```
rsaPublicKey ALGORITHM-ID ::= { OID rsaEncryption PARMS NULL }

rsaSHA-1 ALGORITHM-ID ::= { OID sha1WithRSAEncryption PARMS NULL }

rsaSHA-256 ALGORITHM-ID ::= { OID sha256WithRSAEncryption PARMS NULL }

sha1Identifier ALGORITHM-ID ::= { OID id-SHA1 PARMS NULL }

sha256Identifier ALGORITHM-ID ::= { OID id-SHA256 PARMS NULL }

pkcs-1 OBJECT IDENTIFIER ::= {
     iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }

rsaEncryption OBJECT IDENTIFIER ::=  { pkcs-1 1 }
-- subjectPublicKey syntax
RSAPublicKey  ::=  SEQUENCE  {
     modulus INTEGER,        -- n
     publicExponent INTEGER -- e
}

sha1WithRSAEncryption OBJECT IDENTIFIER  ::=  { pkcs-1 5 }

sha256WithRSAEncryption OBJECT IDENTIFIER  ::=  { pkcs-1 11 }

id-SHA1 OBJECT IDENTIFIER ::= {
     iso(1) identified-organization(3) oiw(14) secsig(3) algorithms(2) 26 }

id-SHA256 OBJECT IDENTIFIER ::= {
     joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101)
     csor(3) nistalgorithm(4) hashalgs(2) 1 }

SubjectPublicKeyInfo ::= SEQUENCE{
   algorithm            AlgorithmIdentifier,
   subjectPublicKey     BIT STRING }

Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension

Extension ::= SEQUENCE {
   extnId            EXTENSION.&id ({ExtensionSet}),
   critical          BOOLEAN DEFAULT FALSE,
   extnValue         OCTET STRING }

ExtensionSet  EXTENSION  ::= { registeredCorporationInfo }

EXTENSION ::= CLASS {
   &id          OBJECT IDENTIFIER UNIQUE,
   &ExtnType }
WITH SYNTAX  {
   SYNTAX               &ExtnType
   IDENTIFIED BY        &id }

AttributeTypeAndValue ::= SEQUENCE {
        type    ATTRIBUTE.&id ({SupportedAttributes}),
        value   ATTRIBUTE.&Type ({SupportedAttributes}{@type})}

Name ::= CHOICE {
        rdnSequence  RDNSequence
}

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::= SET SIZE (1 .. MAX) OF AttributeTypeAndValue

ID ::= OBJECT IDENTIFIER

ATTRIBUTE ::= CLASS {
        &Type,
        &id     OBJECT IDENTIFIER UNIQUE }
WITH SYNTAX {
        WITH SYNTAX &Type
        ID          &id }

SupportedAttributes ATTRIBUTE ::= {
        commonName | organizationName |   -- RelativeDistinguishedName attributes
        timeLimit | suspensionSecretCode  -- regInfo attributes
}

commonName ATTRIBUTE ::= {
        WITH SYNTAX        DirectoryString {ub-common-name}
        ID                 id-at-commonName }

organizationName ATTRIBUTE ::= {
        WITH SYNTAX        DirectoryString {ub-organization-name}
        ID                 id-at-organizationName }

DirectoryString { INTEGER:maxSize } ::= CHOICE {
        printableString         PrintableString (SIZE (1..maxSize)),
        utf8String              UTF8String (SIZE(1..maxSize))
}

timeLimit ATTRIBUTE ::= {
```