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

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

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