



NRG-CPS-K006

**NAREGI**

## **Certificate and CRL Profile**

Ver. 2.5

November 26, 2012

**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 SubjectAlternativeName 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.

1 .	Certificate Profile .....	3
1. 1	SELF SIGN CERTIFICATE (CA CERTIFICATE) .....	3
1. 2	GLOBUS HOST/GFSD/LDAP CERTIFICATE.....	6
1. 3	GLOBUS USER CERTIFICATES .....	9
1. 4	UNICORE SERVER CERTIFICATE.....	12
1. 5	UNICORE CLIENT USER CERTIFICATE.....	15
1. 6	LDAP SERVER CERTIFICATE .....	18
1. 7	GLOBUS/UNICORE CLIENT USER CERTIFICATE .....	21
1. 8	WEB SERVER CERTIFICATE .....	24
2 .	CRL Profile.....	27

# 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

commonName	Value: CGRD
type	Type: OID Value: 2 5 4 3
value	Type: PrintableString Value: NAREGI CA
<b>Subject</b>	
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
<b>SubjectPublicKeyInfo</b>	
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

○Extension Fields

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

1. 2 Globus host/gfsd/LDAP Certificate

○Basic Fields

Version	
Version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique integer
Signature	
algorithmIdentifier	sha256RSA(1024bits)
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 (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: PrintableString Value: CGRD
commonName	

Type	Type: OID Value: 2 5 4 3
Value	Type: PrintableString Value: NAREGI CA
<b>Subject</b>	
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: ldap/FQDN of the host (for ldap) Value: gfsd/FQDN of the host (for gfsd)
<b>SubjectPublicKeyInfo</b>	
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

<b>keyUsage (Critical = TRUE)</b>	
KeyUsage	Type: BitString Value: Digital Signature, Key Encipherment
<b>basicConstraints (Critical = TRUE)</b>	
BasicConstraints CA	Type: Boolean Value: False
<b>authorityKeyIdentifier (Critical = FALSE)</b>	
KeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>subjectKeyIdentifier (Critical = FALSE)</b>	
SubjectKeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>CertificatePolicies (Critical = FALSE)</b>	
PolicyID	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
QualifierID	Type: OID Value: (Refer CPS1.2) pkix-id-qt CPSurl
Qualifier	Type: Value: URI of the CP/CPS <a href="https://www.naregi.org/ca/naregi-cps4.0.pdf">https://www.naregi.org/ca/naregi-cps4.0.pdf</a>
<b>CRLDistributionPoints (Critical = FALSE)</b>	
[0] dist-point [0] fullName :	Value: URI of the CRL <a href="http://www.naregi.org/ca/out-CRL2.crl">http://www.naregi.org/ca/out-CRL2.crl</a>
<b>ExtendedkeyUsage (Critical = FALSE)</b>	
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)
<b>SubjectAlternativeName (Critical = FALSE)</b>	
SubjectAlternativeName	Type: IA5String Value: FQDN of the host

### 1. 3 Globus User Certificates

#### ○Basic Fields

Version	
version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique Integer
signature	
algorithmIdentifier	sha256RSA(1024bits)
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 (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: 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: PrintableString Value: Ira Name
commonName	
type	Type: OID Value: 2 5 4 3
value	Type: PrintableString 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
<b>subjectKeyIdentifier (Critical = FALSE)</b>	
SubjectKeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>keyUsage (Critical = TRUE)</b>	
KeyUsage	Type: BitString Value: digitalSignature, Key Encipherment
<b>basicConstraints (Critical = TRUE)</b>	
BasicConstraints CA	Type: Boolean Value: False
<b>CertificatePolicies (Critical = FALSE)</b>	
PolicyID	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
QualifierID	Type: OID Value: [Refer CPS1.2] pkix-id-qt CPSurl
Qualifier	Type: Value: URI of the CP/GPS <a href="https://www.naregi.org/ca/naregi-cps4.0.pdf">https://www.naregi.org/ca/naregi-cps4.0.pdf</a>
<b>CRLDistributionPoints (Critical = FALSE)</b>	
[0] dist-point [0] fullName :	Value: URI of the CRL <a href="http://www.naregi.org/ca/out-CRL2.crl">http://www.naregi.org/ca/out-CRL2.crl</a>
<b>ExtendedkeyUsage (Critical = FALSE)</b>	
ExtkeyUsage	Type: OID Value: 1.3.6.1.5.5.7.3.2 (clientAuth)

1. 4 Unicore Server Certificate

○Basic Fields

Version	
version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique Integer
signature	
algorithmIdentifier	sha256RSA(1024bits)
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 (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: PrintableString Value: CGRD
commonName	

type	Type: OID Value: 2 5 4 3
value	Type: PrintableString Value: NAREGI CA
<b>Subject</b>	
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)
<b>SubjectPublicKeyInfo</b>	
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

<b>keyUsage (Critical = TRUE)</b>	
KeyUsage	Type: BitString Value: Digital Signature, Key Encipherment
<b>basicConstraints (Critical = TRUE)</b>	
BasicConstraints CA	Type: Boolean Value: False
<b>authorityKeyIdentifier (Critical = FALSE)</b>	
KeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>subjectKeyIdentifier (Critical = FALSE)</b>	
SubjectKeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>CertificatePolicies (Critical = FALSE)</b>	
PolicyID	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
QualifierID	Type: OID Value: (Refer CPS1.2) pkix-id-qt CPSurl
Qualifier	Type: Value: URI of the CP/CPS <a href="https://www.naregi.org/ca/naregi-cps4.0.pdf">https://www.naregi.org/ca/naregi-cps4.0.pdf</a>
<b>CRLDistributionPoints (Critical = FALSE)</b>	
[0] dist-point [0] fullName :	Value: URI of the CRL <a href="http://www.naregi.org/ca/out-CRL2.crl">http://www.naregi.org/ca/out-CRL2.crl</a>
<b>ExtendedkeyUsage (Critical = FALSE)</b>	
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)
<b>SubjectAlternativeName (Critical = FALSE)</b>	
SubjectAlternativeName	Type: IA5String Value: FQDN of the host

1. 5 Unicore Client User Certificate

○Basic Fields

Version	
version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique Integer
signature	
algorithmIdentifier	sha256RSA(1024bits)
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 (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: 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: PrintableString Value: Ira Name
commonName	
type	Type: OID Value: 2 5 4 3
value	Type: PrintableString 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
<b>subjectKeyIdentifier (Critical = FALSE)</b>	
SubjectKeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>keyUsage (Critical = TRUE)</b>	
KeyUsage	Type: BitString Value: digitalSignature, Key Encipherment
<b>basicConstraints (Critical = TRUE)</b>	
BasicConstraints CA	Type: Boolean Value: False
<b>CertificatePolicies (Critical = FALSE)</b>	
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/GPS <a href="https://www.naregi.org/ca/naregi-cps4.0.pdf">https://www.naregi.org/ca/naregi-cps4.0.pdf</a>
<b>CRLDistributionPoints (Critical = FALSE)</b>	
[0] dist-point [0] fullName :	Value: URI of the CRL <a href="http://www.naregi.org/ca/out-CRL2.crl">http://www.naregi.org/ca/out-CRL2.crl</a>
<b>ExtendedkeyUsage (Critical = FALSE)</b>	
ExtkeyUsage	Type: OID Value: 1.3.6.1.5.5.7.3.2 (clientAuth)

1. 6 LDAP Server Certificate

○Basic Fields

Version	
Version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique Integer
Signature	
algorithmIdentifier	sha256RSA(1024bits)
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 (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: PrintableString Value: CGRD
commonName	

type	Type: OID Value: 2 5 4 3
value	Type: PrintableString Value: NAREGI CA
<b>Subject</b>	
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
<b>SubjectPublicKeyInfo</b>	
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

<b>keyUsage (Critical = TRUE)</b>	
KeyUsage	Type: BitString Value: Digital Signature, Key Encipherment
<b>basicConstraints (Critical = TRUE)</b>	
BasicConstraints CA	Type: Boolean Value: False
<b>authorityKeyIdentifier (Critical = FALSE)</b>	
KeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>subjectKeyIdentifier (Critical = FALSE)</b>	
SubjectKeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>CertificatePolicies (Critical = FALSE)</b>	
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 <a href="https://www.naregi.org/ca/naregi-cps4.0.pdf">https://www.naregi.org/ca/naregi-cps4.0.pdf</a>
<b>CRLDistributionPoints (Critical = FALSE)</b>	
[0] dist-point [0] fullName :	Value: URI of the CRL <a href="http://www.naregi.org/ca/out-CRL2.crl">http://www.naregi.org/ca/out-CRL2.crl</a>
<b>ExtendedkeyUsage (Critical = FALSE)</b>	
ExtkeyUsage	Type: OID Value: 1.3.6.1.5.5.7.3.1 (serverAuth)
<b>SubjectAlternativeName (Critical = FALSE)</b>	
SubjectAlternativeName	Type: IA5String Value: FQDN of the host

1. 7 Globus/Unicore Client User Certificate

○Basic Fields

Version	
version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique Integer
signature	
algorithmIdentifier	sha256RSA(1024bits)
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 (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: 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: PrintableString Value: Ira Name
commonName	
type	Type: OID Value: 2 5 4 3
value	Type: PrintableString 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

<b>authorityKeyIdentifier (Critical = FALSE)</b>	
AuthorityKeyIdentifier	

KeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>subjectKeyIdentifier (Critical = FALSE)</b>	
SubjectKeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>basicConstraints (Critical = TRUE)</b>	
BasicConstraints CA	Type: Boolean Value: False
<b>keyUsage (Critical = TRUE)</b>	
KeyUsage	Type: BitString Value: digitalSignature, Key Encipherment
<b>ExtendedkeyUsage (Critical = FALSE)</b>	
Ext KeyUsage	Type: OID Value: ClientAuth
<b>CertificatePolicies (Critical = FALSE)</b>	
PolicyID	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
QualifierID	Type: OID Value: (Refer CPS1.2) pkix-id-qt CPSurl
Qualifier	Type: Value: URI of the CP/CPS <a href="https://www.naregi.org/ca/naregi-cps4.0.pdf">https://www.naregi.org/ca/naregi-cps4.0.pdf</a>
<b>CRLDistributionPoints (Critical = FALSE)</b>	
[0] dist-point [0] fullName :	Value: URI of the CRL <a href="http://www.naregi.org/ca/out-CRL2.crl">http://www.naregi.org/ca/out-CRL2.crl</a>



## 1. 8 Web Server Certificate

### ○Basic Fields

Version	
version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique Integer
signature	
algorithmIdentifier	sha256RSA(1024bits)
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 (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: 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: 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
<b>basicConstraints (Critical = TRUE)</b>	
BasicConstraints CA	Type: Boolean Value: False
<b>authorityKeyIdentifier (Critical = FALSE)</b>	
KeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>subjectKeyIdentifier (Critical = FALSE)</b>	
SubjectKeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
<b>CertificatePolicies (Critical = FALSE)</b>	
PolicyID  QualifierID  Qualifier	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 Type: OID Value: (Refer CPS1.2) pkix-id-qt CPSurl Type: Value: URI of the CP/GPS <a href="https://www.naregi.org/ca/naregi-cps4.0.pdf">https://www.naregi.org/ca/naregi-cps4.0.pdf</a>
<b>CRLDistributionPoints (Critical = FALSE)</b>	
[0] dist-point [0] fullName :	Value: URI of the CRL <a href="http://www.naregi.org/ca/out-CRL2.crl">http://www.naregi.org/ca/out-CRL2.crl</a>
<b>ExtendedkeyUsage (Critical = FALSE)</b>	
ExtkeyUsage	Type: OID Value: 1.3.6.1.5.5.7.3.1 (serverAuth)
<b>SubjectAlternativeName (Critical = FALSE)</b>	
SubjectAlternativeName	Type: IA5String Value: FQDN of the host

## 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: PrintableString Value: CGRD
commonName	
type	Type: OID Value: 2 5 4 3
value	Type: PrintableString

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

Extensions

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