. When the user/service provides plan to use the PKI, they are typically required to design the certification authority structure in **interconnection model**. They also need to decide the **service model** such as integrity and authentication services. In addition, they need to consider **revocation model** that checks the certificate status information. So that the testing framework should be categorized followed by the models where the users and service providers will be based on.

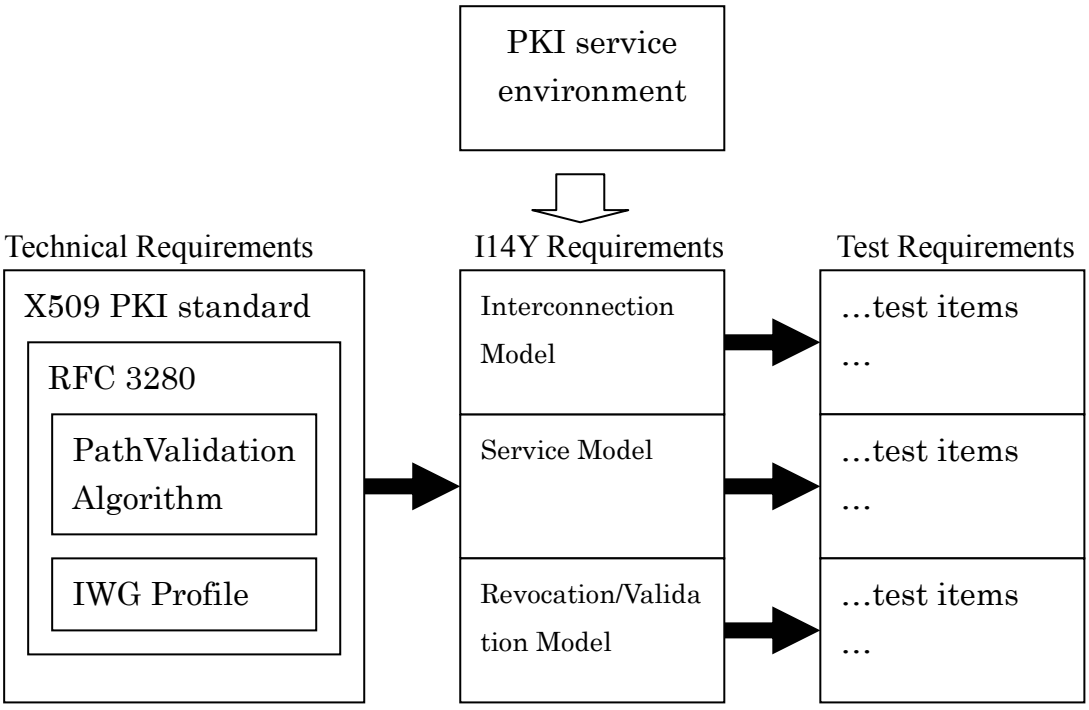

Figure 2.1 Extracting Test Items

Figure 2.1 shows the overall picture of the test designs and workflow. First, the technical requirements are identified in the path processing logic in the

RFC3280 and IWG Certificate and CRL Profile. Then the technical requirements are mapped to the three models, the interconnection model, the service model, and the revocation/validation model, generating a minimum set of the I14Y requirements. Finally each model generates test scenarios and test items to satisfy them.

A test item is an individual test case with a collection of inputs that cause one execution of an application. A set of test items is designed to cover an individual test requirement and can be divided into the success cases and failure cases. NOTE: The case generation depends on the ASN.1 structures of the certificate fields and the requirement of the specification and IWG Certificate and CRL Profile.

The test is conducted using the black box-based testing method, which means that there are several test values used for testing. The test case value is the essential part of testing. As the prefix values to trigger each test, several certificates, CRL/ARL and several initial parameters are provided. In the data, each test case contains verifiable value(s), which are to be evaluated by comparing the output of the application with the expected value or/and test scenario (success or failure) in the document.

In testing, the test planners can combine the models among the interconnection, service, and revocation/validation models to meet their specific requirements in the PKI environment currently concerned.

2.1.2 Test Scope

The test scope includes testing based on the following models:

Table 2.1 Test Models

MODEL	DETAILS
Base	Base
Interconnection Model	Strict Hierarchy
	Cross Certification
	Cross Recognition
	Bridge CA
	Mesh
	Certificate Trust Lists

	Accreditation Certificate
Service Model	Signing
	Encryption
	Authentication
	Notary
Revocation & Validation Model	CRL
	OCSP
	Delegated Path Discovery/Validation

For the base model, it is for the general test cases. For the interconnection model, there are several CA-CA architectures, strict hierarchy, Cross Certification (CC), Cross Recognition (CR), Bridge CA, Mesh, Certificate Trust Lists, and Accreditation Certificate are assumed. For the service models, signing, encryption, authentication, and notary are assumed. For the revocation & validation model, the CRL, OCSP and Delegated Path Discovery/Validation(DPD/DPV)[6] models are included. All the details in the assumptions of the models will be described in clause 2.3.

The scope also includes the testing whether the certificate and CRL have been generated in accordance with the IWG profile. This guideline specifies the requirements of the CA applications and test items.

The scope, however, excludes testing of the Relying Party application to parse ASN.1 structure correctly. This guideline does not include testing of the low level of crypto operations either.

2.1.3 Assumptions

1. The encryption, authentication, and notary services are currently out of scope in this document.

2. The bridge CA model is currently out of scope in this document. However, there are several test items to check the path length in the cross certification model via an anchor CA. In the model, the anchor

[6] RFC3379
Delegated Path Validation and Delegated Path Discovery Protocol Requirements
http://www.ietf.org/rfc/rfc3379.txt

CA can be treated as a Bridge CA to be connected with the other CAs.

3. The OCSP model is currently out of scope in this document.

4. The Cross certification model assumes that the root CA (in the hierarchy) is cross-certifying the other CAs and vice versa. No subordinate CAs are cross-certifying the other CAs.

5. The path processing logic used in this document is derived from RFC3280.

6. The Trust Anchor CA is not used in the certification path. The trust anchor information is used as only input values specified in the RFC 3280.

7. The certificates and corresponding CRLs are signed with the same Certification Authority with the same key.

8. No values are tested in the following extensions…
   - privateKeyUsagePeriod
   - subjectAltName
   - issuerAltName
   - subjectDirectoryAttributes
   - extendedKeyUsage
   - inhibitAnyPolicy
   - freshestCRL
   - authorityInfoAccess
   - subjectInfoAccess

9. No test cases for criticality to save labor, but only critical extensions which defined locally in IWG profile, has test case for criticality.

2.1.4 Test Levels

The testing level indicates how much the application will be interoperable and secure.

The level 0 assumes that the CA application must issue certificates and CRL/ARL, which contains the mandatory fields in IWG profile, and the RP application must validate the components. The tester must run this test and

pass the test. Note that the document typically presumes that the RP application already test this level in the software development stage.

The level 1 assumes that the CA application must issue certificates and CRL/ARL, which contains the optional fields in IWG profile and the RP application must validate the components if necessary. The tester should run this test.

The level 2 assumes that the CA application will specify the multiple values and constraint-related fields in the certificates (such as Policy Constraints and Name Constraints) and the RP application will validate the components. The tester may run this test. Table 2.2 summarizes the test levels.

Table 2.2 Definition of Test Level

Level	Criteria	Description
0	Certificate Issuance	Specify mandatory fields in IWG profile
	Validation Requirements	MUST run this test (or MUST pass in the system test before this guideline is applied)
1	Certificate Issuance	Specify optional fields in IWG profile
	Validation Requirements	SHOULD run this test
2	Certificate Issuance	Specify multiple values and constraints-related values in IWG profile
	Validation Requirements	MAY run this test

2.1.5 Document Conventions

Each test items is specified using the following convention. The interconnection model (**Int**), service model (**Srv**), and revocation model (**Rvk**) contain the categories such as Cross Certification (**CC**) in the interconnection model and Signing (**DS**) in the service model. In the categories, there are test items for Relying Party (**RP**) and Certification Authority (**CA**) applications. Each test item has the number with the test level. The examples are shown below.

- Int.CC.RP.22.Level 0

- Srv.DS.RP.22.Level 1
- Rvk.CRL.RP.25.Level 0

2.1.6 Usage of This Guideline

(1) Outline of this guideline

Specification of path validation, especially in multi-domain PKI, is complex much. Therefore, various PKI applications cannot always implement full path validation function. In multi-domain PKI, it is essential that skilled understanding about path validation whether a PKI application has enough function, because "**What kind of path validation function is required**" and "**How to evaluate**" are vary by each multi-domain PKI. Here issues are what they must need to assess below rightly, and what is difficult.

- Analysis of multi-domain PKI
- Required path validation function
- Expected and right validation result

This clears away such difficulty, and provides a framework for evaluating the path validation function of PKI application in multi-domain PKI without skilled understanding.

Therefore, at first, this defines typical PKI model to analyze multi-domain PKI easily. The guideline users understand easily which model matches each domain, by reference to typical PKI model.

At second, the guideline defines the testing requirements which is necessary for each domain, by extracting from the standards (e.g., ISO/ITU-T and IETF/PKIX and etc.), and set the right expected results. From this, users can learn required testing items and evaluation method easily for their domain.

(a) Definition of PKI model

If some PKI domains, which are operated by each unique security policy, interconnect mutually and provide a service astride both domains, this guideline is as reference for the PKI domains.

This guideline defines the typical PKI model as single PKI domain and a kind of interconnecting. Therefore, these models may correspond to many existing PKI domains. The guideline users can make use of these models as a material for analysis when they interconnect each other.

- What kind of model is my PKI domain?
- What kind of model is a destination PKI domain?

- What is an appropriate model for interconnecting both?
- Etc.

Furthermore, they can also make use of this as material for analysis when they provide a service astride interconnected domains.

- What requirement should they satisfy?
- What information should they process?
- Etc.

This guideline is classified from three viewpoints below to refer easily.

(a) Interconnection method
(b) Service pattern
(c) Path validation method

The users can refer to a necessary model by each viewpoint (a) to (c).

(i) Interconnection model

Users can make use of this as reference when they understand what kind of model their domain or destination domain is, or what is an appropriate model to interconnect mutually or unilaterally. This defined the requirements to establish for each model.

(ii) Revocation and Validation model

Users can make use of this as reference when they understand what kind of revocation information other domain provides, or what kind of revocation information they must process. And this may define what kind of protocol they need to access with the validation server, when it comes onstage in the future.

(iii) Service model

Users can make use of this as reference to learn what kind of service is feasible or what a requirement for the service is.

Specifically, they become able to consider easily the questions shown below.

- What is an appropriate model for interconnecting mutually or unilaterally?
- What service can we provide by interconnection?
- What is a necessary method for certificate/path validation of the destination domain?

(b) Definition and application of the testing criteria

This defines the test criteria which are based on IWG recommended profile. Users can confirm easily and systematically whether their profile is based on IWG recommended profile by meeting these criteria. Also Users can understand easily how compliant with IWG recommended profile, because test level is setting to each test-case.

This is criteria for IWG recommendation profile, but almost is the requirement for standard (X.509 or RFC3280 and so on). So this can apply as criteria of another framework by readjusting test level slightly, not only IWG. For example, when it is made as GPKI criteria, they assign the GPKI minimal requirement as level 0, and assign the other requirement as level 1 or higher. Then they can make the guideline for GPKI.

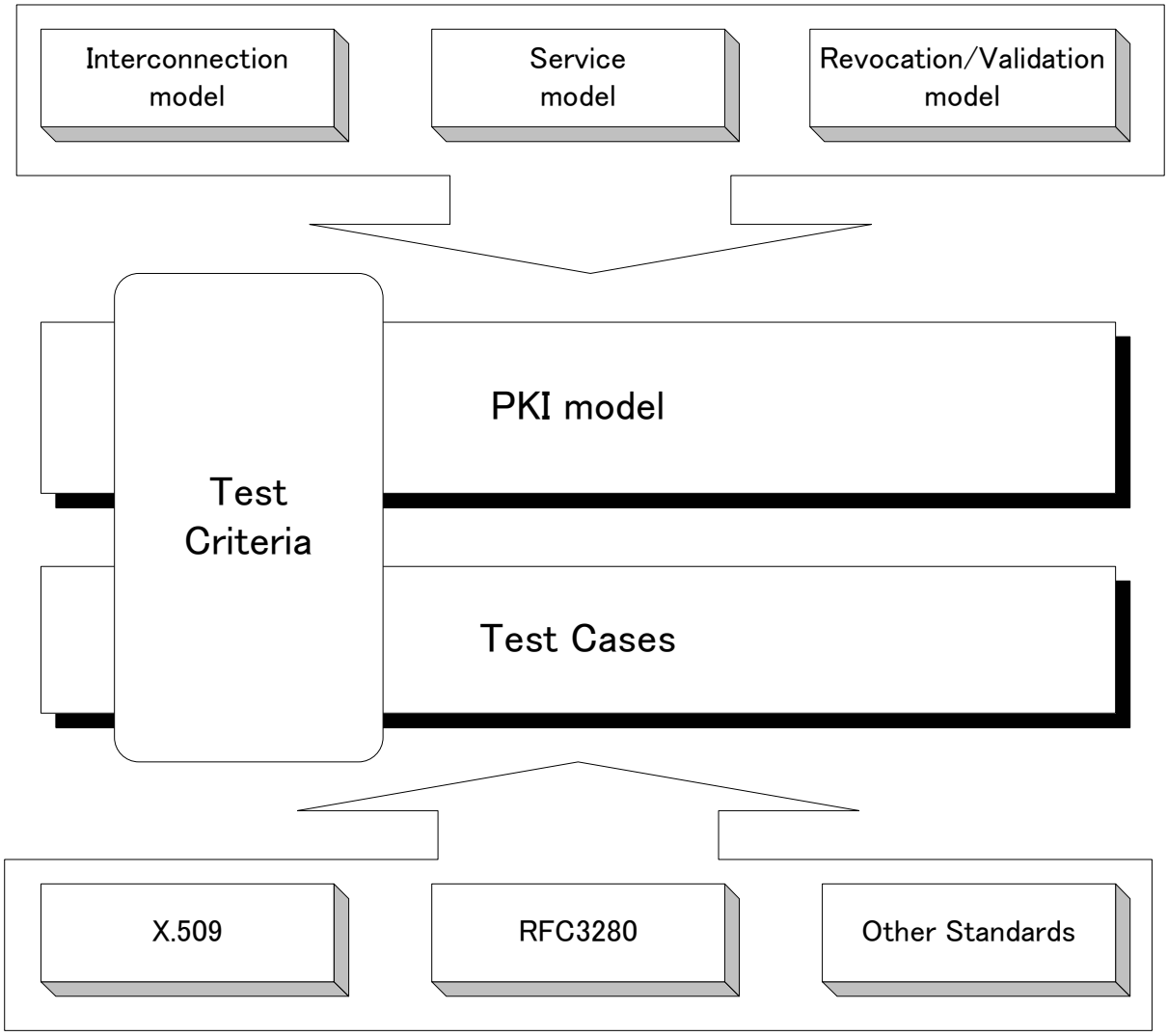

Figure 2.2 Applicablity for other criteria

(2) Who read this guideline?

This is a framework to evaluate a PKI application in multi-domain PKI. Therefore, it should become useful for evaluators of PKI application. Specifically, they may be service providers selecting the PKI application and introducing it into the service, or may be application certifiers accrediting that a certain PKI application satisfies a fixed function.

And a designer of Principal CA, who develops the interconnection with other domain, may make use of the information for the PKI model defined in this guideline as a reference when interconnecting.

(a) Participant of principal CA
  (i) Designing for certificate profile
  (ii) Choice of interconnection model
  (iii) How to provide the revocation information
(b) PKI Service Provider
  (i) Definition of path validation requirement for PKI application
  (ii) Definition of testing requirement for PKI application
  (iii) Requirement for what kind of service provide
(c) Accreditation organization
  (i) Criteria for CA accreditation
  (ii) Criteria for PKI application accreditation
  (iii) Criteria for interconnecting to other PKI domain

This guideline defines CA requirements that CA should clear and relying-party requirements that PKI service provider should clear. Authorization organization can make use of the extracted test items in this document as criteria for each party.

(3) How use this guideline

This guideline defines a lot of test cases to be compliant with IWG recommendation profile and various standards such as ITU-T/X.509 and PKIX/RFC3280. The guideline users can extract just appropriate test cases from this guideline, and then use the test cases to evaluate whether the applications are compliant with the criteria.

The users must obtain the information below for extracting the appropriate

test cases.

- Type of Interconnection to destination domain
- Type of Revocation / Validation at destination domain
- Type of Service between each domains
- Level of compliance to Criteria

The users can extract a set of required and appropriate test cases, according to these information and flow below.

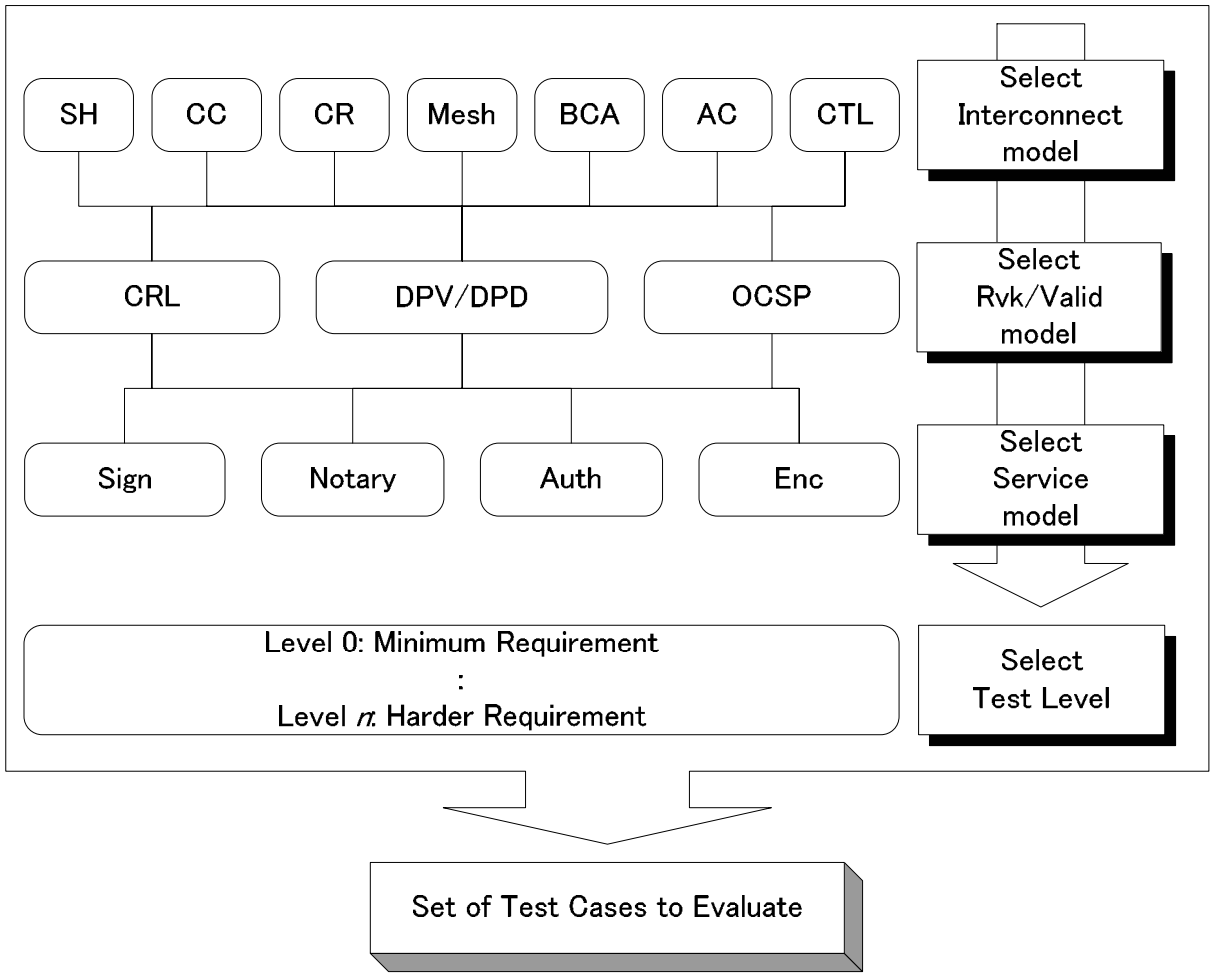

Figure 2.3 Extract required test cases to evaluate

The user, who extracted necessary test cases, can judge easily whether the PKI application has the enough quality for the path validation, by evaluating whether the PKI application obtains the expected result in these test cases.

2.2 Testing Models and Testing Requirements

2.2.1 Analysis of Various PKI domain

This section analyzes and categorizes the various PKI domains from the three viewpoints, CA topology, service model, and revocation/validation model.

(1) Definition of CA topology

This section analyzes and categorizes various CA topologies in the multi domain PKI. Especially 'CA-CA Interoperability'[7] published by PKI Forum[8] is referred.

(a) StrictHierarchy

(i) Definition

- Only Root CA issues self-signed certificate.
- Subordinate CAs don't issue self-signed certificate, only superior CA issues CA certificates to them.
- Subordinate CAs are not allowed to have multi superior CAs.

(ii) Usage

Basically, this model is used in single domain PKI. Many domains may operate CAs in their hierarchic structures with a single policy, and include no certificatePolicies extensions in certificates. This is useful for a vertical organization (e.g., an enterprise) that is applicable easily to the hierarchic structure.

(iii) Advantage and disadvantage

- Applicable to existing applications based on SSL.
- There are many applications, but only a few applications support the path processing.
- A lack of extended ability.
- Subordinate CAs are not allowed to cross-certify other CAs directly.

---

[7] CA-CA Interoperability
http://www.pkiforum.org/pdfs/ca-ca_interop.pdf

[8] PKI Forum
http://www.oasis-open.org/committees/pki/

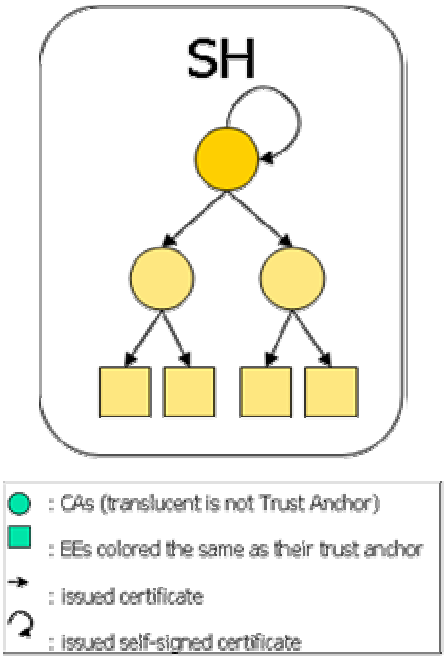

Figure 2.4 Strict Hierarchy model

(b) CrossCertification

(i) Definition

- The model in which CAs issue a cross-certificate to other CAs..

<CITE FROM X.509 4th>

CAs issue certificates to other CAs either as a mechanism to authorize the subject CA's existence (e.g. in a strict hierarchy) or to recognize the existence of the subject CA (e.g. in a distributed trust model). The crosscertificate structure is used for both of these.

- There are two methods in cross-certification.
  - Mutual-certification: each CA issues the cross-certificate one another.
  - Unilateral-certification: only one CA issues the cross-certificate to another CA.
- CAs store cross-certificate by crossCertificatePair format.

(ii) Usage

Topologically speaking, cross-certification merely means issuing a CA certificate except a self-signed certificate. It means a trust relationship between CAs.

This is an original concept of Mesh model, BCA model, accreditation certificate model, and maybe hierarchy model. In a wide sense, this includes

also strict hierarchy model. In a narrow sense, this is used as core techniques of multi domain PKI to build a trust relationship with another domain.

(iii) Advantage and disadvantage

All CA products cannot generate and process the crossCertificatePair. Because this can issue the trust relationship precisely, this is suitable for notary service. Even if CAs revoke a cross-certificate, each subject CA can exist.

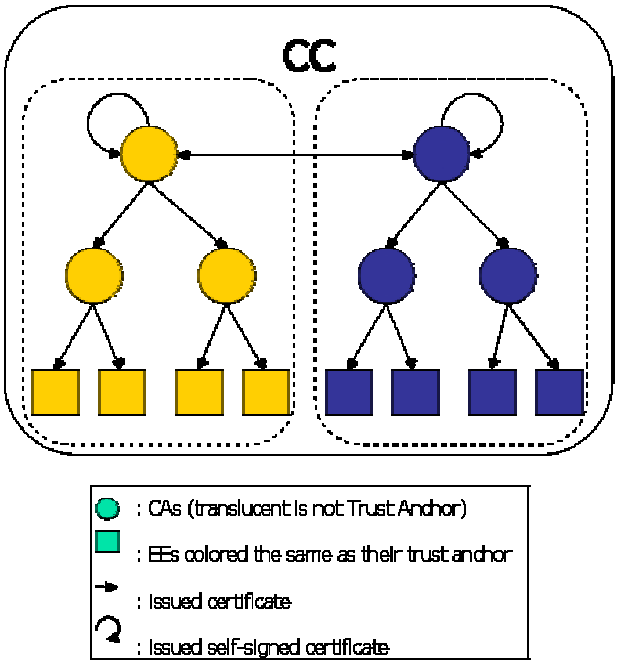

Figure 2.5 Cross Certification model

(c) CrossRecognition

(i) Definition

- The model in which each EE is allowed to specify multiple trust anchors.

(ii) Usage

This is suitable when a strict hierarchy model builds a trust relationship with another one.

(iii) Advantage and disadvantage

Most existing SSL-based applications are grow to be suitable for this by just a little modifying. Because this cannot represent a trust relationship, this model is not suitable to auditing, notary and non-repudiation.

The entity controlling the trust relationship is EE, but not CA.

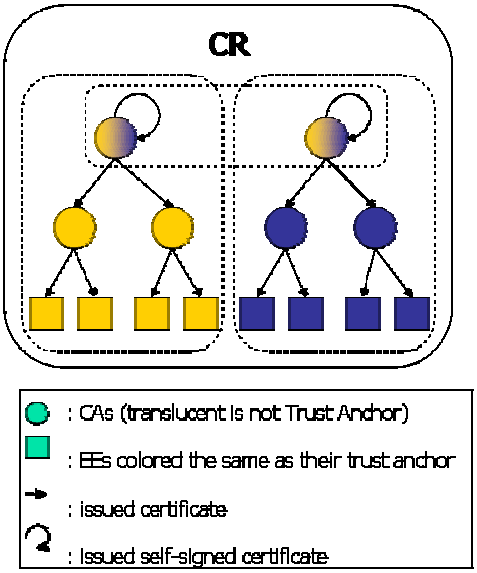

Figure 2.6 Cross Recognition model

(d) Mesh

(i) Definition

- The model in which plural CAs cross-certify at least one other CA.

(ii) Usage

This model is not a CA topology, which is intended to solve certain requirements. Mesh model is merely a result of many cross-certifications.

(iii) Advantage and disadvantage

If each CAs hold their self-signed certificate, they are not effected by the key compromise in other CAs.

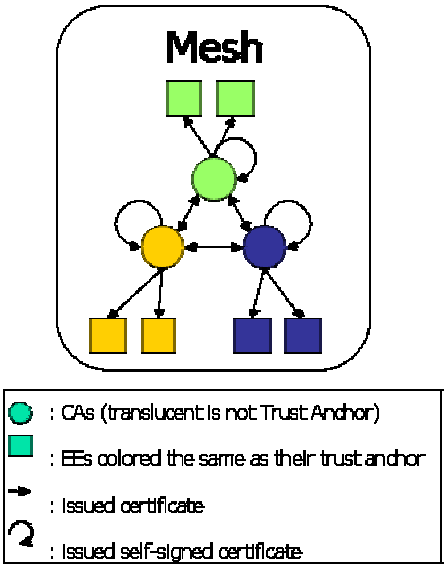

Figure 2.7 Mesh model

(e) BridgeCA

(i) Definition

- The model in which Bridge CA that have self-signed certificate cross-certifies the other plural CAs.

(ii) Usage

This is useful to reduce the complexity of cross-certification. The Bridge CA should be a Trusted Third Party.

(iii) Advantage and disadvantage

- The limited number of cross-certification
- The burden on a Bridge CA operation unit is heavy.
- High skills for path processing are required.

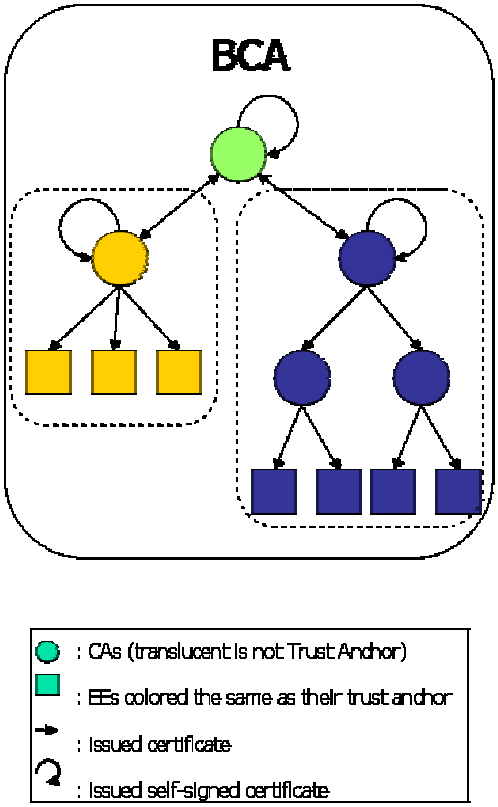

Figure 2.8 Bridge CA model

(f) AccreditationCertificate

(i) Definition

- The model in which only certain CA is allowed to certify plural CAs that have a self-signed certificate.

(ii) Usage

In the case that only the strict hierarchy is supported by the applications, and a CA operation independent from a superior CA is desirable, this model is useful.

(iii) Advantage and disadvantage

- Each CA is able to operate independently from superior CA.
  - *Superior CA compromise, Superior CA key rollover, Exchange of a superior CA, etc...*
- All applications are not necessary to support the path processing because they can process the path as merely strict hierarchy model. This cannot restrict complex constraints in the certification path.
- Subordinate CAs are forbidden to cross-certify other CAs directly, and the accreditation from Accreditation CA is necessary.

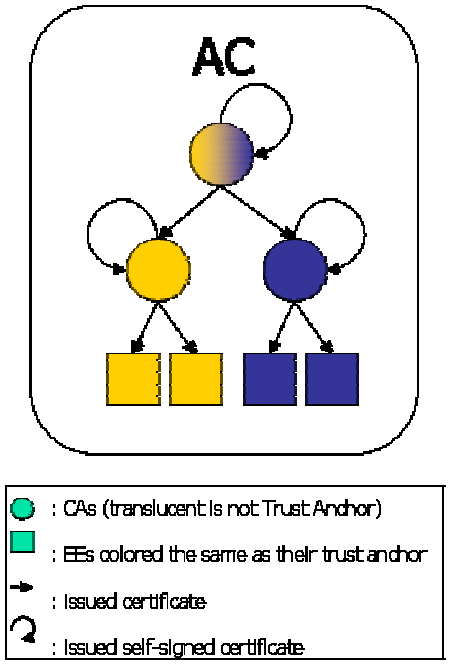

Figure 2.9 Accreditation Certificate model

(g) CertificateTrustLists

(i) Definition

- The trust anchors of each domain issue the certificate trust lists that are lists of trust anchor certificates of the subject domain.
- EEs are allowed to specify other trust anchor certificates in only their CTL when validating the certification path.

(ii) Usage

- When PKI system cannot process or issue the cross-certificate, this model is suitable like Cross-Recognition.
- Especially for a PKI system needing strict audit of interconnection, this model is more suitable than Cross-Recognition.

(iii) Advantage and disadvantage

- In this model, CAs can manage EEs' multiple trust anchors, but EEs cannot manage it.
- CAs do not need to issue a cross-certificate, and applications do not need to process the cross-certificates.
- CAs must issue a certificate trust lists formatted by PKCS#7, and applications must process it.

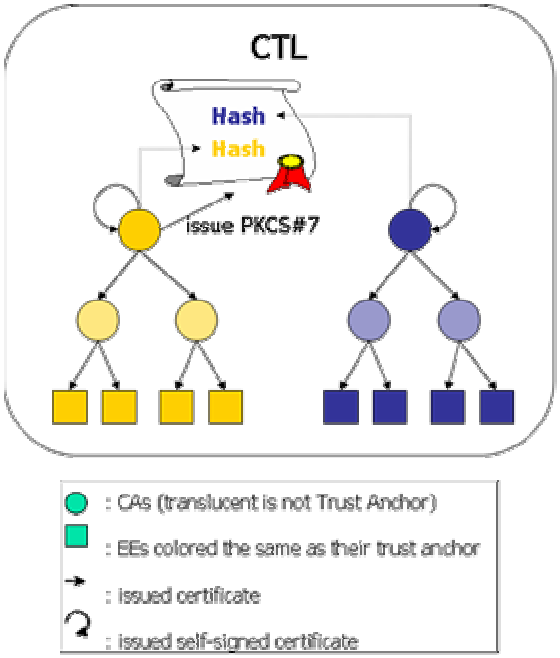

Figure 2.10 Certificate Trust Lists model

(2) Definition of PKI Service model

This section defines the principal service models adopted in the international PKI.

(a) Signing

A typical case is that "a relying-party in Y country validates a signed-data by using a valid certificate in X country." The digital signature will be effective

in the international e-commerce. The typical implementations of this model are PKCS7/CMS singed-data or XMLsignature. In this document, a legal effectiveness is out of scope.

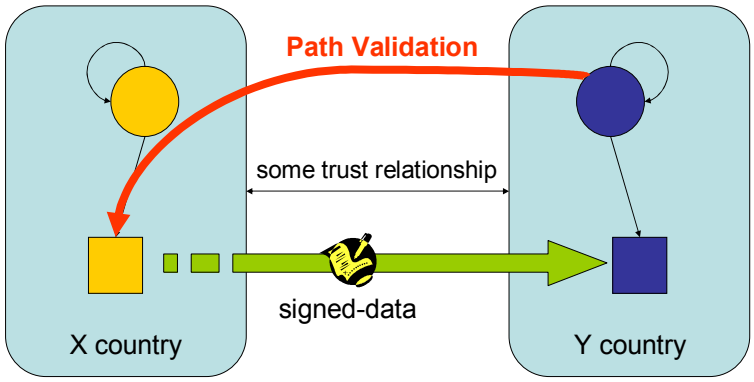

Figure 2.11 Signing model

(b) Notary Service (Long term signature)

A typical case is that "a relying-party in Y country validates a signed-data that existed prior to a particular time in X country." In international mediation, an ability to establish the existence of data prior to the specified times will be necessary. This model may require a TimeStampAuthority or Notary.

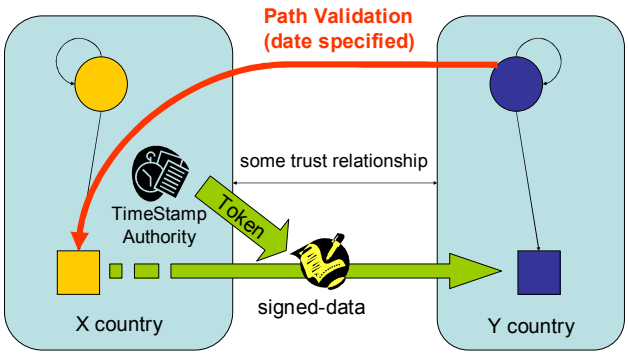

Figure 2.12 Notary model

(c) Authentication

A typical case is that "a client in Y country connects to server in X country by authentication." In the international community, a strict authentication

may be used for distinguishing an individual. A typical implementation of this model is TLS client authentication.

(d) Encryption

A typical case is that "a subscriber in X country encrypts a piece of data by using a certificate of a relying-party in Y country." In the international e-commerce, the encryption is used for the exchange of confidential information. The typical implementation of this model is PKCS7/CMS Encryption-data or XMLsecurity.

(3) Definition of Revocation / Validation model

This section defines the validation models in the international PKI.

(a) CRL

A typical case is that "a relying-party of Y country requires obtaining a CRL for a path processing, which is issued by the issuer of subscriber certificate in X country."

(b) OCSP

A typical case is that "a relying-party of Y country requires a response from an OCSP Responder in X country for validating a subscriber certificate of X country."

The case that "a relying-party of Y country requests to an OCSP Responder in Y country to validate a subscriber certificate of X country" is regarded as a delegated path validation.

(c) Delegated Path Discovery/Validation

A typical case is that "a relying-party of Y country needs a VA (validation authority) of Y country to validate a certificate path between the relying party and a subscriber in X country."

This subsection will be revised after RFC of DPD/DPV is published.

2.2.2 Requirements for Path Processing

This section defines the requirements to confirm the path processing about each model categorized in section 2.2.1. The requirements below are almost derived from ITU-T/X.509, IETF/PKIX RFC3280, and IWG recommended profile.

(1) Base Requirements

CA.01: CAs should issue a certificate that directoryName in its issuer DN and subject DN are encoded by UTF8String except for a country attribute.

[IWG profile]

CA.02: CAs should generate all keyIdentifier by the 160bit SHA-1 hash in all certificates they issue. This is derived from the method defined in paragraph (1) of Section 4.2.1.2 Subject Key Identifier in RFC 3280.

[IWG profile, RFC3280 4.2.1.1 & 4.2.1.2]

CA.03: CAs should generate consistently all keyIdentifiers in all certificates.

[IWG Profile, RFC3280 4.2.1.1 & 4.2.1.2]

CA.04: CAs should issue a certificate including a consistent format of authorityKeyIdentifier in all certificates they issue.

[IWG profile, RFC3280 4.2.1.1]

CA.05: CAs should issue a self-signed certificate which has the basicConstraints present and critical with cA flag asserted.

[IWG profile]

CA.06: CAs should issue a certificate whose validity is encoded by UTCTime.

[X.509 7]

RP.07: The application should validate successfully the correct certification path.

RP.08-11: The application should ensure that the issuer distinguishedName of a certain certificate and the subject distinguishedName of its issuer certificate should be identical about each certificate in the certification path.

[X.509 10.5.1]

RP.12: The application should trace the certification chain by keyIdentifier in authorityKeyIdentifier and subjectKeyIdentifier of each certificate in the certification path.

[RFC3280 4.2.1.2]

RP.13-16: The application should ensure that the validity of each certificate in the certification path should include the current time.

[X.509 10.5.1]

RP.17-18: The application should treat a validity set as UTCTime with a year of 50 about each certificate in the certification path.

[X.509 7]

RP.19: The application should verify each certificate in the certification path by its issuer certificate.

[X.509 10.5.1]

RP.20: The application should ensure whether the subscriber certificate is revoked or not.

[X.509 10.5.1]

RP.21: The application should process a certification path which contains a certificate which has unrecognized extensions.

[X.509 7]

(2) Interconnection requirements

(a) Strict Hierarchy

CA.01: CAs should issue a CA certificate including cA flag set to TRUE in critical basicConstraints extension, except for self-signed certificate.

[X.509 8.4.2.1]

CA.02: CAs should issue a CA certificate including keyCertSign in critical keyUsage extension, except for self-signed certificate.

[X.509 8.2.2.3]

CA.03: CAs should issue a CA certificate including pathLenConstraints in critical basicConstraints extension, except for self-signed certificate.

[X.509 8.4.2.1]

CA.04: CAs should issue CA certificates including a policyIdentifier in critical certificatePolicies extension, except for self-signed certificate.

[X.509 8.2.2.6]

CA.05: CAs should issue CA certificates including plural policyIdentifier in critical certificatePolicies extension, except for self-signed certificate.

[X.509 8.2.2.6]

CA.06: CAs should issue CA certificates including a policyIdentifier in non-critical certificatePolicies extension, except for self-signed certificate.

[X.509 8.2.2.6]

CA.07: CAs should issue CA certificates including plural policyIdentifier in non-critical certificatePolicies extension, except for self-signed certificate.

[X.509 8.2.2.6]

RP.08: The application should validate successfully correct certification path.

RP.09-10: The application should validate a certification path including a subordinate CA certificate.

[X.509 10.5.1]

RP.11-13: The application should ensure whether all CA certificate in the certification path have cA flag set to TRUE in critical basicConstraints extension.

[X.509 10.5.1]

RP.14: The application should ensure whether the certification path length is shorter than pathLenConstraints or not in any CA certificate.

[X.509 10.5.1]

RP.15-17: The application should ensure whether all CA certificate in the certification path have keyCertSign in critical keyUsage extension.

[IWG profile]

RP.18-21: The application should process certificatePolicy in all certificates for validating the certification path.

[X.509 8.1.1]

RP.22: The application should ensure whether all CA certificate in certification path is revoked or not.

[X.509 10.5.1]

RP.23: The application should verify all CA certificates in certification path by its issuer certificate.

[X.509 10.5.1]

(b) Cross Certification

CA.01: CAs should issue a cross-certification request including a subjectKeyIdentifier extension in extensionRequest, and its value should be identical with subjectKeyIdentifier in their self-signed certificate.

[IWG profile]

CA.02: CAs should issue a cross-certificate including SubjectKeyIdentifier, which should be the same as SubjectKeyIdentifier in corresponding cross-certification request.

[IWG profile]

CA.03: CAs should issue a cross-certificate including a policyIdentifier in critical certificatePolicies extension, except for self-signed certificate. This assertion is the same as Int.SH.CA.04 requirement.

[X.509 8.2.2.6]

CA.04: CAs should issue a cross-certificate including plural policyIdentifier in critical certificatePolicies extension, except for self-signed certificate. This assertion is the same as Int.SH.CA.05 requirement.

[X.509 8.2.2.6]

CA.05: CAs should issue a cross-certificate including a policyIdentifier in non-critical certificatePolicies extension, except for self-signed certificate. This assertion is the same as Int.SH.CA.06 requirement.

[X.509 8.2.2.6]

CA.06: CAs should issue a cross-certificate including plural policyIdentifier in non-critical certificatePolicies extension, except for self-signed certificate. This assertion is the same as Int.SH.CA.07 requirement.

[X.509 8.2.2.6]

CA.07: CAs should issue a cross-certificate including a policyMapping extension.

[X.509 8.1.3]

CA.08: CAs should issue a cross-certificate including plural policyMapping extension.

[X.509 8.1.3]

CA.09: CAs should issue a cross-certificate including cA flag set to TRUE in critical basicConstraints extension, except for self-signed certificate. This assertion is the same as Int.SH.CA.01 requirement.

[X.509 8.4.2.1]

CA.10: CAs should issue a cross-certificate including keyCertSign in critical keyUsage extension, except for self-signed certificate.

[X.509 8.2.2.3]

CA.11: CAs should issue a cross-certificate including pathLenConstraints in critical basicConstraints extension, except for self-signed certificate. This assertion is the same as Int.SH.CA.02 requirement.

[X.509 8.4.2.1]

CA.12: CAs should issue a cross-certificate including a critical policyConstraints extension.

[X.509 10.5.2, 10.5.3]

CA.13: CAs should issue a cross-certificate including a critical nameConstraints extension.

[X.509 10.5.2]

CA.14: CAs should issue a cross-certificate including a critical inhibitAnyPolicy extension.

[X.509 10.5.2]

CA.15-18: CAs should issue a certificate that anybody can find out the revocation information.

[IWG profile]

RP.19: The application should validate successfully correct certification path.

RP.20-21: The application should validate a certification path including a cross-certificate.

[X.509 8.1.2]

RP.22-25: The application should process certificatePolicy in all certificates for validating certification path.

[X.509 8.1.1]

RP.26-28: The application should ensure whether all cross-certificates in the certification path have cA flag set to TRUE in critical basicConstraints extension.

[X.509 10.5.1]

RP.29: The application should ensure whether the certification path length is shorter than pathLenConstraints or not in any cross-certificate.

[X.509 10.5.1]

RP.30-32: The application should ensure whether all cross-certificates have keyCertSign in critical keyUsage extension.

[IWG profile]

RP.33-34: The application should process policyConstraints extension in all cross-certificates for validating certification path.

[X.509 10.5.2, 10.5.3]

RP.35-37: The application should process nameConstraints extension in all cross-certificates for validating certification path.

[X.509 10.5.2, 10.5.3]

RP.38: The application should ensure whether all certificates in certification path are revoked or not.

[X.509 10.5.1]

RP.39: The application should verify all cross-certificates in certification path by its issuer certificate.

[X.509 10.5.1]

(c) Cross Recognition

CA.01: CAs should issue CA certificates including a policyIdentifier in critical certificatePolicies extension, except for self-signed certificate. This assertion is tested by testing Int.SH.CA.4 requirement.

[X.509 8.2.2.6]

CA.02: CAs should issue CA certificates including plural policyIdentifier in critical certificatePolicies extension, except for self-signed certificate. This assertion is tested by testing Int.SH.CA.5 requirement.

[X.509 8.2.2.6]

CA.03: CAs should issue CA certificates including a policyIdentifier in non-critical certificatePolicies extension, except for self-signed certificate. This assertion is tested by testing Int.SH.CA.6 requirement.

[X.509 8.2.2.6]

CA.04: CAs should issue CA certificates including plural policyIdentifier in non-critical certificatePolicies extension, except for self-signed certificate. This assertion is tested by testing Int.SH.CA.7 requirement.

[X.509 8.2.2.6]

RP.05: The application should validate successfully correct certification path.

RP.06-08: The application should validate a certification path including other PKI domain certificates from its trust list.

[IWG profile]

RP.09: The application should verify whether trust anchor certificate in certification path was altered or not.

[X.509 10.5.1]

RP.10-13: The application should process certificatePolicy in all certificates for validating certification path.

[X.509 8.1.1]

(d) Mesh (in the future)

TBD in the future.

(e) Bridge CA (in the future)

TBD in the future.

(f) Accreditation Certificate (in the future)

TBD in the future.

(g) Certificate Trust Lists (in the future)

TBD in the future.

(3) Service requirements

(a) Signing

CA.01: CAs should issue an EE certificate including digitalSignature in critical keyUsage extension.

[IWG profile]

CA.02: CAs should issue a CA certificates including a policyIdentifier in critical certificatePolicies extension, except for self-signed certificate. This assertion is tested by testing Int.SH.CA.4 requirement.

[X.509 8.2.2.6]

CA.03: CAs should issue a CA certificates including plural policyIdentifier in critical certificatePolicies extension, except for self-signed certificate. This assertion is tested by testing Int.SH.CA.5 requirement.

[X.509 8.2.2.6]

CA.04: CAs should issue a CA certificates including a policyIdentifier in non-critical certificatePolicies extension, except for self-signed certificate. This assertion is tested by testing Int.SH.CA.6 requirement.

[X.509 8.2.2.6]

CA.05: CAs should issue a CA certificates including plural policyIdentifier in non-critical certificatePolicies extension, except for self-signed certificate. This assertion is tested by testing Int.SH.CA.7 requirement.

[X.509 8.2.2.6]

RP.06: The application should validate successfully correct certification path.

RP.07: The application should ensure whether the subscriber certificate has an appropriate usage in critical keyUsage extension.

[IWG consideration]

RP.08-11: The application should process certificatePolicy in all certificates for validating certification path.

[X.509 8.1.1]

(b) Notary (in the future)

TBD in the future.

May require TSA

Cross-Recognition cannot validate a signed-data that existed before particular time, because trust relationship is established by no signature..

Require signingTime in the signed-data.

Provide the necessary information to validate a certificate (e.g., CRLDP) as to refer from other domains.

(c) Authentication (in the future)

TBD in the future.

Require setting digitalSignature to keyUsage.

Require setting the attribute (e.g., e-mail, iPAddress or dNSName) of entity to subjectAltName.

MAY Require extendedKeyUsage

(d) Encryption (in the future)

TBD in the future.

Obtain a certificate via trustworthy way.

Obtaining a certificate from out-of-band is not trusted in multi domain PKI.

(4) Revocation/Validation requirements

(a) CRL

Be able to obtain appropriate CRL even if other domain EE.

If each CRL is different in revocation information, it should be recognized by other domain EE.

CA.01: CAs should issue a CA (CRL issuer) certificate including CRLSign in critical keyUsage extension.

[IWG profile]

CA.02: CAs should issue a revocation list including a critical issuingDistributionPoints extension.

[IWG profile]

CA.03: CAs should issue a CRL including an onlyContainsUserCerts flag set to TRUE in a critical issuingDistributionPoints extension.

[X.509 8.6.2.2, RFC3280 5.2.5]

CA.04: CAs should issue an ARL including an onlyContainsCACerts flag set to TRUE in a critical issuingDistributionPoints extension.

[X.509 8.6.2.2, RFC3280 5.2.5]

CA.05: CAs should issue a certificate including distributionPoint, when it is not CA entry, in cRLDistributionPoints extension.

[X.509 8.6.2.2, RFC3280 5.2.5]

CA.06: CAs should issue a revocation list including distributionPoint, which is consistent with CRLDistributionPoints extension of the certificate they issue, in issuingDistributionPoint extension.

[RFC3280 5.2.5]

CA.07: CAs should issue a revocation list including keyIdentifier in authorityKeyIdentifier extension.

[IWG profile]

RP.08: The application should validate successfully correct certification path.

RP.09-10: The application should associate a CRL with a certificate to verify.

[X.509 10.5.1]

RP.11: The application should ensure whether the revocationDate of the

certificate is valid or not.

[IWG consideration]

RP.12: The application should verify a revocation list by the revocation list issuer certificate.

[RFC3280 6.3.3 (b)]

RP.13: The application should ensure whether the revocation list issuer certificate has CRLSign in critical keyUsage extension.

[RFC3280 6.3.3 (f)]

RP.14: The application should verify whether revocation list was altered or not.

[X.509 10.5.1, RFC3280 6.3.3 (g)]

RP.15-16: The application should process appropriately a revocation list including an unknown/well-known CRL entry extension if it is critical or not.

[X.509 8]

RP.17-18: The application should process appropriately a revocation list including an unknown/well-known CRL extension if it is critical or not.

[X.509 8]

RP.19-20: The application should process appropriately a certificate when using a revocation list including an onlyContainsUserCerts flag set to TRUE in critical issuingDistributionPoint extension. The certificate has no basicConstraints extension.

[RFC3280 6.3.3 (b)]

RP.21-22: The application should process appropriately a certificate when using a revocation list including an onlyContainsCACerts flag set to TRUE in critical issuingDistributionPoint extension. The certificate has cA flag set to TRUE in critical basicConstraints extension.

[RFC3280 6.3.3 (b)]

RP.23-24: The application should process appropriately a certificate when using a revocation list including an onlyContainsUserCerts flag set to TRUE in critical issuingDistributionPoint extension. The certificate has no basicConstraints extension.

[RFC3280 6.3.3 (b)]

RP.25-26: The application should process appropriately a certificate when using a revocation list including an onlyContainsUserCerts flag set to TRUE in critical issuingDistributionPoint extension. The certificate has cA flag set to TRUE in critical basicConstraints extension.

[RFC3280 6.3.3 (b)]

RP.27-31: The application should ensure whether each distributionPoint are

consistent between a critical issuingDistributionPoint extension in the revocation list and a cRLDistributionPoints extension in the certificate.

[RFC3280 5.2.5]

(b) OCSP (in the future)

TBD in the future.

Trustworthiness to OCSP Responder --- require a validation method for foreign OCSP Responder.

Reachability to OCSP Responder --- URI in AIA should be internet URI.

Reduce the overhead of network transaction.

(c) Delegated Path Discovery/Validation (in the future)

TBD in the future.

2.3 Testing Assumptions

2.3.1 Base model

(a) Entity

Root CA: the only CA which has its self-signed certificate

Subscriber: the end entity whose certificate has been signed by RootCA

Relying Party: the end entity who validates the data signed by subscriber.

(b) Base profile

The followings are only profiles as a summary of certificate in the experiment.

Table 2.1 Base model Certificate Profile

Field	critical flag	Root CA	Sub scriber	note
version	-	x	x	1
serialNumber	-	x	x	
signature	-	x	x	2
validity	-	x	x	3
issuer	-	x	x	4

subject	-	x	x	4
subjectPublicKeyInfo	-	x	x	5
issuerUniqueID	-	-	-	
subjectUniqueID	-	-	-	
authorityKeyIdentifier	n	-	x	
keyIdentifier	-	-	x	6
subjectKeyIdentifier	n	x	x	6
keyUsage	c	-	x	7
certificatePolicies	c	-	-	
policyMappings	n	-	-	
subjectAltName	n	-	-	
basicConstraints	c	-	-	
policyConstraints	c	-	-	
cRLDistributionPoints	n	-	x	
distributionPoint	-	-	x	
fullName	-	-	x	8
1 v3(2)				
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)				
3 UTCTime				
4 UTF8String				
5 rsaEncryption (1 2 840 113549 1 1 1)				
6 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)				
7 only digitalSignature				
8 directoryName or URI				

Table 2.2 Base model CRL Profile

Field	critical flag	CRL	ARL	note
version	-	x	x	1
signature	-	x	x	2
issuer	-	x	x	3
thisUpdate	-	x	x	4
nextUpdate	-	x	x	4
RevockedCertificates	-	x	x	

userCertificate	-	x	x	
revocationDate	-	x	x	4
crlEntryExtensions		-	-	
authorityKeyIdentifier	n	x	x	
keyIdentifier	-	x	x	5
cRLNumber	n	-	-	
issuingDistributionPoint	c	x	x	
distributionPoint	-	x	x	
fullName	-	x	x	6
onlyContainsUserCerts	-	x	-	
onlyContainsCACerts	-	-	x	
1 v2(1)				
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)				
3 UTF8String				
4 UTCTime				
5 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)				
6 directoryName or URI				

(c) Inputs for validation

user-initial-policy-set: any-policy

trustAnchorInfo: Root CA

initial-explicit-policy: false

2.3.2 Interconnection model

(1) Strict Hierarchy

(a) Entity

RootCA: the only CA which has self-signed certificate

SubCA-1: the CA which has had its certificate signed by RootCA

Subscriber-1: the end entity whose certificate has been signed by SubCA-1

SubCA-2: the CA which has had its certificate signed by SubCA-1

Subscriber-2: the end entity whose certificate has been signed by SubCA-2

(b) Base profile

The followings are only profiles as a summary of certificates in the experiment.

Table 2.3 Strict Hierarchy Base Certificate Profile

Field	critical flag	Root CA	Sub CA	Sub scriber	note
version	-	x	x	x	1
serialNumber	-	x	x	x	
signature	-	x	x	x	2
validity	-	x	x	x	3
issuer	-	x	x	x	4
subject	-	x	x	x	4
subjectPublicKeyInfo	-	x	x	x	5
issuerUniqueID	-	-	-	-	
subjectUniqueID	-	-	-	-	
authorityKeyIdentifier	n	-	x	x	
keyIdentifier	-	-	x	x	6
subjectKeyIdentifier	n	x	x	x	6
keyUsage	c	-	-	x	7
certificatePolicies	c	-	x	x	
policyIdentifier	-	-	x	x	8
policyQualifiers	-	-	-	-	
policyMappings	n	-	-	-	
subjectAltName	n	-	-	-	
basicConstraints	c	-	x	-	
cA	-	-	x	x	
pathLenConstraint	-	-	-	-	
policyConstraints	c	-	-	-	
cRLDistributionPoints	n	-	-	x	
distributionPoint	-	-	-	x	
fullName	-	-	-	x	9
1 v3(2)					
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)					
3 UTCTime					
4 UTF8String					
5 rsaEncryption (1 2 840 113549 1 1 1)					
6 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)					
7 only digitalSignature					

8 consistent policyIdentifier
9 directoryName or URI

Table 2.4 Strict Hierarchy Base CRL Profile

Field	critical flag	CRL	ARL	note
version	-	x	x	1
signature	-	x	x	2
issuer	-	x	x	3
thisUpdate	-	x	x	4
nextUpdate	-	x	x	4
RevockedCertificates	-	x	x	
userCertificate	-	x	x	
revocationDate	-	x	x	4
crlEntryExtensions		-	-	
authorityKeyIdentifier	n	x	x	
keyIdentifier	-	x	x	5
cRLNumber	n	-	-	
issuingDistributionPoint	c	x	x	
distributionPoint	-	x	x	
fullName	-	x	x	6
onlyContainsUserCerts	-	x	-	
onlyContainsCACerts	-	-	x	
1 v2(1)				
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)				
3 UTF8String				
4 UTCTime				
5 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)				
6 directoryName or URI				

(c) Inputs for validation

user-initial-policy-set: policy-A

trustAnchorInfo: Root CA

initial-explicit-policy: true

(2) Cross Certification

(a) Entity

RootCA-X: the CA which has its self-signed certificate

RootCA-Y: the CA which has achieved Cross-Certification relationship with RootCA-X

Subscriber-Y: the end entity whose certificate has been signed by RootCA-Y

RootCA-Z: the CA which has achieved Cross-Certification relationship with RootCA-Y

Subscriber-Z: the end entity whose certificate has been signed by RootCA-Z

(b) Base profile

The followings are only profiles as a summary of certificates in the experiment. .

Table 2.5 Cross Certification Base Certificate Profile

Field	critical flag	Root CA	Cross Cert	Sub scriber	note
version	-	x	x	x	1
serialNumber	-	x	x	x	
signature	-	x	x	x	2
validity	-	x	x	x	3
issuer	-	x	x	x	4
subject	-	x	x	x	4
subjectPublicKeyInfo	-	x	x	x	5
issuerUniqueID	-	-	-	-	
subjectUniqueID	-	-	-	-	
authorityKeyIdentifier	n	-	x	x	
keyIdentifier	-	-	x	x	6
subjectKeyIdentifier	n	x	x	x	6
keyUsage	c	-	x	x	7
certificatePolicies	c	-	x	x	
policyMappings	n	-	x	-	
subjectAltName	n	-	-	-	
basicConstraints	c	-	x	-	
cA	-	-	x	-	
pathLenConstraint	-	-	-	-	
policyConstraints	c	-	-	-	

cRLDistributionPoints	n	-	x	x	
distributionPoint	-	x	x	x	
fullName	-	x	x	x	8
1 v3(2)					
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)					
3 UTCTime					
4 UTF8String					
5 rsaEncryption (1 2 840 113549 1 1 1)					
6 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)					
7 only digitalSignature					
8 directoryName or URI					

Table 2.6 Cross Certification Base CRL Profile

Field	critical flag	CRL	ARL	note
version	-	x	x	1
signature	-	x	x	2
issuer	-	x	x	3
thisUpdate	-	x	x	4
nextUpdate	-	x	x	4
RevockedCertificates	-	x	x	
userCertificate	-	x	x	
revocationDate	-	x	x	4
crlEntryExtensions		-	-	
authorityKeyIdentifier	n	x	x	
keyIdentifier	-	x	x	5
cRLNumber	n	-	-	
issuingDistributionPoint	c	x	x	
distributionPoint	-	x	x	
fullName	-	x	x	6
onlyContainsUserCerts	-	x	-	
onlyContainsCACerts	-	-	x	
1 v2(1)				
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)				

3 UTF8String
4 UTCTime
5 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)
6 directoryName or URI

(c) Inputs for validation

user-initial-policy-set: policy-X

trustAnchorInfo: Root CA-X

initial-explicit-policy: true

(3) Cross Recognition

(a) Entity

RootCA-X: the CA which has self-signed certificate

RootCA-Y: the CA which has achieved Cross-Recognition relationship with RootCA-X

Subscriber-Y: the end entity whose certificate has been signed by RootCA-Y

(b) Base profile

The followings are only profiles as a summary of certificates in the experiment. .

Table 2.7 Cross Recognition Base Certificate Profile

Field	critical flag	Root CA	Sub scriber	note
version	-	x	x	1
serialNumber	-	x	x	
signature	-	x	x	2
validity	-	x	x	3
issuer	-	x	x	4
subject	-	x	x	4
subjectPublicKeyInfo	-	x	x	5
issuerUniqueID	-	-	-	
subjectUniqueID	-	-	-	
authorityKeyIdentifier	n	-	x	
keyIdentifier	-	-	x	6

subjectKeyIdentifier	n	x	x	6
keyUsage	c	-	x	7
certificatePolicies	c	-	x	
policyIdentifier	-	-	x	8
policyQualifiers	-	-	-	
policyMappings	n	-	-	
subjectAltName	n	-	-	
basicConstraints	c	-	-	
policyConstraints	c	-	-	
cRLDistributionPoints	n	-	x	
distributionPoint	-	-	x	
fullName	-	-	x	9
1 v3(2)				
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)				
3 UTCTime				
4 UTF8String				
5 rsaEncryption (1 2 840 113549 1 1 1)				
6 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)				
7 only digitalSignature				
8 consistent policyIdentifier				
9 directoryName or URI				

Table 2.8 Cross Recognition Base CRL Profile

Field	critical flag	CRL	ARL	note
version	-	x	x	1
signature	-	x	x	2
issuer	-	x	x	3
thisUpdate	-	x	x	4
nextUpdate	-	x	x	4
RevockedCertificates	-	x	x	
userCertificate	-	x	x	
revocationDate	-	x	x	4

crlEntryExtensions		-	-	
authorityKeyIdentifier	n	x	x	
keyIdentifier	-	x	x	5
cRLNumber	n	-	-	
issuingDistributionPoint	c	x	x	
distributionPoint	-	x	x	
fullName	-	x	x	6
onlyContainsUserCerts	-	x	-	
onlyContainsCACerts	-	-	x	

1 v2(1)

2 sha1withRSAEncryption (1 2 840 113549 1 1 5)

3 UTF8String

4 UTCTime

5 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)

6 directoryName or URI

(c) Inputs for validation

user-initial-policy-set: policy-X, policy-Y

trustAnchorInfo: Root CA-X, RootCA-Y

initial-explicit-policy: true

(4) Mesh

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

(5) Bridge CA

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

(6) Accreditation Certificate

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

(7) Certificate Trust Lists

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

2.3.3 Service model

(1) Signing

(a) Entity

RootCA: the only CA which has self-signed certificate

Subscriber: the end entity whose certificate is issued by RootCA

(b) Base profile

The followings are only profiles as a summary of certificates in the experiment. .

Table 2.9 Signing Base Certificate Profile

Field	critical flag	Root CA	Sub scriber	note
version	-	x	x	1
serialNumber	-	x	x	
signature	-	x	x	2
validity	-	x	x	3
issuer	-	x	x	4
subject	-	x	x	4
subjectPublicKeyInfo	-	x	x	5
issuerUniqueID	-	-	-	
subjectUniqueID	-	-	-	
authorityKeyIdentifier	n	-	x	
keyIdentifier	-	-	x	6
subjectKeyIdentifier	n	x	x	6
keyUsage	c	-	x	7
certificatePolicies	c	-	x	
policyIdentifier	-	-	x	8

policyQualifiers	-	-	-	
policyMappings	n	-	-	
subjectAltName	n	-	-	
basicConstraints	c	-	-	
policyConstraints	c	-	-	
cRLDistributionPoints	n	-	x	
distributionPoint	-	-	x	
fullName	-	-	x	9

1 v3(2)
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)
3 UTCTime
4 UTF8String
5 rsaEncryption (1 2 840 113549 1 1 1)
6 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)
7 only digitalSignature
8 consistent policyIdentifier
9 directoryName or URI

Table 2.10 Signing Base CRL Profile

Field	critical flag	CRL	ARL	note
version	-	x	x	1
signature	-	x	x	2
issuer	-	x	x	3
thisUpdate	-	x	x	4
nextUpdate	-	x	x	4
RevockedCertificates	-	x	x	
userCertificate	-	x	x	
revocationDate	-	x	x	4
crlEntryExtensions		-	-	
authorityKeyIdentifier	n	x	x	
keyIdentifier	-	x	x	5
cRLNumber	n	-	-	

issuingDistributionPoint	c	x	x	
distributionPoint	-	x	x	
fullName	-	x	x	6
onlyContainsUserCerts	-	x	-	
onlyContainsCACerts	-	-	x	
1 v2(1)				
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)				
3 UTF8String				
4 UTCTime				
5 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)				
6 directoryName or URI				

(c) Inputs for validation

user-initial-policy-set: policy-A

trustAnchorInfo: Root CA

initial-explicit-policy: true

(2) Notary

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

(3) Authentication

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

(4) Encryption

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

2.3.4 Revocation/Validation model

(1) CRL

(a) Entity

RootCA-A: the only CA which has self-signed certificate

Subscriber-A: the end entity whose certificate is issued by RootCA-A

SubCA: the CA which has had is certificate issued by RootCA-A

Subscriber-SubCA: the end entity whose certificate has been signed by SubCA

(b) Base profile

The followings are only profiles as a summary of certificates in the experiment. .

Table 2.11 CRL Base Certificate Profile

Field	critical flag	Root CA	Sub scriber	note
version	-	x	x	1
serialNumber	-	x	x	
signature	-	x	x	2
validity	-	x	x	3
issuer	-	x	x	4
subject	-	x	x	4
subjectPublicKeyInfo	-	x	x	5
issuerUniqueID	-	-	-	
subjectUniqueID	-	-	-	
authorityKeyIdentifier	n	-	x	
keyIdentifier	-	-	x	6
subjectKeyIdentifier	n	x	x	6
keyUsage	c	-	x	7
certificatePolicies	c	-	x	
policyIdentifier	-	-	x	8
policyQualifiers	-	-	-	
policyMappings	n	-	-	

subjectAltName	n	-	-	
basicConstraints	c	-	-	
policyConstraints	c	-	-	
cRLDistributionPoints	n	-	x	
distributionPoint	-	-	x	
fullName	-	-	x	9
1 v3(2)				
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)				
3 UTCTime				
4 UTF8String				
5 rsaEncryption (1 2 840 113549 1 1 1)				
6 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)				
7 only digitalSignature				
8 consistent policyIdentifier				
9 directoryName or URI				

Table 2.12 CRL Base CRL Profile

Field	critical flag	CRL	ARL	note
version	-	x	x	1
signature	-	x	x	2
issuer	-	x	x	3
thisUpdate	-	x	x	4
nextUpdate	-	x	x	4
RevockedCertificates	-	x	x	
userCertificate	-	x	x	
revocationDate	-	x	x	4
crlEntryExtensions		-	-	
authorityKeyIdentifier	n	x	x	
keyIdentifier	-	x	x	5
cRLNumber	n	-	-	
issuingDistributionPoint	c	x	x	
distributionPoint	-	x	x	

fullName	-	x	x	6
onlyContainsUserCerts	-	x	-	
onlyContainsCACerts	-	-	x	
1 v2(1)				
2 sha1withRSAEncryption (1 2 840 113549 1 1 5)				
3 UTF8String				
4 UTCTime				
5 160bit SHA-1 aka RFC3280 "4.2.1.2 Subject Key Identifier" (1)				
6 directoryName or URI				

(c) Inputs for validation

user-initial-policy-set: unspecified

trustAnchorInfo: Root CA-A

initial-explicit-policy: unspecified

(2) OCSP

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

(3) Delegated Path Discovery/Validation

TBD in the future.

(a) Entity

(b) Base profile

(c) Inputs for validation

2.4 Testing Items for Base model

See the detail at the end of this guideline.

2.5 Testing Items for Interconnection model

2.5.1 Strict Hierarchy

See at the end of this guideline.

2.5.2 Cross Certification

See at the end of this guideline.

2.5.3 Cross Recognition

See at the end of this guideline.

2.5.4 Mesh

(TBD in the future)

2.5.5 Bridge CA

(TBD in the future)

2.5.6 Accreditation Certificate

(TBD in the future)

2.5.7 Certificate Trust Lists

(TBD in the future)

2.6 Testing Items for Service model

2.6.1 Signing

See at the end of this guideline.

2.6.2 Notary

(TBD in the future)

2.6.3 Authentication

(TBD in the future)

2.6.4 Encryption

(TBD in the future)

2.7 Testing Items for Revocation/Validation model

2.7.1 CRL

See at the end of this guideline.

2.7.2 OCSP

(TBD in the future)

2.7.3 Delegated Path Discovery/Validation

(TBD in the future)

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
CA	CertChains	Base.CA.01	The CA should use the UTF8String encoding of DirectoryString except countryName. **[IWG profile]**		Base.CA.01.01	Issue a certificate that contains DirectoryString encoded as UTF8String.	0			
		Base.CA.02	The CA should calculate a keyIdentifier from the value of PublicKey using 160-bit SHA-1 hash. **[IWG profile, RFC3280 4.2.1.1 & 4.2.1.2]**		Base.CA.02.01	issue a certificate in which subjectKeyIdentifier is the 160-bit SHA-1 hash of subject PublicKey, and in which authorityKeyIdentifier.keyIdentifier is the 160-bit SHA-1 hash of issuer Publickey.	0			
		Base.CA.03	The CA should use unique method to calculate subjectKeyIdentifier of every certificate. **[IWG profile, RFC3280 4.2.1.1 & 4.2.1.2]**		Base.CA.03.01	compare N certificates chosen at random, and check that the keyIdentifier value in every certificate is 160-bit SHA-1 hash of the PublicKey.	0			
		Base.CA.04	The CA should ensure that authorityKeyIdentifier format is consistent in every certificate. **[IWG profile, RFC3280 4.2.1.1]**		Base.CA.04.01	compare two certificates chosen at random, and check that the authorityKeyIdentifier format is consistent.	0			
	Constraints	Base.CA.05	The CA should issue a self-signed certificate which has the basicConstraints present and critical with cA flag asserted. **[IWG profile]**		Base.CA.05.01	Issue a self-signed certificate which has the basicConstraints present and critical with cA flag asserted.	0			
	Validity	Base.CA.06	The CA should encode certificate validity dates as UTCTime. **[X.509 7]**		Base.CA.06.01	issue a certificate in which the Time value is encoded as UTCTime.	0			
RP	NormalCase	Base.RP.07	Base Model Normal Case		Base.RP.07.01	The following path should be successfully validated; every certificate in the path is according to Base Profiles. [RootCA, Subscriber] RootCA issuerDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectKeyID.keyIdentifier: keyID.RootCA 1950 < notBefore < current time < notAfter < 2049 Subscriber issuerDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectDN: cn=Subscriber, ou=Root, o=PVTG Draft, c=AA authorityKeyID.keyIdentifier: keyID.RootCA subjectKeyID.keyIdentifier: keyID.Subscriber 1950 < notBefore < current time < notAfter < 2049	0			
	CertChains	The RP should ensure that issuer DN in a certificate to be verified and subject DN in an issuer certificate are identical.								
		Base.RP.08	The RP should determine that the names are different when they differ by whitespace in values other than countryName. **[RFC3280 4.1.2.4]**		Base.RP.08.01	The following path should be successfully validated; the issuer name in Subscriber is different from the subject name in RootCA by whitespace. [RootCA, Subscriber] RootCA.subjectDN: cn=CA, ou=Root, o=PVTG Draft, c=AA	0	Subscriber	issuer	cn=CA, ou=Root, o=PVTG Draft, c=AA
		Base.RP.09	The RP should determine that the names are different when they differ by capitalization in values other than countryName. **[RFC3280 4.1.2.4]**		Base.RP.09.01	The following path should be successfully validated; the issuer name in Subscriber is different from the subject name in RootCA by capitalization. [RootCA, Subscriber] RootCA.subjectDN: cn=CA, ou=Root, o=PVTG Draft, c=AA	0	Subscriber	issuer	cn=ca, ou=Root, o=PVTG Draft, c=AA
		Base.RP.10	The RP should determine that the names are different when they differ by order. **[X.501 12.5.2]**		Base.RP.10.01	The following path should not be successfully validated; the issuer name in Subscriber is different from the subject name in RootCA by order. [RootCA, Subscriber] RootCA.subjectDN: cn=CA, ou=Root, o=PVTG Draft, c=AA	0	Subscriber	issuer	cn=CA, o=PVTG Draft, ou=Root, c=AA

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP		Base.RP.11	The RP should determine that the names are different when they are completely different. **[X.501 12.5.2]**		Base.RP.11.01	The following path should not be successfully validated; the issuer name in Subscriber differs completely from the subject name in RootCA. [RootCA, Subscriber] RootCA.subjectDN: cn=CA, ou=Root, o=PVTG Draft, c=AA	0	Subscriber	issuer	cn=GE
	CertChains	The RP should ensure that authorityKeyIdentifier.keyIdentifier in a certificate to be verified and subjectKeyIdentifier in an issuer certificate are identical.								
		Base.RP.12	The RP should reject certificate chain when authorityKeyIdentifier.keyIdentifier in a certificate to be verified and subjectKeyIdentifier in an issuer certificate are different. **[RFC3280 4.2.1.2]**		Base.RP.12.01	The following path should not be successfully validated; the authorityKeyIdentifier.keyIdentifier in Subscriber is different from the subjectKeyIdentifier in RootCA. **NOTE**: This may be just test case for the path construction, not for the path validation. At least, No necessary for the path validation testing. [RootCA, Subscriber] RootCA.subjectKeyID: keyID.RootCA	2	Subscriber	authorityKeyID - keyIdentifier	hoge
	Validity	The RP should ensure that all certificates in a certification path are in validity period.								
		Base.RP.13	The RP should reject a certification path when a certificate to be verified has a notBefore later than current time. **[X.509 10.5.1]**		Base.RP.13.01	The following path should not be successfully validated; the notBefore in Subscriber is later than current time. [RootCA, Subscriber] current time < Subscriber.notBefore	0	Subscriber	Validity - notBefore	> current time
		Base.RP.14	The RP should reject certification path when a certificate to be verified has a notAfter earlier than current time. **[X.509 10.5.1]**		Base.RP.14.01	The following path should not be successfully validated; the notAfter in Subscriber is earlier than current time. [RootCA, Subscriber] Subscriber.notAfter < current time	0	Subscriber	Validity - notAfter	< current time
		Base.RP.15	The RP should reject a certification path when an issuer certificate has a notBefore later than current time. **[X.509 10.5.1]**		Base.RP.15.01	The following path should not be successfully validated; the notBefore in RootCA is later than current time. [RootCA, Subscriber] current time < RootCA.notBefore	0	RootCA	Validity - notBefore	> current time
		Base.RP.16	The RP should reject a certification path when an issuer certificate has a notAfter earlier than current time. **[X.509 10.5.1]**		Base.RP.16.01	The following path should not be successfully validated; the notAfter in RootCA is earlier than current time. [RootCA, Subscriber] RootCA.notAfter < current time	0	RootCA	Validity - notAfter	< current time
		Base.RP.17	The RP should a reject certification path when a certificate has a notAfter set 500101000000Z. **[X.509 7]**		Base.RP.17.01	The following path should not be successfully validated; the notAfter in Subscriber has been set 500101000000Z. [RootCA, Subscribber] Subscriber.notAfter: 500101000000Z	0	Subscriber	Validity - notAfter	500101000000Z
		Base.RP.18	The RP should reject a certification path when a certificate has a notBefore set 491231235959Z. **[X.509 7]**		Base.RP.18.01	The following path should not be successfully validated; the not Before in Subscriber has been set 491231235959Z. [RootCA, Subscriber] Subscriber.notBefore: 491231235959Z	0	Subscriber	Validity - notBefore	491231235959Z

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP	Signature	Base.RP.19	The RP should verify signatureValue in a certificate to be verified with a issuer certificate. **[X.509 10.5.1]**		Base.RP.19.01	The following path should not be successfully validated; the signature on Subscriber is invalid. [RootCA, Subscriber] Subscriber.signatureValue: tampered	0	Subscriber	signatureValue	tampered
	Revocation	Base.RP.20	The RP should reject a certification path when a certificate to be verified has been revoked. **[X.509 10.5.1]**		Base.RP.20.01	The following path should not be successfully validated; Subscriber has been revoked. [RootCA, Subscriber] RootCA.CRL.revokedCertificates: Subscriber.serialNumber	0	RootCA.CRL	revokedCertificates	Subscriber.serialNumber
	Constraints	Base.RP.21	The RP should proccess a certification path which contains a certificate which has unrecognized extensions. **[X.509 7]**		Base.RP.21.01	The following path should be successfully validated; Subscriber has an unrecognized extension which is not marked critical. [RootCA, Subscriber] Subscriber.UnknownExt: 001 (non-critical)	0	Subscriber	UnknownExt	non-critical id-pe-unknownExt OID ::= { id-pe 99 } UnknownExt ::= BIT STRING { shima-nagashi (0), hara-kiri (1), otogame-nashi (2) }
					Base.RP.21.02	The following path should not be sccessfully validated; Subscriber has an unrecognized extension which is marked critical. [RootCA, Subscriber] Subscriber.UnknownExt: 01 (critical)	0	Subscriber	UnknownExt	critical

entitiy	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
CA	CertChains	the same as Base Model								
	Validity	the same as Base Model								
	Constraints	Int.SH.CA.01	The CA should issue a CA certificate which has the basicConstraints present and critical with cA flag asserted. [X.509 8.4.2.1]		Int.SH.CA.01.01	Issue a CA certificate which has the basicConstraints present and critical with cA flag asserted.	0			
		Int.SH.CA.02	The CA should issue a CA certificate which has the keyUsage present and critical with keyCertSign bit asserted, except for self-signed certificate. [X.509 8.2.2.3]		Int.SH.CA.02.01	Issue a CA certificate which has the keyUsage present and critical with keyCertSign bit asserted.	0			
		Int.SH.CA.03	The CA should issue a CA certificate which has the basicConstraints present and critical with pathLenConstraints set, except for self-signed certificate. [X.509 8.4.2.1]		Int.SH.CA.03.01	Issue a CA certificate which has the basicConstraints present and critical with pathLenConstraints set.	1			
	CertPolicy	Int.SH.CA.04	The CA should issue a certificate which has the certificatePolicies which contains one policyIdentifier present and critical, except for self-signed certificate.		Int.SH.CA.04.01	Issue a certificate which has the certificatePolicies which contains one policyIdentifier present and critical.	0			
		Int.SH.CA.05	The CA should issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and critical, except for self-signed certificate.		Int.SH.CA.05.01	Issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and critical.	1			
		Int.SH.CA.06	The CA should issue a certificate which has the certificatePolicies which contains one policyIdentifier present and not critical, except for self-signed certificate. [X.509 8.2.2.6]		Int.SH.CA.06.01	Issue a certificate which has the certificatePolicies which contains one policyIdentifier present and not critical.	1			
		Int.SH.CA.07	The CA should issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and not critical, except for self-signed certificate. [X.509 8.2.2.6]		Int.SH.CA.07.01	Issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and not critical.	1			
RP	NormalCase	Int.SH.RP.08	Int.SH Normal Case		Int.SH.RP.08.01	The following path should be successfully validated; every certificate in the path is according to Base Profiles. [RootCA, SubCA-1, Subscriber-1] RootCA issuerDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectKeyID.keyIdentifier: keyID.RootCA SubCA-1 issuerDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectDN: cn=SubCA-1, ou=Sub, ou=Root, o=PVTG Draft, c=AA basicConstraints.cA TRUE (critical) authorityKeyID.keyIdentifier: keyID.RootCA subjectKeyID: keyID.SubCA-1 keyUsage: keyCertSign, cRLSign (critical) certificatePolicies.policyIdentifier: policy-A (critical) Subscriber-1 issuerDN: cn=SubCA-1, ou=Sub, ou=Root, o=PVTG Draft, c=AA subjectDN: cn=Subscriber-1, ou=Sub, ou=Root, o=PVTG Draft, c=AA authorityKeyID.keyIdentifier: keyID.SubCA-1 subjectKeyID: keyID.Subscriber-1 certificatePolicies.policyIdentifier: policy-A (critical)	0			

entitiy	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP	CertChains	The RP should validate a path which contains a subordinate CA certificate.								
		Int.SH.RP.09	The RP shoud ensure that issuer name in one certificate and subject name in its issuer certificate are identical. **[X.509 10.5.1]**	Base.RP.08 Base.RP.09 Base.RP.10 Base.RP.11	Int.SH.RP.09.01	The following path should not be successfully validated; the issuer name in SubCA-1 is different from the subject name in RootCA. [RootCA, SubCA-1, Subscriber-1] RootCA.subjectDN: cn=CA, ou=Root, o=PVTG Draft, c=AA SubCA.issuerDN: cn=hoge, ou=Root, o=PVTG Draft, c=AA	0	SubCA-1	issuer	cn=hoge, ou=Root, o=PVTG Draft, c=AA
		Int.SH.RP.10	The RP should ensure that authorityKeyIdentifier.keyIdentifier in one certificate and subjectKeyIdentifier in its issuer certificate are identical. **[RFC3280 4.2.1.2]**	Base.RP.12	Int.SH.RP.10.01	The following path should not be successfully validated; the authorityKeyIdentifier.keyIdentifier in SubCA-1 is different from the subjectKeyIdentifier in RootCA. **NOTE:** This may be just test case for the path construction, not for the path validation. At least, No necessary for the path validation testing. [RootCA, SubCA-1, Subscriber-1] RootCA.SubjectKeyID: keyID.RootCA SubCA.authorityKeyID.keyIdentifier: hoge	2	SubCA-1	authorityKeyID - keyIdentifier	hoge
	Validity	the same as Base Model								
	Constraints	The RP should process the basicConstraints extensions in all intermediate CA certificates in the certification path.								
		Int.SH.RP.11	The RP should reject a certification path which containis a subordinate CA certificate which does not have a basicConstraints. **[X.509 10.5.1]**		Int.SH.RP.11.01	The following path should not be successfully validated; SubCA-1 does not have a basicConstraints. [RootCA, SubCA-1, Subscriber-1]	0	SubCA-1	basicConstraints	remove
		Int.SH.RP.12	The RP should reject a certification path which contains a subordinate CA certificate which has basicConstraints present and critical with cA flag set to false. **[X.509 10.5.1]**		Int.SH.RP.12.01	The following path should not be successfully validated; SubCA-1 has basicConstraints present and critical with cA flag set to false. [RootCA, SubCA-1, Subscriber-1] SubCA-1.basicConstraints.cA: FALSE	0	SubCA-1	basicConstraints - cA	FALSE
		Int.SH.RP.13	The RP should reject a certification path which contains a subordinate CA certificate which has basicConstraints present and not critical with cA flag asserted.		Int.SH.RP.13.01	The following path should be successfully validated; SubCA-1 has basicConstraints present and not critical with cA flag asserted. [RootCA, SubCA-1, Subscriber-1] SubCA-1.basicConstraints.cA: TRUE (non-critical)	0	SubCA-1	basicConstraints	non-critical
		Int.SH.RP.14	The RP should process basicConstraints.pathLenConstraints in all subordinate CA certificates in the certification path. **[X.509 10.5.1]**		Int.SH.RP.14.01	The following path should be successfully validated; SubCA-1 has the basicConstraints present and critical with pathLenConstraints set to 0. [RootCA, SubCA-1, Subscriber-1] SubCA-1.basicConstraints.pathLenConstraints: 0	1	SubCA-1	basicConstraints - pathLenConstraints	0
					Int.SH.RP.14.02	The following path should not be successfully validated; SubCA-1 has the basicConstraints present and critical with pathLenConstraints set to 0. [RootCA, SubCA-1, SubCA2, Subscriber-2] SubCA-1.basicConstraints.pathLenConstraints: 0				
		The RP should ensure that all intermediate CA certificates have the keyUsage extension present and critical with keyCertSign bit asserted.								
		Int.SH.RP.15	The RP should reject a certification path which contains an intermediate CA certificate which does not have keyUsage extension. **[IWG profile]**		Int.SH.RP.15.01	The following path should not be successfully validated; SubCA-1 does not have a keyUsage. [RootCA, SubCA-1, Subscriber-1]	0	SubCA-1	keyUsage	remove
		Int.SH.RP.16	The RP should reject a certification path which contains an intermediate CA certificate which has the keyUsage present, with a bit other than keyCertSign. **[IWG profile]**		Int.SH.RP.16.01	The following path should not be successfully validated; SubCA-1 has the keyUsage present and critical with digitalSignature bit asserted. [RootCA, SubCA-1, Subscriber-1] SubCA-1.keyUsage: digitalSignature	0	SubCA-1	keyUsage	digitalSignature

entitiy	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP		Int.SH.RP.17	The RP should reject a certification path which contains an intermediate CA certificate which has the keyUsage present and not critical, with keyCertSign bit asserted.		Int.SH.RP.17.01	The following path should be successfully validated; SubCA-1 has the keyUsage present and not critical with keyCertSign bit asserted. [RootCA, SubCA-1, Subscriber-1] SubCA-1.keyUsage: keyCertSign (non-critical)	0	SubCA-1	keyUsage	non-critical
	CertPolicy	The RP should process certificatePolicies in all certificates for validating the certification path.								
		Int.SH.RP.18	The RP should ensure that all certificates in a certification path except self-signed certificate have the same policyIdentifier asserted. **[X.509 8.1.1]**		Int.SH.RP.18.01	The following path should not be successfully validated; Subscriber-1 has an invalid policyIdentifier in the critical certificatePolicies. [RootCA, SubCA-1, Subscriber] SubCA-1 certificatePolicies.policyIdentifier: policy-A (critical) Subscriber-1 certificatePolicies.policyIdentifier: policy-B (critical)	0	Subscriber-1	certificatePolicies - policyIdentifier	policy-B
		Int.SH.RP.19	The RP should process certificatePolicies correctly when it has not been marked critical.		Int.SH.RP.19.01	The following path should be successfully validated; Subscriber-1 has a valid policyIdentifier in the non-critical certificatePolicies. [RootCA, SubCA-1, Subscriber] SubCA-1 certificatePolicies.policyIdentifier: policy-A (critical) Subscriber-1 certificatePolicies.policyIdentifier: policy-A (non-critical)	1	Subscriber-1	certificatePolicies	non-critical
					Int.SH.RP.19.02	The following path should not be successfully validated; Subscriber-1 has an invalid policyIdentifier in the non-critical certificatePolicies. [RootCA, SubCA-1, Subscriber] SubCA-1 certificatePolicies.policyIdentifier: policy-A (critical) Subscriber-1 certificatePolicies.policyIdentifier: policy-B (non-critical)		1. Subscriber-1	1.1 certificatePolicies 1.2 certificatePolicies - policyIdentifiers	2.1. non-critical 2.2. policy-B
		Int.SH.RP.20	The RP should process a certification path which contains a certificate which has plural policyIdentifier present. **[X.509 8.1.1]**		Int.SH.RP.20.01	The following path should be successfully validated; the intermediate certificates have plural policyIdentifier in the critical certificatePolicies, and a valid policyIdentifier appears in all certificates. [RootCA, SubCA-1, SubCA-2, Subscriber-2] SubCA-1 certificatePolicies.policyIdentifier: policy-A, policy-B (critical) SubCA-2 certificatePolicies.policyIdentifier: policy-A, policy-C (critical) Subscriber-2 certificatePolicies.policyIdentifier: policy-A (critical)	1	1. SubCA-1 2. SubCA-2	certificatePolicies - policyIdentifier	1. policy-A, policy-B 2. policy-A, policy-C
					Int.SH.RP.20.02	The following path should not be successfully validated; the intermediate certificates have plural policyIdentifier in the critical certificatePolicies, and a valid policyIdentifier does not appear in Subscriber-2. [RootCA, SubCA-1, SubCA-2, Subscriber-2] SubCA-1 certificatePolicies.policyIdentifier: policy-A, policy-B (critical) SubCA-2 certificatePolicies.policyIdentifier: policy-A, policy-C (critical) Subscriber-2 certificatePolicies.policyIdentifier: policy-C (critical)		1. SubCA-1 2. SubCA-2 3. Subscriber-2	certificatePolicies - policyIdentifier	1. policy-A, policy-B 2. policy-A, policy-C 3. policy-C

entitiy	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP		Int.SH.RP.21	The RP should process a certification path which contains a certificate which has plural policyIdentifier present and not critical.		Int.SH.RP.21.01	The following path should be successfully validated; the intermediate certificates have plural policyIdentifier including a valid policyIdentifier in the critical certificatePolicies, and Subscriber-2 has a valid policyIdentifier in the non-critical certificatePolicies. [RootCA, SubCA-1, SubCA-2, Subscriber-2] SubCA-1 certificatePolicies.policyIdentifier: policy-A, policy-B (critical) SubCA-2 certificatePolicies.policyIdentifier: policy-A, policy-C (critical) Subscriber-2 certificatePolicies.policyIdentifier: policy-A (non-critical)	2	1. SubCA-1 2. SubCA-2 3. Subscriber-2	1. certificatePolicies - policyIdentifier 2. certificatePolicies - policyIdentifier 3. certificatePolicies	1. policy-A, policy-B 2. policy-A, policy-C 3. non-critical
					Int.SH.RP.21.02	The following path should not be successfully validated; the intermediate certificates have plural policyIdentifier including a valid policyIdentifier in the critical certificatePolicies, and Subscriber-2 does not have a valid policyIdentifier in the non-critical certificatePolicies. [RootCA, SubCA, SubCA2, Subscriber] SubCA certificatePolicies.policyIdentifier: policy-A, policy-B (critical) SubCA2 certificatePolicies.policyIdentifier: policy-A, policy-C (critical) Subscriber certificatePolicies.policyIdentifier: policy-C (non-critical)		1. SubCA-1 2. SubCA-2 3. Subscriber-2	1. certificatePolicies - policyIdentifier 2. certificatePolicies - policyIdentifier 3.1 certificatePolicies 3.2 certificatePolicies - policyIdentifier	1. policy-A, policy-B 2. policy-A, policy-C 3.1 non-critical 3.2 policy-C
	Revocation	Int.SH.RP.22	The RP should reject a certification path which contains a intermediate CA certificate revoked. **[X.509 10.5.1]**	Base.RP.20	Int.SH.RP.22.01	The following path should not be successfully validated; SubCA-1 has been revoked. [RootCA, SubCA-1, Subscriber-1]	0	RootCA.CRL (or ARL)	revokedCertificates	SubCA-1.serialNumber
	Signature	Int.SH.RP.23	The RP should verify signatureValue in a intermediate CA certificate with its issuer certificate **[X.509 10.5.1]**	Base.RP.19	Int.SH.RP.23.01	The following path should not be successfully validated; the signature of SubCA-1 is invalid. [RootCA, SubCA-1, Subscriber-1] SubCA-1.signatureValue: tampered	0	SubCA-1	signatureValue	tampered

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
CA	CertChains	Int.CC.CA.01	The CA should issue a cross-certificate request which contains subjectKeyIdentifier in extensionRequest, and its value must be identical with subjectKeyIdentifier in self-signed certificate. **[IWG profile]**		Int.CC.CA.01.01	Issue a cross-certificate request which contains subjectKeyIdentifier in extensionRequest, and its value must be identical with subjectKeyIdentifier in self-signed certificate.	2			
		Int.CC.CA.02	The CA should issue a cross-certificate which contains subjectKeyIdentifier set to the same value in the cross-certificate request. **[IWG profile]**		Int.CC.CA.02.01	Issue a cross-certificate which has the subjectKeyIdentifier set to the same value in cross-certificate request.	2			
	Validity	the same as Base Model								
	CertPolicy	Int.CC.CA.03	The CA should issue a certificate which has the certificatePolicies which contains one policyIdentifier present and critical, except for self-signed certificate.	Int.SH.CA.04	Int.CC.CA.03.01	Issue a certificate which has the certificatePolicies which contains one policyIdentifier present and critical.	0			
		Int.CC.CA.04	The CA should issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and critical, except for self-signed certificate.	Int.SH.CA.05	Int.CC.CA.04.01	Issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and critical.	1	CrossCert	certificatePolicies - policyIdentifier	policy-X, policy-W
		Int.CC.CA.05	The CA should issue a certificate which has the certificatePolicies which contains one policyIdentifier present and not critical, except for self-signed certificate. **[X.509 8.2.2.6]**	Int.SH.CA.06	Int.CC.CA.05.01	Issue a certificate which has the certificatePolicies which contains one policyIdentifier present and not critical.	1	CrossCert	certificatePolicies	non-critical
		Int.CC.CA.06	The CA should issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and not critical, except for self-signed certificate. **[X.509 8.2.2.6]**	Int.SH.CA.07	Int.CC.CA.06.01	Issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and not critical.	2	CrossCert	certificatePolicies - policyIdentifier	non-critical policy-X, policy-W
		Int.CC.CA.07	The CA should issue a cross-certificate which contains one policyMappings. **[X.509 8.1.3]**		Int.CC.CA.07.01	Issue a cross-certificate which has a policyMappings present and non-critical.	0			
		Int.CC.CA.08	The CA should issue a cross-certificate which contains plural PolicyMappings. **[X.509 8.1.3]**		Int.CC.CA.08.01	Issue a cross-certificate which has plural policyMappings present and non-critical.	2	CrossCert	policyMappings	policy-X=policy-Y policy-X=policy-W
	Constraints	Int.CC.CA.09	The CA should issue a CA certificate which has the basicConstraints present and critical with cA flag asserted. **[X.509 8.4.2.1]**	Int.SH.CA.01	Int.CC.CA.09.01	Issue a CA certificate which has the basicConstraints present and critical with cA flag asserted.	0			
		Int.CC.CA.10	The CA should issue a CA certificate which has the keyUsage present and critical with keyCertSign bit asserted, except for self-signed certificate. **[X.509 8.2.2.3]**	Int.SH.CA.02	Int.CC.CA.10.01	Issue a CA certificate which has the keyUsage present and critical with keyCertSign bit asserted.	0			
		Int.CC.CA.11	The CA should issue a CA certificate which has the basicConstraints present and critical with pathLenConstraints set, except for self-signed certificate. **[X.509 8.4.2.1]**	Int.SH.CA.03	Int.CC.CA.11.01	Issue a CA certificate which has the basicConstraints present and critical with pathLenConstraints set.	1	CrossCert	basicConstraints - pathLenConstraints	0
		Int.CC.CA.12	The CA should issue a cross-certificate which contains the policyConstraints present and critical. **[X.509 10.5.2, 10.5.3]**		Int.CC.CA.12.01	Issue a cross-certificate which has the policyConstraints present and critical, and the requireExplicitPolicy is set.	1	CrossCert	policyConstraints - requireExplicitPolicy	0
					Int.CC.CA.12.02	Issue a cross-certificate which has the policyConstraints present and critical, and the inhibitPolicyMapping is set.	1	CrossCert	policyConstraints - inhibitPolicyMapping	0

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
CA		Int.CC.CA.13	The CA should issue a cross-certificate which contains the nameConstraints present and critical. **[X.509 10.5.2]**		Int.CC.CA.13.01	Issue a cross-certificate which has the nameConstraints present and critical, and the permittedSubtrees.base is set in the form DirectoryName encoded as UTF8String.	1	CrossCert	nameConstraints - permitSubtrees - base	ou=Root-Y, o=PVTG Draft, c=BB
					Int.CC.CA.13.02	Issue a cross-certificate which has the nameConstraints present and critical, and the excludedSubtrees.base is set in the form DirectoryName encoded as UTF8String.	1	CrossCert	nameConstraints - excludeSubtrees - base	ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB
		Int.CC.CA.14	The CA should issue a cross-certificate which has the inhibitAnyPolicy present and critical. **[X.509 10.5.2]**		Int.CC.CA.14.01	Issue a cross-certificate which has the inhibitAnyPolicy present and critical.	2	CrossCert	inhibitAnyPolicy - SkipCerts	0
	Revocation	Int.CC.CA.15	The CA should issue a certificate which contains cRLDistributionPoints, except for self-signed certificate. **[IWG profile]**		Int.CC.CA.15.01	Issue a certificate which has cRLDistributionPoints.distributionPoint.fullName present and not critical.	0			
		Int.CC.CA.16	The CA should issue a certificate which has the authorityInfoAccess extensions present and not critical, except for self-signed certificate. **[IWG profile]**		Int.CC.CA.16.01	Issue a certificate which has the authorityInfoAccess extensions present and not critical.	2	ALL	1. authorityInfoAccess - accessMethod 2. authorityInfoAccess - accessLocation	1. id-ad-ocsp 2. http://hoge/
		Int.CC.CA.17	The CA should issue a Certificate Revocation List that contains the issuingDistributionPoint present and critical with the olnyContainsUserCerts component set to true. **[IWG profile]**		Int.CC.CA.17.01	Issue a Certificate Revocation List that contains the issuingDistributionPoint present and critical with the olnyContainsUserCerts component set to true.	1			
		Int.CC.CA.18	The CA should issue an Authority Revocation List that contains the issuingDistributionPoint present and critical with the olnyContainsCACerts component set to true. **[IWG profile]**		Int.CC.CA.18.01	Issue an Authority Revocation List that contains the issuingDistributionPoint present and critical with the olnyContainsCACerts component set to true.	1			
RP	NormalCase	Int.CC.RP.19	Int.CC Normal Case		Int.CC.RP.19.01	The following path should be successfully validated; every certificate in the path is according to Base Profiles. [RootCA-X, CrossY-X, Subscriber] RootCA-X (self-signed) issuerDN: cn=CA-X, ou=Root-X, o=PVTG Draft, c=AA subjectDN: cn=CA-X, ou=Root-X, o=PVTG Draft, c=AA subjectKeyID: keyID.RootCA-X CrossY-X (cross cert issuedTo Y issuedBy X) issuerDN: cn=CA-X, ou=Root-X, o=PVTG Draft, c=AA subjectDN: cn=CA-Y, ou=Root-Y, o=PVTG Draft, c=BB authorityKeyID: keyID.RootCA-X subjectKeyID: keyID.CroosY-X basicConstraints.cA true (critical) keyUsage: keyCertSign, cRLSign (critical) certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y Subscriber-Y issuerDN: cn=CA-Y, ou=Root-Y, o=PVTG Draft, c=BB subjectDN: cn=Subscriber-Y, ou=Root-Y, o=PVTG Draft, c=BB certificatePolicies.policyIdentifier: policy-Y (critical)	0			

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP	CertChains	The RP should validate a path which contains a cross-certificate.								
		Int.CC.RP.20	The RP shoud ensure that issuer name in one certificate and subject name in its issuer certificate are identical. **[X.509 10.5.1]**	Base.RP.08 Base.RP.09 Base.RP.10 Base.RP.11	Int.CC.RP.20.01	The following path should not be successfully validated; the issuer name in CrossY-X is different from the subject name in RootCA-X. [RootCA, CrossY-X, Subscriber-1] RootCA-X.subjectDN: cn=CA-X, ou=Root-X, o=PVTG Draft, c=AA CrossY-X.issuerDN: cn=hoge, ou=Root-X, o=PVTG Draft, c=AA	0	CroosY-X	issuer	cn=hoge, ou=Root-X, o=PVTG Draft , c=AA
		Int.CC.RP.21	The RP should ensure that authorityKeyIdentifier.keyIdentifier in one certificate and subjectKeyIdentifier in its issuer certificate are identical. **[RFC3280 4.2.1.2]**	Base.RP.12	Int.CC.RP.21.01	The following path should not be successfully validated; the authorityKeyIdentifier.keyIdentifier in CroosY-X is different from subjectKeyIdentifier in RootCA-X. **NOTE:** This may be just test case for the path construction, not for the path validation. At least, No necessary for the path validation testing. [RootCA-X, CroosY-X, Subscriber-Y] RootCA-X.SubjectKeyID: keyID.RootCA-X CroosY-X.authorityKeyID.keyIdentifier: hoge	2	CroosY-X	authorityKeyID - keyIdentifier	hoge
	Validity	the same as Base Model								
	CertPolicy	The RP should process certificatePolicies and policyMappings in all certificates for validating the certification path.								
		Int.CC.RP.22	The RP should ensure that all certificates in a certification path except self-signed certificate have the same policyIdentifier asserted. **[X.509 8.1.1]**		Int.CC.RP.22.01	The following path should not be successfully validated; Subscriber-Y has an invalid policyIdentifier in the critical certificatePolicies field. [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y Subscriber-Y certificatePolicies.policyIdentifier: policy-W (critical)	0	Subscriber-Y	certificatePolicies - policyIdentifier	policy-W (critical)
		Int.CC.RP.23	The RP should process certificatePolicies correctly when it has not been marked critical.		Int.CC.RP.23.01	The followin path should be successfully validated; Subscriber-Y has a valid policyIdentifier in the non-critical certificatePolicies. [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y Subscriber certificatePolicies.policyIdentifier: policy-Y (non-critical)	0	Subscriber-Y	certificatePolicies - policyIdentifier	policy-Y (non-critical)
					Int.CC.RP.23.02	The following path should not be successfully validated; Subscriber-Y has an invalid policyIdentifier in the non-critical certificatePolicies. [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y Subscriber certificatePolicies.policyIdentifier: policy-W (non-critical)		Subscriber-Y	certificatePolicies - policyIdentifier	policy-W (non-critical)

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP		Int.CC.RP.24	The RP should process a certification path which contains a certificate which has plural policyIdentifier present. **[X.509 8.1.1]**		Int.CC.RP.24.01	The following path should be successfully validated; CroosY-X has plural policyIdentifier in the critical certificatePolicies, and a valid policyIdentifier appears in all certificates. [RootCA-X, CroosY-X, Subordinate-Y] CroosY-X certificatePolicies.policyIdentifier: policy-X, policy-V (critical) policyMappings: policy-X = policy-Y Subordinate-Y certificatePolicies.policyIdentifier: policy-Y (critical)	1	CrossY-X	certificatePolicies - policyIdentifier	policy-X, policy-V
					Int.CC.RP.24.02	The following path should not be successfully validated; CroosY-X has plural policyIdentifier in the critical certificatePolicies, and a valid policyIdentifier does not appear in Subscriber-Y. [RootCA-X, CroosY-X, Subordinate-Y] CroosY-X certificatePolicies.policyIdentifier: policy-X, policy-V (critical) policyMappings: policy-V = policy-Y Subordinate-Y certificatePolicies.policyIdentifier: policy-Y (critical)		CrossY-X	1.1 certificatePolicies - policyIdentifier 1.2 policyMappings	1.1 policy-X, policy-V 1.2 policy-V = policy-Y
		Int.CC.RP.25	The RP should process a certification path which contains a certificate which has plural policyMappings present. **[X.509 8.1.1]**		Int.CC.RP.25.01	The following path should be successfully validated; CroosY-X has plural policyMappings present, and a valid policyIdentifier appears in all certificates. [RootCA-X, CroosY-X, Subordinate-Y] CroosY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y, policy-X = policy-W Subordinate-Y certificatePolicies.policyIdentifier: policy-W (critical)	1	1. CroosY-X 2. Subscriber-Y	1. policyMappings 2. certificatePolicies - policyIdentifier	1. policy-X = policy-Y, policy-X = policy-W 2. policy-W
					Int.CC.RP.25.02	The following path should not be successfully validated; CroosY-X has plural policyMappings present, and Subscriber-Y has an invalid policyIdentifier in the critical certificatePolicies. [RootCA-X, CroosY-X, Subordinate-Y] CroosY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y, policy-V = policy-W Subordinate-Y certificatePolicies.policyIdentifier: policy-W (critical)	1	1. CroosY-X 2. Subscriber-Y	1. policyMappings 2. certificatePolicies - policyIdentifier	1. policy-X = policy-Y, policy-V = policy-W 2. policy-W
	Constraints	The RP should process the basicConstraints extensions in all cross-certificates in the certification path.								
			The RP should reject a certification path which containis a cross-certificate which does not have a basicConstraints. **[X.509 10.5.1]**	Int.SH.RP.11	Int.CC.RP.26.01	The following path should not be successfully validated; CroosY-X does not have a basicConstraints. [RootCA-X, CroosY-X, Subscriber]	0	CroosY-X	basicConstraints	remove
		Int.CC.RP.27	The RP should reject a certification path which contains a cross-certificate which has basicConstraints present with cA flag set to false. **[X.509 10.5.1]**	Int.SH.RP.12	Int.CC.RP.27.01	The following path should not be successfully validated; CroosY-X has the basicConstraints present and critical, with cA flag set to false. [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X.basicConstraints.cA: FALSE	0	CroosY-X	basicConstraints - cA	FALSE
		Int.CC.RP.28	The RP should reject a certification path which contains a cross-certificate which has basicConstraints present and not critical with cA flag asserted.		Int.CC.RP.28.01	The following path should be successfully validated; CroosY-X has the basicConstraints present and not critical with cA flag asserted. [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X.basicConstraints.cA: TRUE (non-critical)	0	CroosY-X	basicConstraints	non-critical

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP		Int.CC.RP.29	The RP should process basicConstraints.pathLenConstraints in all cross-certificates in the certification path. **[X.509 10.5.1]**	Int.SH.RP.14	Int.CC.RP.29.01	the following path should be successfully validated. [RootCA-X, CroosY-X, Subordinate-Y] CroosY-X.basicConstraints.pathLenConstraints: 0[deafault] **NOTE:** This skipCerts value is adjustable for your hierarchy, if necessary. Deafult(non-hierarchy) is zero.	1	CroosY-X	basicConstraints - pathLenConstraints	default:0 (
					Int.CC.RP.29.02	The following path should not be successfully validated. [RootCA-X, CroosY-X, CrossZ-Y, Subscriber-Z] CroosY-X.basicConstraints.pathLenConstraints: 0[deafult] **NOTE:** This skipCerts value is adjustable for your hierarchy, if necessary. Deafult(non-hierarchy) is zero.				
		The RP should ensure that all intermediate cross-certificates have the keyUsage extension present and critical with keyCertSign bit asserted.								
		Int.CC.RP.30	The RP should reject a certification path which contains an intermediate CA certificate which does not have keyUsage extension. **[IWG profile]**	Int.SH.RP.15	Int.CC.RP.30.01	The following path should not be successfully validated; CroosY-X does not have a keyUsage. [RootCA-X, CroosY-X, Subscriber-Y]	0	CroosY-X	keyUsage	remove
		Int.CC.RP.31	The RP should reject a certification path which contains an intermediate CA certificate which has the keyUsage present and critical, with a bit other than keyCertSign. **[IWG profile]**	Int.SH.RP.16	Int.CC.RP.31.01	The following path should not be successfully validated; CroosY-X has the keyUsage present and critical, with digitalSignature bit asserted. [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X.keyUsage: digitalSignature (critical)	0	CroosY-X	keyuUsage	digitalSignature
		Int.CC.RP.32	The RP should reject a certification path which contains an intermediate CA certificate which has the keyUsage present and not critical, with keyCertSign bit asserted.		Int.CC.RP.32.01	The following path should be successfully validated; CroosY-X has the keyUsage present and not critical with keyCertSign bit asserted. [RootCA-X, CroosY-X, Subordinate-Y] CroosY-X.keyUsage: keyCertSign (non-critical)	0	CroosY-X	keyUsage	non-critical
		The RP should process policyConstraints extensions in all cross-certificates in the certification path.								
		Int.CC.RP.33	The RP should process policyConstraints.requireExplicitPolicy in all cross-certificates in the path. **[X.509 10.5.2, 10.5.3]**		Int.CC.RP.33.01	The following path should be successfully validated; CroosY-X has the critical policyConstraints.requireExplicitPolicy present and set to 1, and Subscriber-Y has an invalid policyIdentifier in the critical certificatePolicies field. [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X policyConstraints.rEP: 1 **NOTE:** This skipCerts value is adjustable for your hierarchy, if necessary. Deafult(non-hierarchy) is one. Subscriber-Y certificatePolicies.policyIdentifier: hoge	2	1. CroosY-X 2. Subscriber-Y	1. policyConstraints - requireExplicitPolicy 2. certificatePolicies - policyIdentifier	1. 1 2. hoge
					Int.CC.RP.33.02	The following path should not be successfully validated; CroosY-X has the critical policyConstraints.requireExplicitPolicy present and set to 0, and Subscriber-Y has an invalid policyIdentifier in the critical certificatePolicies field. [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X policyConstraints.rEP: 0 **NOTE**: This skipCerts value is adjustable for your hierarchy, if necessary. Deafult(non-hierarchy) is zero. Subscriber-Y certificatePolicies.policyIdentifier: hoge		1. CroosY-X 2. Subscriber-Y	1. policyConstraints - requireExplicitPolicy 2. certificatePolicies - policyIdentifier	1. 0 2. hoge

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
		Int.CC.RP.34	The RP should process policyConstraints.inhibitPolicyMapping in all cross-certificates in the path. **[X.509 10.5.2, 10.5.3]**		Int.CC.RP.34.01	The following path should be successfully validated; CroosY-X has policyConstraints present and critical with the inhibitPolicyMapping component set to 1. [RootCA-X, CroosY-X, CrossZ-Y, Subscriber-Z] CroosY-X.policyConstraints.iPM: 1	2	CroosY-X	policyConstraints - inhibitPolicyMapping	1
					Int.CC.RP.34.02	The following path should not be validated successfully; CroosY-X has policyConstraints present and critical with the inhibitPolicyMapping component set to 0. [RootCA-X, CroosY-X, CrossZ-Y, Subscriber-Z] CroosY-X.policyConstraints.iPM: 0		CroosY-X	policyConstraints - inhibitPolicyMapping	0

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP		The RP should process nameConstraints extensions in all cross-certificates in the certification path.								
		Int.CC.RP.35	The RP should process nameConstraints.permittedSubtrees in all cross-certificates in the certification path. **[X.509 10.5.2]**		Int.CC.RP.35.01	The following path should be successfully validated; CroosY-X has the nameConstraints present and critical with the permittedSubtrees.base set "ou=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X.nameConstraints.permittedSubtrees.base: ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y.subject: cn=Subscriber-Y, ou=Root-Y, o=PVTG Draft, c=BB	2	CroosY-X	nameConstraints - permitSubtrees.base	ou=CroosY-X, o=PVTG Draft, c=BB
					Int.CC.RP.35.02	The following path should not be successfully validated; CroosY-X has the nameConstraints present and critical with the permittedSubtrees.base set "ou=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X nameConstraints.permittedSubtrees.base: ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y subjectDN: cn=Subscriber-Y, o=PVTG Draft, c=BB		1. CroosY-X 2. Subscriber-Y	1. nameConstraints - permittedSubtrees.base 2. subject	1. ou=Root-Y, o=PVTG Draft, c=BB 2. cn=Subscriber-Y, o=PVTG Draft, c=BB
		Int.CC.RP.36	The RP should process nameConstraints.excludedSubtrees in all cross-certificates in the certification path. **[X.509 10.5.2]**		Int.CC.RP.36.01	The following path should be successfuly validated; CroosY-X has the nameConstraints present and critical, with the excludedSubtrees.base component set "ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X nameConstraints.excludedSubtrees.base: ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y subject: cn=Subscriber-Y, ou=Root-Y, o=PVTG Draft, c=BB	2	1. CroosY-X 2. Subscriber-Y	1. nameConstraints - excludedSubtrees.base 2. subject	1. ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB 2. cn=Subscriber-Y, ou=Root-Y, o=PVTG Draft, c=BB
					Int.CC.RP.36.02	The following path should not be successfully validated; CroosY-X has the nameConstraints present and critical, with the excludedSubtrees.base set "ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB". Subject name in Subscriber-Y is "cn=Subscriber-Y, ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X nameConstraints.excludedSubtrees.base: ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y subject: cn=Subscriber-Y, ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB		1. CroosY-X 2. Subscriber-Y	1. nameConstraints - excludedSubtrees.base 2. subject	1. ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB 2. cn=Subscriber-Y, ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB
		Int.CC.RP.37	The RP should correctly process a path which contains a cross-certificate including both the nameConstraints.permittedSubtrees and the nameConstraints.excludedSubtrees. **[X.509 10.5.2]**		Int.CC.RP.37.01	The following path should not be successfully validated; CroosY-X has the critical nameConstraints present with permittedSubtrees component set "ou=Root-Y, o=PVTG Draft, c=BB", and with excludedSubtrees component set "ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB". the subject name in Subscriber-Y is "cn=Subscriber-Y, ou=hoge, o=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CroosY-X, Subscriber-Y] CroosY-X nameConstraints.permittedSubtrees.base: ou=Root-Y, o=PVTG Draft, c=BB nameConstraints.excludedSubtrees.base: ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y subject: cn=Subscriber-Y, ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB	2	1. CroosY-X 2. Subscriber-Y	1.1 nameConstraints - permittedSubtrees.base 1.2 nameConstraints - excludedSubtrees.base 2. subject	1.1 ou=Root-Y, o=PVTG Draft, c=BB 1.2 ou=hoge, ou=Root-Y, o=PVTG Draft, c=BB 2. cn=Subscriber-Y, ou=hoge, ou=PVTG Draft, c=BB

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP	Revocation	Int.CC.RP.38	The RP should reject a certification path which contains a cross-certificate revoked. **[X.509 10.5.1]**	Base.RP.20	Int.CC.RP.38.01	The following path should not be successfully validated; CroosY-X has been revoked. [RootCA-X, CroosY-X, Subscriber-Y]	0	RootCA-X.CRL (or ARL)	revokedCertificates	CrossY-X.serialNumber
	Signature	Int.CC.RP.39	The RP should verify signatureValue in a cross-certificate with its issuer certificate. **[X.509 10.5.1]**	Base.RP.19	Int.CC.RP.39.01	The followin path should not be successfully validated; the signature on CroosY-X is invalid. [RootCA-X, CroosY-X, Subscriber-Y]	0	CrossY-X	signatureValue	tampered

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
CA	CertChains	the same as Base Model								
	Validity	the same as Base Model								
	CertPolicy	Int.CR.CA.01	The CA should issue a certificate which has the certificatePolicies which contains one policyIdentifier present and critical, except for self-signed certificate.	Int.SH.CA.04	Int.CR.CA.01.01	Issue a certificate which has the certificatePolicies which contains one policyIdentifier present and critical.	0			
		Int.CR.CA.02	The CA should issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and critical, except for self-signed certificate.	Int.SH.CA.05	Int.CR.CA.02.01	Issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and critical.	1			
		Int.CR.CA.03	The CA should issue a certificate which has the certificatePolicies which contains one policyIdentifier present and not critical, except for self-signed certificate. **[X.509 8.2.2.6]**	Int.SH.CA.06	Int.CR.CA.03.01	Issue a certificate which has the certificatePolicies which contains one policyIdentifier present and not critical.	1			
		Int.CR.CA.04	The CA should issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and not critical, except for self-signed certificate. **[X.509 8.2.2.6]**	Int.SH.CA.07	Int.CR.CA.04.01	Issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and not critical.	2			
RP	NormalCase	Int.CR.RP.05	Int.CR Normal Case		Int.CR.RP.05.01	The following path should be successfully validated; every certificate in the path is according to Base Profiles. [RootCA-Y, Subscriber-Y] RootCA-Y (self-signed) issuerDN: cn=CA-Y, ou=Root-Y, o=PVTG Draft, c=BB subjectDN: cn=CA-Y, ou=Root-Y, o=PVTG Draft, c=BB subjectKeyID.keyIdentifier: keyID.RootCA-Y 1950 < notBefore < current time < notAfter < 2049 Subscriber issuerDN: cn=CA-Y, ou=Root-Y, o=PVTG Draft, c=BB subjectDN: cn=Subscriber-Y, ou=Root-Y, o=PVTG Draft, c=BB authorityKeyID.keyIdentifier: keyID.RootCA-Y subjectKeyID.keyIdentifier: keyID.Subscriber-Y certificatePolicies.policyIdentifier: policy-Y 1950 < notBefore < current time < notAfter < 2049 RP's trust anchor list contains RootCA-Y	0			
	CertChains	The RP should validate a certification path with the trust anchor list.								
		Int.CR.RP.06	The RP should reject a certification path whose trust anchor certificate is not listed on RP's trust anchor list.		Int.CR.RP.06.01	The following path should not be successfully validated; RootCA-Y is not listed on the RP's trust anchor list. [RootCA-Y, Subscriber-Y]	0			
		Int.CR.RP.07	The RP shoud ensure that issuer name in one certificate and subject name in its issuer certificate are identical. **[X.509 10.5.1]**	Base.RP.08 Base.RP.09 Base.RP.10 Base.RP.11	Int.CR.RP.07.01	The following path should not be successfully validated; the issuer name in Subscriber-Y is different from the subject name in RootCA-Y. [RootCA-Y, Subscriber-Y] RootCA-Y.subjectDN: cn=CA-Y, ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y.issuerDN: cn=hoge, ou=Root-Y, o=PVTG Draft, c=BB	0	Subscriber-Y	issuer	cn=hoge, ou=Root-Y, o=PVTG Draft, c=BB
		Int.CR.RP.08	The RP should ensure that authorityKeyIdentifier.keyIdentifier in one certificate and subjectKeyIdentifier in its issuer certificate are identical. **[RFC3280 4.2.1.2]**	Base.RP.12	Int.CR.RP.08.01	The following path should not be successfully validated; the authorityKeyIdentifier.keyIdentifier in Subscriber-Y is different from the subjectKeyIdentifier in RootCA-Y. **NOTE:** This may be just test case for the path construction, not for the path validation. At least, No necessary for the path validation testing. [RootCA-Y, Subscriber-Y] RootCA-Y.subjectKeyID: keyID.RootCA-Y Subscriber-Y.authorityKeyID.keyidentifier: hoge	2	Subscriber-Y	authorityKeyID - keyIdentifier	hoge

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP	Validity	the same as Base Model								
	Signature	Int.CR.RP.09	The RP should reject a certification path whose trust anchor certificate is tamperd. **[X.509 10.5.1]**		Int.CR.RP.09.01	The following path should not be successfully validated; RootCA-Y has been tamperd. [RootCA-Y, Subscriber-Y] RootCA-Y.signatureValue: hoge	0	RootCA-Y	signatureValue	hoge
	CertPolicy	The RP should process certificatePolicies in all certificates for validating the certification path.								
		Int.CR.RP.10	The RP should ensure that all certificates in a certification path except self-signed certificate have a valid policyIdentifier asserted. **[X.509 8.1.1]**	Int.CC.RP.22	Int.CR.RP.10.01	The following path should not be successfully validated; Subscriber-Y does not have a valid policyIdentifier. [RootCA-Y, Subscriber-Y] Subscriber-Y certificatePolicies.policyIdentifier: policy-Z (critical) RP user-initial-policy-set: policy-X, policy-Y	0	Subscriber-Y	certificatePolicies - policyIdentifier	policy-Z (critical)
		Int.CR.RP.11	The RP should process certificatePolicies correctly when it has not been marked critical.		Int.CR.RP.11.01	The following path should be successfully validated; Subscriber-Y has a valid policyIdentifier in non-critical certificatePolicies field. [RootCA-Y, Subscriber-Y] Subscriber-Y certificatePolicies.policyIdentifier: policy-Y (non-critical)	0	Subscriber-Y	certificatePolicies - policyIdentifier	policy-Y (non-critical)
					Int.CR.RP.11.02	The following path should not be successfuly validated; Subscriber-Y does not have a valid policyIdentifier, and certificatePolicies extension has not been marked critical. [RootCA-Y, Subscriber-Y] Subscriber-Y certificatePolicies.policyIdentifier: policy-Z (non-critical)		Subscriber-Y	certificatePolicies - policyIdentifier	policy-Z (non-critical)
		Int.CR.RP.12	The RP should process a certification path which contains a certificate which has plural policyIdentifier present. **[X.509 8.1.1]**	Int.CC.RP.24	Int.CR.RP.12.01	The following path should be successfully validated; Subscriber-Y has plural policyIdentifier in the critical certificatePolicies, in which a valid policyIdentifier is included. [RootCA-Y, Subscriber-Y] Subscriber-Y certificatePolicies.policyIdentifier: policy-Y, policy-Z (critical)	1	Subscriber-Y	certificatePolicies - policyIdentifier	policy-Y, policy-Z (critical)
					Int.CR.RP.12.02	The following path should not be successfully validated; Subscriber-Y has plural policyIdentifier in the critical certificatePolicies, in which a valid policyIdentifier is not included. [RootCA-Y, Subscriber-Y] Subscriber-Y certificatePolicies.policyIdentifier: policy-V, policy-W (critical) RP user-initial-policy-set: policy-X, policy-Y		Subscriber-Y	certificatePolicies - policyIdentifier	policy-V, policy-W (critical)
		Int.CR.RP.13	The RP should process a certification path which contains a certificate which has plural policyIdentifier present and not critical.		Int.CR.RP.13.01	The following path should be successfully validated; Subscriber-Y has plural policyIdentifier in the non-critical certificatePolicies, in which a valid policyIdentifier is included. [RootCA-Y, Subscriber-Y] Subscriber-Y certificatePolicies.policyIdentifier: policy-Y, policy-Z (non-critical)	1	Subscriber-Y	certificatePolicies - policyIdentifier	policy-Y, policy-Z (non-critical)

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
					Int.CR.RP.13.02	The following path should not be successfully validated; Subscriber-Y has plural policyIdentifier in the non-critical certificatePolicies, in which a valid policyIdentifier is not included. [RootCA-Y, Subscriber-Y] Subscriber-Y certificatePolicies.policyIdentifier: policy-V, policy-W (non-critical) RP user-initial-policy-set: policy-X, policy-Y		Subscriber-Y	certificatePolicies - policyIdentifier	policy-V, policy-W (non-critical)
	Revocation	the same as Base Model								

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
CA	CertChains	the same as Base Model								
	Validity	the same as Base Model								
	Constraints	Svc.DS.CA.01	The CA should issue a end-entity certificate which has keyUsage present and critical, with appropriate bit asserted. **[IWG profile]**		Svc.DS.CA.01.01	Issue a certificate which has keyUsage present and critical with digitalSignature bit asserted.	0			
	CertPolicy	Svc.DS.CA.02	The CA should issue a certificate which has the certificatePolicies which contains one policyIdentifier present and critical, except for self-signed certificate.	Int.SH.CA.04	Svc.DS.CA.02.01	Issue a certificate which has the certificatePolicies which contains one policyIdentifier present and critical.	0			
		Svc.DS.CA.03	The CA should issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and critical, except for self-signed certificate.	Int.SH.CA.05	Svc.DS.CA.03.01	Issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and critical.	1			
		Svc.DS.CA.04	The CA should issue a certificate which has the certificatePolicies which contains one policyIdentifier present and not critical, except for self-signed certificate. **[X.509 8.2.2.6]**	Int.SH.CA.06	Svc.DS.CA.04.01	Issue a certificate which has the certificatePolicies which contains one policyIdentifier present and not critical.	1			
		Svc.DS.CA.05	The CA should issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and not critical, except for self-signed certificate. **[X.509 8.2.2.6]**	Int.SH.CA.07	Svc.DS.CA.05.01	Issue a certificate which has the certificatePolicies which contains plural policyIdentifier present and not critical.	2			
RP	NormalCase	Svc.DS.RP.06	Svc.DS Normal Case		Svc.DS.RP.06.01	The following path should be validate successfully; every certificate in the path is according to Base Profiles. [RootCA, Subscriber] RootCA issuerDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectKeyID: keyID.RootCA Subscriber issuerDN: cn=CA, ou=Root, o=PVTG Draft, c=AA subjectDN: cn=Subscriber, ou=Root, o=PVTG Draft, c=AA authorityKeyID.keyIdentifier: keyID.RootCA subjectKeyID: keyID.Subscriber keyUsage: digitalSignature (critical) certificatePolicies.policyIdentifier: policy-A (critical)	0			
	CertChains	the same as Base Model								
	Validity	the same as Base Model								
	Signature	the same as Base Model								
	Constraints	Svc.DS.RP.07	The RP should ensure that a subscriber certificate has appropriate usage in keyUsage extension. **[IWG consideration]**		Svc.DS.RP.07.01	The following path should not be successfully validated; Subscriber does not have keyUsage extensions. [RootCA, Subscriber]	0	Subscriber	keyUsage	remove
					Svc.DS.RP.07.02	The following path should not be successfully validated; Subscriber has the keyUsage present and critical, but digitalSignature bit is not asserted. [RootCA, Subscriber]	0	Subscriber	keyUsage	keyEncipherment (critical)
					Svc.DS.RP.07.03	The following path should be successfully validated; Subscriber has the keyUsage present and not critical, with digitalSignature bit asserted. [RootCA, Subscriber] Subscriber.keyUsage: digitalSignature (non-critical)	0	Subscriber	keyUsage	digitalSignature (non-critical)

entity	category	sequence number	requirement	relevant to ...	test item number	test item	Level	differences		
								Cert type	Field	Value
RP					Svc.DS.RP.07.04	The following path should be successfully validated; Subscriber has the keyUsage present and critical, with digitalSignature and keyAgreement bit asserted. [RootCA, Subscriber] Subscriber.keyUsage: digitalSignature, keyAgreement (critical)	1	Subscriber	keyUsage	digitalSignature, keyAgreement
	CertPolicy	The RP should process certificatePolicies in all certificates for validating the certification path.								
		Svc.DS.RP.08	The RP should ensure that all certificates in a certification path except self-signed certificate have a valid policyIdentifier asserted. **[X.509 8.1.1]**	Int.CC.RP.22	Svc.DS.RP.08.01	The following path should not be successfully validated; Subscriber does not have a valid policyIdentifier. [RootCA, Subscriber] Subscriber certificatePolicies.policyIdentifier: policy-B (critical)	0	Subscriber	certificatePolicies - policyIdentifier	policy-B (critical)
		Svc.DS.RP.09	The RP should process certificatePolicies correctly when it has not been marked critical.		Svc.DS.RP.09.01	The following path should be successfully validated; Subscriber has a valid policyIdentifier in non-critical certificatePolicies field. [RootCA, Subscriber] Subscriber certificatePolicies.policyIdentifier: policy-A (non-critical)	0	Subscriber	certificatePolicies - policyIdentifier	policy-A (non-critical)
					Svc.DS.RP.09.02	The following path should not be successfuly validated; Subscriber does not have a valid policyIdentifier, and certificatePolicies extension has not been marked critical. [RootCA, Subscriber] Subscriber certificatePolicies.policyIdentifier: policy-B (non-critical)		Subscriber	certificatePolicies - policyIdentifier	policy-B (non-critical)
		Svc.DS.RP.10	The RP should process a certification path which contains a certificate which has plural policyIdentifier present. **[X.509 8.1.1]**	Int.CC.RP.24	Svc.DS.RP.10.01	The following path should be successfully validated; Subscriber has plural policyIdentifier in the critical certificatePolicies, in which a valid policyIdentifier is included. [RootCA, Subscriber] Subscriber certificatePolicies.policyIdentifier: policy-A, policy-B (critical)	1	Subscriber	certificatePolicies - policyIdentifier	policy-A, policy-B (critical)
					Svc.DS.RP.10.02	The following path should not be successfully validated; Subscriber has plural policyIdentifier in the critical certificatePolicies, in which a valid policyIdentifier is not included. [RootCA, Subscriber] Subscriber certificatePolicies.policyIdentifier: policy-B, policy-C (critical)		Subscriber	certificatePolicies - policyIdentifier	policy-B, policy-C (critical)
		Svc.DS.RP.11	The RP should process a certification path which contains a certificate which has plural policyIdentifier present and not critical.		Svc.DS.RP.11.01	The following path should be successfully validated; Subscriber has plural policyIdentifier in the non-critical certificatePolicies, in which a valid policyIdentifier is included. [RootCA, Subscriber] Subscriber certificatePolicies.policyIdentifier: policy-A, policy-B (non-critical)	1	Subscriber	certificatePolicies - policyIdentifier	policy-A, policy-B (non-critical)
					Svc.DS.RP.11.02	The following path should not be successfully validated; Subscriber has plural policyIdentifier in the non-critical certificatePolicies, in which a valid policyIdentifier is not included. [RootCA, Subscriber] Subscriber certificatePolicies.policyIdentifier: policy-B, policy-C (non-critical)		Subscriber	certificatePolicies - policyIdentifier	policy-B, policy-C (non-critical)

entity	category	sequence number	requirement		test item number	test item	level	difference parameter		
								type of data	field	value
CA	CertChains	the same as Base Model								
	Validity	the same as Base Model								
	Signature	the same as Base Model								
	Constraints	Rvk.CRL.CA.01	The application (CA) should issue a CRL signer's certificate that contains the keyUsage extension present and critical with the cRLSign flag set to TRUE.		Rvk.CRL.CA.01.01	The application (CA) should issue a CA certificate that has the keyUsage extension present and critical with the cRLSign bit set to TRUE.	0			
	CertPolicy	the same as Base Model								
	Revocation	Rvk.CRL.CA.02	The application (CA) should issue a revocation list that contains the issuingDistributionPoint present and critical. [IWG profile]		Rvk.CRL.CA.02.01	The application (CA) should issue a revocation list that has the issuingDistributionPoint present and critical with the distributionPoint.fullname.	1			
		Rvk.CRL.CA.03	The application (CA) should issue a Certificate Revocation List that conatins the issuingDistributionPoint present and critical with the onlyContainsUserCerts component set to TRUE. [X.509 8.6.2.2, RFC3280 5.2.5]		Rvk.CRL.CA.03.01	The application (CA) should issue a Certificate Revocation List that has the issuingDistributionPoint present and critical with the onlyContainsUserCerts component set to TRUE.	1			
		Rvk.CRL.CA.04	The application (CA) should issue a Authority Revocation List that contains the issuingDistributionPoint present and critical with the onlyContainsCACerts component set to TRUE. [X.509 8.6.2.2, RFC3280 5.2.5]		Rvk.CRL.CA.04.01	The application (CA) should issue a Authority Revocation List that has the issuingDistributionPoint present and critical with the onlyContainsCACerts comonent set to TRUE.	1			
		Rvk.CRL.CA.05	The application (CA) should issue a certificate that contains cRLDistributionPoint entries other than CA entries. [X.509 8.6.2.2, RFC3280 5.2.5]		Rvk.CRL.CA.05.01	The application (CA) should issue a certificate that has the cRLDistribution.fullName present with the fields other than CA entries.	1			
		Rvk.CRL.CA.06	The application (CA) should issue a revocation list that contains the issuingDistributionPoint present and critical with the same distributionPoint value the cRLDistributionPoints has. [RFC3280 5.2.5]		Rvk.CRL.CA.06.01	The application (CA) should issue a Certificate Revocation List that has the issuingDistributionPoint present and critical with the same distributionPoint value the cRLDistributionPoints has.	2			
					Rvk.CRL.CA.06.02	The application (CA) should issue a Authority Revocation List that has the issuingDistributionPoint present and critical with the same distributionPoint value the cRLDistributionPoints has.				
		Rvk.CRL.CA.07	The application (CA) should issue a Certificate Revocation List that contains the authorityKeyIdentifier present. [IWG profile]		Rvk.CRL.CA.07.01	The application (CA) should issue a Certificate Revocation List that has the authorityKeyIdentifier present and non-critical.	0			
					Rvk.CRL.CA.07.02	The application (CA) should issue a Authority Revocation List that has the authorityKeyIdentifier present and non-critical.				

entity	category	sequence number	requirement		test item number	test item	level	difference parameter		
								type of data	field	value
RP	Normal Case	Rvk.CRL.RP.08	Rvk.CRL Normal Case		Rvk.CRL.RP.08.01	The following path should be successfully validated; The path includes a CA certificate, an EE certificate and a CRL that contain the correct fiels. [RootCA-A, Subscriber-A] RootCA-A issuerDN: cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA subjectDN: cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA subjectKeyID.keyIdentifier.keyID.RootCA-A Subscriber-A issuerDN: cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA subjectDN: cn=Subscriber-A, ou=Root-A, o=PVTG Draft, c=AA authorityKeyID.keyIdentifier.keyID.RootCA-A subjectKeyID.keyIdentifier.keyID.Subscriber-A cRLDistributionPoints.distributionPoint.fullName: ldap://foo/cn=CRL,ou=Root-A,o=PVTG %20Draft,c=AA?certificateRevocationList;binary RootCA-A.CRL issuerDN: cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA authorityKeyID.keyIdentifier.keyID.RootCA-A thisUpdate < current time nextUpdate > current time issuingDistributionPoint.distributionPoint.fullName: ldap://foo/cn=CRL,ou=Root-A,o=PVTG %20Draft,c=AA?certificateRevocationList;binary (critical) issuingDistributionPoint.onlyContainsUserCerts:TRUE (critical)	0			
	CertChains	The application (RP) should associate a CRL with a certificate to be verified.								
		Rvk.CRL.RP.09	The application (RP) should ensure that the issuer name in a Certificate Revocation List (CRL) matches the issuer name in a certificate, but the authorityKeyIdentifier fields in the CRL and the certificate differ. **[RFC3280 5.2.1]**		Rvk.CRL.RP.09.01	The following path should not be successfully validated; The path includes a CRL that contains the invalid authorityKeyID.keyIdentifier. **NOTE:** This may be just test case for the path construction, not for the path validation. At least, No necessary for the path validation testing. [RootCA-A, Subscriber-A] Subscriber-A.authorityKeyID.keyIdentifier: keyID.RootCA-A RootCA-A.CRL.authorityKeyID.keyIdentifier: hoge	2	RootCA-A.CRL	authKeyId.keyIdentifier	hoge
		Rvk.CRL.RP.10	The application (RP) should ensure that the authorityKeyIdentifier in a Certificate Revocation List (CRL) matches the authorityKeyIdentifier in a certificate, but the issuer names in the CRL and the certificate differ. **[RFC3280 5.1.2.3, 6.3.3 (b)]**		Rvk.CRL.RP.10.01	The following path should not be successfully validated; The path includes a CRL that contains the invalid issuer name. [RootCA-A, Subscriber-A]	0	RootCA-A.CRL	issuer	cn=hoge, ou=Root-A, o=PVTG Draft, c=AA
	Validity	Rvk.CRL.RP.11	The application (RP) should ensure that the revocationDate of each revoked-certificate entry on a Certificate Revocation List (CRL) is earlier than the thisUpdate time in the CRL. **[IWG consideration]**		Rvk.CRL.RP.11.01	The following path should be validated as "revoked"; The path includes a CRL that contains the revokedCertificates.revocationDate earlier than or equal to its thisUpdate. [RootCA-A, Subscriber-A]	0	RootCA-A.CRL	1) revokedCertificates.userCertificate 2) revokedCertificates.revocationDate	1) Subscriber-A.serialNumber 2) revocationDate <= thisUpdate
					Rvk.CRL.RP.11.02	The following path should not be successfully validated; The path includes a CRL that contains the revokedCertificates.revocationDate later than its thisUpdate. [RootCA-A, Subscriber-A]		RootCA-A.CRL	1) revokedCertificates.userCertificate 2) revokedCertificates.revocationDate	1) Subscriber-A.serialNumber 2) revocationDate > thisUpdate

entity	category	sequence number	requirement		test item number	test item	level	difference parameter		
								type of data	field	value
RP	Signature	Rvk.CRL.RP.12	The application (RP) should verify a Certificate Revocation List (CRL) with the CRL signer's certificate. **[RFC3280 6.3.3 (b)]**		Rvk.CRL.RP.12.01	The following path should be successfully validated; The path includes a CRL and a CA certificate in which the authorityKeyIdentifier.keyIdentifier of the CRL is equal to the subjectKeyIdentifier of the CA certificate. **NOTE:** This may be just test case for the path construction, not for the path validation. At least, No necessary for the path validation testing. [RootCA-A, Subscriber-A]	0			
					Rvk.CRL.RP.12.02	The following path should not be successfully validated; The path includes a CRL that contains the invalid authorityKeyIdentifier. **NOTE:** This may be just test case for the path construction, not for the path validation. At least, No necessary for the path validation testing. [RootCA-A, Subscriber-A]	2	RootCA-A.CRL	AKID	hoge
		Rvk.CRL.RP.13	The application (RP) should ensure that every Certificate Revocation List (CRL) signer's certificate contains the critical keyUsage present with the cRLSign bits set to TRUE. **[RFC3280 6.3.3 (f)]**		Rvk.CRL.RP.13.01	The following path should be successfully validated; The path includes two CA certificates that contain the keyUsage fields present and critical with cRLSign bits set to TRUE. [RootCA-A, SubCA, Subscriber-A]	0			
					Rvk.CRL.RP.13.02	The following path should be successfully validated; The path includes two CA certificates, one contains the keyUsage present and non-critical with cRLSign bits set to TRUE. [RootCA-A, SubCA, Subscriber-A]		SubCA	keyUsage	non-critical
					Rvk.CRL.RP.13.03	The following path should not be successfully validated; The path includes two CA certificates, one contains the keyUsage present and critical with a bit other than cRLSign. [RootCA-A, SubCA, Subscriber-A]		SubCA	keyUsage	keyCertSign only
					Rvk.CRL.RP.13.04	The following path should not be successfully validated; The path includes two CA certificates, one contains the keyUsage present and non-critical with a bit other than cRLSign. [RootCA-A, SubCA, Subscriber-A]		SubCA	keyUsage	non-critical keyCertSign only
					Rvk.CRL.RP.13.05	The following path should not be successfully validated; The path includes two CA certificates that do not contain the keyUsage fields. [RootCA-A, SubCA, Subscriber-A]		SubCA	keyUsage	none
		Rvk.CRL.RP.14	The application (RP) should reject a tampered certificate revocation list (CRL). **[RFC3280 6.3.3 (g)]**		Rvk.CRL.RP.14.01	The following path should not be successfully validated; The path includes a CRL that contains the invalid signature. [RootCA-A, Subscriber-A]	0	RootCA-A.CRL	signature	invalid
	Constraints	Rvk.CRL.RP.15	The application (RP) should reject a certificate revocation list (CRL) that contains an unrecognized critical extension in the crlEntryExtensions field. **[X.509 8]**		Rvk.CRL.RP.15.01	The following path should not be successfully validated; The path includes a CRL that contains an unrecognized critical extension in the crlEntryExtensions field. [RootCA-A, Subscriber-A]	1	RootCA-A.CRL	1) revokedCertificates.userCertificate 2) revokedCertificates.revocationDate 3) revokedCertificates.crlEntryExtension.UnknownForExperiment	1) Subscriber-A.serialNumber 2) revocationDate <= thisUpdate 3) critical id-pe-unknown OID ::= { id-pe 99} unknownForExperiment ::= INTEGER
					Rvk.CRL.RP.15.02	The following path should be validated as "revoked"; The path includes a CRL that contains an unrecognized non-critical extension in the crlEntryExtensions field. [RootCA-A, Subscriber-A]		RootCA-A.CRL	1) revokedCertificates.userCertificate 2) revokedCertificates.revocationDate 3) revokedCertificates.crlEntryExtension.UnknownForExperiment	1) Subscriber-A.serialNumber 2) revocationDate <= thisUpdate 3) non-critical id-pe-unknown OID ::= { id-pe 99} unknownForExperiment ::= INTEGER

entity	category	sequence number	requirement		test item number	test item	level	difference parameter		
								type of data	field	value
RP		Rvk.CRL.RP.16	The application (RP) should recognize and process well-known critical extensions in the crlEntryExtensions field. **[X.509 8]**		Rvk.CRL.RP.16.01	The following path should be successfully validated; The path includes a CRL that contains the certificateIssuer present and critical in the crlEntryExtensions field. [RootCA-A, Subscriber-A] **NOTE:** In the IWG experiment, this test item can not be performed.	1	RootCA-A.CRL	crlEntryExtension.certificateIssuer	critical cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA
		Rvk.CRL.RP.17	The application (RP) should reject a certificate revocation list (CRL) that contains an unrecognized critical extension in the crlExtensions field. **[X.509 8]**		Rvk.CRL.RP.17.01	The following path should not be successfully validated; The path includes a CRL that contains an unrecognized critical extension in the crlExtensions field. [RootCA-A, Subscriber-A]	1	RootCA-A.CRL	crlExtensions.UnknownForExperiment	critical id-pe-unknown OID ::= { id-pe 99} unknownForExperiment ::= INTEGER
					Rvk.CRL.RP.17.02	The following path should be successfully validated; The path includes a CRL that contains an unrecognized non-critical extension in the crlExtensions field. [RootCA-A, Sugscriber-A]		RootCA-A.CRL	crlExtionsions.UnknownForExperiment	non-critical id-pe-unknown OID ::= { id-pe 99} unknownForExperiment ::= INTEGER
		Rvk.CRL.RP.18	The application (RP) should recognize and process well-known critical extensions in the crlExtension field. **[X.509 8]**		Rvk.CRL.RP.18.01	The following path should be successfully validated; The path includes a CRL that contains the issuingDistributionPoint present and critical with the correct distributionPoint. [RootCA-A, Subscriber-A]	1			
	CertPolicy	the same as Base Model								
	Revocation	The application (RP) should recognize and process the critical issuingDistributionPoint in the revocation list in the certification path.								
		The CRL only for EE certificates contains the critical issuingDistributionPoint present with only the onlyContainsCACerts flag set to TRUE.								
		Rvk.CRL.RP.19	The application (RP) should correctly process the certification path when it verifies an EE certificate with the aforementioned certificate revocation list (CRL), which contains the serialNumber of the EE certificate. **[RFC3280 6.3.3 (b)]**		Rvk.CRL.RP.19.01	The following path should not be validated as "revoked"; The path includes a CRL that has the critical issuingDistributionPoint present with only the onlyContainsCACerts flag set to TRUE, and the CRL contains the serialNumber of the EE certificate. [RootCA-A, Subscriber-A] **NOTE:** The validation usually fails when the application checks the onlyContainsCACerts first. However, it may succeed when the application checks the serialNumber first and immediately returns it.	1	RootCA-A.CRL	1) issuingDP.onlyContainsCACerts 2) revokedCertificates.userCertificate 3) revokedCertificates.revocationDate	1) TRUE 2) Subscriber-A.serialNumber 3) revocationDate <= current time
		Rvk.CRL.RP.20	The application (RP) should correctly process the certification path when it verifies an EE certificate with the aforementioned certificate revocation list (CRL), which does not contain the serialNumber of the EE certificate. **[RFC3280 6.3.3 (b)]**		Rvk.CRL.RP.20.01	The following path should not be successfully validated; The path includes a CRL that has the critical issuingDistributionPoint present with only the onlyContainsCACerts flag set to TRUE, and the CRL does not contain the serialNumber of the EE certificate. [RootCA-A, Subscriber-A]	0	RootCA-A.CRL	1) issuingDP.onlyContainsCACerts 2) revokedCertificates.userCertificate 3) revokedCertificates.revocationDate	1) TRUE 2) Subscriber-A.serialNumber 3) revocationdate <= current time

entity	category	sequence number	requirement		test item number	test item	level	difference parameter		
								type of data	field	value
RP		The ARL contains the critical issuingDistributionPoint present with only the onlyContainsCACerts flag set to TRUE.								
		Rvk.CRL.RP.21	The application (RP) should correctly process the certification path when it verifies a CA certificate with the aforementioned authority revocation list (ARL), which contains the serialNumber of the CA certificate.		Rvk.CRL.RP.21.01	The following path should be validated as "revoked"; The path includes a ARL that has the critical issuingDistributionPoint present with only the onlyContainsCACerts flag set to TRUE, and the ARL contains the serialNumber of the Subordinate CA certificate. [RootCA-A, SubCA, Subscriber-A]	0	RootCA-A.ARL	1) revokedCertificates.userCertificate 2) revokedCertificates.revocationDate	1) SubCA.serialNumber 2) revocationDate <= current time
		Rvk.CRL.RP.22	The application (RP) should correctly process the certification path when it verifies a CA certificate with the aforementioned authority revocation list (ARL), which does not contain the serialNumber of the CA certificate. **[RFC3280 6.3.3 (b)]**		Rvk.CRL.RP.22.01	The following path should be successfully validated; The path includes a ARL that has the critical issuingDistributionPoint present with only the onlyContainsCACerts flag set to TRUE, and the ARL does not contain the serialNumber of the Subordinate CA certificate. [RootCA-A, SubCA, Subscriber-A]	0			
		The CRL only for EE certificates contains the critical issuingDistributionPoint present with only the onlyContainsUserCerts flag set to TRUE.								
		Rvk.CRL.RP.23	The application (RP) should correctly process the certification path when it verifies an EE certificate with the aforementioned certificate revocation list (CRL), which contains the serialNumber of the EE certificate. **[RFC3280 6.3.3 (b)]**		Rvk.CRL.RP.23.01	The following path should be validated as "revoked"; The path includes a CRL that has the critical issuingDistributionPoint present with only the onlyContainsUserCerts flag set to TRUE, and the CRL contains the serialNumber of the EE certificate. [RootCA-A, Subscriber-A]	0	RootCA-A.CRL	1) revokedCertificates.UserCertificate 2) revokedCertificates.revocationDate	1) Subscriber-A.serialNumber 2) revocationDate <= current time
		Rvk.CRL.RP.24	The application (RP) should correctly process the certification path when it verifies an EE certificate with the aforementioned certificate revocation list (CRL), which does not contain the serialNumber of the EE certificate. **[RFC3280 6.3.3 (b)]**		Rvk.CRL.RP.24.01	The following path should be successfully validated; The path includes a CRL that has the critical issuingDistributionPoint present with only the onlyContainsUserCerts flag set to TRUE, and the CRL contains the serialNumber of the EE certificate. [RootCA-A, Subscriber-A]	0			
		The ARL contains the critical issuingDistributionPoint present with only the onlyContainsUserCerts flag set to TRUE.								
		Rvk.CRL.RP.25	The application (RP) should correctly process the certification path when it verifies a CA certificate with the aforementioned authority revocation list (ARL), which contains the serialNumber of the CA certificate. **[RFC3280 6.3.3 (b)]**		Rvk.CRL.RP.25.01	The following path should not be validated as "revoked"; The path includes a ARL that has the critical issuingDistributionPoint present with only the onlyContainsUserCerts flag set to TRUE, and the ARL contains the serialNumber of the Subordinate CA certificate. [RootCA-A, SubCA, Subscriber-A]	1	RootCA-A.ARL	1) issuingDP.onlyContainsUserCerts 2) revokedCertificates.userCertificate 3) revokedCertificates.revocationDate	TRUE SubCA.serialNumber revocationDate <= current time
		Rvk.CRL.RP.26	The application (RP) should correctly process the certification path when it verifies a CA certificate with the aforementioned authority revocation list (ARL), which does not contain the serialNumber of the CA certificate. **[RFC3280 6.3.3 (b)]**		Rvk.CRL.RP.26.01	The following path should not be successfully validated; The path includes a ARL that has the critical issuingDistributionPoint present with only the onlyContainsUserCerts flag set to TRUE, and the ARL does not contain the serialNumber of the Subordinate CA certificate. [RootCA-A, SubCA, Subscriber-A]	0	RootCA-A.ARL	issuingDP.onlyContainsUserCerts	TRUE

entity	category	sequence number	requirement		test item number	test item	level	difference parameter		
								type of data	field	value
RP		The certificate in the certification path contains cRLdistributionPoints present with the distributionPoint.fullName, and the corresponding revocation list contains the critical issuingDistributionPoint with the distributionPoint.fullName.								
		Rvk.CRL.RP.27	The application (RP) should correctly process the certification path when one of the cRLDistributionPoints.distributionPoint.fullName entries in the certificate matches one of the critical issuingDistributionPoint.distributionPoint.fullName entries in the corresponding revocation list. **[RFC3280 5.2.5]**		Rvk.CRL.RP.27.01	The following path should be successfully validated; The path includes an EE certificate that contains several cRLDistributionPoints.distributionPoint.fullName entries, and the corresponding CRL that contains several issuingDistributionPoint.distributionPoint.fullName entries. Then one cRLDistributionPoints.distributionPoint.fullName entry in the EE certificate matches one issuingDistributionPoint.distributionPoint.fullName entry in the corresponding CRL. [RootCA-A, Subscriber-A]	2	1) Subscriber-A 2) RootCA-A.CRL	1) cRLDP.distPoint.fullName 2) issuingDP.distPoint.fullName	1) [4] (directoryName) cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA 1) [4] (directoryName) hoge1 2) [4] (directoryName) cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA 2) [4] (directoryName) hoge2
		Rvk.CRL.RP.28	The application (RP) should correctly process the certification path when any one of cRLDistributionPoints.distributionPoint.fullName entries in the certificate does not match any issuingDistributionPoint.distributionPoint.fullName entries in the corresponding revocation list. **[RFC3280 5.2.5]**		Rvk.CRL.RP.28.01	The following path should not be successfully validated; The path includes an EE certificate that contains several cRLDistributionPoints.distributionPoint.fullName entries, and the corresponding CRL that contains several issuingDistributionPoint.distributionPoint.fullName entries. Then any one of cRLDistributionPoints.distributionPoint.fullName entries in the EE certificate does not match any issuingDistributionPoint.distributionPoint.fullName entries in the corresponding CRL. [RootCA-A, Subscriber-A]	2	1) Subscriber-A 2) RootCA-A.CRL	1) cRLDP.distPoint.fullName 2) issuingDP.distPoint.fullName	1) [4] (directoryName) cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA 1) [4] (directoryName) hoge1 2) [4] (directoryName) hoge2 2) [4] (directoryName) hoge3
		Rvk.CRL.RP.29	The application (RP) should correctly process the certification path when it verifies a certificate that contains the cRLDistributionPoints.distributionPoint.fullName, with a revocation list that does not contain the issuingDistributionPoint.distributionPoint.fullName. **[RFC3280 5.2.5]**		Rvk.CRL.RP.29.01	The following path should not be successfully validated; The path includes a CRL that does not have the issuingDistributionPoint.distributionPoint.fullName. [RootCA-A, Subscriber-A]	2	RootCA-A.CRL	issuingDP.distPoint.fullName	None
		The revocation list contains the critical issuingDistributionPoint present with the distributionPoint.								
		Rvk.CRL.RP.30	The application (RP) should correctly process the certification path when it verifies a certificate containing no cRLDistributionPoints fields with the aforementioned revocation list, and when the isuer name of the certificate matches the directoryName in the issuingDistributionPoint field. **[RFC3280 5.2.5]**		Rvk.CRL.RP.30.01	The following path should be successfully validated; The path includes a CRL that only contains the CA entry in the critical issuingDistributionPoint field, which matches the issuer of the EE certificate. [RootCA-A, Subscriber-A]	2	1) Subscriber-A 2) RootCA-A.CRL	1) cRLDP 2) issuingDP.distPoint.fullName	1) None 2) cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA
		Rvk.CRL.RP.31	The application (RP) should correctly process the certification path when it verifies a certificate containing no cRLDistributionPoints fields with the aforementioned revocation list, and when the issuer name of the certificate does not match the directoryName in the issuingDistributionPoint. **[RFC3280 5.2.5]**		Rvk.CRL.RP.31.01	The following path should not be successfully validated; The path includes a CRL that only contains the CA entries in the critical issuingDistributionPoint field, which does not match the issuer of the EE certificate. [RootCA-A, Subscriber-A]	2	1) Subscriber-A 2) RootCA-A.CRL	1) cRLDP 2) issuingDP.distPoint.fullName	1) None 2) cn=hoge, ou=Root-A, o=PVTG Draft, c=AA