NAREGI

Certificate and CRL Profile

Ver. 2.8

December 11, 2013

NAREGI Certification Authority

Change History

Date	Version	Comment
October 20, 2005	1.0	Initial version
April 28, 2006	1.0.1	Erratum correction
July 7, 2006	2.0	Policy ID and OU Name correction
November 21, 2006	2.0.1	ExtendedkeyUsage and CRLDistributionPoints correction
April 2, 2007	2.1	Changed validity of a server certificate and a user certificate for 395 days.
February 21, 2008	2.2	Subject commonName correction BasicConstraints addition SubjectAltervativeName addition ExtendedkeyUsage addition
August 25,2008	2.3	Subject OU Name correction
November 19,2010	2.4	Added gfsd service certificate Policy ID correction
November 26, 2012	2.5	Changed algorithmIdentifier of a server certificate and a user certificate.
December 13, 2012	2.6	Added OCSP server certificate Added OCSP server URI to AuthorityInfoAccess Deleted LDAP entry from commonName list of ‘Globus host/gfsd Certificate’ OID of sha256RSA signature algorithm correction
January 8, 2013	2.7	Changed algorithmIdentifier of a server certificate and a user certificate.
December 11, 2013	2.8	Changed algorithmIdentifier of a server certificate and a user certificate.

1． Certificate Profile

1．1 Self Sign Certificate (CA Certificate)

○Basic Fields

Version	
version	Type：INTEGER Value：2 (version 3)
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique integer
signature	
algorithmIdentifier	sha1RSA(2048bits)
algorithm	Type：OID Value：1 2 840 113549 1 1 5
parameters	Type：NULL Value：None
Validity	
validity	
notBefore	Type：UTC Time Value：yymmddhhmmssZ
notAfter	Type：UTC Time Value：yymmddhhmmssZ （20160331）
Issuer	
countryName	
Type	Type：OID Value：2 5 4 6
Value	Type：PrintableString Value：JP
organizationName	
Type	Type：OID Value：2 5 4 10
Value	Type：PrintableString Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID Value：2 5 4 11
value	Type：PrintableString

	Value : CGRD
commonName	
type	Type : OID
	Value : 2 5 4 3
value	Type : PrintableString
	Value : NAREGI CA
Subject	
countryName	
Type	Type : OID
	Value : 2 5 4 6
Value	Type : PrintableString
	Value : JP
organizationName	
Type	Type : OID
	Value : 2 5 4 10
Value	Type : PrintableString
	Value : National Research Grid Initiative
organizationalUnitName	
type	Type : OID
	Value : 2 5 4 11
value	Type : PrintableStirng
	Value : CGRD
commonName	
type	Type : OID
	Value : 2 5 4 3
value	Type : PrintableString
	Value : NAREGI CA
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(2048bits)
algorithm	Type : OID
	Value : 1 2 840 113549 1 1 1
parameters	Type : NULL
	Value : None
subjectPublicKey	Type : BIT STRING
	Value : Public Key Value

〇Extension Fields

authorityKeyIdentifier (Critical = FALSE)	
KeyIdentifier	Type：OCTET STRING Value：Unique Byte strings
subjectKeyIdentifier (Critical = FALSE)	
SubjectKeyIdentifier	Type：OCTET STRING Value：Unique Byte strings
keyUsage (Critical = TRUE)	
KeyUsage	Type：BitString Value：000001100(keyCertSign,CRLSign)
basicConstraints (Critical = TRUE)	
BasicConstraints CA	 Type：Boolean Value：True（CA）

1．2 Globus host/gfsd Certificate

○Basic Fields

Version	
Version	Type：INTEGER
	Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER
	Value：Unique integer
Signature	
algorithmIdentifier	sha512RSA(1024bits)
Algorithm	Type：OID
	Value：1 2 840 113549 1 1 13
Parameters	Type：NULL
	Value：None
Validity	
validity	
notBefore	Type：UTC Time
	Value：yymmddhhmmssZ
notAfter	Type：UTC Time
	Value：yymmddhhmmssZ （395 days）
Issuer	
countryName	
Type	Type：OID
	Value：2 5 4 6
Value	Type：PrintableString
	Value：JP
organizationName	
Type	Type：OID
	Value：2 5 4 6
Value	Type：UTF8String
	Value：National Research Grid Initiative
organizationalUnitName	
Type	Type：OID
	Value：2 5 4 11
Value	Type：PrintableStirng
	Value：CGRD
commonName	

Type	Type : OID
	Value : 2 5 4 3
Value	Type : PrintableString
	Value : NAREGI CA
Subject	
countryName	
Type	Type : OID
	Value : 2 5 4 6
Value	Type : PrintableString
	Value : JP
organizationName	
Type	Type : OID
	Value : 2 5 4 10
Value	Type : PrintableString
	Value : National Research Grid Initiative
organizationalUnitName	
Type	Type : OID
	Value : 2 5 4 11
Value	Type : PrintableString
	Value : Ira Name
commonName	
Type	Type : OID
	Value : 2 5 4 3
Value	Type : PrintableString
	Value : host/FQDN of the host (for host)
	Value : gfsd/FQDN of the host (for gfsd)
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
AlgorithmIdentifier	RSA(1024bits)
Algorithm	Type : OID
	Value : 1 2 840 113549 1 1 1
Parameters	Type : NULL
	Value : None
subjectPublicKey	Type : BIT STRING
	Value : Public Key Value

○Extension Fields

keyUsage （Critical = TRUE）	
KeyUsage	Type：BitString Value：Digital Signature, Key Encipherment
basicConstraints （Critical = TRUE）	
BasicConstraints CA	 Type：Boolean Value：False
authorityKeyIdentifier (Critical = FALSE)	
KeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
subjectKeyIdentifier （Critical = FALSE）	
SubjectKeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
CertificatePolicies （Critical = FALSE）	
PolicyID QualifierID Qualifier	Type：OID Value：(Refer CPS1.2) 1.2.392.200181.3.1.1 Value：(Refer IGTF-AP-classic-4-3) 1.2.840.113612.5.2.2.1 Type：OID Value：（Refer CPS1.2） pkix-id-qt CPSurl Type： Value：URI of the CP/CPS https://www.naregi.org/ca/naregi-cps4.0.pdf
CRLDistributionPoints （Critical = FALSE）	
[0] dist-point [0] fullName :	 Value：URI of the CRL http://www.naregi.org/ca/out-CRL2.crl
ExtendedkeyUsage （Critical = FALSE）	
ExtkeyUsage	Type：OID Value：1.3.6.1.5.5.7.3.1 (serverAuth) Value：1.3.6.1.5.5.7.3.2 (clientAuth)
SubjectAlternativeName （Critical = FALSE）	
SubjectAlternativeName	Type：IA5String Value：FQDN of the host
AuthorityInfoAccess （Critical = FALSE）	
accessDescription accessMethod	 Type：OID

accessLocation	Value：1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Value：URI of the OCSP server http://ocsp.naregi.org

1．3 Globus User Certificates

○Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha512RSA(1024bits)
algorithm	Type：OID Value：1 2 840 113549 1 1 13
parameters	Type：NULL Value：None
Validity	
validity	
notBefore	Type：UTC Time Value：yymmddhhmmssZ
notAfter	Type：UTC Time Value：yymmddhhmmssZ (395 days)
Issuer	
countryName	
type	Type：OID Value：2 5 4 6
value	Type：PrintableString Value：JP
organizationName	
type	Type：OID Value：2 5 4 11
value	Type：Printable String Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID Value：2 5 4 11
value	Type：PrintableStirng Value：CGRD
commonName	

type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value： NAREGI CA
Subject	
countryName	
type	Type：OID
	Value：2 5 4 6
value	Type：PrintableString
	Value：JP
organizationName	
type	Type：OID
	Value：2 5 4 10
value	Type：PrintableString
	Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID
	Value：2 5 4 11
value	Type：PrintableStirng
	Value：Ira Name
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableStirng
	Value：
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 1
parameters	Type：NULL
	Value：None
subjectPublicKey	Type：BIT STRING
	Value：Public Key value

○Extension Fields

authorityKeyIdentifier (Critical = FALSE)	
AuthorityKeyIdentifier	

KeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
subjectKeyIdentifier （Critical = FALSE）	
SubjectKeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
keyUsage （Critical = TRUE）	
KeyUsage	Type：BitString Value：digitalSignature, Key Encipherment
basicConstraints （Critical = TRUE）	
BasicConstraints CA	 Type：Boolean Value：False
CertificatePolicies （Critical = FALSE）	
PolicyID QualifierID Qualifier	Type：OID Value：[Refer CPS1.2] 1.2.392.200181.3.2.1 Value：(Refer IGTF-AP-classic-4-3) 1.2.840.113612.5.2.2.1 Type：OID Value：[Refer CPS1.2] pkix-id-qt CPSurl Type： Value：URI of the CP/CPS https://www.naregi.org/ca/naregi-cps4.0.pdf
CRLDistributionPoints （Critical = FALSE）	
[0] dist-point [0] fullName :	 Value：URI of the CRL http://www.naregi.org/ca/out-CRL2.crl
ExtendedkeyUsage （Critical = FALSE）	
ExtkeyUsage	Type：OID Value：1.3.6.1.5.5.7.3.2 (clientAuth)
AuthorityInfoAccess （Critical = FALSE）	
accessDescription accessMethod accessLocation	 Type：OID Value：1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Value：URI of the OCSP server http://ocsp.naregi.org

1．4 Unicore Server Certificate

○Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha512RSA(1024bits)
algorithm	Type：OID Value：1 2 840 113549 1 1 13
parameters	Type：NULL Value：None
Validity	
validity	
notBefore	Type：UTC Time Value：yymmddhhmmssZ
notAfter	Type：UTC Time Value：yymmddhhmmssZ (395 days)
Issuer	
countryName	
type	Type：OID Value：2 5 4 6
value	Type：PrintableString Value：JP
organizationName	
type	Type：OID Value：2 5 4 6
value	Type：UTF8String Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID Value：2 5 4 11
value	Type：PrintableStirng Value：CGRD
commonName	

type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value： NAREGI CA
Subject	
countryName	
type	Type：OID
	Value：2 5 4 6
value	Type：PrintableString
	Value：JP
organizationName	
type	Type：OID
	Value：2 5 4 10
value	Type：PrintableString
	Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID
	Value：2 5 4 11
value	Type：PrintableString
	Value：Ira Name
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value：gateway/FQDN of host (for gateway)
	Value：njs/FQDN of host(for njs)
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
AlgorithmIdentifier	RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 1
parameters	Type：NULL
	Value：None
subjectPublicKey	Type：BIT STRING
	Value：Public Key Value

○Extension Fields

keyUsage （Critical = TRUE）	
KeyUsage	Type：BitString Value：Digital Signature, Key Encipherment
basicConstraints （Critical = TRUE）	
BasicConstraints CA	 Type：Boolean Value：False
authorityKeyIdentifier (Critical = FALSE)	
KeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
subjectKeyIdentifier （Critical = FALSE）	
SubjectKeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
CertificatePolicies （Critical = FALSE）	
PolicyID QualifierID Qualifier	Type：OID Value：(Refer CPS1.2) 1.2.392.00200181.3.3.1 Value：(Refer IGTF-AP-classic-4-3) 1.2.840.113612.5.2.2.1 Type：OID Value：（Refer CPS1.2） pkix-id-qt CPSurl Type： Value：URI of the CP/CPS https://www.naregi.org/ca/naregi-cps4.0.pdf
CRLDistributionPoints （Critical = FALSE）	
[0] dist-point [0] fullName :	 Value：URI of the CRL http://www.naregi.org/ca/out-CRL2.crl
ExtendedkeyUsage （Critical = FALSE）	
ExtkeyUsage	Type：OID Value：1.3.6.1.5.5.7.3.1 （serverAuth） Value：1.3.6.1.5.5.7.3.2 （clientAuth）
SubjectAlternativeName （Critical = FALSE）	
SubjectAlternativeName	Type：IA5String Value：FQDN of the host
AuthorityInfoAccess （Critical = FALSE）	
accessDescription accessMethod	 Type：OID

accessLocation	Value：1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Value：URI of the OCSP server http://ocsp.naregi.org

1．5 Unicore Client User Certificate

○Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha512RSA(1024bits)
algorithm	Type：OID Value：1 2 840 113549 1 1 13
parameters	Type：NULL Value：None
Validity	
validity	
notBefore	Type：UTC Time Value：yymmddhhmmssZ
notAfter	Type：UTC Time Value：yymmddhhmmssZ (395 days)
Issuer	
countryName	
type	Type：OID Value：2 5 4 6
value	Type：PrintableString Value：JP
organizationName	
type	Type：OID Value：2 5 4 10
value	Type：PrintableString Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID Value：2 5 4 11
value	Type：PrintableStirng Value：CGRD

commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value： NAREGI CA
Subject	
countryName	
type	Type：OID
	Value：2 5 4 6
value	Type：PrintableString
	Value：JP
organizationName	
type	Type：OID
	Value：2 5 4 10
value	Type：PrintableString
	Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID
	Value：2 5 4 11
value	Type：PrintableStirng
	Value：Ira Name
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableStirng
	Value：
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 1
parameters	Type：NULL
	Value：None
subjectPublicKey	Type：BIT STRING
	Value：Public Key Value

○Extension Fields

authorityKeyIdentifier (Critical = FALSE)

AuthorityKeyIdentifier	
KeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
subjectKeyIdentifier （Critical = FALSE）	
SubjectKeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
keyUsage （Critical = TRUE）	
KeyUsage	Type：BitString Value：digitalSignature, Key Encipherment
basicConstraints （Critical = TRUE）	
BasicConstraints	
CA	Type：Boolean Value：False
CertificatePolicies （Critical = FALSE）	
PolicyID	Type：OID Value：(Refer CPS1.2) 1.2.392.00200181.3.4.1 Value：(Refer IGTF-AP-classic-4-3) 1.2.840.113612.5.2.2.1
QualifierID	Type：OID Value：(Refer CPS1.2) pkix-id-qt CPSurl
Qualifier	Type： Value：URI of the CP/CPS https://www.naregi.org/ca/naregi-cps4.0.pdf
CRLDistributionPoints （Critical = FALSE）	
[0] dist-point	
[0] fullName :	Value：URI of the CRL http://www.naregi.org/ca/out-CRL2.crl
ExtendedkeyUsage （Critical = FALSE）	
ExtkeyUsage	Type：OID Value：1.3.6.1.5.5.7.3.2 (clientAuth)
AuthorityInfoAccess （Critical = FALSE）	
accessDescription	
accessMethod	Type：OID Value：1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
accessLocation	Value：URI of the OCSP server http://ocsp.naregi.org

1．6 LDAP Server Certificate

○Basic Fields

Version	
Version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
Signature	
algorithmIdentifier	sha512RSA(1024bits)
Algorithm	Type：OID Value：1 2 840 113549 1 1 13
parameters	Type：NULL Value：None
Validity	
validity	
notBefore	Type：UTC Time Value：yymmddhhmmssZ
notAfter	Type：UTC Time Value：yymmddhhmmssZ (395 days)
Issuer	
countryName	
type	Type：OID Value：2 5 4 6
value	Type：PrintableString Value：JP
organizationName	
type	Type：OID Value：2 5 4 6
value	Type：UTF8String Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID Value：2 5 4 11
value	Type：PrintableStirng Value：CGRD
commonName	

type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value： NAREGI CA
Subject	
countryName	
type	Type：OID
	Value：2 5 4 6
value	Type：PrintableString
	Value：JP
organizationName	
type	Type：OID
	Value：2 5 4 10
value	Type：PrintableString
	Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID
	Value：2 5 4 11
value	Type：PrintableString
	Value：Ira Name
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value：FQDN of the host
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
AlgorithmIdentifier	RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 1
parameters	Type：NULL
	Value：None
subjectPublicKey	Type：BIT STRING
	Value：Public Key value

○Extension Fields

keyUsage （Critical = TRUE）	
KeyUsage	Type：BitString

	Value：Digital Signature, Key Encipherment
basicConstraints （Critical = TRUE）	
BasicConstraints	
CA	Type：Boolean Value：False
authorityKeyIdentifier (Critical = FALSE)	
KeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
subjectKeyIdentifier （Critical = FALSE）	
SubjectKeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
CertificatePolicies （Critical = FALSE）	
PolicyID	Type：OID Value：(Refer CPS1.2) 1.2.392.00200181.3.5.1 Value：(Refer IGTF-AP-classic-4-3) 1.2.840.113612.5.2.2.1
QualifierID	Type：OID Value：（Refer CPS1.2） pkix-id-qt CPSurl
Qualifier	Type： Value：URI of the CP/CPS https://www.naregi.org/ca/naregi-cps4.0.pdf
CRLDistributionPoints （Critical = FALSE）	
[0] dist-point	
[0] fullName :	Value：URI of the CRL http://www.naregi.org/ca/out-CRL2.crl
ExtendedkeyUsage （Critical = FALSE）	
ExtkeyUsage	Type：OID Value：1.3.6.1.5.5.7.3.1 （serverAuth）
SubjectAlternativeName （Critical = FALSE）	
SubjectAlternativeName	Type：IA5String Value：FQDN of the host
AuthorityInfoAccess （Critical = FALSE）	
accessDescription	
accessMethod	Type：OID Value：1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
accessLocation	Value：URI of the OCSP server http://ocsp.naregi.org

1．7 Globus/Unicore Client User Certificate

○Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha512RSA(1024bits)
algorithm	Type：OID Value：1 2 840 113549 1 1 13
parameters	Type：NULL Value：None
Validity	
validity	
notBefore	Type：UTC Time Value：yymmddhhmmssZ
notAfter	Type：UTC Time Value：yymmddhhmmssZ (395 days)
Issuer	
countryName	
type	Type：OID Value：2 5 4 6
value	Type：PrintableString Value：JP
organizationName	
type	Type：OID Value：2 5 4 10
value	Type：PrintableString Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID Value：2 5 4 11
value	Type：PrintableStirng Value：CGRD
commonName	

type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value： NAREGI CA
Subject	
countryName	
type	Type：OID
	Value：2 5 4 6
value	Type：PrintableString
	Value：JP
organizationName	
type	Type：OID
	Value：2 5 4 10
value	Type：PrintableString
	Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID
	Value：2 5 4 11
value	Type：PrintableStirng
	Value：Ira Name
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableStirng
	Value：
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 1
parameters	Type：NULL
	Value：None
subjectPublicKey	Type：BIT STRING
	Value：Public Key Value

○Extension Fields

authorityKeyIdentifier (Critical = FALSE)	
AuthorityKeyIdentifier	

KeyIdentifier	Type : OCTET STRING Value : Unique Byte Strings
subjectKeyIdentifier （Critical = FALSE）	
SubjectKeyIdentifier	Type : OCTET STRING Value : Unique Byte Strings
basicConstraints （Critical = TRUE）	
BasicConstraints CA	 Type : Boolean Value : False
keyUsage （Critical = TRUE）	
KeyUsage	Type : BitString Value : digitalSignature, Key Encipherment
ExtendedkeyUsage （Critical = FALSE）	
Ext KeyUsage	Type : OID Value : ClientAuth
CertificatePolicies （Critical = FALSE）	
PolicyID QualifierID Qualifier	Type : OID Value : (Refer CPS1.2) 1.2.392.00200181.3.6.1 Value : (Refer IGTF-AP-classic-4-3) 1.2.840.113612.5.2.2.1 Type : OID Value : (Refer CPS1.2) pkix-id-qt CPSurl Type : Value : URI of the CP/CPS https://www.naregi.org/ca/naregi-cps4.0.pdf
CRLDistributionPoints （Critical = FALSE）	
[0] dist-point [0] fullName :	 Value : URI of the CRL http://www.naregi.org/ca/out-CRL2.crl
AuthorityInfoAccess （Critical = FALSE）	
accessDescription accessMethod accessLocation	 Type : OID Value : 1.3.6.1.5.5.7.48.1 (id-ad-ocsp) Value : URI of the OCSP server http://ocsp.naregi.org

1．8 Web Server Certificate

○Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha512RSA(1024bits)
algorithm	Type：OID Value：1 2 840 113549 1 1 13
parameters	Type：NULL Value：None
Validity	
validity	
notBefore	Type：UTC Time Value：yymmddhhmmssZ
notAfter	Type：UTC Time Value：yymmddhhmmssZ (395 days)
Issuer	
countryName	
type	Type：OID Value：2 5 4 6
value	Type：PrintableString Value：JP
organizationName	
type	Type：OID Value：2 5 4 6
value	Type：UTF8String Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID Value：2 5 4 11
value	Type：PrintableStirng Value：CGRD
commonName	

type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value： NAREGI CA
Subject	
countryName	
type	Type：OID
	value：2 5 4 6
value	Type：PrintableString
	Value：JP
organizationName	
type	Type：OID
	Value：2 5 4 10
value	Type：PrintableString
	Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID
	Value：2 5 4 11
value	Type：PrintableString
	Value：Ira Name
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value：FQDN of the host
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
AlgorithmIdentifier	RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 1
parameters	Type：NULL
	Value：None
subjectPublicKey	Type：BIT STRING
	Value：Public Key value

○Extension Fields

keyUsage （Critical = TRUE）	
KeyUsage	Type：BitString

	Value：Digital Signature, Key Encipherment
basicConstraints （Critical = TRUE）	
BasicConstraints	
CA	Type：Boolean
	Value：False
authorityKeyIdentifier (Critical = FALSE)	
KeyIdentifier	Type：OCTET STRING
	Value：Unique Byte Strings
subjectKeyIdentifier （Critical = FALSE）	
SubjectKeyIdentifier	Type：OCTET STRING
	Value：Unique Byte Strings
CertificatePolicies （Critical = FALSE）	
PolicyID	Type：OID
	Value：(Refer CPS1.2) 1.2.392.00200181.3.7.1
	Value：(Refer IGTF-AP-classic-4-3) 1.2.840.113612.5.2.2.1
QualifierID	Type：OID
	Value：（Refer CPS1.2） pkix-id-qt CPSurl
Qualifier	Type：
	Value：URI of the CP/CPS
	https://www.naregi.org/ca/naregi-cps4.0.pdf
CRLDistributionPoints （Critical = FALSE）	
[0] dist-point	
[0] fullName :	Value：URI of the CRL
	http://www.naregi.org/ca/out-CRL2.crl
ExtendedkeyUsage （Critical = FALSE）	
ExtkeyUsage	Type：OID
	Value：1.3.6.1.5.5.7.3.1 （serverAuth）
SubjectAlternativeName （Critical = FALSE）	
SubjectAlternativeName	Type：IA5String
	Value：FQDN of the host
AuthorityInfoAccess （Critical = FALSE）	
accessDescription	
accessMethod	Type：OID
	Value：1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
accessLocation	Value：URI of the OCSP server
	http://ocsp.naregi.org

1．9 OCSP Server Certificate

○Basic Fields

Version	
version	Type：INTEGER
	Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER
	Value：Unique Integer
signature	
algorithmIdentifier	sha512RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 13
parameters	Type：NULL
	Value：None
Validity	
validity	
notBefore	Type：UTC Time
	Value：yymmddhhmmssZ
notAfter	Type：UTC Time
	Value：yymmddhhmmssZ (395 days)
Issuer	
countryName	
type	Type：OID
	Value：2 5 4 6
value	Type：PrintableString
	Value：JP
organizationName	
type	Type：OID
	Value：2 5 4 6
value	Type：UTF8String
	Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID
	Value：2 5 4 11
value	Type：PrintableStirng
	Value：CGRD
commonName	

type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value： NAREGI CA
Subject	
countryName	
type	Type：OID
	value：2 5 4 6
value	Type：PrintableString
	Value：JP
organizationName	
type	Type：OID
	Value：2 5 4 10
value	Type：PrintableString
	Value：National Research Grid Initiative
organizationalUnitName	
type	Type：OID
	Value：2 5 4 11
value	Type：PrintableString
	Value：Ira Name
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value：FQDN of the host
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
AlgorithmIdentifier	RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 1
parameters	Type：NULL
	Value：None
subjectPublicKey	Type：BIT STRING
	Value：Public Key value

○Extension Fields

keyUsage （Critical = TRUE）	
KeyUsage	Type：BitString

	Value：Digital Signature, Key Encipherment
basicConstraints （Critical = TRUE）	
BasicConstraints	
CA	Type：Boolean
	Value：False
authorityKeyIdentifier (Critical = FALSE)	
KeyIdentifier	Type：OCTET STRING
	Value：Unique Byte Strings
subjectKeyIdentifier （Critical = FALSE）	
SubjectKeyIdentifier	Type：OCTET STRING
	Value：Unique Byte Strings
CertificatePolicies （Critical = FALSE）	
PolicyID	Type：OID
	Value：(Refer CPS1.2) 1.2.392.00200181.3.8.1
	Value：(Refer IGTF-AP-classic-4-3) 1.2.840.113612.5.2.2.1
QualifierID	Type：OID
	Value：(Refer CPS1.2) pkix-id-qt CPSurl
Qualifier	Type：
	Value：URI of the CP/CPS
	https://www.naregi.org/ca/naregi-cps4.0.pdf
CRLDistributionPoints （Critical = FALSE）	
[0] dist-point	
[0] fullName :	Value：URI of the CRL
	http://www.naregi.org/ca/out-CRL2.crl
ExtendedkeyUsage （Critical = FALSE）	
ExtkeyUsage	Type：OID
	Value：1.3.6.1.5.5.7.3.9 (ocspSigning)
SubjectAlternativeName （Critical = FALSE）	
SubjectAlternativeName	Type：IA5String
	Value：FQDN of the host
AuthorityInfoAccess （Critical = FALSE）	
accessDescription	
accessMethod	Type：OID
	Value：1.3.6.1.5.5.7.48.1 (id-ad-ocsp)
accessLocation	Value：URI of the OCSP server
	http://ocsp.naregi.org

2． CRL Profile

○Basic Fields

Version	
version	Type：INTEGER Value：1
Signature	
algorithmIdentifier	sha1RSA(1024bits)
algorithm	Type：OID Value：1 2 840 113549 1 1 5
parameters	Type：NULL Value：None
ThisUpdate	
thisUpdate	Type：UTC Time Value：yymmddhhmmssZ （at signing time）
NextUpdate	
nextUpdate	Type：UTC Time Value：yymmddhhmmssZ (After 30Days)
Issuer	
countryName	
type	Type：OID Value：2 5 4 6
value	Type：PrintableString Value：JP
organizationName	
type	Type：OID Value：2 5 4 10
value	Type：PrintableString Value：National Research Grid Initiative,
organizationalUnitName	
type	Type：OID Value：2 5 4 11
value	Type：PrintableStirng Value：CGRD
commonName	
type	Type：OID Value：2 5 4 3
value	Type：PrintableString

	Value： NAREGI CA
RevokedCertificates	
userCertificate	Type：INTEGER Value：Unique Integer
revocationDate	Type：UTC Time Value：yymmddhhmmssZ
crlEntryExtensions	
reasonCode	Type：OID Value：2 5 29 21

○Extensions

authorityKeyIdentifier (Critical = FALSE)	
KeyIdentifier	Type：OCTET STRING Value：Unique Byte Strings
cRLNumber(Critical = FALSE)	
CRLNumber	Type：INTEGER Value：Unique Integer
issuingDistributionPoint (Critical = TRUE)	
DistributionPoint	
distributionPointName	Value：URI of the CRL http://www.naregi.org/ca/out-CRL2.crl
fullName	
OnlyContainsUserCerts	Type：BOOLEAN Value：TRUE