

KEK GRID CA

Certificate and CRL Profile

Ver. 2.0.0

April 8, 2008



Computing Research Center, High Energy Accelerator

Research Organization (KEK), Japan

1. Certificate Profile	3
1.1 CA Self Signed Certificate	3
1.2 Globus Server Certificate	4
1.3 Globus Client Certificate	7
1.4 Web Server Certificate	9
2. Certificate Revocation List Profile	11

Revision History Table

Date of revision or approval by the PMA	KEK GRID CA CP and CPS	Certificate and CRL Profile	Enrollment Manual
N/A	Version: 1.0.0 CP/CPS OID: 1.3.6.1.4.1.200198.1.10.2	Version: 1.0	Version: 1.0
September 26, 2007	Version: 1.10.0 CP/CPS OID: 0.2.440.200198.1.10.2	Version: 1.10	Version: 1.6
April 8, 2008	Version: 2.0.0 CP/CPS OID: 0.2.440.200198.1.10.1.2.0	Version: 2.0.0	Version: 1.7

1. Certificate Profile

1.1 CA Self Signed Certificate

Basic Fields

Version	
version	Type: Integer Value: 2 (version 3)
SerialNumber	
certificateSerialNumber	Type: Integer Value: Integer
signature	
algorithmIdentifier algorithm	sha1RSA (2048bit) 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: Printable String Value: JP
organizationName Type	Type: OID Value: 2 5 4 10
Value	Type: Printable String Value: KEK
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value: CRC
commonName type	Type: OID Value: 2 5 4 3
value	Type: Printable String Value: KEK GRID Certificate Authority
Subject	
countryName Type	Type: OID Value: 2 5 4 6
Value	Type: Printable String Value: JP
organizationName Type	Type: OID Value: 2 5 4 10

Value	Type: Printable String Value: KEK
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value: CRC
commonName type	Type: OID Value: 2 5 4 3
value	Type: Printable String Value: KEK GRID Certificate Authority
SubjectPublicKeyInfo	
s subjectPublicKeyInfo algorithmIdentifier algorithm	RSA (2048bit) 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= FALSE)	
KeyUsage	Type: Bit String Value: Certificate Sign, CRL Sign
basicConstraints (Critical= TRUE)	
BasicConstraints cA	Type: Boolean Value: True (CA)
PathLenConstraint	Type: Integer Value: NULL

1.2 Globus Server Certificate

Globus Server Certificate includes both host certificate and ldap certificate typically used in Grid environment with Globus Toolkit.

Basic Fields

Version	
version	Type: Integer Value: 2
SerialNumber	
c certificateSerialNumber	Type: Integer

	Value: Unique Integer
signature	
algorithmIdentifier algorithm	sha1RSA (1024bit) 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: Printable String Value: JP
organizationName type	Type: OID Value: 2 5 4 10
value	Type: Printable String Value: KEK
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value: CRC
commonName type	Type: OID Value: 2 5 4 3
value	Type: Printable String Value: KEK GRID Certificate Authority
Subject	
countryName type	Type: OID Value: 2 5 4 6
value	Type: Printable String Value: JP
organizationName type	Type: OID Value: 2 5 4 10
value	Type: Printable String Value: KEK
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value: CRC
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value:

optional commonName type	Type: OID Value: 2 5 4 3
value	Type: Printable String Value: <i>host/FQDN of the host (for host)</i> Value: <i>FQDN of the host (for host)</i> Value: <i>ldap/FQDN of the host (for ldap)</i>
SubjectPublicKeyInfo	
subjectPublicKeyInfo algorithmIdentifier algorithm	RSA(1024bit) 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: Bit String Value: Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
basicConstraints (Critical= TRUE)	
BasicConstraints cA	Type: Boolean Value: False
PathLenConstraint	Type: Integer Value: NULL
CertificatePolicies (Critical= FALSE)	
PolicyID	Type: OID Value: 0 2 440 200198 1 10 2
QualifierID	Type: OID Value: 1 3 6 1 5 5 7 2 1 (id-qt-cps)
Qualifier	Type: IA5 String Value: URI of the CP/CPS
CRLDistributionPoints (Critical= FALSE)	
cRLDistributionPoints	Type: IA5 String Value: URI of the CRL
IssuerAlternativeName (Critical= FALSE)	
issuerAltName	Type: IA5 String Value: URI of KEK GRID Certificate Authority
ExtendedkeyUsage (Critical= FALSE)	
extKeyUsage	Type: OID Value: 1.3.6.1.5.5.7.3.1 (Server Authentication) Value: 1.3.6.1.5.5.7.3.2 (Client Authentication)
SubjectAlternativeName (Critical= FALSE)	

subjectAltName optional	Type: Printable String Value:
----------------------------	----------------------------------

1.3 Globus Client Certificate

Basic Fields

Version	
version	Type: Integer Value: 2
SerialNumber	
certificateSerialNumber	Type: Integer Value: Unique Integer
signature	
algorithmIdentifier algorithm	sha1RSA (1024bit) 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: Printable String Value: JP
organizationName type	Type: OID Value: 2 5 4 10
value	Type: Printable String Value: KEK
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value: CRC
commonName type	Type: OID Value: 2 5 4 3
value	Type: Printable String Value: KEK GRID Certificate Authority
Subject	
countryName type	Type: OID Value: 2 5 4 6
value	Type: Printable String Value: JP
organizationName	

type	Type: OID Value: 2 5 4 10
value	Type: Printable String Value: KEK
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value: CRC
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value:
optional commonName type	Type: OID Value: 2 5 4 3
value	Type: Printable String Value:
SubjectPublicKeyInfo	
subjectPublicKeyInfo algorithmIdentifier algorithm	sha1RSA (1024bit) 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
PathLenConstraint	Type: Integer Value: NULL
keyUsage (Critical= TRUE)	
KeyUsage	Type: Bit String Value: Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment
CertificatePolicies (Critical= FALSE)	
PolicyID	Type: OID Value: 0 2 440 200198 1 10 2
QualifierID	Type: OID Value: 1 3 6 1 5 5 7 2 1 (id-qt-cps)
Qualifier	Type: IA5 String Value: URI of the CP/CPS

CRLDistributionPoints (Critical= FALSE)	
cRLDistributionPoints	Type: IA5 String Value: URI of the CRL
IssuerAlternativeName (Critical= FALSE)	
issuerAltName	Type: IA5 String Value: URI of KEK GRID Certificate Authority
ExtendedkeyUsage (Critical= FALSE)	
extKeyUsage	Type: OID Value: 1.3.6.1.5.5.7.3.2 (Client Authentication)
SubjectAlternativeName (Critical= FALSE)	
subjectAltName	Type: Printable String Value:
optional	

1.4 Web Server Certificate

Basic Fields

Version	
version	Type: Integer Value: 2
SerialNumber	
certificateSerialNumber	Type: Integer Value: Unique Integer
signature	
algorithmIdentifier algorithm	sha1RSA (1024bit) 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: Printable String Value: JP
organizationName type	Type: OID Value: 2 5 4 10
value	Type: Printable String Value: KEK
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value: CRC
commonName	

type	Type: OID Value: 2 5 4 3
value	Type: Printable String Value: KEK GRID Certificate Authority

Subject

countryName	Type: OID Value: 2 5 4 6
type	Type: Printable String Value: JP
value	
organizationName	Type: OID Value: 2 5 4 10
type	Type: Printable String Value: KEK
value	
organizationalUnitName	Type: OID Value: 2 5 4 11
type	Type: Printable String Value: CRC
value	
organizationalUnitName	Type: OID Value: 2 5 4 11
type	Type: Printable String Value:
value	
optional commonName	Type: OID Value: 2 5 4 3
type	Type: Printable String Value: <i>ServerName (for Web Server)</i>
value	

SubjectPublicKeyInfo

subjectPublicKeyInfo	sha1RSA (1024bit)
algorithmIdentifier	Type: OID Value: 1 2 840 113549 1 1 1
algorithm	Type: NULL Value: None
parameters	Type: Bit String Value: Public Key Value
subjectPublicKey	

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	Type: Boolean Value: False
cA	Type: Integer Value: NULL
PathLenConstraint	

keyUsage (Critical= TRUE)	
KeyUsage	Type: Bit String Value: 0xa8 (Digital Signature, key Encipherment, Key Agreement)
ExtendedKeyUsage (Critical= FALSE)	
extendedKeyUsage	Type: OID Value: 1 3 6 1 5 5 7 3 1 (Server Authentication)
Netscape Cert Type (Critical= FALSE)	
nsCertType	Type: Bit String Value: 0x40 (SSL Server)
Netscape Comment (Critical= FALSE)	
nsComment	Type: Printable String Value: SSL Server Certificate for Limited Purpose
CertificatePolicies (Critical= FALSE)	
PolicyID	Type: OID Value: 0 2 440 200198 1 10 2
QualifierID	Type: OID Value: 1 3 6 1 5 5 7 2 1 (id-qt-cps)
Qualifier	Type: IA5 String Value: URI of the CP/CPS
CRLDistributionPoints (Critical= FALSE)	
cRLDistributionPoints	Type: IA5 String Value: URI of the CRL
IssuerAlternativeName (Critical= FALSE)	
issuerAltName	Type: IA5 String Value: URI of KEK GRID Certificate Authority
SubjectAlternativeName (Critical= FALSE)	
subjectAltName	Type: Printable String Value:
optional	

2. Certificate Revocation List Profile

Basic Field

Version	
version	Type: Integer Value: 1
signature	
algorithmIdentifier algorithm	sha1RSA (2048bit) 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 30 days)
Issuer	
countryName type	Type: OID

value	Value: 2 5 4 6 Type: Printable String Value: JP
organizationName type	Type: OID Value: 2 5 4 10
value	Type: Printable String Value: KEK
organizationalUnitName type	Type: OID Value: 2 5 4 11
value	Type: Printable String Value: CRC
commonName type	Type: OID Value: 2 5 4 3
value	Type: Printable String Value: KEK GRID Certificate Authority
RevokedCertificates	
userCertificate	Type: Integer Value: Unique Integer
revocationDate	Type: UTC Time Value: YYMMDDHHMMSSZ
crlEntryExtensions reasonCode type	Type: OID Value: 2 5 29 21
value	Type: Enumerated unspecified(0), keyCompromise(1), cACompromise(2), affiliationChanged(3), superseded(4), cessationOfOperation(5), certificateHold(6), removeFromCRL(8), privilegeWithdrawn(9), aaCompromise(10)

Extension Fields

authorityKeyIdentifier (Critical= FALSE)	
KeyIdentifier	Type: Octet String Value: Unique Byte Strings
cRLNumber (Critical= FALSE)	
cRLNumber	Type: Integer Value: Unique Integer
issuingDistributionPoint (Critical = TRUE)	
DistributionPoint d istributionPointName	Type: IA5 String Value: URI of the CRL