付録 2

証明書検証に関する標準

付録２－１

パス検証テストガイドライン

JKST-IWG

Path Processing Testing Guideline 2004

JKST-IWG

Mar 07, 2004

- CHANGES -

Date	Comments	Detail
28 Feb 2003	Published	First Edition
8 Mar 2004	Update	Add DN matching, LDAP URI and UTF8 CJK test items to Int.SH model. (Section 2.2.2 (2) (a)). Revokation model and service model are organized. Add description about IWG test tool and PPTG Test Item Selecting Worksheet as appendix.

- Table of Contents –

1 Introduction

1.1 Background

The Interoperability Working Group (IWG), formed by Japan, Korea, Singapore and Chinese Taipei 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 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 in 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 coexist.

1.2 Objectives

The objective of this document is to test the path validation processing logic in the Relying Party (RP) 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 transactions. By developing this document, the IWG will facilitate the

---

[1] Achieving PKI Interoperability 2003
Results of the JKST-IWG Interoperability project
http://www.japanpkiforum.jp/shiryou/IWG_2002/FinalReport2003-Version1.0.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

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

The test items are constructed based on the PKI trust model. The trust model includes Base (**Base**), Strict Hierarchy (**SH**), Cross Certification (**CC**), and Cross Recognition (**CR**). The **Base** covers the very simple PKI trust model which consists of only RootCA and Subscriber as entities. The **SH** covers test cases for the extension fields for the hierarchical model and also covers the advanced test cases of the **DN** matching rule, **LDAPURI**, and **CJK** characters. The **CC** and **CR** covers specific requirements for their own models such as policy mapping extension in CC model. In addition, the **CRL** covers the test cases for CRL fields and for CRLDistributionPoints and IssuingDistributionPoint.

Table 2.1 shows the overview of test items. The table summarizes test items necessary to test the certificate path processing module in a specific trust model. For example, **SH** requires the SH.8, Base8-1, CRL9-10, Base13-18, CRL11-12, Base19, CRL14, Base 20, and SH22-23.

Table 2.1 Test Models and Test Items

---

[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

Trust Model			Opt	Base	SH	CR	CC
Test Items	Basic Field	Normal Case		Base.7	SH.8	CR.5	CC.19
		DN matching		Base8-11			
		DN matching Advanced	✓		SH.DN		
		DN matching in CRL		CRL.9-10			
		Validity		Base13-18			
		Validity in CRL		CRL.11-12			
		Signature		Base.19			
		Signature of CRL		CRL.14			
		Revocation		Base.20			
					SH.22-23		
	Extension	AKID / SKID	✓	Base.12	SH.9-10	CR.6-8	CC.20-21
		basicConstraint			SH.11-14		CC.26-29
		keyUsage			SH.15-17		CC.30-32
		for DigitalSignature	✓	DS.7			
		in CRL		CRL.13			
		certificatePolicy			SH.18-21	CR.10-13	CC.22-23
		policyConstraints					CC.33-34
		policyMappings					CC.24-25
		nameConstraints					CC.35-39
		cRLDP / iDP		CRL.18-31			
					SH.LDAPURI		
		UTF8 CJK	✓		SH.CJK		
		Unknown Extension		Base.21			
		CRL Entry Extension		CRL.15-17			

The test cases are categorized into the Mandatory and Optional. The Mandatory test cases are considered necessary to test in the aforementioned trust model. For the mandatory basic fields of certificate, **Base** test cases and **CRL** test cases are prepared. For the extension fields of certificate, when you use particular extensions, corresponding test categories (**Base**, **SH**, **CR**, **CC**) cover the test cases.

On the other hand, the Optional test cases are up to your decision. The optional test cases include Advanced DN matching rule, AKID/SKID, some Key Usage test, and CJK Characters in UTF8String.

The detailed information is specified in the attached document for the test items.

The guideline includes the following test cases:

- Normal test cases
- DN matching test cases (issuer and subject fields)
- Validity checking test cases
- Signature checking test cases
- Revocation checking test cases
- Authority Key Identifier and Subject Key Identifier test cases
- Basic Constraints test cases
- Key Usage test cases
- Certificate Policy test cases
- Policy Constraints test cases
- Policy Mappings test cases

- Name Constraints test cases
- CRL Distribution Points and Issuing Distribution Point test case
- UTF8 CJK characters test cases
- Unknown Extension test cases
- CRL Entry Extension test cases

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 is divided into either a success case or a failure case.

A test is conducted using the black box-based testing method. In the method, test case values are the essential part of testing. Certificates, CRL/ARL, and several initial parameters are prepared and provided as input values. Each test case contains verifiable value(s), which are to be evaluated by comparing the output of the application with the expected value in the document.

The test planners can combine the cases among the interconnection, service, and revocation to meet their specific requirements in the PKI environment.

2.1.2 Assumptions

1. 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.

2. 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.

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

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

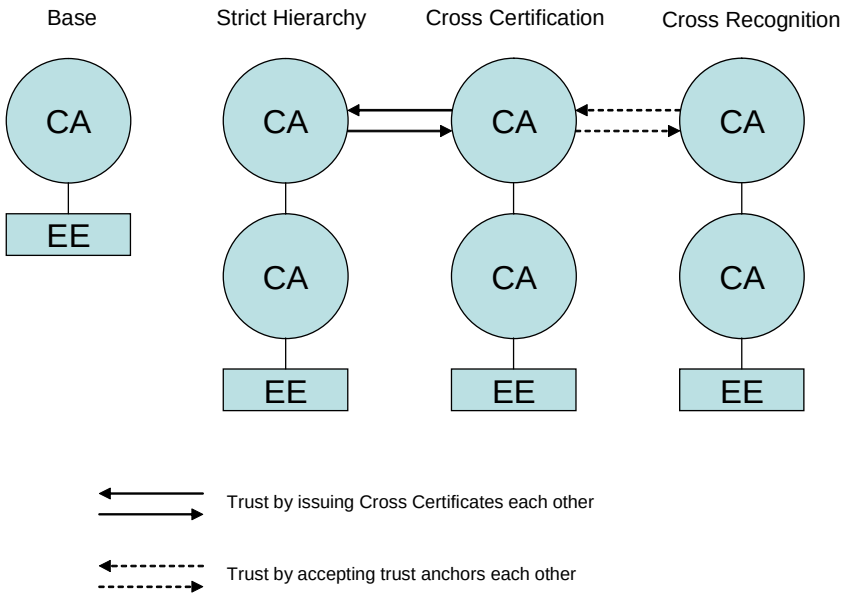
[6] RFC3379
Delegated Path Validation and Delegated Path Discovery Protocol Requirements
http://www.ietf.org/rfc/rfc3379.txt

5. No test cases for criticality, but only critical extensions which defined locally in IWG profile, have test cases for criticality.

2.1.3 Test Environment

(1) CA hierarchical structure

The test environment assumes the following structures.



The Base model does not have any subordinate CAs. This CA issues certificates to End Entity (EE) directly. The Strict Hierarchy model has a subordinate CA and the subordinate CA issues certificates to EE. The Cross Certification model cross-certifies with other trust anchor CAs by issuing cross certificates. The Cross Recognition model has a trust relationship by accepting the trust anchor certificates each other. This model does not issue cross certificate or any certificates to establish a trust relationship.

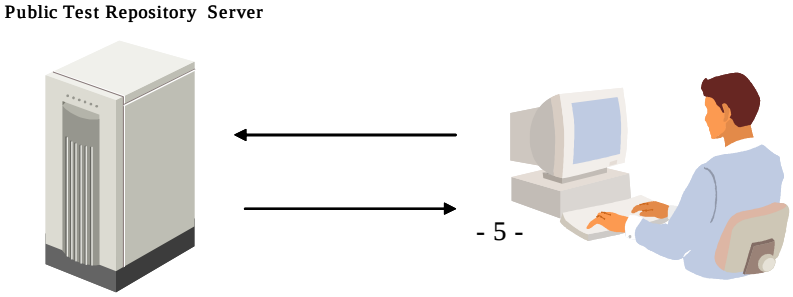
(2) Relying Party Test Environment

The guideline assumes that test planners will prepare the followings at least:

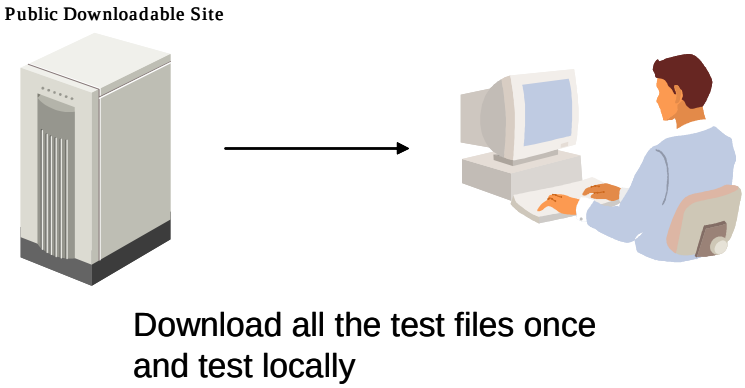
- ✓ A certificate path processing module
- ✓ The module can read Certificates and CRLs
- ✓ The module can set initial parameters

The guideline expects the following test scenarios:

1) Accessing to the public repository servers and test with the servers:



2) Obtaining the test files and conducting the test locally:



(3) Using the Test Tool

The guideline prepares a test tool that supports the certificate path processing test. The test tool includes the following functions:

1) Generate new test items
2) Modify test items
3) Storing test items as test files
4) Storing test items as a LDIF file
3) Storing test items in public repository servers

Please refer to the details of the Test Tool at Appendix A : IWG Test Tools of this document.

2.1.4 Document Conventions

Each test items is specified using the following convention. The interconnection model (**Int**) contains Strict Hierarchy (**SH**), Cross Certification (**CC**), and Cross Recognition (**CR**). Also, there are several test cases for Signing (**DS**) and revocation (**Rvk**). In addition, DN matching rules (**DN**), LDAP URI (**LDAPURI**) and CJK characters **(CJK**) test cases are included in the SH model.

To describe the test entity as relying party, each test item has the number with the following notation. The examples are shown below.

- SH.01
- CC.22
- CR.07

2.1.5 Usage of This Guideline

(1) Outline of this guideline

The specification of path validation, especially in multi-domain PKI, is complex. So the test requirements of Relying Party often become unclear. The following is a step to determine the test cases using this guideline.

(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 typical PKI trust models. The guideline users can make use of these models as a fundamental for analysis when they determine test cases.

This guideline classifies the trust model below:

(a) Base (No hierarchy)
(b) Strict Hierarchy
(c) Cross Certification
(d) Cross Recognition

(b) Definition of certificate and crl profiles

After determining the trust model, the next step is to check your certificate and crl profiles. The guideline categorizes the test items followed by the basic fields and Extension fields, one-to-one matching as much as possible. The guideline defines mandatory and optional test cases to meet your specific needs. When you need to check DN matching test cases, key usage test cases, and CJK character test cases, you may choose further optional 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) Base Model

(i) Definition

- Only Root CA issues self-signed certificate
- One Root CA issues Subscriber certificate

(ii) Usage

This is the most simple PKI model.

(iii) Advantage and disadvantage

- Applicable to existing applications based on SSL.
- A lack of extended ability.

(b) 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/

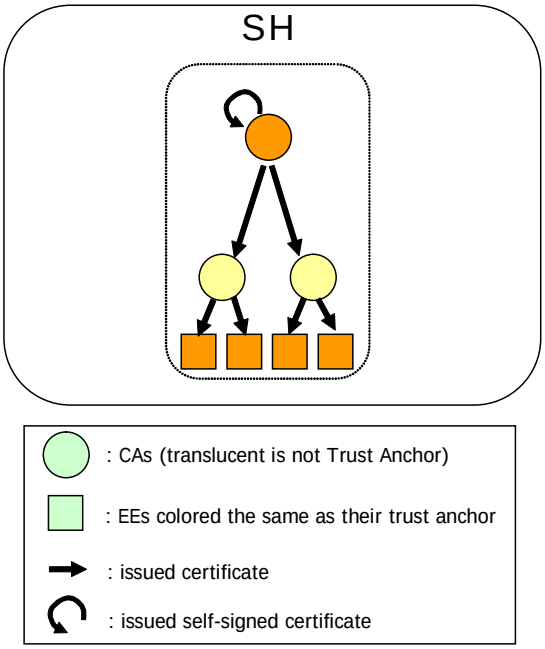


Figure 2.4 Strict Hierarchy model

(c) 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.

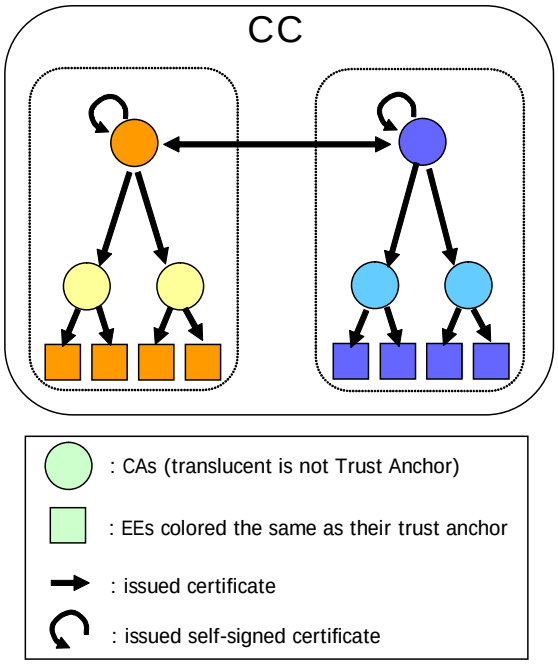


Figure 2.5 Cross Certification model

(d) 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.

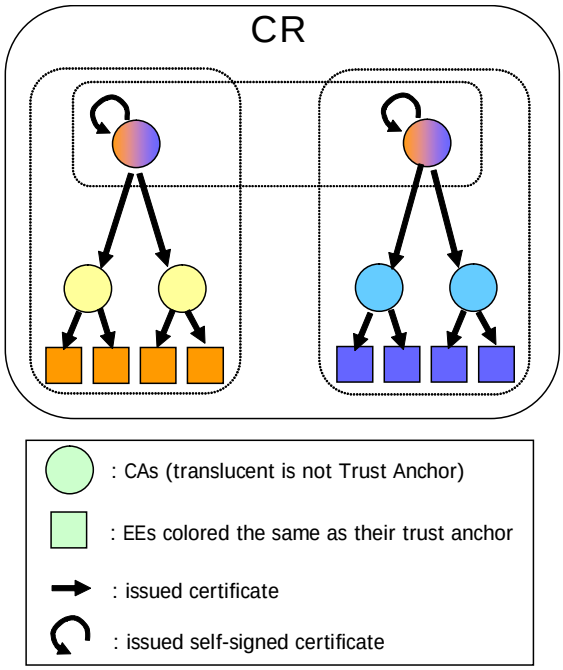


Figure 2.6 Cross Recognition model

(e) 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.

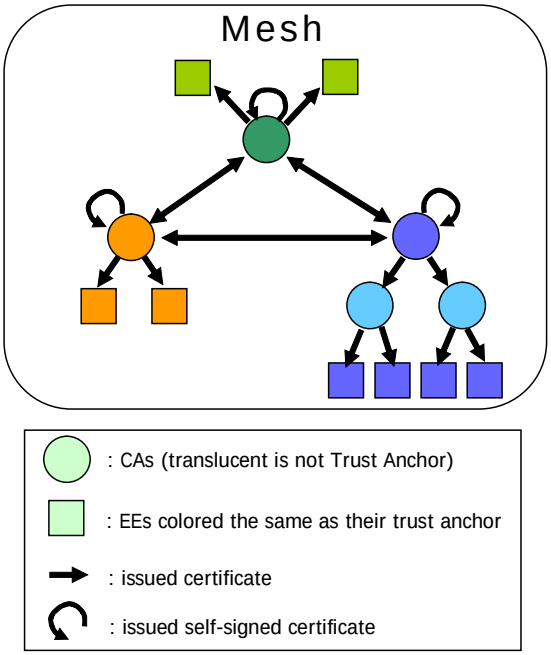


Figure 2.7 Mesh model

(f) 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.

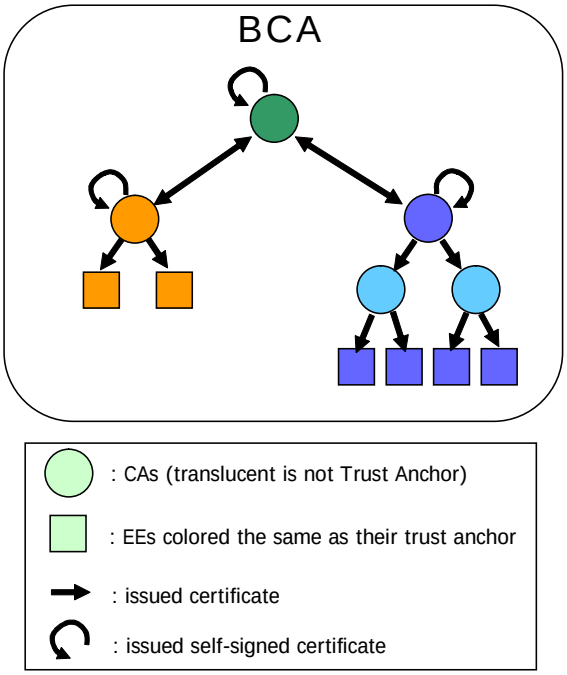


Figure 2.8 Bridge CA model

(g) 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.

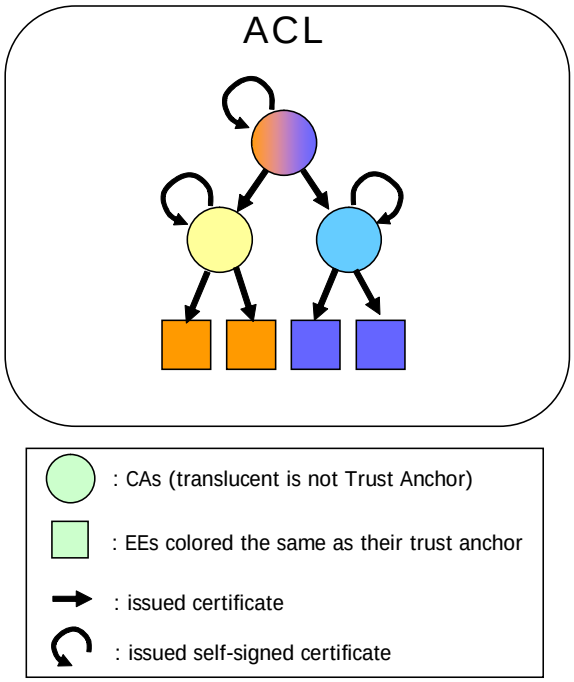


Figure 2.9 Accreditation Certificate model

(h) 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.

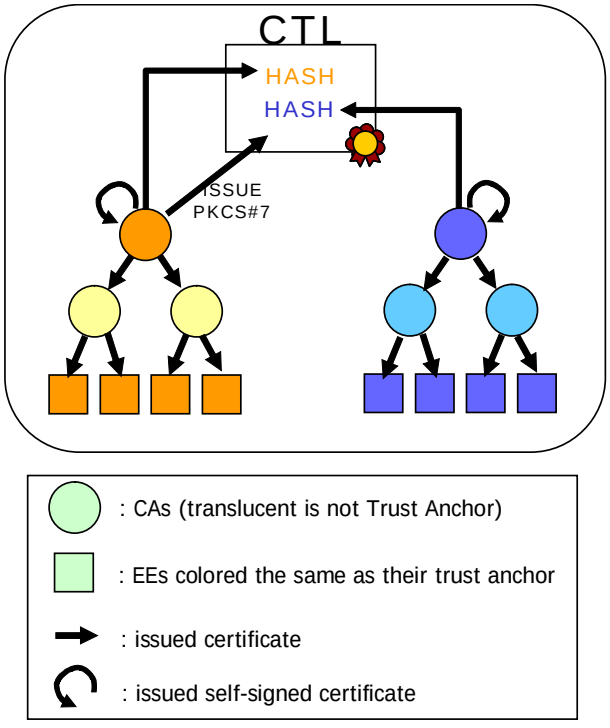


Figure 2.10 Certificate Trust Lists model

2.2.2 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 Model Test Cases

(a) CA requirements

Base.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]

Base.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]

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

[IWG Profile, RFC3280 4.2.1.1 & 4.2.1.2]

Base.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]

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

[IWG profile]

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

[X.509 7]

(b) Test Item Requirements

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

Base.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]

Base.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]

Base.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]

Base.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]

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

[X.509 10.5.1]

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

[X.509 10.5.1]

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

[X.509 7]

(2) Strict Hierarchy Model Test Cases

(a) CA Requirements

SH.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]

SH.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]

SH.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]

SH.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]

SH.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]

SH.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]

SH.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]

(b) Test Item Requirements

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

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

[X.509 10.5.1]

SH.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]

SH.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]

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

[IWG profile]

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

[X.509 8.1.1]

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

[X.509 10.5.1]

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

[X.509 10.5.1]

SH.DN.01: The application should validate successfully the correct certification path.

SH.DN.02: The RP should determine that the names are identifcal when they differ by whitespace in an attribute value (including leading and tailing whitespaces and more than one consesutive whitespace charactes in the value).

[X.520(02_01) 6.1][RFC3280 4.1.2.4]

SH.DN.03: The RP should determine that the names are identifcal when they differ by capitalization.

[X.520(02_01) 6.11] [RFC3280 4.1.2.4]

SH.DN.04: The RP should determine that the names are identifcal when they differ in ASN.1 encording type but contains the same character sets.

[X.520 (02_01) 6.11]

SH.DN.05: The RP should determine that the names are different when they differ by order.

[X.501(93_03) 12.5.2]

SH.DN.06: The RP should determine that the names are different when they are completely different.

[X.501(93_03) 12.5.2]

SH.DN.07: The RP should determine that the names are identifcal when they use identical CJK charactes which is encorded in UTF8.

[RFC3280 4.1.2.4]

SH.LDAPURI.01: The RP should validate as revoked when cRLDistribution Points.distributionPoint.fullName is represented with LDAP URI.

SH.LDAPURI.02: The RP should ignore the white space on either side of the delimiter in LDAP URI.

[RFC 1779] [RFC2253 4]

SH.LDAPURI.03: The RP should ignore the white space on either side of "=" which separates attribute type and attribute value in LDAP URI.

[RFC1779] [RFC2253 4]

SH.LDAPURI.04: The RP should determine semicolon in LDAP URI as delimiter.

[RFC1779] [RFC2253 4]

SH.LDAPURI.05: The RP should determine escaped character in LDAP URI.

[RFC1179][RFC1738 2.2][RFC2253 2.4][RFC2255][IWG Recommendation]

SH.LDAPURI.06: The RP should determine portnumber information in LDAPURI other than "389".

[RFC 2255 3][IWG Recommendation]

SH.CJK.01: The RP should process a certification path when DN contains Unicode "CJK Unified Ideographs(4E00-9FAF)" characters.

[RFC 1779][RFC2253 4][Unicode Standard 4.0]

SH.CJK.02: The RP should process a certification path when DN contains Unicode "CJK Compatibility Ideographs(F900-FAFF)" characters.

[RFC 1779][RFC2253 4][Unicode Standard 4.0]

SH.CJK.03: The RP should process a certification path when DN contains Unicode "Hiragana(3040-309F)" characters.

[RFC 1779][RFC2253 4][Unicode Standard 4.0]

SH.CJK.04: The RP should process a certification path when DN contains Unicode "Katakana(30A0-30FF)" characters.

[RFC 1779][RFC2253 4][Unicode Standard 4.0]

SH.CJK.05: The RP should process a certification path when DN contains Unicode "Halfwidth and Fullwidth Forms(FF00-FFEF)" characters.

[RFC 1779][RFC2253 4][Unicode Standard 4.0]

SH.CJK.06: The RP should process a certification path when DN contains Unicode "Hangul Syllables(AC00-D7AF)" characters.

[RFC 1779][RFC2253 4][Unicode Standard 4.0]

SH.CJK.07: The RP should process a certification path when DN contains Unicode "CJK Symbols and Punctuations" characters.

[RFC 1779][RFC2253 4][Unicode Standard 4.0]

SH.CJK.08: The RP should process a certification path when DN contains

Unicode CJK and ASCII characters.

[RFC 1779][RFC2253 4][Unicode Standard 4.0]

(3) Cross Certification Model Test Cases

(a) CA Requirements

CC.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]

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

[IWG profile]

CC.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 SH.CA.04 requirement.

[X.509 8.2.2.6]

CC.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 SH.CA.05 requirement.

[X.509 8.2.2.6]

CC.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 SH.CA.06 requirement.

[X.509 8.2.2.6]

CC.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 SH.CA.07 requirement.

[X.509 8.2.2.6]

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

[X.509 8.1.3]

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

[X.509 8.1.3]

CC.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 SH.CA.01 requirement.

[X.509 8.4.2.1]

CC.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]

CC.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 SH.CA.02 requirement.

[X.509 8.4.2.1]

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

[X.509 10.5.2, 10.5.3]

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

[X.509 10.5.2]

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

[X.509 10.5.2]

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

[IWG profile]

(b) Test Item Requirements

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

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

[X.509 8.1.2]

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

[X.509 8.1.1]

CC.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]

CC.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]

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

[IWG profile]

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

[X.509 10.5.2, 10.5.3]

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

[X.509 10.5.2, 10.5.3]

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

[X.509 10.5.1]

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

[X.509 10.5.1]

(4) Cross Recognition test cases

(a) CA Requirements

CR.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 SH.CA.4 requirement.

[X.509 8.2.2.6]

CR.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 SH.CA.5 requirement.

[X.509 8.2.2.6]

CR.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 SH.CA.6 requirement.

[X.509 8.2.2.6]

CR.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 SH.CA.7 requirement.

[X.509 8.2.2.6]

(b) Test Item Requirements

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

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

[IWG profile]

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

[X.509 10.5.1]

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

[X.509 8.1.1]

(5) Service test cases

(a) Signing

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

[IWG profile]

DS.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 SH.CA.4 requirement.

[X.509 8.2.2.6]

DS.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 SH.CA.5 requirement.

[X.509 8.2.2.6]

DS.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 SH.CA.6 requirement.

[X.509 8.2.2.6]

DS.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 SH.CA.7 requirement.

[X.509 8.2.2.6]

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

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

[IWG consideration]

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

[X.509 8.1.1]

(6) Revocation test cases

(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.

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

[IWG profile]

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

[IWG profile]

CRL.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]

CRL.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]

CRL.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]

CRL.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]

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

[IWG profile]

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

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

[X.509 10.5.1]

CRL.11: The application should ensure whether the revocationDate of the certificate is valid or not.

[IWG consideration]

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

[RFC3280 6.3.3 (b)]

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

[RFC3280 6.3.3 (f)]

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

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

CRL.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]

CRL.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]

CRL.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)]

CRL.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)]

CRL.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)]

CRL.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)]

CRL.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]

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

2.3.3 Service

(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

2.3.4 Revocation

(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

3 Test Items

In this section, all of the test items for the 'Path Processing Testing Guideline' is described.

3.1 Base Model Test Items

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	Normal Test Case										
		Base.07	01	OK	Base Model Normal Case		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				
	DN matching Basic Test Case										
		Base.08	01	OK	The RP should determine that the names are different when they differ by whitespace in values other than countryName. **[RFC3280 4.1.2.4]**		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 Subscriber.issuerDN: cn=CA, ou=Root, o=PVTG[]Draft, c=AA		Subscriber	issuer	cn=CA, ou=Root, o=PVTG Draft, c=AA
		Base.09	01	OK	The RP should determine that the names are different when they differ by capitalization in values other than countryName. **[RFC3280 4.1.2.4]**		The issuer name in Subscriber is different from the subject name in RootCA by capitalization. [RootCA, Subscriber] RootCA.subjectDN:Prin:cn=CA, ou=Root, o=PVTG Draft, c=AA Subscriber.issuerDN:Prin:cn=ca, ou=Root, o=PVTG Draft, c=AA		Subscriber	issuer	cn=ca, ou=Root, o=PVTG Draft, c=AA
		Base.10	01	NG	The RP should determine that the names are different when they differ by order. **[X.501 12.5.2]**		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 Subscriber.issuerDN: cn=CA, o=PVTG Draft, ou=Root, c=AA		Subscriber	issuer	cn=CA, o=PVTG Draft, ou=Root, c=AA
		Base.11	01	NG	The RP should determine that the names are different when they are completely different. **[X.501 12.5.2]**		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 Subscriber.issuerDN: cn=GE		Subscriber	issuer	cn=GE
	DN matching Basic Test Case (CRL)										
		CRL.10	01	NG	The RP should determine that the names are different when they are completely different. **[X.501 12.5.2]**		The path includes a CRL that contains the invalid issuer name. [RootCA-A, Subscriber-A]		RootCA-A.CRL	issuer	cn=foo, ou=Root-A, o=PVTG Draft, c=AA

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	Validity										
		Base.13	01	NG	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]**		The notBefore in Subscriber is later than current time. [RootCA, Subscriber] current time < Subscriber.notBefore		Subscriber	Validity - notBefore	> current time
		Base.14	01	NG	The RP should reject certification path when a certificate to be verified has a notAfter earlier than current time. **[X.509 10.5.1]**		The notAfter in Subscriber is earlier than current time. [RootCA, Subscriber] Subscriber.notAfter < current time		Subscriber	Validity - notAfter	< current time
		Base.15	01	NG	The RP should reject a certification path when an issuer certificate has a notBefore later than current time. **[X.509 10.5.1]**		The notBefore in RootCA is later than current time. [RootCA, Subscriber] current time < RootCA.notBefore		RootCA	Validity - notBefore	> current time
		Base.16	01	NG	The RP should reject a certification path when an issuer certificate has a notAfter earlier than current time. **[X.509 10.5.1]**		The notAfter in RootCA is earlier than current time. [RootCA, Subscriber] RootCA.notAfter < current time		RootCA	Validity - notAfter	< current time
		Base.17	01	NG	The RP should a reject certification path when a certificate has a notAfter set 500101000000Z. **[X.509 7]**		The notAfter in Subscriber has been set 500101000000Z. [RootCA, Subscribber] Subscriber.notAfter: 500101000000Z		Subscriber	Validity - notAfter	500101000000Z
		Base.18	01	NG	The RP should reject a certification path when a certificate has a notBefore set 491231235959Z. **[X.509 7]**		The not Before in Subscriber has been set 491231235959Z. [RootCA, Subscriber] Subscriber.notBefore: 491231235959Z		Subscriber	Validity - notBefore	491231235959Z
	Validity (CRL)										
		CRL.11	01	RV	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]**		The path includes a CRL that contains the revokedCertificates.revocationDate earlier than or equal to its thisUpdate. [RootCA-A, Subscriber-A]		RootCA-A.CRL	1) revokedCertificates.userCertificate 2) revokedCertificates.revocationDate	1) Subscriber-A.serialNumber 2) revocationDate <= thisUpdate
			02	NG			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
	Signature Checking Test Case										
		Base.19	01	NG	The RP should verify signatureValue in a certificate to be verified with a issuer certificate. **[X.509 10.5.1]**		The signature on Subscriber is invalid. [RootCA, Subscriber] Subscriber.signatureValue: tampered		Subscriber	signatureValue	tampered
	Signature Checking Test Case (CRL)										
		CRL.14	01	NG	The application (RP) should reject a tampered certificate revocation list (CRL). **[RFC3280 6.3.3 (g)]**		The path includes a CRL that contains the invalid signature. [RootCA-A, Subscriber-A]		RootCA-A.CRL	signature	invalid

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	Revocation Checking Test Case										
		Base.20	01	RV	The RP should reject a certification path when a certificate to be verified has been revoked. **[X.509 10.5.1]**		Subscriber has been revoked. [RootCA, Subscriber] RootCA.CRL.revokedCertificates: Subscriber.serialNumber		RootCA.CRL	revokedCertificates	Subscriber.serialNumber
	Unknown Extension Test Case										
		Base.21	01	OK	The RP should proccess a certification path which contains a certificate which has unrecognized extensions. **[X.509 7]**		Subscriber has an unrecognized extension which is not marked critical. [RootCA, Subscriber] Subscriber.UnknownExt: 123 (non-critical)		Subscriber	UnknownExt	non-critical id-pe-unknownExt OID ::= { id-pe 99 } UnknownExt ::= INTEGER
			02	NG			Subscriber has an unrecognized extension which is marked critical. [RootCA, Subscriber]		Subscriber	UnknownExt	critical
	Unknown Extension Test Case (CRL)										
		CRL.17	01	NG	The application (RP) should reject a certificate revocation list (CRL) that contains an unrecognized critical extension in the crlExtensions field. **[X.509 8]**		The path includes a CRL that contains an unrecognized critical extension in the crlExtensions field. [RootCA-A, Subscriber-A]		RootCA-A.CRL	crlExtensions.UnknownForExperiment	critical id-pe-unknown OID ::= { id-pe 99} unknownForExperiment ::= INTEGER
			02	OK			The path includes a CRL that contains an unrecognized non-critical extension in the crlExtensions field. [RootCA-A, Subscriber-A]		RootCA-A.CRL	crlExtionsions.UnknownForExperiment	non-critical id-pe-unknown OID ::= { id-pe 99} unknownForExperiment ::= INTEGER
		CRL.18	01	OK	The application (RP) should recognize and process well-known critical extensions in the crlExtension field. **[X.509 8]**		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]				
	Unknown Extension Test Case (CRL entry)										
		CRL.15	01	NG	The application (RP) should reject a certificate revocation list (CRL) that contains an unrecognized critical extension in the crlEntryExtensions field. **[X.509 8]**		The path includes a CRL that contains an unrecognized 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) critical id-pe-unknown OID ::= { id-pe 99} unknownForExperiment ::= INTEGER
			02	RV			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
		CRL.16	01	OK	The application (RP) should recognize and process well-known critical extensions in the crlEntryExtensions field. **[X.509 8]**		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.		RootCA-A.CRL	crlEntryExtension.certificateIssuer	critical cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	cRLDistributionPoints(cRLDP) and issuingDistributionPoint(iDP) Test Case (matching)										
		CRL.27	01	OK	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.		The path includes an EE certificate that contains several cRLDP.distributionPoint.fullName entries, and the corresponding CRL that contains several iDP.distributionPoint.fullName entries. Then one cRLDP.distributionPoint.fullName entry in the EE certificate matches one iDP.distributionPoint.fullName entry in the corresponding CRL. [RootCA-A, Subscriber-A]	Opt	1) Subscriber-A 2) RootCA-A.CRL	1) cRLDP.distPoint.fullName 2) iDP.distPoint.fullName	1) [4] (directoryName) cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA 1) [4] (directoryName) foo1 2) [4] (directoryName) cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA 2) [4] (directoryName) foo2
		CRL.28	01	NG	The application (RP) should correctly process the certification path when any one of cRLDP.distributionPoint.fullName entries in the certificate does not match any iDP.distributionPoint.fullName entries in the corresponding revocation list. **[RFC3280 5.2.5]**		The path includes an EE certificate that contains several cRLDP.distributionPoint.fullName entries, and the corresponding CRL that contains several iDP.distributionPoint.fullName entries. Then any one of cRLDP.distributionPoint.fullName entries in the EE certificate does not match any iDP.distributionPoint.fullName entries in the corresponding CRL. [RootCA-A, Subscriber-A]	Opt	1) Subscriber-A 2) RootCA-A.CRL	1) cRLDP.distPoint.fullName 2) iDP.distPoint.fullName	1) [4] (directoryName) cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA 1) [4] (directoryName) foo1 2) [4] (directoryName) foo2 2) [4] (directoryName) foo3
		CRL.29	01	NG	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.		The path includes a CRL that does not have the iDP.distributionPoint.fullName. [RootCA-A, Subscriber-A]	Opt	RootCA-A.CRL	iDP.distPoint.fullName	None
		CRL.30	01	OK	The application (RP) should correctly process the certification path when it verifies a certificate containing no cRLDP fields with the aforementioned revocation list, and when the isuer name of the certificate matches the directoryName in the iDP field.		The path includes a CRL that only contains the CA entry in the critical iDP field, which matches the issuer of the EE certificate. [RootCA-A, Subscriber-A]	Opt	1) Subscriber-A 2) RootCA-A.CRL	1) cRLDP 2) iDP.distPoint.fullName	1) None 2) cn=CA-A, ou=Root-A, o=PVTG Draft, c=AA
		CRL.31	01	NG	The application (RP) should correctly process the certification path when it verifies a certificate containing no cRLDP fields with the aforementioned revocation list, and when the issuer name of the certificate does not match the directoryName in the iDP. **[RFC3280 5.2.5]**		The path includes a CRL that only contains the CA entries in the critical iDP field, which does not match the issuer of the EE certificate. [RootCA-A, Subscriber-A]	Opt	1) Subscriber-A 2) RootCA-A.CRL	1) cRLDP 2) iDP.distPoint.fullName	1) None 2) cn=foo, ou=Root-A, o=PVTG Draft, c=AA

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	cRLDistributionPoints(cRLDP) and issuingDistributionPoint(iDP) Test Case (onlyContains flag)										
		CRL.19	01	NG	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)]**		The path includes a CRL that has the critical iDP 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.	Opt	RootCA-A.CRL	1) iDP.onlyContainsCACerts 2) revokedCertificates.userCertificate 3) revokedCertificates.revocationDate	1) TRUE 2) Subscriber-A.serialNumber 3) revocationDate <= current time
		CRL.20	01	NG	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)]**		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]	Opt	RootCA-A.CRL	1) iDP.onlyContainsCACerts 2) revokedCertificates.userCertificate 3) revokedCertificates.revocationDate	1) TRUE 2) Subscriber-A.serialNumber 3) revocationdate <= current time
		CRL.23	01	RV	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.		The path includes a CRL that has the critical iDP present with only the onlyContainsUserCerts flag set to TRUE, and the CRL contains the serialNumber of the EE certificate. [RootCA-A, Subscriber-A]	Opt	RootCA-A.CRL	1) revokedCertificates.UserCertificate 2) revokedCertificates.revocationDate	1) Subscriber-A.serialNumber 2) revocationDate <= current time
		CRL.24	01	OK	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)]**		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]	Opt			
	Additional keyUsage Extension Test Case for Digital Signature										
		DS.07	01	NG	The RP should ensure that a subscriber certificate has appropriate usage in keyUsage extension. **[IWG consideration]**		Subscriber does not have keyUsage extensions. [RootCA, Subscriber]	Opt	Subscriber	keyUsage	remove
			02	NG			Subscriber has the keyUsage present and critical, but digitalSignature bit is not asserted. [RootCA, Subscriber] Subscriber.keyUsage: keyEncipherment (critical)	Opt	Subscriber	keyUsage	keyEncipherment (critical)
			03	OK			Subscriber has the keyUsage present and not critical, with digitalSignature bit asserted. [RootCA, Subscriber] Subscriber.keyUsage: digitalSignature (non-critical)	Opt	Subscriber	keyUsage	digitalSignature (non-critical)
			04	OK			Subscriber has the keyUsage present and critical, with digitalSignature and keyAgreement bit asserted. [RootCA, Subscriber] Subscriber.keyUsage: digitalSignature, keyAgreement (critical)	Opt	Subscriber	keyUsage	digitalSignature, keyAgreement

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	certificatePolicy Extension Test Case										
		DS.08	01	NG	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]**	CC.RP.22	Subscriber does not have a valid policyIdentifier. [RootCA, Subscriber] Subscriber:certificatePolicies.policyIdentifier: policy-B (critical)	Opt	Subscriber	certificatePolicies - policyIdentifier	policy-B (critical)
		DS.09	01	OK	The RP should process certificatePolicies correctly when it has not been marked critical.		Subscriber has a valid policyIdentifier in non-critical certificatePolicies field. [RootCA, Subscriber] Subscriber:certificatePolicies.policyIdentifier: policy-A (non-critical)	Opt	Subscriber	certificatePolicies - policyIdentifier	policy-A (non-critical)
			02	NG			Subscriber does not have a valid policyIdentifier, and certificatePolicies extension has not been marked critical. [RootCA, Subscriber] Subscriber:certificatePolicies.policyIdentifier: policy-B (non-critical)	Opt	Subscriber	certificatePolicies - policyIdentifier	policy-B (non-critical)
		DS.10	01	OK	The RP should process a certification path which contains a certificate which has plural policyIdentifier present. **[X.509 8.1.1]**	CC.RP.24	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)	Opt	Subscriber	certificatePolicies - policyIdentifier	policy-A, policy-B (critical)
			02	NG			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	Opt	Subscriber	certificatePolicies - policyIdentifier	policy-B, policy-C (critical)
		DS.11	01	OK	The RP should process a certification path which contains a certificate which has plural policyIdentifier present and not critical.		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)	Opt	Subscriber	certificatePolicies - policyIdentifier	policy-A, policy-B (non-critical)
			02	NG			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)	Opt	Subscriber	certificatePolicies - policyIdentifier	policy-B, policy-C (non-critical)

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	Authority Key Identifier and Subject Key Identifier Test Case										
		Base.12	01	OK	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]**		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 Subscriber.authorityKeyID.keyIdentifier: foo	Opt	Subscriber	authorityKeyID - keyIdentifier	foo
	authorityKeyIdentifier and subjectKey Identifier Extension Test Case (CRL)										
		CRL.12	01	OK	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]		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.	Opt			
			02	OK			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.	Opt	RootCA-A.CRL	AKID	foo

NOTE: Exp Value: (OK) Path SHOULD be validated successfully (NG) Path SHOULD NOT be validated. (RV) Path SHOULD be validated as 'REVOKED'.

3.2 Strict Hierarchy Model Test Items

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	Normal Test Case										
		SH.08	01	OK	SH Normal Case		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)				
	DN matching Basic Test Case										
		SH.09	01	NG	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.08 Base.09 Base.10 Base.11	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=foo, ou=Root, o=PVTG Draft, c=AA		SubCA-1	issuer	cn=foo, ou=Root, o=PVTG Draft, c=AA

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	Additional DN matching Test Case										
		SH.DN.01	01	OK	DN Normal Case		The following path should be successfully validated; every certificate in the path. [RootCA, SubCA, Subscriber] RootCA issuerDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectKeyID.keyIdentifier: keyID.RootCA 1950 < notBefore < current time < notAfter < 2049 SubCA issuerDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA authorityKeyID.keyIdentifier: keyID.RootCA subjectKeyID.keyIdentifier: keyID.SubCA Subscriber issuerDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA subjectDN: cn=Test Business Subscriber, ou=Sub, ou=Root, o=PPTG, c=AA authorityKeyID.keyIdentifier: keyID.SubCA subjectKeyID.keyIdentifier: keyID.Subscriber 1950 < notBefore < current time < notAfter < 2049	Opt			
		SH.DN.02	01	OK	The RP should determine that the names are identifcal when they differ by whitespace in an attribute value (including leading and tailing whitespaces and more than one consesutive whitespace charactes in the value). **[X.520 (02_01) 6.1]** **[RFC3280 4.1.2.4]**		The following path should be successfully validated; the issuer name in Subscriber is differnt from the subject name in SubCA by whitespace in an attribute value. [RootCA,SubtCA, Subscriber] SubCA.subjectDN: cn=Test[][]Sub[]CA, ou=Sub, ou=Root, o=PPTG, c=AA Subscriber.issuerDN: cn=[][]Test[][]Sub[][][]CA[], ou=Sub, ou=Root, o=PPTG, c=AA	Opt	Subscriber	issuer.DN	EE.issuer:PrintableString: [][]Test[][]SubCA[] <=> SubCA.subject:PrintableString: Test[]SubCA
		SH.DN.03	01	OK	The RP should determine that the names are identifcal when they differ by capitalization **[X.520 (02_01) 6.11]** **[RFC3280 4.1.2.4]**		The following path should be successfully validated; the issuer name in Subscriber is different from the subject name in SubCA by capitalization. [RootCA,SubtCA, Subscriber] SubCA.subjectDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA Subscriber.issuerDN: cn=TEST SUB CA, ou=Sub, ou=Root, o=PPTG, c=AA	Opt	Subscriber	issuer.DN	EE.issuer:PrintableString: TEST SUBCA <=> SubCA.subject:PrintableString: Test SubCA
		SH.DN.4	01	OK	The RP should determine that the names are identifcal when they differ in ASN.1 encording type but contains the same character sets. **[X.520 (02_01) 6.11]**		The following path should be successfully validated; the issuer name in Subscriber and the subject name in SubCA differs in ASN.1 encoding type but contains the same string value. [RootCA, SubCA, Subscriber] SubCA.subjectDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA (encorded in PrintableString) Subscriber.issuerDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA (encorded in UTF8String)	Opt	Subscriber	issuer.DN	EE.issuer:UTF8String: Test SubCA <=> SubCA.subject:PrintableString: Test SubCA

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
		SH.DN.5	01	NG	The RP should determine that the names are different when they differ by order. **[X.501(93_03) 12.5.2]**		The following path should not be successfully validated; the issuer name in Subscriber is different from the subject name in SubCA by order. [RootCA, SubCA, Subscriber] SubCA.subjectDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA Subscriber.issuerDN: cn=Test Sub CA, ou=Root, ou=Sub, o=PPTG, c=AA	Opt	Subscriber	issuer.DN	EE.issuer: *, ou=Root, ou=Sub, * <=> SubCA.subject: *, ou=Sub, ou=Root, *
		SH.DN.6	01	NG	The RP should determine that the names are different when they are completely different. **[X.501(93_03) 12.5.2]**		The following path should not be successfully validated; the issuer name in Subscriber differs completely from the subject name in SubCA. [RootCA, SubCA, Subscriber] SubCA.subjectDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA Subscriber.issuerDN: cn=TestCA,c=ZZ	Opt	Subscriber	issuer.DN	EE.issuer: *, c=AA <=> SubCA.subject: *, c=ZZ
		SH.DN.7	01	OK	The RP should determine that the names are identifcal when they use identical CJK charactes (encorded in UTF8). **[RFC3280 4.1.2.4]**		The following path should be successfully validated; every certificate in the path. [RootCA, SubCA, Subscriber] RootCA issuerDN: cn=<CJKs>, ou=<CJKs>, o=<CJKs>, c=AA subjectDN: cn=<CJKs>, ou=<CJKs>, o=<CJKs>, c=AA subjectKeyID.keyIdentifier: keyID.RootCA 1950 < notBefore < current time < notAfter < 2049 SubCA issuerDN: cn=<CJKs>, ou=<CJKs>, o=<CJKs>, c=AA subjectDN: cn=<CJKs>, ou=<CJKs>, ou=<CJKs>, o=<CJKs>, c=AA authorityKeyID.keyIdentifier: keyID.RootCA subjectKeyID.keyIdentifier: keyID.SubCA Subscriber issuerDN: cn=<CJKs> ou=<CJKs>, ou=<CJKs>, o=<CJKs>, c=AA subjectDN: cn=<CJKs>, ou=<CJKs>, ou=<CJKs>, o=<CJKs>, c=AA	Opt	1) RootCA 2) SubCA 3) Subscriber	issuer.DNs and subject.DNs	issuer.DNs and subject.DNs contains CJK

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	basicConstraints Extension Test Case										
		SH.11	01	NG	The RP should reject a certification path which containis a subordinate CA certificate which does not have a basicConstraints. **[X.509 10.5.1]**		SubCA-1 does not have a basicConstraints. [RootCA, SubCA-1, Subscriber-1]		SubCA-1	basicConstraints	remove
		SH.12	01	NG	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]**		SubCA-1 has basicConstraints present and critical with cA flag set to false. [RootCA, SubCA-1, Subscriber-1] SubCA-1.basicConstraints.cA: FALSE		SubCA-1	basicConstraints - cA	FALSE
		SH.13	01	OK	The RP should reject a certification path which contains a subordinate CA certificate which has basicConstraints present and not critical with cA flag asserted.		SubCA-1 has basicConstraints present and not critical with cA flag asserted. [RootCA, SubCA-1, Subscriber-1] SubCA-1.basicConstraints.cA: TRUE (non-critical)		SubCA-1	basicConstraints	non-critical
		SH.14	01	OK	The RP should process basicConstraints.pathLenConstraints in all subordinate CA certificates in the certification path. **[X.509 10.5.1]**		SubCA-1 has the basicConstraints present and critical with pathLenConstraints set to 0. [RootCA, SubCA-1, Subscriber-1] SubCA-1.basicConstraints.pathLenConstraints: 0		SubCA-1	basicConstraints - pathLenConstraints	0
			02	NG			SubCA-1 has the basicConstraints present and critical with pathLenConstraints set to 0. [RootCA, SubCA-1, SubCA2, Subscriber-2] SubCA-1.basicConstraints.pathLenConstraints: 0				
	keyUsage Extension Test Case										
		SH.15	01	NG	The RP should reject a certification path which contains an intermediate CA certificate which does not have keyUsage extension. **[IWG profile]**		SubCA-1 does not have a keyUsage. [RootCA, SubCA-1, Subscriber-1]		SubCA-1	keyUsage	remove
		SH.16	01	NG	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]**		SubCA-1 has the keyUsage present and critical with digitalSignature bit asserted. [RootCA, SubCA-1, Subscriber-1] SubCA-1.keyUsage: digitalSignature		SubCA-1	keyUsage	digitalSignature
		SH.17	01	OK	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.		SubCA-1 has the keyUsage present and not critical with keyCertSign bit asserted. [RootCA, SubCA-1, Subscriber-1] SubCA-1.keyUsage: keyCertSign (non-critical)		SubCA-1	keyUsage	non-critical

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	keyUsage Extension Test Case (CRL)										
		SH.CRL.13	01	OK	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)]**		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]				
			02	OK			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
			03	NG			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
			04	NG			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
			05	NG			The path includes two CA certificates that do not contain the keyUsage fields. [RootCA-A, SubCA, Subscriber-A]		SubCA	keyUsage	none
	certificatePolicy Extension Test Case										
		SH.18	01	NG	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]**		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)		Subscriber-1	certificatePolicies - policyIdentifier	policy-B
		SH.19	01	OK	The RP should process certificatePolicies correctly when it has not been marked critical.		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-		Subscriber-1	certificatePolicies	non-critical
			02	NG			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-		1. Subscriber-1	1.1 certificatePolicies 1.2 certificatePolicies - policyIdentifiers	2.1. non-critical 2.2. policy-B

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
		SH.20	01	OK	The RP should process a certification path which contains a certificate which has plural policyIdentifier present. **[X.509 8.1.1]**		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. SubCA-1 2. SubCA-2	certificatePolicies - policyIdentifier	1. policy-A, policy-B 2. policy-A, policy-C
			02	NG			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
		SH.21	01	OK	The RP should process a certification path which contains a certificate which has plural policyIdentifier present and not critical.		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-		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
			02	NG			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-2.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 Checking Test Case										
		SH.22	01	NG	The RP should reject a certification path which contains a intermediate CA certificate revoked.	Base.20	SubCA-1 has been revoked. [RootCA, SubCA-1, Subscriber-1]		RootCA.CRL (or ARL)	revokedCertificates	SubCA-1.serialNumber
	Signature Checking Test Case										
		SH.23	01	NG	The RP should verify signatureValue in a intermediate CA certificate with its issuer certificate. **[X.509 10.5.1]**	Base.19	The signature on SubCA-1 is invalid. [RootCA, SubCA-1, Subscriber-1] SubCA-1.signatureValue: tampered		SubCA-1	signatureValue	tampered

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	cRLDistributionPoints and issuingDistributionPoint Test Case (onlyContains flag)										
		SH.CRL.21	01	RV	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)]**		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]	Opt	RootCA-A.ARL	1) revokedCertificates.userCertificate 2) revokedCertificates.revocationDate	1) SubCA.serialNumber 2) revocationDate <= current time
		SH.CRL.22	01	OK	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)]**		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]	Opt			
		SH.CRL.25	01	RV	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)]**		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]	Opt	RootCA-A.ARL	1) issuingDP.onlyContainsUserCerts 2) revokedCertificates.userCertificate 3) revokedCertificates.revocationDate	TRUE SubCA.serialNumber revocationDate <= current time
		SH.CRL.26	01	NG	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)]**		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]	Opt	RootCA-A.ARL	issuingDP.onlyContainsUserCerts	TRUE

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	cRLDistributionPoints and issuingDistributionPoint Test Case (LDAP URI)										
					Normal Case						
		SH.LDAPURI.0	01	RV	LDAP URI Normal Case		[RootCA, SubCA, Subscriber] RootCA issuerDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectKeyID.keyIdentifier: keyID.RootCA 1950 < notBefore < current time < notAfter < 2049 SubCA issuerDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA authorityKeyID.keyIdentifier: keyID.RootCA subjectKeyID.keyIdentifier: keyID.SubCA Subscriber issuerDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA subjectDN: cn=Test Business Subscriber, ou=Sub, ou=Root, o=PPTG, c=AA authorityKeyID.keyIdentifier: keyID.SubCA subjectKeyID.keyIdentifier: keyID.Subscriber 1950 < notBefore < current time < notAfter < 2049	Opt	1) Subscriber 2) SubCA	1) cRLDP.distPoint.fullName 2) revokedCertificates.userCertificate	1) ldap://example.tld/cn=Test%20Sub%20CA,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList 2) Subscriber.serialNumber EE.Cert.cRLDP = SubCA.CRL.iDP
			02	RV			[RootCA, SubCA] RootCA issuerDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectKeyID.keyIdentifier: keyID.RootCA 1950 < notBefore < current time < notAfter < 2049 SubCA issuerDN: cn=Test Root CA, ou=Root, o=PPTG, c=AA subjectDN: cn=Test Sub CA, ou=Sub, ou=Root, o=PPTG, c=AA authorityKeyID.keyIdentifier: keyID.RootCA subjectKeyID.keyIdentifier: keyID.SubCA	Opt	1) SubCA 2) RootCA.ARL	1) cRLDP.distPoint.fullName 2) revokedCertificates.userCertificate	1) ldap://example.tld/cn=Test%20Root%20CA,ou=Root,o=PPTG,c=AA?AuthorityRevocationList 2) SubCA.serialNumber SubCA.Cert.cRLDP = RootCA.ARL.iDP
					White Space Normalization						
		SH.LDAPURI.0	01	RV	The RP should ignore the white space on either side of the delimiter in LDAP URI. **[RFC 1779]** **[RFC2253 4]**		The path includes the CRL which contains the serialNumber of the Subscriber certificate. And the cRLDP.distPoint.fullName in Subscriber includes white space on either side of the delimiter(","). [RootCA, SubCA, Subscriber] SubCA.CRL.revokedCertificates.userCertificate: Subscriber.serialNumber Subscriber.cRLDP.distPoint.fullName: ldap://example.tld/cn=Test%20Sub%20CA%20,%20ou=Sub%20%20%20,%20%20%20ou=Root,o=PPTG,c=AA?certificateRevocationList	Opt	1) Subscriber 2) SubCA.CRL	1) cRLDP.distPoint.fullName 2) revokedCertificates.userCertificate	1)ldap://example.tld/cn=Test%20Sub%20CA%20,%20ou=%Sub%20%20%20,%20%20%20ou=Root,o=PPTG,c=AA?certificateRevocationList 2)Subscriber.serialNumber EE.Cert.cRLDP = SubCA.CRL.iDP SubCA.subject.DN: cn=Test SubCA,ou=Sub EE.Cert.cRLDP: cn=Test SubCA[],[]ou=Sub (URI encoded)
		SH.LDAPURI.0	01	RV	The RP should ignore the white space on either side of "=" which separates attribute type and attribute value in LDAP URI. **[RFC1779]** **[RFC2253 4]**		The path includes the CRL which contains the serialNumber of the Subscriber certificate. And the cRLDP.distPoint.fullName in Subscriber includes white space on either side of "=". [RootCA, SubCA, Subscriber] SubCA.CRL.revokedCertificates.userCertificate: Subscriber.serialNumber Subscriber.cRLDP.distPoint.fullName: ldap://example.tld/cn%20=%20Test%20Sub%20CA,ou%20%20%20=%20%20%20Sub,ou=Root,o=PPTG,c=AA?certificateRevocati	Opt	1) Subscriber 2) SubCA.CRL	1) cRLDP.distPoint.fullName 2) revokedCertificates.userCertificate	1)ldap://example.tld/cn%20=%20Test%20Sub%20CA,ou%20%20%20=%20%20%20Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList 2)Subscriber.serialNumber EE.Cert.cRLDP = SubCA.CRL.iDP SubCA.subject.DN: cn=Test SubCA EE.Cert.cRLDP: cn[]=[]Test SubCA (URI encoded)

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
					Semi-colon delimiter						
		SH.LDAPURI.4	01	RV	The RP should determine semicolon in LDAP URI as delimiter. **[RFC1779]** **[RFC2253 4]**		The following path should be validated as "revoked"; The path includes the CRL which contains the serialNumber of the Subscriber certificate. And the cRLDP.distPoint.fullName in Subscriber includes semicolon character as delimiter instead of comma character. [RootCA, SubCA, Subscriber] SubCA.CRL.revokedCertificates.userCertificate: Subscriber.serialNumber Subscriber.cRLDP.distPoint.fullName: ldap://example.tld/cn=Test%20Root%20CA;ou=Sub;ou=Root;o=P	Opt	1) Subscriber 2) SubCA.CRL	1) cRLDP.distPoint.fullNam e 2) revokedCertificates.user Certificate	1)ldap://example.tld/cn=Test%20Root%20CA;ou=Sub;ou=Root;o=PPTG;c=AA?certificateRevocationList 2)Subscriber.serialNumber RDN delimiter "," => ";"
					Back Slash Escaping						
		SH.LDAPURI.5	01	RV	The RP should determine escaped character in LDAP URI. **[RFC1179]** **[RFC1738 2.2]** **[RFC2253 2.4]** **[RFC2255]** **[IWG Recommendation]**		The path includes the CRL which contains the serialNumber of the Subscriber certificate. And the cRLDP.distPoint.fullName in Subscriber includes comma character which is prefixed by a backslash character as attribute value. [RootCA, SubCA, Subscriber] SubCA.CRL.revokedCertificates.userCertificate: Subscriber.serialNumber Subscriber.cRLDP.distPoint.fullName: ldap://example.tld/cn=Test%5c,Sub%20CA,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList	Opt	1) Subscriber 2) SubCA.CRL	1) cRLDP.distPoint.fullNam e 2) revokedCertificates.user Certificate	1)ldap://example.tld/cn=Test%5c,Sub%20CA,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList 2)Subscriber.serialNumber \, (escape)=> %5c,
			02	RV			The path includes the CRL which contains the serialNumber of the Subscriber certificate. And the cRLDP.distPoint.fullName in Subscriber includes comma character which is prefixed by a backslash character as attributevalue. And the comma(",") is encoded. [RootCA, SubCA, Subscriber] SubCA.CRL.revokedCertificates.userCertificate: Subscriber.serialNumber Subscriber.cRLDP.distPoint.fullName: ldap://example.tld/cn=Test%5c2cSub%20CA,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList	Opt	1) Subscriber 2) SubCA.CRL	1) cRLDP.distPoint.fullNam e 2) revokedCertificates.user Certificate	1)ldap://example.tld/cn=Test%5c2cSub%20CA,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList 2)Subscriber.serialNumber \, (escape)=> %5c2c
			03	RV			The path includes the CRL which contains the serialNumber of the Subscriber certificate. And the cRLDP.distPoint.fullName in Subscriber includes RDN sequence which has comma character and is enclosed in double quotes. [RootCA, SubCA, Subscriber] SubCA.CRL.revokedCertificates.userCertificate: Subscriber.serialNumber Subscriber.cRLDP.distPoint.fullName: ldap://example.tld/cn=%22Test,Sub%20CA%22,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList	Opt	1) Subscriber 2) SubCA.CRL	1) cRLDP.distPoint.fullNam e 2) revokedCertificates.user Certificate	1)ldap://example.tld/cn=%22Test,Sub%20CA%22,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList 2)Subscriber.serialNumber "cn=AA,o=Sub" (escape)=> %22cn=AA,o=Sub%22

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
		Port Number									
		SH.LDAPURI.(	01	RV	The RP should determine portnumber information in LDAPURI other than "389". **[RFC 2255 3]** **[IWG Recommendation]**		The path includes the CRL which contains the serialNumber of the Subscriber certificate. And the cRLDP.distPoint.fullName in Subscriber gives host portnumber other than "389". [RootCA, SubCA, Subscriber] SubCA.CRL.revokedCertificates.userCertificate: Subscriber.serialNumber Subscriber.cRLDP.distPoint.fullName: ldap://example.tld:8389/cn=Test%20Business%20Subscriber,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList;binary	Opt	1) Subscriber 2) SubCA.CRL	1) cRLDP.distPoint.fullName 2) revokedCertificates.userCertificate	1)ldap://example.tld:8389/cn=Test%20Business%20Subscriber,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList;binary 2)Subscriber.serialNumber LDAP Port 8379
	cRLDistributionPoints and issuingDistributionPoint Test Case (CJK)										
		Unicode CJK Unified Ideographs (Range:4E00-9FAF)									
		SH.CJK.01	01	OK	The RP should process a certification path when DN contains Unicode "CJK Unified Ideographs(4E00-9FAF)" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Unified Ideographs". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. **中日韓** (U+4E2D, U+65E5, U+97D3)
			02	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Unified Ideographs". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. **中日韓** => %E4%B8%AD%E6%97%A5%E9%9F%93
			03	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Unified Ideographs". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". **中日韓** => %5CE4%5CB8%5CAD%5CE6%5C97%5CA5%5CE9%5C9F%5C93
		Unicode CJK Compatibility Ideographs (Range:F900-FAFF)									
		SH.CJK.2	01	OK	The RP should process a certification path when DN contains Unicode "CJK Compatibility Ideographs(F900-FAFF)" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Compatibility Ideographs". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. **豈鶴練** (U+F900, U+F996, U+FA2D)
			02	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Compatibility Ideographs". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. **豈鶴練** => %EF%A4%80%EF%A8%AD%EF%A6%96
			03	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Compatibility Ideographs". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". **豈鶴練** => %5CEF%5CA4%5C80%5CEF%5CA8%5CAD%5CEF%5CA6%5C96

entitiy	category	sequence number	requirement	relevant to ...	test item number	Exp Value	test item	Level	differences		
									Cert type	Field	Value
		Port Number									
		SH.LDAPURI.6	The RP should determine portnumber information in LDAPURI other than "389". **[RFC 2255 3]** **[IWG Recommendation]**		SH.LDAPURI.06.01	RV	The path includes the CRL which contains the serialNumber of the Subscriber certificate. And the cRLDP.distPoint.fullName in Subscriber gives host portnumber other than "389". [RootCA, SubCA, Subscriber] SubCA.CRL.revokedCertificates.userCertificate: Subscriber.serialNumber Subscriber.cRLDP.distPoint.fullName: ldap://example.tld:8389/cn=Test%20Business%20Subscriber,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList;binary	Opt	1) Subscriber 2) SubCA.CRL	1) cRLDP.distPoint.fullName 2) revokedCertificates.userCertificate	1)ldap://example.tld:8389/cn=Test%20Business%20Subscriber,ou=Sub,ou=Root,o=PPTG,c=AA?certificateRevocationList;binary 2)Subscriber.serialNumber LDAP Port 8379
	cRLDistributionPoints and issuingDistributionPoint Test Case (CJK)										
		Unicode CJK Unified Ideographs (Range:4E00-9FAF)									
		SH.CJK.01	The RP should process a certification path when DN contains Unicode "CJK Unified Ideographs(4E00-9FAF)" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		SH.CJK.01.01	OK	The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Unified Ideographs". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. **中日韓** (U+4E2D, U+65E5, U+97D3)
					SH.CJK.01.02	OK	The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Unified Ideographs". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. **中日韓** => %E4%B8%AD%E6%97%A5%E9%9F%93
					SH.CJK.01.03	OK	The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Unified Ideographs". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". **中日韓** => %5CE4%5CB8%5CAD%5CE6%5C97%5CA5%5CE9%5C9F%5C93
		Unicode CJK Compatibility Ideographs (Range:F900-FAFF)									
		SH.CJK.2	The RP should process a certification path when DN contains Unicode "CJK Compatibility Ideographs(F900-FAFF)" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		SH.CJK.02.01	OK	The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Compatibility Ideographs". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. **豈鶴練** (U+F900, U+F996, U+FA2D)
					SH.CJK.02.02	OK	The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Compatibility Ideographs". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. **豈鶴練** => %EF%A4%80%EF%A8%AD%EF%A6%96
					SH.CJK.02.03	OK	The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Compatibility Ideographs". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". **豈鶴練** => %5CEF%5CA4%5C80%5CEF%5CA8%5CAD%5CEF%5CA6%5C96

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
		Unicode Hiragana (Range:3040-309F)									
		SH.CJK.3	01	OK	The RP should process a certification path when DN contains Unicode "Hiragana(3040-309F)" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Hiragana". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. はな (U+306F, U+306A)
			02	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Hiragana". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. はな => %E3%81%AF%E3%81%AA
			03	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Hiragana". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". はな => %5CE3%5C81%5CAF%5CE3%5C81%5CAA
		Unicode Katakana (Range:30A0-30FF)									
		SH.CJK.4	01	OK	The RP should process a certification path when DN contains Unicode "Katakana(30A0-30FF)" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Katakana". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. テスト (U+30C6, U+30B9, U+30C8)
			02	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Katakana". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. テスト => %E3%83%86%E3%82%B9%E3%83%88
			03	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Katakana". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". テスト => %5CE3%5C83%5C86%5CE3%5C82%5CB9%5CE3%5C83%5C88

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
		Unicode Halfwidth and Fullwidth Forms (Range:FF00-FFEF)									
		SH.CJK.5	01	OK	The RP should process a certification path when DN contains Unicode "Halfwidth and Fullwidth Forms(FF00-FFEF)" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Halfwidth and Fullwidth Forms". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. ＼￥₹ (U+FF3C, U+FFE5, U+FF8F)
			02	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Halfwidth and Fullwidth Forms". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. ＼￥₹ => %EF%BC%BC%EF%BF%A5%EF%BE%8F
			03	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Halfwidth and Fullwidth Forms". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". ＼￥₹ => %5CEF%5CBC%5CBC%5CEF%5CBF%5CA5%5CEF%5CBE%5C8F
		Unicode Hangul Syllables (Range:AC00-D7AF)									
		SH.CJK.6	01	OK	The RP should process a certification path when DN contains Unicode "Hangul Syllables(AC00-D7AF)" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Hangul Syllables". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. 한국 (U+D55C, U+AD6D)
			02	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Hangul Syllables". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. 한국 => %ED%95%9C%EA%B5%AD
			03	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "Hangul Syllables". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". 한국 => %5CED%5C95%5C9C%5CEA%5CB5%5CAD

entitiy	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
		Unicode CJK Symbols and Punctuations (Range:3000-303F)									
		SH.CJK.7	01	OK	The RP should process a certification path when DN contains Unicode "CJK Symbols and Punctuations" characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Symbols and Punctuations". And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. **【々**『(U+3010, U+3005, U+300E)
			02	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Symbols and Punctuations". And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. **【々**『=> %E3%80%90%E3%80%85%E3%80%8E
			03	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains "CJK Symbols and Punctuations". And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". **【々**『=> %5CE3%5C80%5C90%5CE3%5C80%5C85%5CE3%5C80%5C8E
		Unicode CJK characters mixed with ASCII characters									
		SH.CJK.8	01	OK	The RP should process a certification path when DN contains Unicode CJK and ASCII characters. [RFC 1779] [RFC2253 4] [Unicode Standard 4.0]		The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains CJK and ASCII characters. And the distributionPoint of cRLDP and iDP is represented as directory name. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is DN of UTF8String. **中華民國**Singapore한국**日本** **中華民國** : U+4E2D, U+83EF, U+6C11, U+570B 한국 : U+D55C, U+AD6D **日本** : U+65E5, U+672C
			02	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains CJK and ASCII characters. And the cRLDP and iDP is represented as LDAP URI. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string. **中華民國**Singapore한국**日本** => %E4%B8%AD%E8%8F%AF%E6%B0%91%E5%9C%8BSingapore%ED%95%9C%EA%B5%AD%E6%97%A5%E6%9C%AC
			03	OK			The following path should be successfully validated; The path includes the certificates and CRLs which issuer name, subject name, cRLDP and iDP contains CJK and ASCII characters. And the cRLDP and iDP is represented as LDAP URI with escaping back slash. [RootCA, SubCA(UTF8 CJK), Subscriber(UTF8 CJK)]	Opt	1) Subscriber 2) SubCA.CRL	1)issuer 1)cRLDP.distPoint.fullName 2)subject 2)CRL.iDP.distPoint.fullName	cRLDP and iDP is LDAPURI where CJK characters are escaped as hexadecimal string then escaped with back slash "%5c". **中華民國**Singapore한국**日本** => %5CE4%5CB8%5CAD%5CE8%5C8F%5CAF%5CE6%5CB0%5C91%5CE5%5C9C%5C8BSingapore%5CED%5C95%5C9C%5CEA%5CB5%5CAD%5CE6%5C97%5CA5%5CE6%5
	authorityKeyIdentifier and subjectKey Identifier Extension Test Case										
		SH.10	01	OK	The RP should ensure that authorityKeyIdentifier.keyIdentifier in one certificate and subjectKeyIdentifier in its issuer certificate are identical. **[RFC3280 4.2.1.2]**	Base.12	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: foo	Opt	SubCA-1	authorityKeyID - keyIdentifier	foo

NOTE: Exp Value: (OK) Path SHOULD be validated successfully (NG) Path SHOULD NOT be validated. (RV) Path SHOULD be validated as 'REVOKED'.

3.3 Cross Certification Model Test Items

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	Normal Test Case										
		CC.19	01	OK	CC Normal Case		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.CrossY-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				
	DN matching Basic Test Case										
		CC.20	01	NG	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.08 Base.09 Base.10 Base.11	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=foo, ou=Root-X, o=PVTG Draft, c=AA		CrossY-X	issuer	cn=foo, ou=Root-X, o=PVTG Draft , c=AA
	certificatePolicies and policyMappings Extension Test Case										
		CC.22	01	NG	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]**		Subscriber-Y has an invalid policyIdentifier in the critical certificatePolicies field. [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y Subscriber-Y certificatePolicies.policyIdentifier: policy-W (critical)		Subscriber-Y	certificatePolicies - policyIdentifier	policy-W (critical)
		CC.23	01	OK	The RP should process certificatePolicies correctly when it has not been marked critical.		Subscriber-Y has a valid policyIdentifier in the non-critical certificatePolicies. [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y Subscriber certificatePolicies.policyIdentifier: policy-Y (non-critical)		Subscriber-Y	certificatePolicies - policyIdentifier	policy-Y (non-critical)

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
			02	NG			Subscriber-Y has an invalid policyIdentifier in the non-critical certificatePolicies. [RootCA-X, CrossY-X, Subscriber-Y] CrossY-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)
		CC.24	01	OK	The RP should process a certification path which contains a certificate which has plural policyIdentifier present. **[X.509 8.1.1]**		CrossY-X has plural policyIdentifier in the critical certificatePolicies, and a valid policyIdentifier appears in all certificates. [RootCA-X, CrossY-X, Subordinate-Y] CrossY-X certificatePolicies.policyIdentifier: policy-X, policy-V (critical) policyMappings: policy-X = policy-Y Subordinate-Y certificatePolicies.policyIdentifier: policy-Y (critical)		CrossY-X	certificatePolicies - policyIdentifier	policy-X, policy-V
			02	NG			CrossY-X has plural policyIdentifier in the critical certificatePolicies, and a valid policyIdentifier does not appear in Subscriber-Y. [RootCA-X, CrossY-X, Subordinate-Y] CrossY-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
		CC.25	01	OK	The RP should process a certification path which contains a certificate which has plural policyMappings present. **[X.509 8.1.1]**		CrossY-X has plural policyMappings present, and a valid policyIdentifier appears in all certificates. [RootCA-X, CrossY-X, Subordinate-Y] CrossY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y, policy-X = policy-W Subordinate-Y certificatePolicies.policyIdentifier: policy-W (critical)		1. CrossY-X 2. Subscriber-Y	1. policyMappings 2. certificatePolicies - policyIdentifier	1. policy-X = policy-Y, policy-X = policy-W 2. policy-W
			02	NG			CrossY-X has plural policyMappings present, and Subscriber-Y has an invalid policyIdentifier in the critical certificatePolicies. [RootCA-X, CrossY-X, Subordinate-Y] CrossY-X certificatePolicies.policyIdentifier: policy-X (critical) policyMappings: policy-X = policy-Y, policy-V = policy-W Subordinate-Y certificatePolicies.policyIdentifier: policy-W (critical)		1. CrossY-X 2. Subscriber-Y	1. policyMappings 2. certificatePolicies - policyIdentifier	1. policy-X = policy-Y, policy-V = policy-W 2. policy-W

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	basicConstraints Extension Test Case										
		CC.26	01	NG	The RP should reject a certification path which containis a cross-certificate which does not have a basicConstraints. **[X.509 10.5.1]**	SH.11	CrossY-X does not have a basicConstraints. [RootCA-X, CrossY-X, Subscriber]		CrossY-X	basicConstraints	remove
		CC.27	01	NG	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]**	SH.12	CrossY-X has the basicConstraints present and critical, with cA flag set to false. [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X.basicConstraints.cA: FALSE		CrossY-X	basicConstraints - cA	FALSE
		CC.28	01	OK	The RP should reject a certification path which contains a cross-certificate which has basicConstraints present and not critical with cA flag asserted.		CrossY-X has the basicConstraints present and not critical with cA flag asserted. [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X.basicConstraints.cA: TRUE (non-critical)		CrossY-X	basicConstraints	non-critical
		CC.29	01	OK	The RP should process basicConstraints.pathLenConstraints in all cross-certificates in the certification path. **[X.509 10.5.1]**	SH.14	[RootCA-X, CrossY-X, Subordinate-Y] CrossY-X.basicConstraints.pathLenConstraints: 0[deafault] NOTE: This skipCerts value is adjustable for your hierarchy, if necessary. Deafult(non-hierarchy) is zero.		CrossY-X	basicConstraints - pathLenConstraints	default:0 (
			02	NG			[RootCA-X, CrossY-X, CrossZ-Y, Subscriber-Z] CrossY-X.basicConstraints.pathLenConstraints: 0[deafult] NOTE: This skipCerts value is adjustable for your hierarchy, if necessary. Deafult(non-hierarchy) is zero.				
	keyUsage Extension Test Case										
		CC.30	01	NG	The RP should reject a certification path which contains an intermediate CA certificate which does not have keyUsage extension. **[IWG profile]**	SH.15	CrossY-X does not have a keyUsage. [RootCA-X, CrossY-X, Subscriber-Y]		CrossY-X	keyUsage	remove
		CC.31	01	NG	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]**	SH.16	CrossY-X has the keyUsage present and critical, with digitalSignature bit asserted. [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X.keyUsage: digitalSignature (critical)		CrossY-X	keyuUsage	digitalSignature
		CC.32	01	OK	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.		CrossY-X has the keyUsage present and not critical with keyCertSign bit asserted. [RootCA-X, CrossY-X, Subordinate-Y] CrossY-X.keyUsage: keyCertSign (non-critical)		CrossY-X	keyUsage	non-critical

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	policyConstraints Extension Test Case										
		CC.33	01	OK	The RP should process policyConstraints.requireExplicitPolicy in all cross-certificates in the path. **[X.509 10.5.2, 10.5.3]**		CrossY-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, CrossY-X, Subscriber-Y] CrossY-X policyConstraints.rEP: 1 NOTE: This skipCerts value is adjustable for your hierarchy, if necessary. Deafult(non-hierarchy) is one. Subscriber-Y certificatePolicies.policyIdentifier: foo		1. CrossY-X 2. Subscriber-Y	1. policyConstraints - requireExplicitPolicy 2. certificatePolicies - policyIdentifier	1. 1 2. foo
			02	NG			CrossY-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, CrossY-X, Subscriber-Y] CrossY-X policyConstraints.rEP: 0 NOTE: This skipCerts value is adjustable for your hierarchy, if necessary. Deafult(non-hierarchy) is zero. Subscriber-Y certificatePolicies.policyIdentifier: foo		1. CrossY-X 2. Subscriber-Y	1. policyConstraints - requireExplicitPolicy 2. certificatePolicies - policyIdentifier	1. 0 2. foo
		CC.34	01	OK	The RP should process policyConstraints.inhibitPolicyMapping in all cross-certificates in the path. **[X.509 10.5.2, 10.5.3]**		CrossY-X has policyConstraints present and critical with the inhibitPolicyMapping component set to 1. [RootCA-X, CrossY-X, CrossZ-Y, Subscriber-Z] CrossY-X.policyConstraints.iPM: 1		CrossY-X	policyConstraints - inhibitPolicyMapping	1
			02	NG			CrossY-X has policyConstraints present and critical with the inhibitPolicyMapping component set to 0. [RootCA-X, CrossY-X, CrossZ-Y, Subscriber-Z] CrossY-X.policyConstraints.iPM: 0		CrossY-X	policyConstraints - inhibitPolicyMapping	0

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	nameConstraints Extension Test Case										
		CC.35	01	OK	The RP should process nameConstraints.permittedSubtrees in all cross-certificates in the certification path. **[X.509 10.5.2]**		CrossY-X has the nameConstraints present and critical with the permittedSubtrees.base set "ou=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X.nameConstraints.permittedSubtrees.base: ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y.subject: cn=Subscriber-Y, ou=Root-Y, o=PVTG Draft,		CrossY-X	nameConstraints - permitSubtrees.base	ou=CrossY-X, o=PVTG Draft, c=BB
			02	NG			CrossY-X has the nameConstraints present and critical with the permittedSubtrees.base set "ou=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X nameConstraints.permittedSubtrees.base: ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y subjectDN: cn=Subscriber-Y, o=PVTG Draft, c=BB		1. CrossY-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
		CC.36	01	OK	The RP should process nameConstraints.excludedSubtrees in all cross-certificates in the certification path. **[X.509 10.5.2]**		CrossY-X has the nameConstraints present and critical, with the excludedSubtrees.base component set "ou=foo, ou=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X nameConstraints.excludedSubtrees.base: ou=foo, ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y subject: cn=Subscriber-Y, ou=Root-Y, o=PVTG Draft, c=BB		1. CrossY-X 2. Subscriber-Y	1. nameConstraints - excludedSubtrees.base 2. subject	1. ou=foo, ou=Root-Y, o=PVTG Draft, c=BB 2. cn=Subscriber-Y, ou=Root-Y, o=PVTG Draft, c=BB
			02	NG			CrossY-X has the nameConstraints present and critical, with the excludedSubtrees.base set "ou=foo, ou=Root-Y, o=PVTG Draft, c=BB". Subject name in Subscriber-Y is "cn=Subscriber-Y, ou=foo, ou=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X nameConstraints.excludedSubtrees.base: ou=foo, ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y subject: cn=Subscriber-Y, ou=foo, ou=Root-Y, o=PVTG Draft,		1. CrossY-X 2. Subscriber-Y	1. nameConstraints - excludedSubtrees.base 2. subject	1. ou=foo, ou=Root-Y, o=PVTG Draft, c=BB 2. cn=Subscriber-Y, ou=foo, ou=Root-Y, o=PVTG Draft, c=BB
		CC.37	01	NG	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]**		CrossY-X has the critical nameConstraints present with permittedSubtrees component set "ou=Root-Y, o=PVTG Draft, c=BB", and with excludedSubtrees component set "ou=foo, ou=Root-Y, o=PVTG Draft, c=BB". the subject name in Subscriber-Y is "cn=Subscriber-Y, ou=foo, o=Root-Y, o=PVTG Draft, c=BB". [RootCA-X, CrossY-X, Subscriber-Y] CrossY-X nameConstraints.permittedSubtrees.base: ou=Root-Y, o=PVTG Draft, c=BB nameConstraints.excludedSubtrees.base: ou=foo, ou=Root-Y, o=PVTG Draft, c=BB Subscriber-Y subject: cn=Subscriber-Y, ou=foo, ou=Root-Y, o=PVTG Draft,		1. CrossY-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=foo, ou=Root-Y, o=PVTG Draft, c=BB 2. cn=Subscriber-Y, ou=foo, ou=PVTG Draft, c=BB

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	Revocation Checking Test Case										
		CC.38	01	NG	The RP should reject a certification path which contains a cross-certificate revoked. **[X.509 10.5.1]**	Base.20	CrossY-X has been revoked. [RootCA-X, CrossY-X, Subscriber-Y]		RootCA-X.CRL (or ARL)	revokedCertificates	CrossY-X.serialNumber
	Signature Checking Test Case										
		CC.39	01	NG	The RP should verify signatureValue in a cross-certificate with its issuer certificate. **[X.509 10.5.1]**	Base.19	The signature on CrossY-X is invalid. [RootCA-X, CrossY-X, Subscriber-Y]		CrossY-X	signatureValue	tampered
	authorityKeyIdentifier and subjectKey Identifier Extension Test Case										
		CC.21	01	OK	The RP should ensure that authorityKeyIdentifier.keyIdentifier in one certificate and subjectKeyIdentifier in its issuer certificate are identical. **[RFC3280 4.2.1.2]**	Base.12	The authorityKeyIdentifier.keyIdentifier in CrossY-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, CrossY-X, Subscriber-Y] RootCA-X.SubjectKeyID: keyID.RootCA-X	Opt	CrossY-X	authorityKeyID - keyIdentifier	foo

NOTE: Exp Value: (OK) Path SHOULD be validated successfully (NG) Path SHOULD NOT be validated. (RV) Path SHOULD be validated as 'REVOKED'.

3.4 Cross Recognition Model Test Items

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
RP	Normal Test Case										
		CR.05	01	OK	CR Normal Case		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				
	Trust Anchor List Test Case										
		CR.06	01	NG	The RP should reject a certification path whose trust anchor certificate is not listed on RP's trust anchor list.		The following path should not be successfully validated; RootCA-Y is not listed on the RP's trust anchor list. [RootCA-Y, Subscriber-Y]				
	DN matching Basic Test Case										
		CR.07	01	NG	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.08 Base.09 Base.10 Base.11	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=foo, ou=Root-Y, o=PVTG Draft, c=BB		Subscriber-Y	issuer	cn=foo, ou=Root-Y, o=PVTG Draft, c=BB
	Signature Checking Test Case										
		CR.09	01	NG	The RP should reject a certification path whose trust anchor certificate is tamperd. **[X.509 10.5.1]**		RootCA-Y has been tamperd. [RootCA-Y, Subscriber-Y] RootCA-Y.signatureValue: foo		RootCA-Y	signatureValue	foo

entity	category	test item number		Exp Value	requirement	relevant to ...	test item	Level	differences		
									Cert type	Field	Value
	certificatePolicies Extension Test Case										
		CR.10	01	NG	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]**	CC.22	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		Subscriber-Y	certificatePolicies - policyIdentifier	policy-Z (critical)
		CR.11	01	OK	The RP should process certificatePolicies correctly when it has not been marked critical.		Subscriber-Y has a valid policyIdentifier in non-critical certificatePolicies field. [RootCA-Y, Subscriber-Y] Subscriber-Y:certificatePolicies.policyIdentifier: policy-Y (non-critical)		Subscriber-Y	certificatePolicies - policyIdentifier	policy-Y (non-critical)
			02	NG			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)
		CR.12	01	OK	The RP should process a certification path which contains a certificate which has plural policyIdentifier present. **[X.509 8.1.1]**	CC.24	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)		Subscriber-Y	certificatePolicies - policyIdentifier	policy-Y, policy-Z (critical)
			02	NG			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)
		CR.13	01	OK	The RP should process a certification path which contains a certificate which has plural policyIdentifier present and not critical.		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)		Subscriber-Y	certificatePolicies - policyIdentifier	policy-Y, policy-Z (non-critical)
			02	NG			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)
	authorityKeyIdentifier and subjectKey Identifier Extension Test Case										
		CR.08	01	OK	The RP should ensure that authorityKeyIdentifier.keyIdentifier in one certificate and subjectKeyIdentifier in its issuer certificate are identical. **[RFC3280 4.2.1.2]**	Base.12	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: foo	Opt	Subscriber-Y	authorityKeyID - keyIdentifier	foo

NOTE: Exp Value: (OK) Path SHOULD be validated successfully (NG) Path SHOULD NOT be validated. (RV) Path SHOULD be validated as 'REVOKED'.

4 Appendix A : IWG Test Tools

4.1 Introduction

The IWG Test Tools was developed by the JKST-IWG (Japan, Korea, Singapore and Chinese Taipei Interoperability Working Group) in 2004.

The goal of the tool is to help conduct certificate path processing testing which based on The IWG Path Processing Testing Guideline, X.509 and RFC3280 certificate path validation algorithm.

The test tools provides the following features:

- Open Source Software distributed with Apache-like lincence.
- Multiple CA
- Multiple LDAP repository
- Test case database for path processing testing
- Easy accessible web browser based interface
- Flexible certificate and CRL issuance (e.g. ext., Unicode CJK)
- Cooperative test case design environment.
- LDIF loader to import former test data into database
- LDIF generator to export to LDAP repository
- JKST-IWG Path Processing Test Data in 2003 and 2004.
- Easy to re-build test environment.
- Cross certification with CA products.
- All of these functions are provided by ONLY ONE Linux PC.

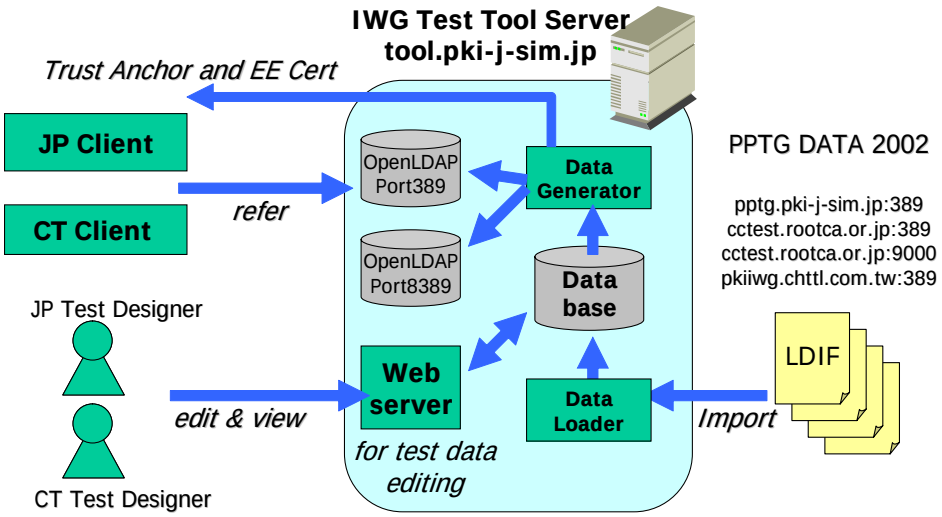


Figure 4-1 PPTG experiment 2003 using IWG test tools.

4.2 Designing Test Item

To design test items, take following steps.

1. Specify which trust model will be used.
3. Specify which CRL model will be used.
2. Make a list of entities.
4. Specify the range of data record ID numbers .
5. Generate keypairs for each entities.
6. Create certificate data.
7. Create CRL data.
8. Create Cross Certificate Pair data if necessary
9. Set LDAP entry data for each entities.
10. Set LDAP repository data for each LDAP servers.

4.3 Testing Execution

To execute testing, take following steps.

1. Setup repositories.
2. Generate LDIF files for each LDAP servers.
3. Get trust anchor and subscriber certificates.
4. Setup certification path validation client.
5. execute testing.

4.4 Setup

4.4.1 Download

IWG Test Tools requires open source softwares as below.

1) Chanllenge PKI Test Suite (http://www.jnsa.org/mpki/)
1-1) OpenSSL
1-2) OpenLDAP
1-3) AiCrypto Library (http://mars.elcom.nitech.ac.jp/security/aicrypto-e.html)
1-4) PostgreSQL
1-5) Apache (or Other Web Server)
1-6) Perl

Executables and sources of IWG Test Tools will be distributed from the IWG official web site near in the future.

4.4.2 Install

Installation guide of IWG test tools will be find in the IWG official site near in the future.

4.4.3 System Requirements for Test Tool Server

- Intel(R) Pentium(R) compatible processor 300MHz or above
- RedHat 7.3 or above
- 64MB RAM or above
- 200MB of available hard-disk space
- NIC

4.5 Test Data

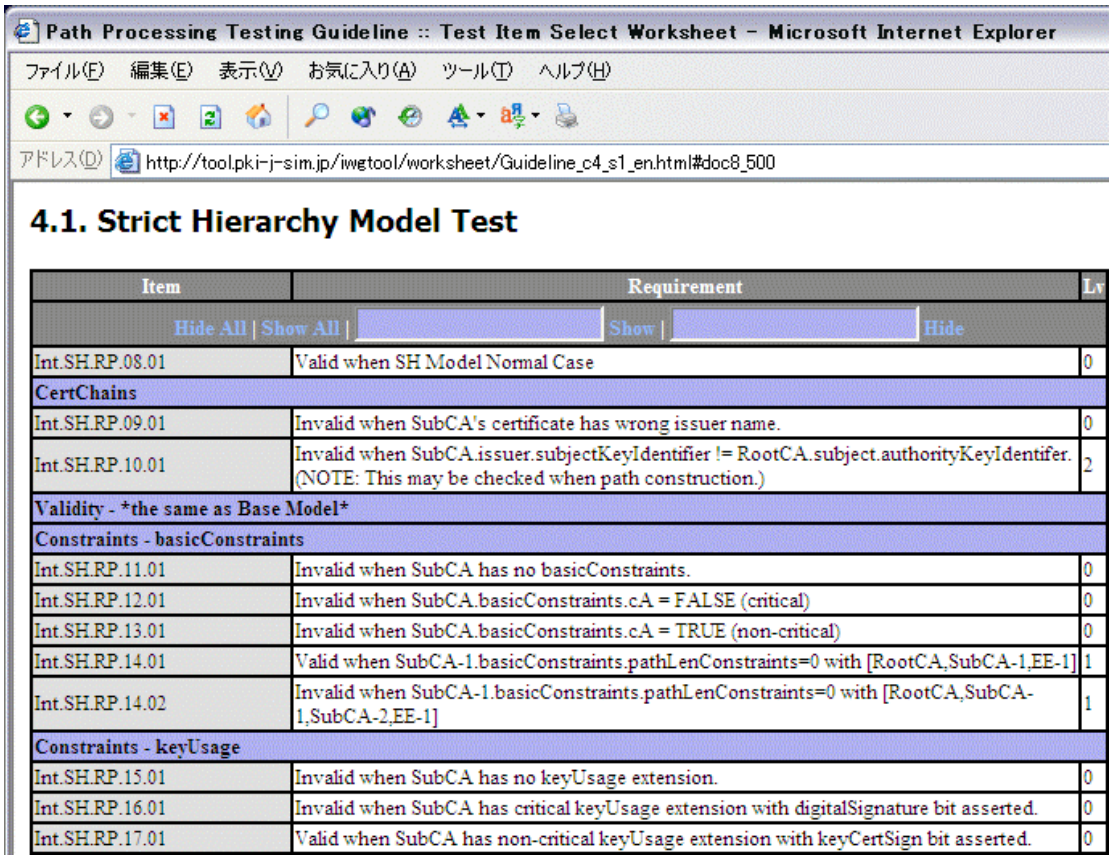
The database records for test data of PPTG experiment in 2002 and 2003 are following.

Year	C	HOST	port	ID range	Notes
2002	JP	pptg.pki-j-sim.jp	389	7100000 -	
	TW	pkiiwg.chttl.com.tw	389	7210000 -	
	KR	cctest.rootca.or.kr	389	7250000 -	for KR RootCA
	KR	cctest.rootca.or.kr	9000	7290000 -	for KR SubCA
2003	JP	tool.pki-j-sim.jp	389	7700000 -	UTF8 CJK
	JP	tool.pki-j-sim.jp	389	7900000 -	DN matching
	JP	tool.pki-j-sim.jp	389	7901000 -	LDAP URI port 389
	JP	tool.pki-j-sim.jp	8389	7901120 -	LDAP URI port 8389

5 Appendix B : Path Processing Test Item Selecting Worksheet

The 'Path Processing Test Item Selecting Worksheet' is an online contents to view and select all of PPTG test items.

The URL of the worksheet will be announced on the IWG official site.



Item	Requirement	Lv
Hide All | Show All |	Show | Hide	
Int.SH.RP.08.01	Valid when SH Model Normal Case	0
CertChains		
Int.SH.RP.09.01	Invalid when SubCA's certificate has wrong issuer name.	0
Int.SH.RP.10.01	Invalid when SubCA.issuer.subjectKeyIdentifier != RootCA.subject.authorityKeyIdentifer. (NOTE: This may be checked when path construction.)	2
Validity - *the same as Base Model*		
Constraints - basicConstraints		
Int.SH.RP.11.01	Invalid when SubCA has no basicConstraints.	0
Int.SH.RP.12.01	Invalid when SubCA.basicConstraints.cA = FALSE (critical)	0
Int.SH.RP.13.01	Invalid when SubCA.basicConstraints.cA = TRUE (non-critical)	0
Int.SH.RP.14.01	Valid when SubCA-1.basicConstraints.pathLenConstraints=0 with [RootCA,SubCA-1,EE-1]	1
Int.SH.RP.14.02	Invalid when SubCA-1.basicConstraints.pathLenConstraints=0 with [RootCA,SubCA-1,SubCA-2,EE-1]	1
Constraints - keyUsage		
Int.SH.RP.15.01	Invalid when SubCA has no keyUsage extension.	0
Int.SH.RP.16.01	Invalid when SubCA has critical keyUsage extension with digitalSignature bit asserted.	0
Int.SH.RP.17.01	Valid when SubCA has non-critical keyUsage extension with keyCertSign bit asserted.	0

Figure 5-1 Path Processing Test Item Selecting Worksheet

5.1 Showing and Hiding Test Items

You can show or hide test items by the functions below.

1) Click 'Hide All' – Hide all test items
2) Click 'Show All' – Show all test items
3) Type keyword which you want to see then click 'Show' – Show items matched to the keyword.
4) Type keyword which you want to hide then click 'Hide' – Hide items matched to the keyword.

5.2 Keywords

Available keywords are like below.

1) test item name
2) X.509 extension name
3) descriptoin of test case
4) trust model
5) and others

Keyword matching used in the worksheet is incasesensitive matching.