Appendix A 証明書/CRLプロファイル

A.1 自己署名証明書（模擬商工会議所認証局）

Fields	generation	Type of ASN.1	value
version	o	INTEGER	2(V3)
serialNumber	o	INTEGER	…
signature	o		
algorithm	o	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o		
issure	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	ou=Business Certification Service, o=The Japan Chamber of Commerce and Industry (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
validity	o		
notBefore	o	UTC TIME	041210000000Z
notAfter	o	UTC TIME	060401000000Z
subject	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	ou=Business Certification Service, o=The Japan Chamber of Commerce and Industry (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
subjectPublicKeyInfo	o		
algorithmIdentifier	o		
algorithm	o	OID	1.2.840.113549.1.1.1 (rsaEncryption)
parameters	x		-
subjectPublicKey	o	BIT STRING (2,048bit)	2048bit
issureUniqueID	x		-
subjectUniqueID	x		-
authorityKeyIdentifier	- NC		
keyIdentifier	o	OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-		-
otherName	-		-
rfc822Name	-		-
dNSName	-		-
x400Address	-		-
directoryName	-	UTF8String or PrintableString(for Country attribute)	-
ediPartyName	-		-
uriformResourceIdentifier	-		-
iPAddress	-		-
registeredID	-		-
authorityCertSerialNumber	-	INTEGER	-

Fields	generation		Type of ASN.1	value
subjectKeyIdentifier	o	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage	-	C	BIT STRING	
digitalSignature	-			-
nonRepudiation	-			-
keyEncipherment	-			-
dataEncipherment	-			-
keyAgreement	-			-
keyCertSign	o			o
cRLSign	o			o
encipherOnly	-			-
decipherOnly	-			-
extKeyUsage	x	-		-
privateKeyUsagePeriod	x	-		-
notBefore	x			-
notAfter	x			-
certificatePolicies	-	C/NC		-
policyIdentifier	-		OID	-
policyQualifiers	-			-
policyQualifierId	-		OID	-
qualifier	-			-
cPSuri	-		IA5String	-
userNotice	-			-
noticeRef	-			-
organization	-		DisplayText	-
noticeNumbers	-		INTEGER	-
explicitText	-		VisibleString	-
policyMappings	x	-		-
issureDomainPolicy	x		OID	-
subjectDomainPolicy	x		OID	-
subjectAltName	-	NC	GeneralNames	
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			ou=ビジネス認証サービス, o=模擬日本商工会議所, o=日本PKIフォーラム - ECOパイロットプロジェクト, c=JP
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
issureAltName	-	NC	GeneralNames	
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			ou=ビジネス認証サービス, o=模擬日本商工会議所, o=日本PKIフォーラム - ECOパイロットプロジェクト, c=JP
ediPartyName	-			-

Fields	generation		Type of ASN.1	value
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
subjectDirectryAttributes	x	-		-
type	x			-
values	x			-
basicConstraints	o	C		
cA	o		BOOLEAN	TRUE
pathLenConstraint	-		INTEGER	-
nameConstraints	x	-		-
permittedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
excludedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
policyConstraints	x	-		-
requireExplicitPolicy	x			-
inhibitPolicyMapping	x			-
cRLDistributionPoints	-	NC	SEQUENCE SIZE (1..MAX) OF DistributionPoint	
distributionPoint	-			-
fullname	-		GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-

Fields	generation		Type of ASN.1	value
uriformResourceIdentifier	-			ldap://ca01.pki-j-sim.jp/ou=Business%20Certification%20Service,o=The%20Japan%20Chamber%20of%20Commerce%20and%20Industry%20(simulated),o=Japan%20PKI%20Forum%20-%20ECO%20Pilot%20Project,c=JP?authorityRevocationList;binary
iPAddress	-			-
registeredID	-			-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
unused	-			-
keyCompromise	-			-
cACompromise	-			-
affiliationChanged	-			-
superseded	-			-
cessationOfOperation	-			-
certificateHold	-			-
privilegeWithdrawn	-			-
aACompromise	-			-
cRLIssuer	-			-
authorityInfoAccess	-	-	SEQUENCE SIZE (1..MAX) OF AccessDescliption	-
AccessDescliption	-			-
accessMethod	-			-
accessLocation	-		GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
InhibitAnyPolicy	x	-	INTEGER	-
FreshestCRL	x	-		-
distributionPoint	x			-
fullname	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
nameRelativeToCRLIssuer	x			-
type	x			-
vale	x			-
reasons	x			-
unused	x			-

Fields		generation		Type of ASN.1	value
keyCompromise		x			-
cACompromise		x			-
affiliationChanged		x			-
superseded		x			-
cessationOfOperation		x			-
certificateHold		x			-
privilegeWithdrawn		x			-
aACompromise		x			-
cRLIssuer		x			-
SubjectInfoAccessSyntax		x	-		-
accessMethod		x			-
accessLocation		x			-

o: MUST, x: NOT used, -: optional or not-defined

A.2 CRL（模擬商工会議所認証局）

Fields	generation	Type of ASN.1	value
version	o	INTEGER	2(V3)
serialNumber	o	INTEGER	…
signature	o		
algorithm	o	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o		
issure	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	ou=Business Certification Service, o=The Japan Chamber of Commerce and Industry (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
thisUpdate	o	UTC TIME	0411210042000Z (**更新で変更される**)
nextUpdate	o	UTC TIME	050320042000Z (**更新で変更される**)
revokedCertificates	o		
serialNumber	o	INTEGER	…
revocationDate	o	UTC TIME	…

Extentions

authorityKeyIdentifier	o	NC		
keyIdentifier	o		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-		DirectoryName	
authorityCertSerialNumber	-		INTEGER	
issureAltName	x	NC		-
cRLNumber	o	NC	INTEGER	…
deltaCRLIndicator	-	C		-
baseCRLNumber	-			
issuingDistributionPoint	o	C		
distributionPoint	-			
fullName	-		URI	ldap://ca01.pki-j-sim.jp/ou=Business%20Certification%20Service,o=The%20Japan%20Chamber%20of%20Commerce%20and%20Industry%20(simulated), o=Japan%20PKI%20Forum%20-%20ECO%20Pilot%20Project, c=JP?certificateRevocationList;binary
nameRelativeToCRLIssuer	-			-
onlyContainsUserCerts	o		BOOLEAN	TRUE
onlyContainsCACerts	-			-
onlySomeReasons	x			-
indirectCRL	-			-

Fields	generation		Type of ASN.1	value
FreshestCRL	-	NC		-
distributionPoint	-			-
fullName	-		URI	-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
cRLIssuer	-			-
crlScope	x			-
PerAuthorityScope	x			-
authorityName	x			-
distributionPoint	x			-
onlyContain	x			-
onlySomeReasons	x			-
serialNumberRange	x			-
startingNumber	x			-
endingNumber	x			-
subjectKeyIdRange	x			-
startingNumber	x			-
endingNumber	x			-
nameSubtree	x			-
baseRevocationInfo	x			-
cRLStreamIdentifier	x			-
cRLNumber	x			-
cRLStreamIdentifier	x			-
EntryExtentions				
resonCode	o	NC		…
holdInstructionCode	x			-
invalidityDate	-	NC		-
certificateIssuer	x			-

o: MUST, x: NOT used, -: optional or not-defined

A.3 ARL（模擬商工会議所認証局）

Fields	generation	Type of ASN.1	value
version	o	INTEGER	2(V3)
serialNumber	o	INTEGER	…
signature	o		
algorithm	o	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o		
issure	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	ou=Business Certification Service, o=The Japan Chamber of Commerce and Industry (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
thisUpdate	o	UTC TIME	0411210042000Z **(更新で変更される)**
nextUpdate	o	UTC TIME	050320042000Z **(更新で変更される)**
revokedCertificates	o		
serialNumber	o	INTEGER	…
revocationDate	o	UTC TIME	…

Extentions

authorityKeyIdentifier	o	NC		
keyIdentifier	o		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-		DirectoryName	
authorityCertSerialNumber	-		INTEGER	
issureAltName	x	NC		-
cRLNumber	o	NC	INTEGER	…
deltaCRLIndicator	-	C		-
baseCRLNumber	-			
issuingDistributionPoint	o	C		
distributionPoint	-			
fullName	-		URI	ldap://ca01.pki-j-sim.jp/ou=Business%20Certification%20Service,o=The%20Japan%20Chamber%20of%20Commerce%20and%20Industry%20(simulated),o=Japan%20PKI%20Forum%20-%20ECO%20Pilot%20Project,c=JP?authorityRevocationList;binary
nameRelativeToCRLIssuer	-			-
onlyContainsUserCerts	-			-
onlyContainsCACerts	o		BOOLEAN	TRUE
onlySomeReasons	x			-
indirectCRL	-			-
FreshestCRL	-	NC		-

Fields	generation		Type of ASN.1	value
distributionPoint	-			-
fullName	-		URI	-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
cRLIssuer	-			-
crlScope	x			-
PerAuthorityScope	x			-
authorityName	x			-
distributionPoint	x			-
onlyContain	x			-
onlySomeReasons	x			-
serialNumberRange	x			-
startingNumber	x			-
endingNumber	x			-
subjectKeyIdRange	x			-
startingNumber	x			-
endingNumber	x			-
nameSubtree	x			-
baseRevocationInfo	x			-
cRLStreamIdentifier	x			-
cRLNumber	x			-
cRLStreamIdentifier	x			-
EntryExtentions				
resonCode	o	NC		…
holdInstructionCode	x			-
invalidityDate	-	NC		-
certificateIssuer	x			-

o: MUST, x: NOT used, -: optional or not-defined

A.4 ECO発行者証明書（模擬商工会議所認証局発行EE）

Fields	generation		Type of ASN.1	value
version	o		INTEGER	2(V3)
serialNumber	o		INTEGER	…
signature	o			
algorithm	o		OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o			
issure	o			
type	o		OID	
value	o		UTF8String or PrintableString(for Country attribute)	ou=Business Certification Service, o=The Japan Chamber of Commerce and Industry (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
validity	o			
notBefore	o		UTC TIME	041210050000Z
notAfter	o		UTC TIME	060331235959Z
subject	o			
type	o		OID	
value	o		UTF8String or PrintableString(for Country attribute)	T=ECO-Issuer-01, cn=Taro Nippon, o=Japan PKI Forum - ECO Pilot Project, c=JP
subjectPublicKeyInfo	o			
algorithmIdentifier	o			
algorithm	o		OID	1.2.840.113549.1.1.1 (rsaEncryption)
parameters	x			-
subjectPublicKey	o		BIT STRING (2,048bit)	1024bit
issureUniqueID	x			-
subjectUniqueID	x			-
authorityKeyIdentifier	o	NC		
keyIdentifier	o		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-			-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-		UTF8String or PrintableString(for Country attribute)	-
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
authorityCertSerialNumber	-		INTEGER	-
subjectKeyIdentifier	o	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2

Fields	generation		Type of ASN.1	value
keyUsage	o	C	BIT STRING	
digitalSignature	-			o
nonRepudiation	-			-
keyEncipherment	-			-
dataEncipherment	-			-
keyAgreement	-			-
keyCertSign	-			-
cRLSign	-			-
encipherOnly	-			-
decipherOnly	-			-
extKeyUsage	x	-		-
privateKeyUsagePeriod	x	-		-
notBefore	x			-
notAfter	x			-
certificatePolicies	o	C/NC		(NC)
policyIdentifier	o		OID	0.2.440.20013.1.2004.1
policyQualifiers	-			-
policyQualifierId	-		OID	-
qualifier	-			-
cPSuri	-		IA5String	-
userNotice	-			-
noticeRef	-			-
organization	-		DisplayText	-
noticeNumbers	-		INTEGER	-
explicitText	-		VisibleString	-
policyMappings	x	-		-
issureDomainPolicy	x		OID	-
subjectDomainPolicy	x		OID	-
subjectAltName	-	NC	GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			T=ECO**発行者**-01, cn=**日本太郎**, o=**日本PKIフォーラム** - ECO**パイロットプロジェクト**, L=**東京**,c=JP
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
issureAltName	-	NC	GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			ou=**ビジネス認証サービス**, o=**模擬日本商工会議所**, o=**日本PKIフォーラム** - ECO**パイロットプロジェクト**, c=JP
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
subjectDirectryAttributes	x	-		-
type	x			-

Fields	generation		Type of ASN.1	value
values	x			-
basicConstraints	-	-		-
cA	-		BOOLEAN	-
pathLenConstraint	-		INTEGER	-
nameConstraints	x	-		-
permittedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
excludedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
policyConstraints	x	-		-
requireExplicitPolicy	x			-
inhibitPolicyMapping	x			-
cRLDistributionPoints	o	NC	SEQUENCE SIZE (1..MAX) OF DistributionPoint	-
distributionPoint	-			-
fullname	-		GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	(o)			ldap://ca01.pki-j-sim.jp/ou=Business%20Certification%20Service,o=The%20Japan%20Chamber%20of%20Commerce%20and%20Industry%20(simulated),o=Japan%20PKI%20Forum%20-%20ECO%20Pilot%20Project,c=JP?certificateRevocationList;binary
iPAddress	-			-
registeredID	-			-

Fields	generation		Type of ASN.1	value
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
unused	-			-
keyCompromise	-			-
cACompromise	-			-
affiliationChanged	-			-
superseded	-			-
cessationOfOperation	-			-
certificateHold	-			-
privilegeWithdrawn	-			-
aACompromise	-			-
cRLIssuer	-			-
authorityInfoAccess	x	-	SEQUENCE SIZE (1..MAX) OF AccessDescliption	-
AccessDescliption	x			-
accessMethod	x			-
accessLocation	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
InhibitAnyPolicy	x	-	INTEGER	-
FreshestCRL	x	-		-
distributionPoint	x			-
fullname	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
nameRelativeToCRLIssuer	x			-
type	x			-
vale	x			-
reasons	x			-
unused	x			-
keyCompromise	x			-
cACompromise	x			-
affiliationChanged	x			-
superseded	x			-
cessationOfOperation	x			-
certificateHold	x			-
privilegeWithdrawn	x			-
aACompromise	x			-
cRLIssuer	x			-
SubjectInfoAccessSyntax	x	-		-
accessMethod	x			-
accessLocation	x			-

o: MUST, x: NOT used, -: optional or not-defined

A.5 ECO送信者S/MIME証明書（模擬商工会議所認証局発行EE）

Fields	generation	Type of ASN.1	value
version	o	INTEGER	2(V3)
serialNumber	o	INTEGER	…
signature	o		
algorithm	o	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o		
issure	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	ou=Business Certification Service, o=The Japan Chamber of Commerce and Industry (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
validity	o		
notBefore	o	UTC TIME	041210000000Z
notAfter	o	UTC TIME	060331235959Z
subject	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	cn=ECO sender, o=Japan PKI Forum - ECO Pilot Project, c=JP
subjectPublicKeyInfo	o		
algorithmIdentifier	o		
algorithm	o	OID	1.2.840.113549.1.1.1 (rsaEncryption)
parameters	x		-
subjectPublicKey	o	BIT STRING (2,048bit)	1024bit
issureUniqueID	x		-
subjectUniqueID	x		-
authorityKeyIdentifier	o NC		
keyIdentifier	o	OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-		-
otherName	-		-
rfc822Name	-		-
dNSName	-		-
x400Address	-		-
directoryName	-	UTF8String or PrintableString(for Country attribute)	-
ediPartyName	-		-
uriformResourceIdentifier	-		-
iPAddress	-		-
registeredID	-		-
authorityCertSerialNumber	-	INTEGER	-

Fields	generation		Type of ASN.1	value
subjectKeyIdentifier	o	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage	o	C	BIT STRING	
digitalSignature	-			o (**署名用**)
nonRepudiation	-			-
keyEncipherment	-			o (**暗号化用**)
dataEncipherment	-			-
keyAgreement	-			-
keyCertSign	-			-
cRLSign	-			-
encipherOnly	-			-
decipherOnly	-			-
extKeyUsage	x	-		-
privateKeyUsagePeriod	x	-		-
notBefore	x			-
notAfter	x			-
certificatePolicies	o	C/NC		(NC)
policyIdentifier	o		OID	0.2.440.20013.1.2004.2
policyQualifiers	-			-
policyQualifierId	-		OID	-
qualifier	-			-
cPSuri	-		IA5String	-
userNotice	-			-
noticeRef	-			-
organization	-		DisplayText	-
noticeNumbers	-		INTEGER	-
explicitText	-		VisibleString	-
policyMappings	x	-		-
issureDomainPolicy	x		OID	-
subjectDomainPolicy	x		OID	-
subjectAltName	-	NC	GeneralNames	-
otherName	-			-
rfc822Name	-			**ccij@pki-j-sim.jp**
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
issureAltName	-	NC	GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			ou=**ビジネス認証サービス**, o=**模擬日本商工会議所**, o=**日本PKIフォーラム** - ECO**パイロットプロジェクト実験**, c=JP
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-

Fields	generation		Type of ASN.1	value
registeredID	-			-
subjectDirectryAttributes	x	-		-
type	x			-
values	x			-
basicConstraints	-	-		-
cA	-		BOOLEAN	-
pathLenConstraint	-		INTEGER	-
nameConstraints	x	-		-
permittedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
excludedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
policyConstraints	x	-		-
requireExplicitPolicy	x			-
inhibitPolicyMapping	x			-
cRLDistributionPoints	o	NC	SEQUENCE SIZE (1..MAX) OF DistributionPoint	-
distributionPoint	-			-
fullname	-		GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-

Fields	generation		Type of ASN.1	value
uriformResourceIdentifier	o			ldap://ca01.pki-j-sim.jp/ou=Business%20Certification%20Service,o=The%20Japan%20Chamber%20of%20Commerce%20and%20Industry%20(simulated),o=Japan%20PKI%20Forum%20-%20ECO%20Pilot%20Project,c=JP?certificateRevocationList;binary
iPAddress	-			-
registeredID	-			-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
unused	-			-
keyCompromise	-			-
cACompromise	-			-
affiliationChanged	-			-
superseded	-			-
cessationOfOperation	-			-
certificateHold	-			-
privilegeWithdrawn	-			-
aACompromise	-			-
cRLIssuer	-			-
authorityInfoAccess	x	-	SEQUENCE SIZE (1..MAX) OF AccessDescliption	-
AccessDescliption	x			-
accessMethod	x			-
accessLocation	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
InhibitAnyPolicy	x	-	INTEGER	-
FreshestCRL	x	-		-
distributionPoint	x			-
fullname	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
nameRelativeToCRLIssuer	x			-
type	x			-
vale	x			-
reasons	x			-

Fields	generation		Type of ASN.1	value
unused	x			-
keyCompromise	x			-
cACompromise	x			-
affiliationChanged	x			-
superseded	x			-
cessationOfOperation	x			-
certificateHold	x			-
privilegeWithdrawn	x			-
aACompromise	x			-
cRLIssuer	x			-
SubjectInfoAccessSyntax	x	-		-
accessMethod	x			-
accessLocation	x			-

o: MUST, x: NOT used, -: optional or not-defined

A.6 自己署名証明書（模擬財務省認証局）

Fields	generation		Type of ASN.1	value
version	o		INTEGER	2(V3)
serialNumber	o		INTEGER	…
signature	o			
algorithm	o		OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o			
issure	o			
type	o		OID	
value	o		UTF8String or PrintableString(for Country attribute)	ou=MOF Certification Authority (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
validity	o			
notBefore	o		UTC TIME	041210000000Z
notAfter	o		UTC TIME	060401000000Z
subject	o			
type	o		OID	
value	o		UTF8String or PrintableString(for Country attribute)	ou=MOF Certification Authority (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
subjectPublicKeyInfo	o			
algorithmIdentifier	o			
algorithm	o		OID	1.2.840.113549.1.1.1 (rsaEncryption)
parameters	x			-
subjectPublicKey	o		BIT STRING (2,048bit)	2048bit
issureUniqueID	x			-
subjectUniqueID	x			-
authorityKeyIdentifier	-	NC		
keyIdentifier	(o)		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-			-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-		UTF8String or PrintableString(for Country attribute)	-
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
authorityCertSerialNumber	-		INTEGER	-
subjectKeyIdentifier	o	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage	-	C	BIT STRING	
digitalSignature	-			-
nonRepudiation	-			-

Fields	generation		Type of ASN.1	value
keyEncipherment	-			-
dataEncipherment	-			-
keyAgreement	-			-
keyCertSign	o			o
cRLSign	o			o
encipherOnly	-			-
decipherOnly	-			-
extKeyUsage	x	-		-
privateKeyUsagePeriod	x	-		-
notBefore	x			-
notAfter	x			-
certificatePolicies	-	C/NC		-
policyIdentifier	-		OID	-
policyQualifiers	-			-
policyQualifierId	-		OID	-
qualifier	-			-
cPSuri	-		IA5String	-
userNotice	-			-
noticeRef	-			-
organization	-		DisplayText	-
noticeNumbers	-		INTEGER	-
explicitText	-		VisibleString	-
policyMappings	x	-		-
issureDomainPolicy	x		OID	-
subjectDomainPolicy	x		OID	-
subjectAltName	-	NC	GeneralNames	
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			ou=**模擬財務省認証局**, o=**日本PKIフォーラム** - ECO**パイロットプロジェクト**, c=JP
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
issureAltName	-	NC	GeneralNames	
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			ou=**模擬財務省認証局**, o=**日本PKIフォーラム** - ECO**パイロットプロジェクト**, c=JP
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
subjectDirectryAttributes	x	-		-
type	x			-
values	x			-
basicConstraints	o	C		
cA	o		BOOLEAN	TRUE
pathLenConstraint	-		INTEGER	-
nameConstraints	x	-		-

Fields	generation		Type of ASN.1	value
permittedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
excludedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
policyConstraints	x	-		-
requireExplicitPolicy	x			-
inhibitPolicyMapping	x			-
cRLDistributionPoints	-	NC	SEQUENCE SIZE (1..MAX) OF DistributionPoint	-
distributionPoint	-			-
fullname	-		GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	-			ldap://ca02.pki-j-sim.jp/ou=MOF%20Certification%20Authority%20(simulated),o=Japan%20PKI Forum%20-%20ECO%20Pilot%20Project,c=JP?authorityRevocationList;binary
iPAddress	-			-
registeredID	-			-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
unused	-			-
keyCompromise	-			-
cACompromise	-			-
affiliationChanged	-			-
superseded	-			-
cessationOfOperation	-			-
certificateHold	-			-

Fields	generation		Type of ASN.1	value
privilegeWithdrawn	-			-
aACompromise	-			-
cRLIssuer	-			-
authorityInfoAccess	-	-	SEQUENCE SIZE (1..MAX) OF AccessDescliption	-
AccessDescliption	-			-
accessMethod	-			-
accessLocation	-		GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
InhibitAnyPolicy	x	-	INTEGER	-
FreshestCRL	x	-		-
distributionPoint	x			-
fullname	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
nameRelativeToCRLIssuer	x			-
type	x			-
vale	x			-
reasons	x			-
unused	x			-
keyCompromise	x			-
cACompromise	x			-
affiliationChanged	x			-
superseded	x			-
cessationOfOperation	x			-
certificateHold	x			-
privilegeWithdrawn	x			-
aACompromise	x			-
cRLIssuer	x			-
SubjectInfoAccessSyntax	x	-		-
accessMethod	x			-
accessLocation	x			-

o: MUST, x: NOT used, -: optional or not-defined

A.7 CRL（模擬財務省認証局）

Fields	generation	Type of ASN.1	value
version	o	INTEGER	2(V3)
serialNumber	o	INTEGER	…
signature	o		
algorithm	o	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o		
issure	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	ou=MOF Certification Authority (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
thisUpdate	o	UTC TIME	041210071847Z (**更新により変更される**)
nextUpdate	o	UTC TIME	050320071847Z (**更新により変更される**)
revokedCertificates	o		
serialNumber	o	INTEGER	…
revocationDate	o	UTC TIME	…

Extentions

authorityKeyIdentifier	o	NC		
keyIdentifier	o		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-		DirectoryName	-
authorityCertSerialNumber	-		INTEGER	-
issureAltName	x	-		-
cRLNumber	o	NC	INTEGER	…
deltaCRLIndicator	-	C		-
baseCRLNumber	-			-
issuingDistributionPoint	o	C		
distributionPoint	-			-
fullName	-		URI	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	-			ldap://ca02.ki-j-sim.jp/ou=MOF%20Certification%20Authority%20(simulated),o=Japan%20PKI Forum%20-%20ECO%20Pilot%20Project,c=JP?certificateRevocationList;binary
iPAddress	-			-
registeredID	-			-
nameRelativeToCRLIssuer	-			-
onlyContainsUserCerts	o		BOOLEAN	TRUE
onlyContainsCACerts	-			-
onlySomeReasons	x			-
indirectCRL	-			-

Fields	generation		Type of ASN.1	value
FreshestCRL	-	NC		-
distributionPoint	-			-
fullName	-		URI	-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
cRLIssuer	-			-
crlScope	x			-
PerAuthorityScope	x			-
authorityName	x			-
distributionPoint	x			-
onlyContain	x			-
onlySomeReasons	x			-
serialNumberRange	x			-
startingNumber	x			-
endingNumber	x			-
subjectKeyIdRange	x			-
startingNumber	x			-
endingNumber	x			-
nameSubtree	x			-
baseRevocationInfo	x			-
cRLStreamIdentifier	x			-
cRLNumber	x			-
cRLStreamIdentifier	x			-

EntryExtentions

resonCode	o	NC		…
holdInstructionCode	x			-
invalidityDate	-	NC		-
certificateIssuer	x			-

o: MUST, x: NOT used, -: optional or not-defined

A.8 ARL（模擬財務省認証局）

Fields	generation	Type of ASN.1	value
version	o	INTEGER	2(V3)
serialNumber	o	INTEGER	…
signature	o		
algorithm	o	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o		
issure	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	ou=MOF Certification Authority (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
thisUpdate	o	UTC TIME	0412100718472 (**更新により変更される**)
nextUpdate	o	UTC TIME	0503200718472 (**更新により変更される**)
revokedCertificates	o		
serialNumber	o	INTEGER	…
revocationDate	o	UTC TIME	…

Extentions

authorityKeyIdentifier	o	NC		
keyIdentifier	o		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-		DirectoryName	-
authorityCertSerialNumber	-		INTEGER	-
issureAltName	x	-		-
cRLNumber	o	NC	INTEGER	…
deltaCRLIndicator	-	C		-
baseCRLNumber	-			-
issuingDistributionPoint	o	C		
distributionPoint	-			-
fullName	-		URI	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	-			ldap://ca02.ki-j-sim.jp/ou=MOF%20Certification%20Authority%20(simulated),o=Japan%20PKI Forum%20-%20ECO%20Pilot%20Project,c=JP?authorityRevocationList;binary
iPAddress	-			-
registeredID	-			-
nameRelativeToCRLIssuer	-			-
onlyContainsUserCerts	-			-
onlyContainsCACerts	o		BOOLEAN	TRUE
onlySomeReasons	x			-
indirectCRL	-			-

Fields	generation		Type of ASN.1	value
FreshestCRL	-	NC		-
distributionPoint	-			-
fullName	-		URI	-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
cRLIssuer	-			-
crlScope	x			-
PerAuthorityScope	x			-
authorityName	x			-
distributionPoint	x			-
onlyContain	x			-
onlySomeReasons	x			-
serialNumberRange	x			-
startingNumber	x			-
endingNumber	x			-
subjectKeyIdRange	x			-
startingNumber	x			-
endingNumber	x			-
nameSubtree	x			-
baseRevocationInfo	x			-
cRLStreamIdentifier	x			-
cRLNumber	x			-
cRLStreamIdentifier	x			-
EntryExtentions				
resonCode	o	NC		…
holdInstructionCode	x			-
invalidityDate	-	NC		-
certificateIssuer	x			-

o: MUST, x: NOT used, -: optional or not-defined

A.9 ECO検証者証明書（模擬財務省認証局発行EE）

Fields	generation	Type of ASN.1	value
version	o	INTEGER	2(V3)
serialNumber	o	INTEGER	…
signature	o		
algorithm	o	OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o		
issure	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	ou=MOF Certification Authority (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
validity	o		
notBefore	o	UTC TIME	041216000000Z
notAfter	o	UTC TIME	060331235959Z
subject	o		
type	o	OID	
value	o	UTF8String or PrintableString(for Country attribute)	cn=MOF Validation Authority (simulated), ou=MOF certification Authority (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
subjectPublicKeyInfo	o		
algorithmIdentifier	o		
algorithm	o	OID	1.2.840.113549.1.1.1 (rsaEncryption)
parameters	x		-
subjectPublicKey	o	BIT STRING (2,048bit)	**1024bit**
issureUniqueID	x		-
subjectUniqueID	x		-
authorityKeyIdentifier	o NC		
keyIdentifier	o	OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-		-
otherName	-		-
rfc822Name	-		-
dNSName	-		-
x400Address	-		-
directoryName	-	UTF8String or PrintableString(for Country attribute)	-
ediPartyName	-		-
uriformResourceIdentifier	-		-
iPAddress	-		-
registeredID	-		-
authorityCertSerialNumber	-	INTEGER	-

Fields	generation		Type of ASN.1	value
subjectKeyIdentifier	o	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage	o	C	BIT STRING	
digitalSignature	-			o
nonRepudiation	-			-
keyEncipherment	-			-
dataEncipherment	-			-
keyAgreement	-			-
keyCertSign	-			-
cRLSign	-			-
encipherOnly	-			-
decipherOnly	-			-
extKeyUsage	-	NC		1.3.6.1.5.5.7.3.9 (OCSPSigning)
privateKeyUsagePeriod	x	-		-
notBefore	x			-
notAfter	x			-
certificatePolicies	o	C/NC		(C)
policyIdentifier	o		OID	0.2.440.20013.1.2004.2
policyQualifiers	-			*
policyQualifierId	-		OID	-
qualifier	-			-
cPSuri	-		IA5String	-
userNotice	-			-
noticeRef	-			-
organization	-		DisplayText	-
noticeNumbers	-		INTEGER	-
explicitText	-		VisibleString	-
policyMappings	x	-		-
issureDomainPolicy	x		OID	-
subjectDomainPolicy	x		OID	-
subjectAltName	-	NC	GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
issureAltName	-	NC	GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			ou=**模擬財務省認証局**, o=**日本PKIフォーラム** - ECO**パイロットプロジェクト**, c=JP
ediPartyName	-			-
uriformResourceIdentifier	-			-

Fields	generation		Type of ASN.1	value
iPAddress	-			-
registeredID	-			-
subjectDirectryAttributes	x	-		-
type	x			-
values	x			-
basicConstraints	-	-		-
cA	-		BOOLEAN	-
pathLenConstraint	-		INTEGER	-
nameConstraints	x	-		-
permittedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
excludedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
policyConstraints	x	-		-
requireExplicitPolicy	x			-
inhibitPolicyMapping	x			-
cRLDistributionPoints	o	NC	SEQUENCE SIZE (1..MAX) OF DistributionPoint	-
distributionPoint	-			-
fullname	-		GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	(o)			ldap://ca02.pki-j-sim.jp/ou=MOF%20Certification%20Authority%20(simulated),o=Japan%20PKI Forum%20-%20ECO%20Pilot%20Project,c=JP?certificateRevocationList;binary
iPAddress	-			-

Fields	generation		Type of ASN.1	value
registeredID	-			-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
unused	-			-
keyCompromise	-			-
cACompromise	-			-
affiliationChanged	-			-
superseded	-			-
cessationOfOperation	-			-
certificateHold	-			-
privilegeWithdrawn	-			-
aACompromise	-			-
cRLIssuer	-			-
authorityInfoAccess	x	-	SEQUENCE SIZE (1..MAX) OF AccessDescliption	-
AccessDescliption	x			-
accessMethod	x			-
accessLocation	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
InhibitAnyPolicy	x	-	INTEGER	-
FreshestCRL	x	-		-
distributionPoint	x			-
fullname	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
nameRelativeToCRLIssuer	x			-
type	x			-
vale	x			-
reasons	x			-
unused	x			-
keyCompromise	x			-
cACompromise	x			-
affiliationChanged	x			-
superseded	x			-
cessationOfOperation	x			-
certificateHold	x			-
privilegeWithdrawn	x			-
aACompromise	x			-
cRLIssuer	x			-
SubjectInfoAccessSyntax	x	-		-
accessMethod	x			-
accessLocation	x			-

o: MUST, x: NOT used, -: optional or not-defined

A.10 ECO受信者S/MIME証明書（模擬財務省認証局発行EE）

Fields	generation		Type of ASN.1	value
version	o		INTEGER	2(V3)
serialNumber	o		INTEGER	…
signature	o			
algorithm	o		OID	1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
parameters	o			
issure	o			
type	o		OID	
value	o		UTF8String or PrintableString(for Country attribute)	ou=MOF Certification Authority (simulated), o=Japan PKI Forum - ECO Pilot Project, c=JP
validity	o			
notBefore	o		UTC TIME	041210000000Z
notAfter	o		UTC TIME	0603312359592
subject	o			
type	o		OID	
value	o		UTF8String or PrintableString(for Country attribute)	cn=custom, o=Japan PKI Forum - ECO Pilot Project, c=JP
subjectPublicKeyInfo	o			
algorithmIdentifier	o			
algorithm	o		OID	1.2.840.113549.1.1.1 (rsaEncryption)
parameters	x			-
subjectPublicKey	o		BIT STRING (2,048bit)	1024bit
issureUniqueID	x			-
subjectUniqueID	x			-
authorityKeyIdentifier	o	NC		
keyIdentifier	o		OCTET STRING	The hash value of Issuer's pubic key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
authorityCertIssuer	-			-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-		UTF8String or PrintableString(for Country attribute)	-
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
authorityCertSerialNumber	-		INTEGER	-
subjectKeyIdentifier	o	NC	OCTET STRING	The value of the Subject's public key (SHA1 160bit) The 1st calculation method in RFC3280 ch.4.2.1.2
keyUsage	o	C	BIT STRING	

Fields	generation		Type of ASN.1	value
digitalSignature	-			o (**署名用**)
nonRepudiation	-			-
keyEncipherment	-			o (**暗号化用**)
dataEncipherment	-			-
keyAgreement	-			-
keyCertSign	-			-
cRLSign	-			-
encipherOnly	-			-
decipherOnly	-			-
extKeyUsage	x	-		-
privateKeyUsagePeriod	x	-		-
notBefore	x			-
notAfter	x			-
certificatePolicies	o	C/NC		(NC)
policyIdentifier	o		OID	0.2.440.20013.1.2004.2
policyQualifiers	-			-
policyQualifierId	-		OID	-
qualifier	-			-
cPSuri	-		IA5String	-
userNotice	-			-
noticeRef	-			-
organization	-		DisplayText	-
noticeNumbers	-		INTEGER	-
explicitText	-		VisibleString	-
policyMappings	x	-		-
issureDomainPolicy	x		OID	-
subjectDomainPolicy	x		OID	-
subjectAltName	-	NC	GeneralNames	-
otherName	-			-
rfc822Name	-			**customjp@pki-j-sim.jp**
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
issureAltName	-	NC	GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			ou=**模擬財務省認証局**, o=**日本PKIフォーラム** - ECO**パイロットプロジェクト**, c=JP
ediPartyName	-			-
uriformResourceIdentifier	-			-
iPAddress	-			-
registeredID	-			-
subjectDirectryAttributes	x	-		-
type	x			-
values	x			-
basicConstraints	-	-		-
cA	-		BOOLEAN	-
pathLenConstraint	-		INTEGER	-
nameConstraints	x	-		-
permittedSubtrees	x			-

Fields	generation		Type of ASN.1	value
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
excludedSubtrees	x			-
base	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
minimum	x			-
maxmum	x			-
policyConstraints	x	-		-
requireExplicitPolicy	x			-
inhibitPolicyMapping	x			-
cRLDistributionPoints	o	NC	SEQUENCE SIZE (1..MAX) OF DistributionPoint	-
distributionPoint	-			-
fullname	-		GeneralNames	-
otherName	-			-
rfc822Name	-			-
dNSName	-			-
x400Address	-			-
directoryName	-			-
ediPartyName	-			-
uriformResourceIdentifier	(o)			ldap://ca02.ki-j-sim.jp/ou=MOF%20Certification%20Authority%20(simulated),o=Japan%20PKI Forum%20-%20ECO%20Pilot%20Project,c=JP?certificateRevocationList;binary
iPAddress	-			-
registeredID	-			-
nameRelativeToCRLIssuer	-			-
type	-			-
vale	-			-
reasons	-			-
unused	-			-
keyCompromise	-			-
cACompromise	-			-
affiliationChanged	-			-
superseded	-			-
cessationOfOperation	-			-
certificateHold	-			-

Fields	generation		Type of ASN.1	value
privilegeWithdrawn	-			-
aACompromise	-			-
cRLIssuer	-			-
authorityInfoAccess	x	-	SEQUENCE SIZE (1..MAX) OF AccessDescliption	-
AccessDescliption	x			-
accessMethod	x			-
accessLocation	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
InhibitAnyPolicy	x	-	INTEGER	-
FreshestCRL	x	-		-
distributionPoint	x			-
fullname	x		GeneralNames	-
otherName	x			-
rfc822Name	x			-
dNSName	x			-
x400Address	x			-
directoryName	x			-
ediPartyName	x			-
uriformResourceIdentifier	x			-
iPAddress	x			-
registeredID	x			-
nameRelativeToCRLIssuer	x			-
type	x			-
vale	x			-
reasons	x			-
unused	x			-
keyCompromise	x			-
cACompromise	x			-
affiliationChanged	x			-
superseded	x			-
cessationOfOperation	x			-
certificateHold	x			-
privilegeWithdrawn	x			-
aACompromise	x			-
cRLIssuer	x			-
SubjectInfoAccessSyntax	x	-		-
accessMethod	x			-
accessLocation	x			-

o: MUST, x: NOT used, -: optional or not-defined