```
    &id    OBJECT IDENTIFIER UNIQUE,
    &Type  OPTIONAL
}
WITH SYNTAX { OID &id [PARMS &Type] }

SupportedAlgorithms ALGORITHM-ID ::= { ..., -- extensible
                                       rsaPublicKey |
                                       rsaSHA-1 |
                                       rsaSHA-256 }

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

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

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

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 | countryName | organizationName | organizationalUnitName }

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

countryName ATTRIBUTE ::= {
        WITH SYNTAX        PrintableString (SIZE (2))
        ID                 id-at-countryName }

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

organizationalUnitName ATTRIBUTE ::= {
        WITH SYNTAX        DirectoryString {ub-organizational-unit-name}
        ID                 id-at-organizationalUnitName }

id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}

id-at-commonName              OBJECT IDENTIFIER ::= {id-at 3}
id-at-countryName             OBJECT IDENTIFIER ::= {id-at 6}
id-at-organizationName        OBJECT IDENTIFIER ::= {id-at 10}
id-at-organizationalUnitName  OBJECT IDENTIFIER ::= {id-at 11}

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

ub-common-name               INTEGER ::= 64
ub-organization-name         INTEGER ::= 64
ub-organizational-unit-name  INTEGER ::= 64

END
```

2　Implicitly Tagged Module

```
MOJCorpCertImplicit { 1 2 392 100300 1 4 2 }
```