National Center for High-performance Computing (NCHC)
Certificate and CRL Profile

Version 1.0

(November 22, 2005)

Contents

1. 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 Algorithm Parameters	sha1RSA(1024bit) Type: OID Value:1 2 840 113549 1 1 5 Type: NULL Value: None
Validity	
validity notBefore notAfter	 Type: UTC Time Value: yymmddhhmmssZ Type: UTC Time Value: yymmddhhmmssZ
Issuer	
countryName Type Value organizationName Type Value organizationalUnitName Type Value commonName Type Value	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: PrintableString Value: NCHC Type: OID Value: 2 5 4 11 Type: PrintableString Value: GOC Type: OID Value: 2 5 4 3 Type: PrintableString Value: NCHC CA
Subject	
countryName Type Value organizationName Type Value	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: PrintableString

	Value: NCHC
organizationalUnitName	
Type	Type: OID Value: 2 5 4 11
Value	Type: PrintableString Value: GOC
commonName	
Type	Type: OID Value: 2 5 4 3
Value	Type: PrintableString Value: NCHC CA
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 / Access Grid - Conference Host / Sensor Net Host / LDAP Certificate

Basic Fields

Version	
Version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Integer
Signature	
algorithmIdentifier Algorithm Parameters	sha1RSA(1024bit) Type: OID Value: 1 2 840 113549 1 1 5 Type: NULL Value: None
Validity	
Validity notBefore notAfter	 Type: UTC Time Value: yymmddhhmmssZ Type: UTC Time Value: yymmddhhmmssZ
Issuer	
countryName Type Value organizationName Type Value organizationalUnitName Type Value commonName Type Value	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: PrintableString Value: NCHC Type: OID Value: 2 5 4 11 Type: PrintableString Value: GOC Type: OID Value: 2 5 4 3 Type: PrintableString Value: NCHC CA
Subject	
countryName Type Value organizationName Type Value	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: PrintableString

	Value: NCHC
organizationalUnitName	
Type	Type: OID Value: 2 5 4 11
Value	Type: PrintableString Value: GOC
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 ladp)
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: Unique Byte Strings
KeyUsage (Critical = TRUE)	
KeyUsage	Type: BitString Value: Digital Signature, Key Encipherment
BasicConstraints (Critical = TRUE)	
BasicConstraints	
CA	Type: Boolean Value: False
CertificatePolicies (Critical = FALSE)	
PolicyID	Type: OID Value: (Refer CPS1.2)
QualifierID	Type: OID Value:（Refer CPS1.2）
Qualifier	Type: PrintableString Value: URI of the CP/CPS
CRLDistributionPoints (Critical = FALSE)	
CRLDistributionPoints	Type: PrintableString Value: URI of the CRL

3. Globus User / Access Grid - Conference User / Sensor Net User Certificates

Basic Fields

Version	
Version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique Integer
Signature	
algorithmIdentifier Algorithm Parameters	sha1RSA(1024bit) Type: OID Value: 1 2 840 113549 1 1 5 Type: NULL Value: None
Validity	
Validity notBefore notAfter	 Type: UTC Time Value: yymmddhhmmssZ Type: UTC Time Value: yymmddhhmmssZ
Issuer	
countryName Type Value organizationName Type Value organizationalUnitName Type Value commonName Type Value	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: Printable String Value: NCHC Type: OID Value: 2 5 4 11 Type: PrintableString Value: GOC Type: OID Value: 2 5 4 3 Type: PrintableString Value: NCHC CA
Subject	
countryName Type Value organizationName Type Value	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: PrintableString

	Value: NCHC
organizationalUnitName	
Type	Type: OID Value: 2 5 4 11
Value	Type: PrintableStirng Value: GOC
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: 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]
QualifierID	Type: OID Value: [Refer CPS1.2]
Qualifier	Type: PrintableString Value: URI of the CP/CPS
CRLDistributionPoints (Critical = FALSE)	
CRLDistributionPoints	Type: PrintableString Value: URI of the CRL

4. Unicore Host Certificate

Basic Fields

Version	
version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Integer
Signature	
algorithmIdentifier algorithm parameters	sha1RSA(1024bit) Type: OID Value: 1 2 840 113549 1 1 5 Type: NULL Value: None
Validity	
validity notBefore notAfter	 Type: UTC Time Value: yymmddhhmmssZ Type: UTC Time Value: yymmddhhmmssZ
Issuer	
countryName type value organizationName type value organizationalUnitName type value commonName type value	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: PrintableString Value: NCHC Type: OID Value: 2 5 4 11 Type: PrintableString Value: GOC Type: OID Value: 2 5 4 3 Type: PrintableString Value: NCHC CA
Subject	
countryName type value organizationName type value organizationalUnitName	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: PrintableString Value: NCHC

type	Type: OID Value: 2 5 4 11
value	Type: PrintableString Value: GOC
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 Byte Strings
SubjectKeyIdentifier (Critical = FALSE)	
SubjectKeyIdentifier	Type: OCTET STRING Value: Unique Byte Strings
KeyUsage (Critical = TRUE)	
KeyUsage	Type: BitString Value: Digital Signature, Key Encipherment
BasicConstraints (Critical = TRUE)	
BasicConstraints	
CA	Type: Boolean Value: False
CertificatePolicies (Critical = FALSE)	
PolicyID	Type: OID Value: (Refer CPS1.2)
QualifierID	Type: OID Value:（Refer CPS1.2）
Qualifier	Type: PrintableString Value: URI of the CP/CPS
CRLDistributionPoints (Critical = FALSE)	
CRLDistributionPoints	Type: PrintableString Value: URI of the CRL

5. Unicore User Certificates

Basic Fields

Version	
version	Type: INTEGER Value: 2
SerialNumber	
certificateSerialNumber	Type: INTEGER Value: Unique Integer
Signature	
algorithmIdentifier algorithm parameters	sha1RSA(1024bit) Type: OID Value: 1 2 840 113549 1 1 5 Type: NULL Value: None
Validity	
validity notBefore notAfter	 Type: UTC Time Value: yymmddhhmmssZ Type: UTC Time Value: yymmddhhmmssZ
Issuer	
countryName type value organizationName type value organizationalUnitName type value commonName type value	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: Printable String Value: NCHC Type: OID Value: 2 5 4 11 Type: PrintableString Value: GOC Type: OID Value: 2 5 4 3 Type: PrintableString Value: NCHC CA
Subject	
countryName type value organizationName type value organizationalUnitName	 Type: OID Value: 2 5 4 6 Type: PrintableString Value: TW Type: OID Value: 2 5 4 10 Type: PrintableString Value: NCHC

type	Type: OID Value: 2 5 4 11
value	Type: PrintableStirng Value: GOC
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)	
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]
QualifierID	Type: OID Value: [Refer CPS1.2]
Qualifier	Type: PrintableString Value: URI of the CP/CPS
CRLDistributionPoints (Critical = FALSE)	
CRLDistributionPoints	Type: PrintableString Value: URI of the CRL

2. CRL Profile

Basic Fields

Version	
version	Type:INTEGER Value:1
Signature	
algorithmIdentifier algorithm parameters	sha1RSA(1024bit) Type:OID Value:1 2 840 113549 1 1 5 Type:NULL Value:None
ThisUpdate	
thisUpdate	Type:UTC Time Value:yymmddhhmmssZ
NextUpdate	
nextUpdate	Type:UTC Time Value:yymmddhhmmssZ
Issuer	
countryName type value organizationName type value organizationalUnitName type value commonName type value	 Type:OID Value:2 5 4 6 Type:PrintableString Value:TW Type:OID Value:2 5 4 10 Type:PrintableString Value:NCHC Type:OID Value:2 5 4 11 Type:PrintableString Value:GOC Type:OID Value:2 5 4 3 Type:PrintableString Value:NCHC CA
RevokedCertificates	
userCertificate revocationDate crlEntryExtensions reasonCode	Type:INTEGER Value:Unique Integer Type:UTC Time Value:yymmddhhmmssZ Type:OID Value:2 5 29 21

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