# NECTEC-GOC CA
# Certificate and CRL Profile
# Version 1.0


**National Electronics and Computer Technology Center**

**October 2006**

# 1. Certificate Profile

## 1.1 Self Sign Certificate (CA Certificate)

### Basic Fields

| **Version** | |
|---|---|
| version | Type: INTEGER<br>Value:2 (version 3) |
| **Serial Number** | |
| CertificateSerialNumber | Type: INTEGER<br>Value: integer |
| **Signature** | |
| algorithmIdentifier | sha1RSA(2048bits) |
| algorithm | Type: OID<br>Value:1 2 840 113549 1 1 5 |
| parameters | Type: Null<br>Value: None |
| **Validity** | |
| validity | |
| notBefore | Type: UTC Time<br>Value: yymmddhhmmssZ |
| notAfter | Type: UTC Time<br>Value: yymmddhhmmssZ |
| **Issuer** | |
| countryName | |
| Type | Type: OID<br>Value: 2 5 4 6 |
| Value | Type: PrintableString<br>Value: TH |
| organizationName | |
| Type | Type: OID<br>Value: 2 5 4 10 |
| Value | Type: PrintableString<br>Value: NECTEC |
| organizationUnitName | |
| Type | Type: OID<br>Value: 2 5 4 11 |
| Value | Type: PrintableString<br>Value: GOC |

| | |
|---|---|
| commonName | |
| Type | Type: OID<br>Value: 2 5 4 3 |
| Value | Type: PrintableString<br>Value: NECTEC GOC CA |
| **Subject** | |
| countryName | |
| Type | Type: OID<br>Value: 2 5 4 6 |
| Value | Type: PrintableString<br>Value: TH |
| organizationName | |
| Type | Type: OID<br>Value: 2 5 4 10 |
| Value | Type: PrintableString<br>Value: NECTEC |
| organizationUnitName | |
| Type | Type: OID<br>Value: 2 5 4 11 |
| Value | Type: PrintableString<br>Value: GOC |
| commonName | |
| Type | Type: OID<br>Value: 2 5 4 3 |
| Value | Type: PrintableString<br>Value: NECTEC GOC CA |
| **SubjectPublicKeyInfo** | |
| subjectPublicKeyInfo | |
| algorithmIdentifier | RSA(2048bits) |
| algorithm | Type: OID<br>Value:1 2 840 113549 1 1 1 |
| parameters | Type: NULL<br>Value: None |
| subjectPublicKey | Type: BIT STRING<br>Value: Public Key Value |

**Extension Fields**

| **authorityKeyIdentifier (Critical=FALSE)** | |
|---|---|
| KeyIdentifier | Type: OCTEC STRING<br>Value: Byte Strings |

| **subjectKeyIdentifier (Critical=FALSE)** | |
|---|---|
| subjectKeyIdentifier | Type: OCTEC STRING<br>Value: Unique String |
| **keyUsage (Critical=TRUE)** | |
| keyUsage | Type: BitString<br>Value: crlSign, keyCertSign |
| **basicConstraints (Critical=TRUE)** | |
| basicConstraints | |
| CA | Type: Boolean<br>Value: TRUE (CA) |

## 1.2 Globus Host Certificate

### Basic Fields

| **Version** | |
|---|---|
| version | Type: INTEGER<br>Value:2 |
| **Serial Number** | |
| CertificateSerialNumber | Type: INTEGER<br>Value: Integer |
| **Signature** | |
| algorithmIdentifier | sha1RSA(1024bits) |
| algorithm | Type: OID<br>Value:1 2 840 113549 1 1 5 |
| parameters | Type: Null<br>Value: None |
| **Validity** | |
| Validity | |
| notBefore | Type: UTC Time<br>Value: yymmddhhmmssZ |
| notAfter | Type: UTC Time<br>Value: yymmddhhmmssZ |
| **Issuer** | |
| countryName | |
| Type | Type: OID<br>Value: 2 5 4 6 |
| Value | Type: PrintableString<br>Value: TH |
| organizationName | |

| | |
|---|---|
| Type | Type: OID<br>Value: 2 5 4 10 |
| Value | Type: PrintableString<br>Value: NECTEC |
| organizationUnitName | |
| Type | Type: OID<br>Value: 2 5 4 11 |
| Value | Type: PrintableString<br>Value: GOC |
| commonName | |
| Type | Type: OID<br>Value: 2 5 4 3 |
| Value | Type: PrintableString<br>Value: NECTEC GOC CA |
| **Subject** | |
| countryName | |
| Type | Type: OID<br>Value: 2 5 4 6 |
| Value | Type: PrintableString<br>Value: TH |
| organizationName | |
| Type | Type: OID<br>Value: 2 5 4 10 |
| Value | Type: PrintableString<br>Value: NECTEC |
| organizationUnitName | |
| Type | Type: OID<br>Value: 2 5 4 11 |
| Value | Type: PrintableString<br>Value: GOC |
| commonName | |
| Type | Type: OID<br>Value: 2 5 4 3 |
| Value | Type: PrintableString<br>Value: host/FQDN of the host (for host) |
| **SubjectPublicKeyInfo** | |
| subjectPublicKeyInfo | |
| algorithmIdentifier | RSA(1024bits) |
| algorithm | Type: OID<br>Value:1 2 840 113549 1 1 1 |
| parameters | Type: NULL<br>Value: None |

| | |
|---|---|
| subjectPublicKey | Type: BIT STRING<br>Value: Public Key Value |

**Extension Fields**

| **authorityKeyIdentifier (Critical=FALSE)** | |
|---|---|
| keyIdentifier | Type: OCTEC STRING<br>Value: Unique Byte Strings |
| **subjectKeyIdentifier (Critical=FALSE)** | |
| subjectKeyIdentifier | Type: OCTEC STRING<br>Value: Unique Byte Strings |
| **keyUsage (Critical=TRUE)** | |
| keyUsage | Type: BitString<br>Value: digitalSignature, keyEncipherment, dataEncipherment |
| **basicConstraints (Critical=TRUE)** | |
| basicConstraints | |
| CA | Type: Boolean<br>Value: FALSE |
| **extendedKeyUsage (Critical=FALSE)** | |
| extendedKeyUsage | Type: BitString<br>Value: serverAuth |
| **CertificatePolicies (Critical=FALSE)** | |
| policyIdentifier | Type: OID<br>Value: (Refer CPS 1.2) |
| CPS.1 | Type: IA5String<br>Value: URI of the NECTEC-GOC CA CP/CPS |
| **UserNotice (Critical=FALSE)** | |
| explicitText | Type: OCTEC String<br>Value: Byte Strings |
| **CRLDistributionPoints (Critical=FALSE)** | |
| CRLDistributionPoints | Type: IA5 String<br>Value: URI of CRL |
| **IssuerAlternativeName (Critical=FALSE)** | |
| IssuerAlternativeName | Type: PrintableString<br>Value: Email address of NECTEC-GOC CA |
| **SubjectAlternativeName (Critical=FALSE)** | |
| SubjectAlternativeName | Type: PrintableString<br>Value: FQDN |

## 1.3 Globus User Certificate

### Basic Fields

| **Version** | |
|---|---|
| version | Type:INTEGER<br>Value:2 |
| **Serial Number** | |
| CertificateSerialNumber | Type: INTEGER<br>Value: Unique Integer |
| **Signature** | |
| algorithmIdentifier | sha1RSA(1024bits) |
| algorithm | Type: OID<br>Value:1 2 840 113549 1 1 5 |
| parameters | Type: Null<br>Value: None |
| **Validity** | |
| Validity | |
| notBefore | Type: UTC Time<br>Value: yymmddhhmmssZ |
| notAfter | Type: UTC Time<br>Value: yymmddhhmmssZ |
| **Issuer** | |
| countryName | |
| Type | Type: OID<br>Value: 2 5 4 6 |
| Value | Type: PrintableString<br>Value: TH |
| organizationName | |
| Type | Type: OID<br>Value: 2 5 4 10 |
| Value | Type: PrintableString<br>Value: NECTEC |
| organizationUnitName | |
| Type | Type: OID<br>Value: 2 5 4 11 |
| Value | Type: PrintableString<br>Value: GOC |
| commonName | |
| Type | Type: OID<br>Value: 2 5 4 3 |

| | |
|---|---|
| Value | Type: PrintableString<br>Value: NECTEC GOC CA |
| **Subject** | |
| countryName | |
| Type | Type: OID<br>Value: 2 5 4 6 |
| Value | Type: PrintableString<br>Value: TH |
| organizationName | |
| Type | Type: OID<br>Value: 2 5 4 10 |
| Value | Type: PrintableString<br>Value: NECTEC |
| organizationUnitName | |
| Type | Type: OID<br>Value: 2 5 4 11 |
| Value | Type: PrintableString<br>Value: GOC |
| commonName | |
| Type | Type: OID<br>Value: 2 5 4 3 |
| Value | Type: PrintableString<br>Value: |
| Pkcs9email | |
| Type | Type: OID<br>Value: 1 2 840 113549 1 9 1 |
| Value | Type: IA5String<br>Value: |
| optional | |
| **SubjectPublicKeyInfo** | |
| subjectPublicKeyInfo | |
| algorithmIdentifier | RSA(1024bits) |
| algorithm | Type: OID<br>Value:1 2 840 113549 1 1 1 |
| parameters | Type: NULL<br>Value: None |
| subjectPublicKey | Type: BIT STRING<br>Value: Public Key Value |

**Extension Fields**

| **authorityKeyIdentifier (Critical=FALSE)** | |
|---|---|
| keyIdentifier | Type: OCTEC STRING<br>Value: Byte Strings |
| **subjectKeyIdentifier (Critical=FALSE)** | |
| subjectKeyIdentifier | Type: OCTEC STRING<br>Value: Unique String |
| **keyUsage (Critical=TRUE)** | |
| keyUsage | Type: BitString<br>Value: nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment |
| **basicConstraints (Critical=TRUE)** | |
| basicConstraints | |
| CA | Type: Boolean<br>Value: FALSE |
| **extendedKeyUsage (Critical=FALSE)** | |
| extendedKeyUsage | Type: BitString<br>Value: clientAuth |
| **CertificatePolicies (Critical=FALSE)** | |
| policyIdentifier | Type: OID<br>Value: (Refer CPS 1.2) |
| CPS.1 | Type: IA5String<br>Value: URI of the NECTEC-GOC CA CP/CPS |
| **UserNotice (Critical=FALSE)** | |
| explicitText | Type: OCTEC String<br>Value: Byte Strings |
| **CRLDistributionPoints (Critical=FALSE)** | |
| CRLDistributionPoints | Type: IA5 String<br>Value: URI of CRL |
| **IssuerAlternativeName (Critical=FALSE)** | |
| IssuerAlternativeName | Type: PrintableString<br>Value: Email address of NECTEC-GOC CA |
| **SubjectAlternativeName (Critical=FALSE)** | |
| subjectAlternativeName | Type: PrintableString<br>Value: Email Address of User |

# 2 CRL Profile

### Basic Fields

| **Version** | |
|---|---|
| version | Type: INTEGER<br>Value:1 |
| **Signature** | |
| algorithmIdentifier | sha1RSA(1024bits) |
| algorithm | Type: OID<br>Value:1 2 840 113549 1 1 5 |
| parameters | Type: Null<br>Value: None |
| **ThisUpdate** | |
| thisUpdate | Type: UTC Time<br>Value: yymmddhhmmssZ |
| **NextUpdate** | |
| nextUpdate | Type: UTC Time<br>Value: yymmddhhmmssZ |
| **Issuer** | |
| countryName | |
| Type | Type: OID<br>Value: 2 5 4 6 |
| Value | Type: PrintableString<br>Value: TH |
| organizationName | |
| Type | Type: OID<br>Value: 2 5 4 10 |
| Value | Type: PrintableString<br>Value: NECTEC |
| organizationUnitName | |
| Type | Type: OID<br>Value: 2 5 4 11 |
| Value | Type: PrintableString<br>Value: GOC |
| commonName | |
| Type | Type: OID<br>Value: 2 5 4 3 |
| Value | Type: PrintableString<br>Value: NECTEC GOC CA |

| **revokedCertificates** | |
|---|---|
| userCertificate | Type: INTEGER<br>Value: Unique Integer |
| revocationDate | Type: UTC Time<br>Value: yymmddhhmmssZ |
| crlEntryExtensions | Type: OID<br>Value:2 5 29 21 |
| reasonCode | Type: ENUMERATED<br>Value: unspecified(0), keyCompromise(1), cACompromise(2), affiliationChanged(3),superseded(4), cessationOfOperation(5), certificateHold(6),removeFromCRL(7), privilegeWithdrawn(9), asaCompromise(10) |

## 2.2 Extensions

| **authorityKeyIdentifier (Critical=FALSE)** | |
|---|---|
| KeyIdentifier | Type: OCTEC String<br>Value: |
| **cRLNumber (Critical=FALSE)** | |
| cRLNumber | Type: INTEGER<br>Value: integer |
| **issuingDistributionPoints (Critical=TRUE)** | |
| DistributionPoints | |
| distributionPointName | Type:IA5 String<br>Value: URL of the CRL |

# Bibliography

**[RFC3280]**

R. Housley, W. Polk, W. Ford and D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, April 2002.