Certificate and CRL Profile

Ver. 1.2

March 20, 2007

Grid Technology Research Center,

National Institute of Advanced Industrial Science and Technology

(AIST), Japan

Certificate Profile

（1） Self Sign Certificate （CA Certificate）

Basic Fields

Version	
version	Type:INTEGER Value:2 (version 3)
SerialNumber	
certificateSerialNumber	Type：INTEGER Value：integer
signature	
algorithmIdentifier	sha1RSA(1024bit)
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
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:：AIST
organizationalUnitName	
type	Type:：OID Value:：2 5 4 11
value	Type:：PrintableString Value:：GRID
commonName	

type	Type: : OID
	Value: : 2 5 4 3
value	Type: : PrintableString
	Value: : Certificate Authority
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: : AIST
organizationalUnitName	
type	Type: : OID
	Value: : 2 5 4 11
value	Type: : PrintableString
	Value: : GRID
commonName	
type	Type: : OID
	Value: : 2 5 4 3
value	Type: : PrintableString
	Value: : Certificate Authority
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(2048bit)
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:: Byte strings
subjectKeyIdentifier (Critical= FALSE)	
SubjectKeyIdentifier	Type:: OCTET STRING Value:: Unique String
keyUsage (Critical= TRUE)	
KeyUsage	Type:: BitString Value:: 000001100(Certificate Sign, CRL Sign)
basicConstraints (Critical= TRUE)	
BasicConstraints CA	 Type:: Boolean Value:: True(CA)

（２） Globus host/LDAP Certificate

Basic Fields

Version	
version	Type::INTEGER Value::2
SerialNumber	
certificateSerialNumber	Type::INTEGER Value::Integer
signature	
algorithmIdentifier	sha1RSA(1024bit)
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
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::AIST
organizationalUnitName	
type	Type::OID Value::2 5 4 11
value	Type::PrintableString Value::GRID
commonName	

type	Type::OID
	Value::2 5 4 3
value	Type::PrintableString
	Value::Certificate Authority
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::AIST
organizationalUnitName	
type	Type::OID
	Value::2 5 4 11
value	Type::PrintableString
	Value::GRID
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)
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(1024bit)
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::
keyUsage (Critical= TRUE)	
KeyUsage	Type:: BitString Value:: Digital Signature, Key Encipherment, Data Encipherment
basicConstraints (Critical= TRUE)	
BasicConstraints CA	 Type:: Boolean Value:: False
CertificatePolicies (Critical= FALSE)	
PolicyID QualifierID Qualifier	Type:: OID Value:: (Refer CPS1.2) Type:: OID Value:: (Refer CPS1.2) Type:: PrintableString Value:: URI of the CP/CPS
CRLDistributionPoints (Critical= FALSE)	
CRLDistributionPoints	Type:: PrintableString Value:: URI of the CRL
IssuerAlternativeName (Critical= FALSE)	
IssuerAlternativeName	Type:: PrintableString Value:: Email address of AIST GRID CA
ExtKeyUsage (Critical= FALSE)	
ExtKeyUsage	Type:: OID Value:: 1.3.6.1.5.5.7.3.1 Value:: 1.3.6.1.5.5.7.3.2
SubjetAlternativeName (Critical= FALSE)	
SubjectAlternativeName	Type:: IA5String Value:: FQDN of the host

（３） Globus User Certificates

Basic Fields

Version	
version	Type::INTEGER Value::2
SerialNumber	
certificateSerialNumber	Type::INTEGER Value::Unique Integer
signature	
algorithmIdentifier	sha1RSA(1024bit)
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
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::Printable String
	Value::AIST
organizationalUnitName	
type	Type::OID
	Value::2 5 4 11
value	Type::PrintableString
	Value::GRID
commonName	

type	Type:: OID
	Value:: 2 5 4 3
value	Type:: PrintableString
	Value:: Certificate Authority
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:: AIST
organizationalUnitName	
type	Type:: OID
	Value:: 2 5 4 11
value	Type:: PrintableStirng
	Value:: GRID
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::
optional	
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	
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:: Value
subjectKeyIdentifier (Critical= FALSE)	
SubjectKeyIdentifier	Type:: OCTET STRING Value:: Value
keyUsage (Critical= TRUE)	
KeyUsage	Type:: BitString Value:: (digitalSignature, nonRepudiation,) Key Encipherment, Data Encipherment
basicConstraints (Critical= TRUE)	
BasicConstraints CA	 Type:: Boolean Value:: False
CertificatePolicies (Critical= FALSE)	
PolicyID QualifierID Qualifier	Type:: OID Value:: [Refer CPS1.2] Type:: OID Value:: [Refer CPS1.2] Type:: PrintableString Value:: URI of the CP/CPS
CRLDistributionPoints (Critical= FALSE)	
CRLDistributionPoints	Type:: PrintableString Value:: URI of the CRL
IssuerAlternativeName (Critical= FALSE)	
IssuerAlternativeName	Type:: PrintableString Value:: Email address of AIST GRID CA
ExtKeyUsage (Critical= FALSE)	
ExtkeyUsage	Type:: OID Value:: 1.3.6.1.5.5.7.3.2

（4）Unicore Server Certifiate

Basic Fields

Version	
version	Type::INTEGER Value::2
SerialNumber	
certificateSerialNumber	Type::INTEGER Value::Unique Integer
signature	
algorithmIdentifier	sha1RSA(1024bit)
algorithm	Type::OID Value::1 2 840 113549 1 1 5
parameters	Type::NULL Value::
Validity	
validity	
notBefore	Type::UTC Time Value::yymmddhhmmssZ
notAfter	Type::UTC Time Value::yymmddhhmmssZ
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::AIST
organizationalUnitName	
type	Type::OID Value::2 5 4 11
value	Type::PrintableString Value::GRID

commonName	
type	Type: : OID
	Value: : 2 5 4 3
value	Type: : PrintableString
	Value: : Certificate Authority
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: : AIST
organizationalUnitName	
type	Type: : OID
	Value: : 2 5 4 11
value	Type: : PrintableString
	Value: : GRID
commonName	
type	Type: : OID
	Value: : 2 5 4 3
value	Type: : PrintableString
	Value: :
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(1024bit)
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 String
subjectKeyIdentifier (Critical= FALSE)	
SubjectKeyIdentifier	Type:: OCTET STRING Value:: Unique
keyUsage (Critical= TRUE)	
KeyUsage	Type:: BitString Value:: Digital Signature, Key Encipherment, Data Encipherment
basicConstraints (Critical= TRUE)	
BasicConstraints CA	 Type:: Boolean Value:: False
CertificatePolicies (Critical= FALSE)	
PolicyID QualifierID Qualifier	Type:: OID Value:: [Refer CPS1.2] Type:: OID Value:: [Refer CPS1.2] Type:: PrintableString Value:: URI of the host
CRLDistributionPoints (Critical= FALSE)	
CRLDistributionPoints	Type:: PrintableString Value:: URI of the CRL
IssuerAlternativeName (Critical= FALSE)	
IssuerAlternativeName	Type:: PrintableString Value:: Email address of AIST GRID CA
ExtKeyUsage (Critical= FALSE)	
ExtKeyUsage	Type:: OID Value:: 1.3.6.1.5.5.7.3.1 Value:: 1.3.6.1.5.5.7.3.2
SubjetAlternativeName (Critical= FALSE)	
SubjectAlternativeName	Type:: IA5String Value:: FQDN of the host

（5） Unicore　Client User Certificate

Basic Fields

Version	
version	Type::INTEGER Value::2
SerialNumber	
certificateSerialNumber	Type::INTEGER Value::Unique Integer
signature	
algorithmIdentifier	sha1RSA(1024bit)
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
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::Printable String Value::AIST
organizationalUnitName	
type	Type::OID Value::2 5 4 11
value	Type::PrintableString Value::GRID
commonName	
type	Type::OID

	Value::2 5 4 3
value	Type::PrintableString
	Value::Certificate Authority
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::AIST
organizationalUnitName	
type	Type::OID
	Value::2 5 4 11
value	Type::PrintableStirng
	Value::GRID
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::
optional	
SubjectPublicKeyInfo	
subjectPublicKeyInfo	
algorithmIdentifier	RSA(1024bit)
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 Strings
subjectKeyIdentifier (Critical= FALSE)	
SubjectKeyIdentifier	Type::OCTET STRING Value::Unique Bite String
keyUsage (Critical= TRUE)	
KeyUsage	Type::BitString Value::(digitalSignature, nonRepudiation,) Key Encipherment, Data Encipherment
basicConstraints (Critical= TRUE)	
BasicConstraints CA	 Type::Boolean Value::False
CertificatePolicies (Critical= FALSE)	
PolicyID QualifierID Qualifier	Type::OID Value::[Refer CPS1.2] Type::OID Value::[Refer CPS1.2] Type:: PrintableString Value:: URI of the CP/CPS
CRLDistributionPoints (Critical= FALSE)	
CRLDistributionPoints	Type::PrintableString Value::URI of the CRL
IssuerAlternativeName (Critical= FALSE)	
IssuerAlternativeName	Type::PrintableString Value::Email address of AIST GRID CA
ExtKeyUsage (Critical= FALSE)	
ExtkeyUsage	Type::OID Value::1.3.6.1.5.5.7.3.2

2. CRL Profile

Basic Field

Version	
version	Type::INTEGER Value::1
signature	
algorithmIdentifier	sha1RSA(1024bit)
algorithm	Type::OID Value::1 2 840 113549 1 1 5
parameters	Type::NULL Value::None
ThisUpdate	
thisUpdate	Type::UTC Time Value::yymmddhhmmssZ
NextUpdate	
nextUpdate	Type::UTC Time Value::yymmddhhmmssZ
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::AIST
organizationalUnitName	
type	Type::OID Value::2 5 4 11
value	Type::PrintableString Value::GRID
commonName	
type	Type::OID Value::2 5 4 3
value	Type::PrintableString

	Value::Certificate Authority
RevokedCertificates	
userCertificate	Type::INTEGER Value::Unique Integer
revocationDate	Type::UTC Time Value::yymmddhhmmssZ
crlEntryExtensions reasonCode	Type::OID Value::2 5 29 21
	Type: ENUMERATED
value	unspecified(0), keyCompromise(1), cACompromise(2), affiliationChanged(3), superseded(4), cessationOfOperation(5), certificateHold(6), removeFromCRL(8), privilegeWithdrawn(9), aaCompromise(10)

Extensions

authorityKeyIdentifier (Critical= FALSE)	
KeyIdentifier	Type::OCTET STRING Value::
cRLNumber(Critical= FALSE)	
CRLNumber	Type::INTEGER Value::
issuingDistributionPoint (Critical = TRUE)	
DistributionPoint distributionPointName	Type: PrintableString Value: URI of the CRL