NAREGI

Certificate and CRL Profile

Ver. 2.0

July 7, 2006

National Research Grid Initiative

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

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

○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/LDAP Certificate

◯Basic Fields

Version	
Version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique integer
signature	
algorithmIdentifier	sha1RSA(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 (1year)
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：CGRD
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value：host/Server Name or ldap/Server Name
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) 1.2.392.00200181.3.1.1 Type : OID Value : (Refer CPS1.2) pkix-id-qt CPSurl Type : Value : URI of the CP/CPS https://www.naregi.org/ca/naregi-cps2.0.pdf
CRLDistributionPoints (Critical = FALSE)	
[0] dist-point [0] fullName :	 Value : URI of the CRL https://www.naregi.org/ca/out-CRL2.crl

1．3 Globus User Certificates

◯Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha1RSA(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 (1year)
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：CGRD
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableStirng
	Value：
pkcs9email	
type	Type：OID
	Value：1.2.840.113549.1.9.1
value	Type：IA5String
	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
CertificatePolicies (Critical = FALSE)	
PolicyID QualifierID Qualifier	Type：OID Value：[Refer CPS1.2] 1.2.392.00200181.3.2.1 Type：OID Value：[Refer CPS1.2] pkix-id-qt CPSurl Type： Value：URI of the CP/CPS https://www.naregi.org/ca/naregi-cps2.0.pdf
CRLDistributionPoints (Critical = FALSE)	
[0] dist-point [0] fullName :	 Value：URI of the CRL https://www.naregi.org/ca/out-CRL2.crl

1．4 Unicore Server Certificate

◯Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha1RSA(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 (1year)
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：CGRD
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value：gateway/Server Name or njs/Server Name
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 PathLenConstraint	 Type : Boolean Value : False Type : INTEGER Value : NULL
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 Type : OID Value : (Refer CPS1.2) pkix-id-qt CPSurl Type : Value : URI of the CP/CPS https://www.naregi.org/ca/naregi-cps2.0.pdf
CRLDistributionPoints (Critical = FALSE)	
[0] dist-point [0] fullName :	 Value : URI of the CRL https://www.naregi.org/ca/out-CRL2.crl

1．5 Unicore Client User Certificate

○Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha1RSA(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 (1year)
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：CGRD
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableStirng
	Value：
pkcs9email	
type	Type：OID
	Value：1.2.840.113549.1.9.1
value	Type：IA5String
	Value：
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(1024bits)
algorithm	Type：OID
	Value：1 2 840 113549 1 1 1
parameters	Type：NULL

subjectPublicKey	Value : None 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
CertificatePolicies (Critical = FALSE)	
PolicyID QualifierID Qualifier	Type : OID Value : (Refer CPS1.2) 1.2.392.00200181.3.4.1 Type : OID Value : (Refer CPS1.2) pkix-id-qt CPSurl Type : Value : URI of the CP/CPS https://www.naregi.org/ca/naregi-cps2.0.pdf
CRLDistributionPoints (Critical = FALSE)	
[0] dist-point [0] fullName :	 Value : URI of the CRL https://www.naregi.org/ca/out-CRL2.crl

1．6 LDAP Server Certificate

◯Basic Fields

Version	
Version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
Signature	
algorithmIdentifier	sha1RSA(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 (1year)
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：CGRD
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value：Server Name
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 PathLenConstraint	 Type : Boolean Value : False Type : INTEGER Value : NULL
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) 1.2.392.00200181.3.5.1 Type : OID Value : (Refer CPS1.2) pkix-id-qt CPSurl Type : Value : URI of the CP/CPS https://www.naregi.org/ca/naregi-cps2.0.pdf
CRLDistributionPoints (Critical = FALSE)	
[0] dist-point [0] fullName :	 Value : URI of the CRL https://www.naregi.org/ca/out-CRL2.crl

1．7 Globus/Unicore Client User Certificate

○Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha1RSA(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 (1year)
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：CGRD
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableStirng
	Value：
pkcs9email	
type	Type：OID
	Value：1.2.840.113549.1.9.1
value	Type：IA5String
	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
ExtendedkeyUsage (Critical = FALSE)	
Ext KeyUsage OID	Type : OID Value : Code-signning
CertificatePolicies (Critical = FALSE)	
PolicyID QualifierID Qualifier	Type : OID Value : (Refer CPS1.2) 1.2.392.00200181.3.6.1 Type : OID Value : (Refer CPS1.2) pkix-id-qt CPSurl Type : Value : URI of the CP/CPS https://www.naregi.org/ca/naregi-cps2.0.pdf
CRLDistributionPoints (Critical = FALSE)	
[0] dist-point [0] fullName :	 Value : URI of the CRL https://www.naregi.org/ca/out-CRL2.crl

1．8 Web Server Certificate

◯Basic Fields

Version	
version	Type：INTEGER Value：2
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：Unique Integer
signature	
algorithmIdentifier	sha1RSA(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 (1year)
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：CGRD
commonName	
type	Type：OID
	Value：2 5 4 3
value	Type：PrintableString
	Value：Server Name
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
PathLenConstraint	Type : INTEGER Value : NULL
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
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-cps2.0.pdf
CRLDistributionPoints (Critical = FALSE)	
[0] dist-point [0] fullName :	Value : URI of the CRL https://www.naregi.org/ca/out-CRL2.crl

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
	https://www.naregi.org/ca/out-CRL2.crl
fullName	
OnlyContainsUserCerts	Type:BOOLEAN
	Value:TRUE