# The F.A.T.Book

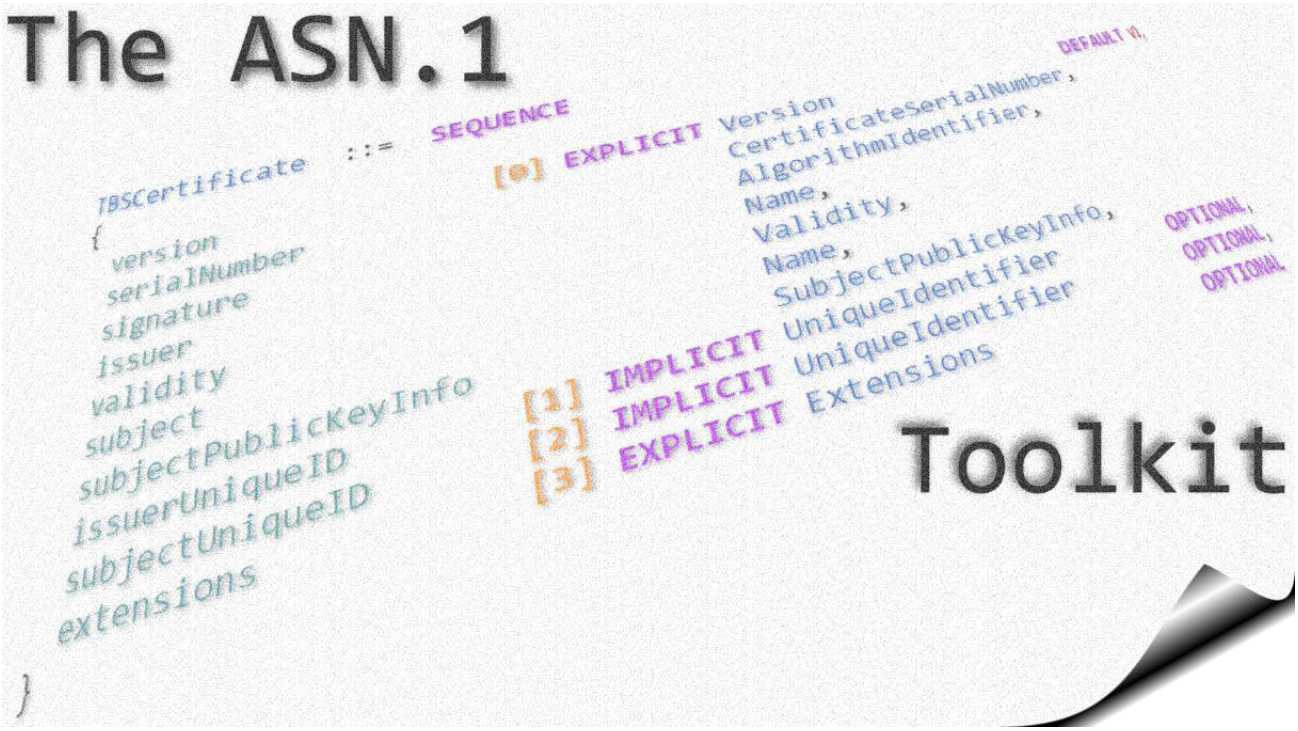
## *The **F**amous **A**SN.1 **T**ypes Book*

## *(and ASN.1 value definitions)*

*A cross-reference of cryptography- and PKI-related ASN.1 structures (types) and pre-defined values*

Version 1.1 dated 09/11/2024

*written by Ingo A. Kubbilun (Germany, Europe, Planet Earth)*



## DISCLAIMER

THE DOCUMENT IN-HAND AND ANY RELATED SOFTWARE IS PROVIDED BY **THE AUTHOR** "*AS IS*" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION).

# Document revision

| Version: | Date: | Author: | Comments / changes: |
|---|---|---|---|
| 0.1 | 12/22/2023 | Ingo A. Kubbilun | document creation |
| 1.0 | 01/21/2024 | Ingo A. Kubbilun | 1st published version |
| 1.1 | 09/11/2024 | Ingo A. Kubbilun | PDF link in TBSCertificate (version) fixed |
| | | | |

# Table of Contents

# List of Tables

# List of Figures

# Web resources / bibliography

| Tag | Description | URL |
|---|---|---|
| [ITU-T X.680] | Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation | https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.680-201508-I!!PDF-E&type=items |
| [ITU-T X.690] | Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) | https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.690-201508-I!!PDF-E&type=items |
| | | |
| | | |

# Acronyms & Abbreviations

| Acronym | Meaning |
|---|---|
| ASN.1 | Abstract Syntax Notation ONE (ITU-T X.680 series of specifications) |
| BER | Basic Encoding Rules (ITU-T X.690) |
| DER | Distinguished Encoding Rules (ITU-T X.690) |
| | |

# 1 Introduction

This is the '*F.A.T.Book*', the book of '***famous ASN.1 types***' (**and values**). You can simply call it '*The FATBook*'.

It is a cross-reference of 417 ASN.1 (famous) types and 392 ASN.1 (famous) value definitions.

What is the 'added value' of this document? All ASN.1 types are pretty-printed with full in-document links so that you can trace a specific ASN.1 type definition down to its simple parts. The ASN.1 type and value definitions in this document are spread over many RFCs and other specifications – this document consolidates all of these types and values in a single PDF.

Furthermore, each ASN.1 type definition comes with the hexadecimal ASN.1 tags printed in the first column of a type definition. So, for instance, if you use a simple ASN.1 dump tool, you can use the ASN.1 type definitions in this document to 'understand' what you are currently seeing, which parts of a type are simply 'not there' because of DEFAULT and OPTIONAL ASN.1 clauses, etc.

Please do read the introduction of chapter 2 beginning on page 35 for details.

Chapter 3 beginning on page 157 presents all ASN.1 value definitions found in the standards and specifications mentioned above.

The full DER encoding of all values is presented in a subsection of that value definition. If you think that you do not need such kind of information, then please have a look at section 3.304 (page 260) *"ASN.1 value 'rSASSA-PSS-Default-Params'"*: An X.509v3 certificate signed by a Certification Authority using the (default) RSA-PSS algorithm would 'show' you just an empty ASN.1 sequence (encoding `0x30,0x00`) in an ASN.1 dump tool for the signature algorithm parameters. In fact, this empty ASN.1 sequence stands for:

- Hash algorithm is SHA-1;
- Mask generation algorithm is mgf1 with SHA-1;
- Salt length is 20 bytes;
- Trailer field 'BC' is used.

The ASN.1 sequence is empty because all default values are in effect. The document in-hand illustrates you in these cases, '*what is going on*'.

## 1.1 Who should read/use this reference?

This reference is dedicated to people working with ASN.1, writing software that makes use of ASN.1 BER/DER encodings or just people interested in ASN.1.

### 1.1.1 Required knowledge

You **SHOULD** be familiar with (can be easily looked up in the World Wide Web):

- Abstract Syntax Notation ONE (ASN.1);

- what a T-L-V is (tag – length – value);
- BER/DER encodings;
- what implicit or explicit tagging is, respectively;
- two's complement (to understand why a specific ASN.1 integer value is represented as presented in this reference);

### 1.1.2 Optional / additional knowledge

You **MAY** be familiar with:

- PKIX standards;
- PKCS standards (Public Key Cryptography Standards) – PKCS#1, PKCS#5, PKCS#8, PKCS#9, PKCS#10, and PKCS#12
- Public Key Infrastructures (in general);
- X.509v3 digital certificates and certificate revocation lists (CRLs);
- LDAP (Lightweight Directory Access Protocol);
- OCSP (Online Certificate Status Protocol);
- CMP and CRMF (Certificate Manage Protocol and Certificate Request Message Format);
- public key algorithms, e.g. DSA, RSA, DH, ECDSA, ECDH, EdDSA, other…
- card verifiable certificates (CV certificates according to ISO 7816 standards track).

## 1.2 Typography and colors

The content of this document was generated in a semi-automated way. The software I am currently finishing (will be published on github in the near future) is a so called 'SimpleASN.1 parser' ('*simplified ASN.1*') that generates a symbolic ASN.1 database out of simplified ASN.1 source (definitions), which are 'understandable' by the stupid parser I wrote.

The ASN.1 database is the foundation of a symbolic ASN.1 dump tool and a full software suite called '*The ASN.1 toolkit*" (see https://www.asn1toolkit.org).

I decided to use the symbolic ASN.1 database to generate this reference as the very first publication of my (home) work.

The ASN.1 toolkit emits Rich Text Format documents as well as HTML and of course plain text output. I converted the HTML output to the MS word DOCX format. To my regret, I could not find a single software on this planet that could perform the job fully automated. Many additional hours of stupid, additional formatting have been invested in the document in-hand. In version 1.0 of the document, they are formatting bugs – this is for sure. But the content should be accurate, though.

The *'color code'* is summarized by Table 1 (the font is always the monotype Consolas font, 11pt[1]):

| Content: | Appearance: | Example: |
|---|---|---|
| ASN.1 keyword/ built-in type | bold+magenta | `INTEGER` |
| type name | bold+blue | `TBSCertificate` (first letter should be capital) |
| component names in constructed types | dark cyan | `hashAlgorithm` |
| ASN.1 remarks | italic+green | (introduced by the ASN.1 typical two hyphens)<br>`-- this is a remark` |
| ASN.1 tag numbers | bold+orange | `[0]` |
| ASN.1 values and constants | bold+red | `sha1Identifier, v1` |

**Table 1: Colors, bold, and italic used in this document.**

Although there is no direct (static) visual feedback for document links (e.g. the often-used underlining), just hover with your mouse over text content and the mouse shape changes if you can follow an in-document link.

## 1.3 Important remark

PLEASE SAVE THE ENVIRONMENT –
PLEASE **DO NOT** PRINT THIS BOOK.

[1] In rare cases, the point size is reduced to 10, 9 or 8 points if the definition is too wide.

# 2 ASN.1 type definitions

This chapter presents all ASN.1 types that are part of the symbolic ASN.1 database generated by the SimplASN.1 (simplified ASN.1) parser.

The left-hand side of a type definition shows the ASN.1 tags associated with a row. Because of the conversion from HTML to DOCX, there is a small vertical offset in the table.

If there is an explicit ASN.1 tag followed by the (implicit) tag, then the secondary tag is displayed in square brackets.

Two special tokens may be shown here:

1. '**CHO**' if the ASN.1 type is a CHOICE, which is some kind of 'virtual type' that does not have an ASN.1 tag associated with it. The ASN.1 tag of the CHOICE is the ASN.1 tag of the actual choice taken;
2. '**ANY**' if the ASN.1 type is an ANY type without an explicit tag. The actual ASN.1 tag depends on the actual ASN.1 type selected.

## 2.1 ASN.1 type 'AAControls'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30  AAControls ::= SEQUENCE
    {
02    pathLenConstraint              INTEGER  (0..MAX) OPTIONAL,
A0    permittedAttrs    [0] IMPLICIT AttrSpec OPTIONAL,
A1    excludedAttrs     [1] IMPLICIT AttrSpec OPTIONAL,
01    permitUnSpecified              BOOLEAN  DEFAULT TRUE
    }
```

## 2.2 ASN.1 type 'ACClearAttrs'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
 30  ACClearAttrs ::= SEQUENCE
     {
CHO    acIssuer GeneralName,
 02    acSerial INTEGER,
 30    attrs    SEQUENCE OF Attribute
     }
```

## 2.3 ASN.1 type 'AbandonRequest'

Source of definition: 'LDAP (RFC 4511)'

```
AbandonRequest ::= [APPLICATION 16] IMPLICIT MessageID
```

## 2.4 ASN.1 type 'AcceptableResponses'

Source of definition: 'OCSP (RFC 6960)'

```
AcceptableResponses ::= SEQUENCE OF OBJECT IDENTIFIER
```

## 2.5 ASN.1 type 'AccessDescription'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
AccessDescription ::= SEQUENCE
{
  accessMethod   OBJECT IDENTIFIER,
  accessLocation GeneralName
}
```

## 2.6 ASN.1 type 'AddRequest'

Source of definition: 'LDAP (RFC 4511)'

```
AddRequest ::= [APPLICATION 8] IMPLICIT SEQUENCE
{
  entry      LDAPDN,
  attributes AttributeList
}
```

## 2.7 ASN.1 type 'AddResponse'

Source of definition: 'LDAP (RFC 4511)'

```
69 AddResponse ::= [APPLICATION 9] IMPLICIT LDAPResult
```

## 2.8 ASN.1 type 'AdministrationDomainName'

Source of definition: 'CRL structures'

```
62 AdministrationDomainName ::= [APPLICATION 2] EXPLICIT CHOICE
   {
12   numeric   NumericString   (SIZE (0..ub-domain-name-length)),
13   printable PrintableString (SIZE (0..ub-domain-name-length))
   }
```

## 2.9 ASN.1 type 'AlgorithmIdentifier'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
30 AlgorithmIdentifier ::= SEQUENCE
   {
06   algorithm  OBJECT IDENTIFIER,
ANY  parameters ANY               OPTIONAL
   }
```

## 2.10 ASN.1 type 'AnotherName'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 AnotherName ::= SEQUENCE
   {
06   type-id              OBJECT IDENTIFIER,
A0   value   [0] EXPLICIT ANY
   }
```

## 2.11 ASN.1 type 'ArchiveCutoff'

Source of definition: 'OCSP (RFC 6960)'

```
18 ArchiveCutoff ::= GeneralizedTime
```

## 2.12 ASN.1 type 'AssertionValue'

Source of definition: 'LDAP (RFC 4511)'

```
04 AssertionValue ::= OCTET STRING
```

## 2.13 ASN.1 type 'AttCertIssuer'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
CHO AttCertIssuer ::= CHOICE
    {
 30   v1Form              GeneralNames,
 A0   v2Form [0] IMPLICIT V2Form
    }
```

## 2.14 ASN.1 type 'AttCertValidityPeriod'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 AttCertValidityPeriod ::= SEQUENCE
   {
18   notBeforeTime GeneralizedTime,
18   notAfterTime  GeneralizedTime
   }
```

## 2.15 ASN.1 type 'AttCertVersion'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
AttCertVersion ::= INTEGER
{
  v2(1)
}
```

## 2.16 ASN.1 type 'AttCertVersionV1'

Source of definition: 'AttributeCertificateVersion1 (RFC 5662)'

```
AttCertVersionV1 ::= INTEGER
{
  v1(0)
}
```

## 2.17 ASN.1 type 'AttrSpec'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
AttrSpec ::= SEQUENCE OF OBJECT IDENTIFIER
```

## 2.18 ASN.1 type 'Attribute'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
Attribute ::= SEQUENCE
{
  type   AttributeType,
  values SET OF AttributeValue
}
```

## 2.19 ASN.1 type 'AttributeCertificate'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 AttributeCertificate ::= SEQUENCE
   {
30   acinfo              AttributeCertificateInfo,
30   signatureAlgorithm  AlgorithmIdentifier,
03   signatureValue      BIT STRING
   }
```

## 2.20 ASN.1 type 'AttributeCertificateInfo'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
 30 AttributeCertificateInfo ::= SEQUENCE
    {
 02   version                 AttCertVersion,
 30   holder                  Holder,
CHO   issuer                  AttCertIssuer,
 30   signature               AlgorithmIdentifier,
 02   serialNumber            CertificateSerialNumber,
 30   attrCertValidityPeriod  AttCertValidityPeriod,
 30   attributes              SEQUENCE OF Attribute,
 03   issuerUniqueID          UniqueIdentifier        OPTIONAL,
 30   extensions              Extensions              OPTIONAL
    }
```

## 2.21 ASN.1 type 'AttributeCertificateInfoV1'

Source of definition: 'AttributeCertificateVersion1 (RFC 5662)'

```
    30 AttributeCertificateInfoV1 ::= SEQUENCE
       {
    02   version               AttCertVersionV1        DEFAULT v1,
   CHO   subject               CHOICE
         {
A0[30]     baseCertificateID [0] EXPLICIT IssuerSerial,
A1[30]     subjectName       [1] EXPLICIT GeneralNames
         },
    30   issuer                GeneralNames,
    30   signature             AlgorithmIdentifier,
    02   serialNumber          CertificateSerialNumber,
    30   attCertValidityPeriod AttCertValidityPeriod,
    30   attributes            SEQUENCE OF Attribute,
    03   issuerUniqueID        UniqueIdentifier        OPTIONAL,
    30   extensions            Extensions              OPTIONAL
       }
```

## 2.22 ASN.1 type 'AttributeCertificateV1'

Source of definition: 'AttributeCertificateVersion1 (RFC 5662)'

```
30 AttributeCertificateV1 ::= SEQUENCE
   {
30   acInfo              AttributeCertificateInfoV1,
30   signatureAlgorithm  AlgorithmIdentifier,
03   signature           BIT STRING
   }
```

## 2.23 ASN.1 type 'AttributeCertificateV2'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 AttributeCertificateV2 ::= AttributeCertificate
```

## 2.24 ASN.1 type 'AttributeDescription'

Source of definition: 'LDAP (RFC 4511)'

```
04 AttributeDescription ::= LDAPString
```

## 2.25 ASN.1 type 'AttributeList'

Source of definition: 'LDAP (RFC 4511)'

```
30 AttributeList ::= SEQUENCE OF LDAPAttribute
```

## 2.26 ASN.1 type 'AttributeSelection'

Source of definition: 'LDAP (RFC 4511)'

```
30 AttributeSelection ::= SEQUENCE OF LDAPString
```

## 2.27 ASN.1 type 'AttributeSet'

Source of definition: 'PKCS #8'

```
31 AttributeSet ::= SET OF Attribute
```

## 2.28 ASN.1 type 'AttributeType'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
06 AttributeType ::= OBJECT IDENTIFIER
```

## 2.29 ASN.1 type 'AttributeTypeAndValue'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
30 AttributeTypeAndValue ::= SEQUENCE
   {
06   type  AttributeType,
ANY  value AttributeValue
   }
```

## 2.30 ASN.1 type 'AttributeValue'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
ANY AttributeValue ::= ANY
```

## 2.31 ASN.1 type 'AttributeValueAssertion'

Source of definition: 'LDAP (RFC 4511)'

```
30 AttributeValueAssertion ::= SEQUENCE
   {
04   attributeDesc  AttributeDescription,
04   assertionValue AssertionValue
   }
```

## 2.32 ASN.1 type 'Attributes'

Source of definition: 'PKCS #10'

```
31 Attributes ::= SET OF Attribute
```

## 2.33 ASN.1 type 'AuthAttributes'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 AuthAttributes ::= SET SIZE (1..MAX) OF Attribute
```

## 2.34 ASN.1 type 'AuthenticatedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 AuthenticatedData ::= SEQUENCE
   {
02   version                     CMSVersion,
A0   originatorInfo   [0] IMPLICIT OriginatorInfo                    OPTIONAL,
31   recipientInfos               RecipientInfos,
30   macAlgorithm                 MessageAuthenticationCodeAlgorithm,
A1   digestAlgorithm  [1] IMPLICIT DigestAlgorithmIdentifier         OPTIONAL,
30   encapContentInfo             EncapsulatedContentInfo,
A2   authAttrs        [2] IMPLICIT AuthAttributes                    OPTIONAL,
04   mac                          MessageAuthenticationCode,
A3   unauthAttrs      [3] IMPLICIT UnauthAttributes                  OPTIONAL
   }
```

## 2.35 ASN.1 type 'AuthenticatedSafe'

Source of definition: 'PKCS #12'

```
30 AuthenticatedSafe ::= SEQUENCE OF ContentInfo
```

## 2.36 ASN.1 type 'AuthenticationChoice'

Source of definition: 'LDAP (RFC 4511)'

```
CHO AuthenticationChoice ::= CHOICE
    {
80    simple [0] IMPLICIT OCTET STRING,
A3    sasl   [3] IMPLICIT SaslCredentials
    }
```

## 2.37 ASN.1 type 'Authenticator'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
0C Authenticator ::= UTF8String
```

## 2.38 ASN.1 type 'AuthorityInfoAccessSyntax'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 AuthorityInfoAccessSyntax ::= SEQUENCE SIZE (1..MAX) OF AccessDescription
```

## 2.39 ASN.1 type 'AuthorityKeyIdentifier'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 AuthorityKeyIdentifier ::= SEQUENCE
   {
80   keyIdentifier             [0] IMPLICIT KeyIdentifier           OPTIONAL,
A1   authorityCertIssuer       [1] IMPLICIT GeneralNames            OPTIONAL,
82   authorityCertSerialNumber [2] IMPLICIT CertificateSerialNumber OPTIONAL
   }
```

## 2.40 ASN.1 type 'BaseCRLNumber'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
02 BaseCRLNumber ::= CRLNumber
```

## 2.41 ASN.1 type 'BaseDistance'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
02 BaseDistance ::= INTEGER (0..MAX)
```

## 2.42 ASN.1 type 'BasicConstraints'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 BasicConstraints ::= SEQUENCE
   {
01   cA                 BOOLEAN DEFAULT FALSE,
02   pathLenConstraint  INTEGER (0..MAX) OPTIONAL
   }
```

## 2.43 ASN.1 type 'BasicOCSPResponse'

Source of definition: 'OCSP (RFC 6960)'

```
   30 BasicOCSPResponse ::= SEQUENCE
      {
   30   tbsResponseData                ResponseData,
   30   signatureAlgorithm             AlgorithmIdentifier,
   03   signature                      BIT STRING,
A0[30]  certs             [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL
      }
```

## 2.44 ASN.1 type 'BindRequest'

Source of definition: 'LDAP (RFC 4511)'

```
60 BindRequest ::= [APPLICATION 0] IMPLICIT SEQUENCE
   {
02   version        INTEGER              (1..127),
04   name           LDAPDN,
CHO  authentication AuthenticationChoice
   }
```

## 2.45 ASN.1 type 'BindResponse'

Source of definition: 'LDAP (RFC 4511)'

```
61 BindResponse ::= [APPLICATION 1] IMPLICIT SEQUENCE
   {
0A   resultCode                     ENUMERATED
     {
       success(0),
       operationsError(1),
       protocolError(2),
       timeLimitExceeded(3),
       sizeLimitExceeded(4),
       compareFalse(5),
       compareTrue(6),
       authMethodNotSupported(7),
       strongerAuthRequired(8),
       referral(10),
       adminLimitExceeded(11),
       unavailableCriticalExtension(12),
       confidentialityRequired(13),
       saslBindInProgress(14),
       noSuchAttribute(16),
       undefinedAttributeType(17),
       inappropriateMatching(18),
       constraintViolation(19),
       attributeOrValueExists(20),
       invalidAttributeSyntax(21),
       noSuchObject(32),
       aliasProblem(33),
       invalidDNSyntax(34),
       aliasDereferencingProblem(36),
       inappropriateAuthentication(48),
       invalidCredentials(49),
       insufficientAccessRights(50),
       busy(51),
       unavailable(52),
       unwillingToPerform(53),
       loopDetect(54),
       namingViolation(64),
       objectClassViolation(65),
       notAllowedOnNonLeaf(66),
       notAllowedOnRDN(67),
       entryAlreadyExists(68),
       objectClassModsProhibited(69),
       affectsMultipleDSAs(71),
```

```
    other(80)
  },
04  matchedDN                       LDAPDN,
04  diagnosticMessage               LDAPString,
A3  referral          [3] IMPLICIT Referral     OPTIONAL,
87  serverSaslCreds   [7] IMPLICIT OCTET STRING OPTIONAL
}
```

## 2.46 ASN.1 type 'BuiltInDomainDefinedAttribute'

Source of definition: 'CRL structures'

```
30 BuiltInDomainDefinedAttribute ::= SEQUENCE
{
13  type  PrintableString (SIZE (1..ub-domain-defined-attribute-type-length)),
13  value PrintableString (SIZE (1..ub-domain-defined-attribute-value-length))
}
```

## 2.47 ASN.1 type 'BuiltInDomainDefinedAttributes'

Source of definition: 'CRL structures'

```
30 BuiltInDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF BuiltInDomainDefinedAttribute
```

## 2.48 ASN.1 type 'BuiltInStandardAttributes'

Source of definition: 'CRL structures'

```
30 BuiltInStandardAttributes ::= SEQUENCE
   {
61   country-name                          CountryName              OPTIONAL,
62   administration-domain-name             AdministrationDomainName OPTIONAL,
80   network-address            [0] IMPLICIT NetworkAddress           OPTIONAL,
81   terminal-identifier        [1] IMPLICIT TerminalIdentifier       OPTIONAL,
A2   private-domain-name        [2] EXPLICIT PrivateDomainName        OPTIONAL,
83   organization-name          [3] IMPLICIT OrganizationName         OPTIONAL,
84   numeric-user-identifier    [4] IMPLICIT NumericUserIdentifier    OPTIONAL,
A5   personal-name              [5] IMPLICIT PersonalName             OPTIONAL,
A6   organizational-unit-names  [6] IMPLICIT OrganizationalUnitNames  OPTIONAL
   }
```

## 2.49 ASN.1 type 'CAKeyUpdAnnContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
 30 CAKeyUpdAnnContent ::= SEQUENCE
    {
CHO   oldWithNew CMPCertificate,
CHO   newWithOld CMPCertificate,
CHO   newWithNew CMPCertificate
    }
```

## 2.50 ASN.1 type 'CMPCertStatus'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 CMPCertStatus ::= SEQUENCE
   {
04   certHash   OCTET STRING,
02   certReqId  INTEGER,
30   statusInfo PKIStatusInfo OPTIONAL
   }
```

## 2.51 ASN.1 type 'CMPCertificate'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

The following definition contains one German-specific choice, the '*gematikCVCert*', which is a '*card verifiable certificate*' (CVC) according to the ISO 7816 standards track. This is **not** part of RFC 4210/4211!

Please follow the in-document link to '*GermanCVCertificate*' to see its definition. The German Gematik defines an extension to the CMP protocol that enables the issuance of CV certificates. Such a CV certificate comes with a CMP response, explicitly tagged with no. 4.

```
     CHO CMPCertificate ::= CHOICE
         {
      30   x509v3PKCert               Certificate,
A4[7F21]   gematikCVCert [4] EXPLICIT GermanCVCertificate
         }
```

## 2.52 ASN.1 type 'CMSVersion'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
   CMSVersion ::= INTEGER
02 {
     v0(0),
     v1(1),
     v2(2),
     v3(3),
     v4(4),
     v5(5)
   }
```

## 2.53 ASN.1 type 'CPSuri'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
16 CPSuri ::= IA5String
```

## 2.54 ASN.1 type 'CRLAnnContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 CRLAnnContent ::= SEQUENCE OF CertificateList
```

## 2.55 ASN.1 type 'CRLBag'

Source of definition: 'PKCS #12'

```
30 CRLBag ::= SEQUENCE
   {
     crlId                OBJECT IDENTIFIER,
06   crlValue [0] EXPLICIT ANY
A0 }
```

## 2.56 ASN.1 type 'CRLDistributionPoints'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
```

## 2.57 ASN.1 type 'CRLNumber'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
02 CRLNumber ::= INTEGER (0..MAX)
```

## 2.58 ASN.1 type 'CRLReason'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
0A CRLReason ::= ENUMERATED
   {
     unspecified(0),
     keyCompromise(1),
     cACompromise(2),
     affiliationChanged(3),
     superseded(4),
     cessationOfOperation(5),
     certificateHold(6),
     removeFromCRL(8),
     privilegeWithdrawn(9),
     aACompromise(10)
   }
```

## 2.59 ASN.1 type 'CRMFControls'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 CRMFControls ::= SEQUENCE SIZE (1..MAX) OF AttributeTypeAndValue
```

## 2.60 ASN.1 type 'CRMFEncryptedKey'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
CHO CRMFEncryptedKey ::= CHOICE
    {
 30   encryptedValue              EncryptedValue,
 A0   envelopedData  [0] IMPLICIT EnvelopedData
    }
```

## 2.61 ASN.1 type 'CVCertDate'

Source of definition: 'German Gematik/BSI-specific (gemSpec_PKI and Technical Guideline TR-03110, part 3)'

*Please note: There is currently **no** ASN.1 definition in this technical guideline. The content is presented as a bunch of tables, which was converted to this ASN.1 type definition.*

```
12 CVCertDate ::= NumericString (SIZE (6))
```

## 2.62 ASN.1 type 'CVSubjectPublicKeyInfo'

Source of definition: 'German Gematik/BSI-specific (gemSpec_PKI and Technical Guideline TR-03110, part 3)'

*Please note: There is currently **no** ASN.1 definition in this technical guideline. The content is presented as a bunch of tables, which was converted to this ASN.1 type definition.*

```
30 CVSubjectPublicKeyInfo ::= SEQUENCE
   {
06   algorithm              OBJECT IDENTIFIER,
81   p          [1] IMPLICIT INTEGER          OPTIONAL,
82   a          [2] IMPLICIT INTEGER          OPTIONAL,
83   b          [3] IMPLICIT INTEGER          OPTIONAL,
84   G          [4] IMPLICIT OCTET STRING     OPTIONAL,
85   r          [5] IMPLICIT INTEGER          OPTIONAL,
86   Y          [6] IMPLICIT OCTET STRING,
87   f          [7] IMPLICIT INTEGER          OPTIONAL
   }
```

## 2.63 ASN.1 type 'CertAnnContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
CHO CertAnnContent ::= CMPCertificate
```

## 2.64 ASN.1 type 'CertBag'

Source of definition: 'PKCS #12'

```
30 CertBag ::= SEQUENCE
   {
06   certId                  OBJECT IDENTIFIER,
A0   certValue [0] EXPLICIT ANY
   }
```

## 2.65 ASN.1 type 'CertConfirmContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 CertConfirmContent ::= SEQUENCE OF CMPCertStatus
```

## 2.66 ASN.1 type 'CertID'

Source of definition: 'OCSP (RFC 6960)'

```
30 CertID ::= SEQUENCE
   {
30   hashAlgorithm  AlgorithmIdentifier,
04   issuerNameHash OCTET STRING,
04   issuerKeyHash  OCTET STRING,
02   serialNumber   CertificateSerialNumber
   }
```

## 2.67 ASN.1 type 'CertId'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
 30 CertId ::= SEQUENCE
    {
CHO   issuer       GeneralName,
 02   serialNumber INTEGER
    }
```

## 2.68 ASN.1 type 'CertOrEncCert'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
   CHO CertOrEncCert ::= CHOICE
       {
    A0   certificate   [0] EXPLICIT CMPCertificate,
A1[30]   encryptedCert [1] EXPLICIT EncryptedValue
       }
```

## 2.69 ASN.1 type 'CertPolicyId'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
06 CertPolicyId ::= OBJECT IDENTIFIER
```

## 2.70 ASN.1 type 'CertRepMessage'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
    30 CertRepMessage ::= SEQUENCE
       {
A1[30]   caPubs   [1] EXPLICIT SEQUENCE SIZE (1..MAX) OF CMPCertificate OPTIONAL,
    30   response              SEQUENCE OF CertResponse
       }
```

## 2.71 ASN.1 type 'CertReq'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 CertReq ::= CertRequest
```

## 2.72 ASN.1 type 'CertReqMessages'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 CertReqMessages ::= SEQUENCE SIZE (1..MAX) OF CertReqMsg
```

## 2.73 ASN.1 type 'CertReqMsg'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 CertReqMsg ::= SEQUENCE
   {
30   certReq CertRequest,
CHO  popo    ProofOfPossession                                  OPTIONAL,
30   regInfo SEQUENCE SIZE (1..MAX) OF AttributeTypeAndValue OPTIONAL
   }
```

## 2.74 ASN.1 type 'CertRequest'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 CertRequest ::= SEQUENCE
   {
02   certReqId    INTEGER,
30   certTemplate CertTemplate,
30   controls     CRMFControls OPTIONAL
   }
```

## 2.75 ASN.1 type 'CertResponse'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 CertResponse ::= SEQUENCE
   {
02   certReqId        INTEGER,
30   status           PKIStatusInfo,
30   certifiedKeyPair CertifiedKeyPair OPTIONAL,
04   rspInfo          OCTET STRING     OPTIONAL
   }
```

## 2.76 ASN.1 type 'CertStatus'

Source of definition: 'OCSP (RFC 6960)'

```
CHO CertStatus ::= CHOICE
    {
 80   good    [0] IMPLICIT NULL,
 A1   revoked [1] IMPLICIT RevokedInfo,
 82   unknown [2] IMPLICIT UnknownInfo
    }
```

## 2.77 ASN.1 type 'CertTemplate'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 CertTemplate ::= SEQUENCE
   {
80   version      [0] IMPLICIT Version              OPTIONAL,
81   serialNumber [1] IMPLICIT INTEGER              OPTIONAL,
A2   signingAlg   [2] IMPLICIT AlgorithmIdentifier  OPTIONAL,
A3   issuer       [3] IMPLICIT Name                 OPTIONAL,
A4   validity     [4] IMPLICIT OptionalValidity     OPTIONAL,
A5   subject      [5] IMPLICIT Name                 OPTIONAL,
A6   publicKey    [6] IMPLICIT SubjectPublicKeyInfo OPTIONAL,
87   issuerUID    [7] IMPLICIT UniqueIdentifier     OPTIONAL,
88   subjectUID   [8] IMPLICIT UniqueIdentifier     OPTIONAL,
A9   extensions   [9] IMPLICIT Extensions           OPTIONAL
   }
```

## 2.78 ASN.1 type 'Certificate'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
30 Certificate ::= SEQUENCE
   {
30   tbsCertificate     TBSCertificate,
30   signatureAlgorithm AlgorithmIdentifier,
03   signature          BIT STRING
   }
```

## 2.79 ASN.1 type 'CertificateChoices'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO CertificateChoices ::= CHOICE
    {
 30   certificate                    Certificate,
 A0   extendedCertificate [0] IMPLICIT ExtendedCertificate,
 A1   v1AttrCert          [1] IMPLICIT AttributeCertificateV1,
 A2   v2AttrCert          [2] IMPLICIT AttributeCertificateV2,
 A3   other               [3] IMPLICIT OtherCertificateFormat
    }
```

## 2.80 ASN.1 type 'CertificateHolderAuthorizationTemplate'

Source of definition: 'German Gematik/BSI-
specific (gemSpec_PKI and Technical Guideline TR-03110, part 3)'

*Please note: There is currently **no** ASN.1 definition in this technical guideline. The content is presented as a bunch of tables, which was converted to this ASN.1 type definition.*

```
30 CertificateHolderAuthorizationTemplate ::= SEQUENCE
   {
06   chatType                                OBJECT IDENTIFIER,
53   chatContent [APPLICATION 19] IMPLICIT OCTET STRING
   }
```

## 2.81 ASN.1 type 'CertificateIssuer'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 CertificateIssuer ::= GeneralNames
```

## 2.82 ASN.1 type 'CertificateList'

Source of definition: 'CRL structures'

```
30 CertificateList ::= SEQUENCE
   {
30   tbsCertList         TBSCertList,
30   signatureAlgorithm AlgorithmIdentifier,
03   signature           BIT STRING
   }
```

## 2.83 ASN.1 type 'CertificatePolicies'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 CertificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation
```

## 2.84 ASN.1 type 'CertificateProfileIdentifier'

Source of definition: 'German Gematik/BSI-
specific (gemSpec_PKI and Technical Guideline TR-03110, part 3)'

*Please note: There is currently **no** ASN.1 definition in this technical guideline. The content is presented as a bunch of tables, which was converted to this ASN.1 type definition.*

```
   CertificateProfileIdentifier ::= INTEGER
02 {
     machineReadableTravelDocumentsV1(0),
     gematikCVCertGen2(70)
   }
```

## 2.85 ASN.1 type 'CertificateSerialNumber'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
02 CertificateSerialNumber ::= INTEGER
```

## 2.86 ASN.1 type 'CertificateSet'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 CertificateSet ::= SET OF CertificateChoices
```

## 2.87 ASN.1 type 'CertificationRequest'

Source of definition: 'PKCS #10'

```
30 CertificationRequest ::= SEQUENCE
   {
30   certificationRequestInfo CertificationRequestInfo,
30   signatureAlgorithm       AlgorithmIdentifier,
03   signature                BIT STRING
   }
```

## 2.88 ASN.1 type 'CertificationRequestInfo'

Source of definition: 'PKCS #10'

```
30 CertificationRequestInfo ::= SEQUENCE
   {
02   version                    INTEGER
     {
       v1(0)
     },
CHO  subject                    Name,
30   subjectPKInfo              SubjectPublicKeyInfo,
A0   attributes    [0] IMPLICIT Attributes
   }
```

## 2.89 ASN.1 type 'CertifiedKeyPair'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
    30 CertifiedKeyPair ::= SEQUENCE
       {
   CHO   certOrEncCert                CertOrEncCert,
A0[30]   privateKey      [0] EXPLICIT EncryptedValue     OPTIONAL,
A1[30]   publicationInfo [1] EXPLICIT PKIPublicationInfo OPTIONAL
       }
```

## 2.90 ASN.1 type 'Challenge'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 Challenge ::= SEQUENCE
   {
30   owf       AlgorithmIdentifier OPTIONAL,
04   witness   OCTET STRING,
04   challenge OCTET STRING
   }
```

## 2.91 ASN.1 type 'Characteristic-two'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 Characteristic-two ::= SEQUENCE
   {
02   m          INTEGER,
06   basis      OBJECT IDENTIFIER,
ANY  parameters ANY
   }
```

## 2.92 ASN.1 type 'ClassList'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
03 ClassList ::= BIT STRING
   {
     unmarked(0),
     unclassified(1),
     restricted(2),
     confidential(3),
     secret(4),
     topSecret(5)
   }
```

## 2.93 ASN.1 type 'Clearance'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 Clearance ::= SEQUENCE
   {
06   policyId           OBJECT IDENTIFIER,
03   classList          ClassList               DEFAULT { unclassified },
31   securityCategories SET OF SecurityCategory OPTIONAL
   }
```

## 2.94 ASN.1 type 'CommonName'

Source of definition: 'CRL structures'

```
13 CommonName ::= PrintableString (SIZE (1..ub-common-name-length))
```

## 2.95 ASN.1 type 'CompareRequest'

Source of definition: 'LDAP (RFC 4511)'

```
6E CompareRequest ::= [APPLICATION 14] IMPLICIT SEQUENCE
   {
04   entry LDAPDN,
30   ava   AttributeValueAssertion
   }
```

## 2.96 ASN.1 type 'CompareResponse'

Source of definition: 'LDAP (RFC 4511)'

```
6F CompareResponse ::= [APPLICATION 15] IMPLICIT LDAPResult
```

## 2.97 ASN.1 type 'ContentEncryptionAlgorithmIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 ContentEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
```

## 2.98 ASN.1 type 'ContentInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 ContentInfo ::= SEQUENCE
   {
06   contentType             ContentType,
A0   content     [0] EXPLICIT ANY
   }
```

## 2.99 ASN.1 type 'ContentType'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
06 ContentType ::= OBJECT IDENTIFIER
```

## 2.100 ASN.1 type 'Control'

Source of definition: 'LDAP (RFC 4511)'

```
30 Control ::= SEQUENCE
   {
04   controlType  LDAPOID,
01   criticality  BOOLEAN      DEFAULT FALSE,
04   controlValue OCTET STRING OPTIONAL
   }
```

## 2.101 ASN.1 type 'Controls'

Source of definition: 'LDAP (RFC 4511)'

```
30 Controls ::= SEQUENCE OF Control
```

## 2.102 ASN.1 type 'Countersignature'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 Countersignature ::= SignerInfo
```

## 2.103 ASN.1 type 'CountryName'

Source of definition: 'CRL structures'

```
61 CountryName ::= [APPLICATION 1] EXPLICIT CHOICE
   {
12   x121-dcc-code         NumericString   (SIZE (ub-country-name-numeric-length)),
13   iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length))
   }
```

## 2.104 ASN.1 type 'CrlID'

Source of definition: 'OCSP (RFC 6960)'

```
    30 CrlID ::= SEQUENCE
       {
A0[16]   crlUrl  [0] EXPLICIT IA5String       OPTIONAL,
A1[02]   crlNum  [1] EXPLICIT INTEGER         OPTIONAL,
A2[18]   crlTime [2] EXPLICIT GeneralizedTime OPTIONAL
       }
```

## 2.105 ASN.1 type 'Curve'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 Curve ::= SEQUENCE
   {
04   a    FieldElement,
04   b    FieldElement,
03   seed BIT STRING   OPTIONAL
   }
```

## 2.106 ASN.1 type 'DHBMParameter'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 DHBMParameter ::= SEQUENCE
   {
30   owf AlgorithmIdentifier,
30   mac AlgorithmIdentifier
   }
```

## 2.107 ASN.1 type 'DHPublicKey'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
02 DHPublicKey ::= INTEGER
```

## 2.108 ASN.1 type 'DSA-Sig-Value'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

```
30 DSA-Sig-Value ::= SEQUENCE
   {
02   r INTEGER,
02   s INTEGER
   }
```

## 2.109 ASN.1 type 'DSAPublicKey'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
02 DSAPublicKey ::= INTEGER
```

## 2.110 ASN.1 type 'DSS-Parms'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

```
30 DSS-Parms ::= SEQUENCE
   {
02   p INTEGER,
02   q INTEGER,
02   g INTEGER
   }
```

## 2.111 ASN.1 type 'DelRequest'

Source of definition: 'LDAP (RFC 4511)'

```
4A DelRequest ::= [APPLICATION 10] IMPLICIT LDAPDN
```

## 2.112 ASN.1 type 'DelResponse'

Source of definition: 'LDAP (RFC 4511)'

```
6B DelResponse ::= [APPLICATION 11] IMPLICIT LDAPResult
```

## 2.113 ASN.1 type 'Digest'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
04 Digest ::= OCTET STRING
```

## 2.114 ASN.1 type 'DigestAlgorithmIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 DigestAlgorithmIdentifier ::= AlgorithmIdentifier
```

## 2.115 ASN.1 type 'DigestAlgorithmIdentifiers'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier
```

## 2.116 ASN.1 type 'DigestInfo'

Source of definition: 'PKCS #1'

```
30 DigestInfo ::= SEQUENCE
   {
30   digestAlgorithm AlgorithmIdentifier,
04   digest          OCTET STRING
   }
```

## 2.117 ASN.1 type 'DigestedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 DigestedData ::= SEQUENCE
   {
02   version          CMSVersion,
30   digestAlgorithm  DigestAlgorithmIdentifier,
30   encapContentInfo EncapsulatedContentInfo,
04   digest           Digest
   }
```

## 2.118 ASN.1 type 'DirectoryString'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO DirectoryString ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..MAX)),
 13   printableString PrintableString (SIZE (1..MAX)),
 1C   universalString UniversalString (SIZE (1..MAX)),
 0C   utf8String      UTF8String      (SIZE (1..MAX)),
 1E   bmpString       BMPString       (SIZE (1..MAX))
    }
```

## 2.119 ASN.1 type 'DisplayText'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
CHO DisplayText ::= CHOICE
    {
 16   ia5String     IA5String     (SIZE (1..200)),
 1A   visibleString VisibleString (SIZE (1..200)),
 1E   bmpString     BMPString     (SIZE (1..200)),
 0C   utf8String    UTF8String    (SIZE (1..200))
    }
```

## 2.120 ASN.1 type 'DistinguishedName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
30 DistinguishedName ::= RDNSequence
```

## 2.121 ASN.1 type 'DistributionPoint'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 DistributionPoint ::= SEQUENCE
   {
A0   distributionPoint [0] IMPLICIT DistributionPointName OPTIONAL,
81   reasons           [1] IMPLICIT ReasonFlags           OPTIONAL,
A2   cRLIssuer         [2] IMPLICIT GeneralNames          OPTIONAL
   }
```

## 2.122 ASN.1 type 'DistributionPointName'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
CHO DistributionPointName ::= CHOICE
    {
A0    fullName                [0] IMPLICIT GeneralNames,
A1    nameRelativeToCRLIssuer [1] IMPLICIT RelativeDistinguishedName
    }
```

## 2.123 ASN.1 type 'DomainComponent'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
16 DomainComponent ::= IA5String
```

## 2.124 ASN.1 type 'DomainParameters'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 DomainParameters ::= SEQUENCE
   {
02   p               INTEGER,
02   g               INTEGER,
02   q               INTEGER,
02   j               INTEGER         OPTIONAL,
30   validationParms ValidationParms OPTIONAL
   }
```

## 2.125 ASN.1 type 'Dss-Parms'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 Dss-Parms ::= SEQUENCE
   {
02   p INTEGER,
02   q INTEGER,
02   g INTEGER
   }
```

## 2.126 ASN.1 type 'Dss-Sig-Value'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 Dss-Sig-Value ::= SEQUENCE
   {
02   r INTEGER,
02   s INTEGER
   }
```

## 2.127 ASN.1 type 'ECDSA-Sig-Value'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 ECDSA-Sig-Value ::= SEQUENCE
   {
02   r INTEGER,
02   s INTEGER
   }
```

## 2.128 ASN.1 type 'ECPVer'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
   ECPVer ::= INTEGER
02 {
     ecpVer1(1)
   }
```

## 2.129 ASN.1 type 'ECParameters'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 ECParameters ::= SEQUENCE
   {
02   version   ECPVer,
30   fieldID   FieldID,
30   curve     Curve,
04   base      ECPoint,
02   order     INTEGER,
02   cofactor  INTEGER OPTIONAL
   }
```

## 2.130 ASN.1 type 'ECPoint'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
04 ECPoint ::= OCTET STRING
```

## 2.131 ASN.1 type 'EDIPartyName'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30  EDIPartyName ::= SEQUENCE
    {
A0    nameAssigner [0] IMPLICIT DirectoryString OPTIONAL,
A1    partyName    [1] IMPLICIT DirectoryString
    }
```

## 2.132 ASN.1 type 'EcpkParameters'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
CHO EcpkParameters ::= CHOICE
    {
 30   ecParameters ECParameters,
 06   namedCurve   OBJECT IDENTIFIER,
 05   implicitlyCA NULL
    }
```

## 2.133 ASN.1 type 'EmailAddress'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
16  EmailAddress ::= IA5String (SIZE (1..ub-emailaddress-length))
```

## 2.134 ASN.1 type 'EncKeyWithID'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
    EncKeyWithID ::= SEQUENCE
30  {
      privateKey PrivateKeyInfo,
30    identifier CHOICE
CHO   {
        string      UTF8String,
0C      generalName GeneralName
CHO   } OPTIONAL
    }
```

## 2.135 ASN.1 type 'EncapsulatedContentInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
  30 EncapsulatedContentInfo ::= SEQUENCE
     {
  06   eContentType              ContentType,
A0[04] eContent     [0] EXPLICIT OCTET STRING OPTIONAL
     }
```

## 2.136 ASN.1 type 'EncodingParameters'

Source of definition: 'PKCS #1'

```
04 EncodingParameters ::= OCTET STRING (SIZE (0..MAX))
```

## 2.137 ASN.1 type 'EncryptedContent'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
04 EncryptedContent ::= OCTET STRING
```

## 2.138 ASN.1 type 'EncryptedContentInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
EncryptedContentInfo ::= SEQUENCE
{
  contentType                                ContentType,
  contentEncryptionAlgorithm                 ContentEncryptionAlgorithmIdentifier,
  encryptedContent           [0] IMPLICIT    EncryptedContent                        OPTIONAL
}
```

## 2.139 ASN.1 type 'EncryptedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
EncryptedData ::= SEQUENCE
{
  version                               CMSVersion,
  encryptedContentInfo                  EncryptedContentInfo,
  unprotectedAttrs     [1] IMPLICIT     UnprotectedAttributes OPTIONAL
}
```

## 2.140 ASN.1 type 'EncryptedKey'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
EncryptedKey ::= OCTET STRING
```

## 2.141 ASN.1 type 'EncryptedPrivateKeyInfo'

Source of definition: 'PKCS #8'

```
EncryptedPrivateKeyInfo ::= SEQUENCE
{
  encryptionAlgorithm AlgorithmIdentifier,
  encryptedData       P8EncryptedData
}
```

## 2.142 ASN.1 type 'EncryptedValue'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 EncryptedValue ::= SEQUENCE
   {
A0   intendedAlg [0] IMPLICIT AlgorithmIdentifier OPTIONAL,
A1   symmAlg     [1] IMPLICIT AlgorithmIdentifier OPTIONAL,
82   encSymmKey  [2] IMPLICIT BIT STRING          OPTIONAL,
A3   keyAlg      [3] IMPLICIT AlgorithmIdentifier OPTIONAL,
84   valueHint   [4] IMPLICIT OCTET STRING        OPTIONAL,
03   encValue                  BIT STRING
   }
```

## 2.143 ASN.1 type 'EnvelopedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 EnvelopedData ::= SEQUENCE
   {
02   version                         CMSVersion,
A0   originatorInfo       [0] IMPLICIT OriginatorInfo        OPTIONAL,
31   recipientInfos                   RecipientInfos,
30   encryptedContentInfo             EncryptedContentInfo,
A1   unprotectedAttrs     [1] IMPLICIT UnprotectedAttributes OPTIONAL
   }
```

## 2.144 ASN.1 type 'ErrorMsgContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 ErrorMsgContent ::= SEQUENCE
   {
30   pKIStatusInfo PKIStatusInfo,
02   errorCode     INTEGER       OPTIONAL,
30   errorDetails  PKIFreeText   OPTIONAL
   }
```

## 2.145 ASN.1 type 'ExtKeyUsageSyntax'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
```

## 2.146 ASN.1 type 'ExtendedCertificate'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 ExtendedCertificate ::= SEQUENCE
   {
30   extendedCertificateInfo ExtendedCertificateInfo,
30   signatureAlgorithm       SignatureAlgorithmIdentifier,
03   signature                Signature
   }
```

## 2.147 ASN.1 type 'ExtendedCertificateInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 ExtendedCertificateInfo ::= SEQUENCE
   {
02   version     CMSVersion,
30   certificate Certificate,
31   attributes  UnauthAttributes
   }
```

## 2.148 ASN.1 type 'ExtendedCertificateOrCertificate'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO ExtendedCertificateOrCertificate ::= CHOICE
    {
 30   certificate                     Certificate,
 A0   extendedCertificate [0] IMPLICIT ExtendedCertificate
    }
```

## 2.149 ASN.1 type 'ExtendedNetworkAddress'

Source of definition: 'CRL structures'

```
CHO ExtendedNetworkAddress ::= CHOICE
    {
 30   e163-4-address              SEQUENCE
      {
 80     number      [0] IMPLICIT NumericString (SIZE (1..ub-e163-4-number-length)),
 81     sub-address [1] IMPLICIT NumericString (SIZE (1..ub-e163-4-sub-address-length)) OPTIONAL
      },
 A0   psap-address   [0] IMPLICIT PresentationAddress
    }
```

## 2.150 ASN.1 type 'ExtendedRequest'

Source of definition: 'LDAP (RFC 4511)'

```
 77 ExtendedRequest ::= [APPLICATION 23] IMPLICIT SEQUENCE
    {
 80   requestName  [0] IMPLICIT LDAPOID,
 81   requestValue [1] IMPLICIT OCTET STRING OPTIONAL
    }
```

## 2.151 ASN.1 type 'ExtendedResponse'

Source of definition: 'LDAP (RFC 4511)'

```
 78 ExtendedResponse ::= [APPLICATION 24] IMPLICIT SEQUENCE
    {
 0A   resultCode                      ENUMERATED
      {
        success(0),
        operationsError(1),
        protocolError(2),
        timeLimitExceeded(3),
        sizeLimitExceeded(4),
        compareFalse(5),
        compareTrue(6),
        authMethodNotSupported(7),
        strongerAuthRequired(8),
        referral(10),
```

```
      adminLimitExceeded(11),
      unavailableCriticalExtension(12),
      confidentialityRequired(13),
      saslBindInProgress(14),
      noSuchAttribute(16),
      undefinedAttributeType(17),
      inappropriateMatching(18),
      constraintViolation(19),
      attributeOrValueExists(20),
      invalidAttributeSyntax(21),
      noSuchObject(32),
      aliasProblem(33),
      invalidDNSyntax(34),
      aliasDereferencingProblem(36),
      inappropriateAuthentication(48),
      invalidCredentials(49),
      insufficientAccessRights(50),
      busy(51),
      unavailable(52),
      unwillingToPerform(53),
      loopDetect(54),
      namingViolation(64),
      objectClassViolation(65),
      notAllowedOnNonLeaf(66),
      notAllowedOnRDN(67),
      entryAlreadyExists(68),
      objectClassModsProhibited(69),
      affectsMultipleDSAs(71),
      other(80)
    },
04  matchedDN                       LDAPDN,
04  diagnosticMessage               LDAPString,
A3  referral           [3] IMPLICIT Referral     OPTIONAL,
8A  responseName      [10] IMPLICIT LDAPOID      OPTIONAL,
8B  responseValue     [11] IMPLICIT OCTET STRING OPTIONAL
  }
```

## 2.152 ASN.1 type 'Extension'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
30 Extension ::= SEQUENCE
   {
06   extnID    OBJECT IDENTIFIER,
01   critical  BOOLEAN           DEFAULT FALSE,
04   extnValue OCTET STRING
   }
```

## 2.153 ASN.1 type 'ExtensionAttribute'

Source of definition: 'CRL structures'

```
30 ExtensionAttribute ::= SEQUENCE
   {
80   extension-attribute-type  [0] IMPLICIT INTEGER (0..ub-extension-attributes),
A1   extension-attribute-value [1] EXPLICIT ANY
   }
```

## 2.154 ASN.1 type 'ExtensionAttributes'

Source of definition: 'CRL structures'

```
31 ExtensionAttributes ::= SET SIZE (1..ub-extension-attributes) OF ExtensionAttribute
```

## 2.155 ASN.1 type 'ExtensionORAddressComponents'

Source of definition: 'CRL structures'

```
31 ExtensionORAddressComponents ::= PDSParameter
```

## 2.156 ASN.1 type 'ExtensionPhysicalDeliveryAddressComponents'

Source of definition: 'CRL structures'

```
31 ExtensionPhysicalDeliveryAddressComponents ::= PDSParameter
```

## 2.157 ASN.1 type 'Extensions'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

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

## 2.158 ASN.1 type 'FieldElement'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
04 FieldElement ::= OCTET STRING
```

## 2.159 ASN.1 type 'FieldID'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 FieldID ::= SEQUENCE
   {
06   fieldType  OBJECT IDENTIFIER,
ANY  parameters ANY
   }
```

## 2.160 ASN.1 type 'Filter'

Source of definition: 'LDAP (RFC 4511)'

```
CHO Filter ::= CHOICE
    {
 A0   and              [0] IMPLICIT SET SIZE (1..MAX) OF Filter,
 A1   or               [1] IMPLICIT SET SIZE (1..MAX) OF Filter,
 A2   not              [2] IMPLICIT Filter,
 A3   equalityMatch    [3] IMPLICIT AttributeValueAssertion,
 A4   substrings       [4] IMPLICIT SubstringFilter,
 A5   greaterOrEqual   [5] IMPLICIT AttributeValueAssertion,
 A6   lessOrEqual      [6] IMPLICIT AttributeValueAssertion,
 87   present          [7] IMPLICIT AttributeDescription,
 A8   approxMatch      [8] IMPLICIT AttributeValueAssertion,
 A9   extensibleMatch [9] IMPLICIT MatchingRuleAssertion
    }
```

## 2.161 ASN.1 type 'FreshestCRL'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 FreshestCRL ::= CRLDistributionPoints
```

## 2.162 ASN.1 type 'GenMsgContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 GenMsgContent ::= SEQUENCE OF InfoTypeAndValue
```

## 2.163 ASN.1 type 'GenRepContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 GenRepContent ::= SEQUENCE OF InfoTypeAndValue
```

## 2.164 ASN.1 type 'GeneralName'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
CHO GeneralName ::= CHOICE
    {
A0    otherName                  [0] IMPLICIT AnotherName,
81    rfc822Name                 [1] IMPLICIT IA5String,
82    dNSName                    [2] IMPLICIT IA5String,
A3    x400Address                [3] IMPLICIT ORAddress,
A4    directoryName              [4] IMPLICIT Name,
A5    ediPartyName               [5] IMPLICIT EDIPartyName,
86    uniformResourceIdentifier  [6] IMPLICIT IA5String,
87    iPAddress                  [7] IMPLICIT OCTET STRING,
88    registeredID               [8] IMPLICIT OBJECT IDENTIFIER
    }
```

## 2.165 ASN.1 type 'GeneralNames'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
```

## 2.166 ASN.1 type 'GeneralSubtree'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 GeneralSubtree ::= SEQUENCE
   {
CHO   base                 GeneralName,
80    minimum [0] IMPLICIT BaseDistance DEFAULT 0,
81    maximum [1] IMPLICIT BaseDistance OPTIONAL
   }
```

## 2.167 ASN.1 type 'GeneralSubtrees'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree
```

## 2.168 ASN.1 type 'GermanCVCertificate'

Source of definition: 'German Gematik/BSI-specific (gemSpec_PKI and Technical Guideline TR-03110, part 3)'

*Please note: There is currently **no** ASN.1 definition in this technical guideline. The content is presented as a bunch of tables, which was converted to this ASN.1 type definition.*

```
7F21 GermanCVCertificate ::= [APPLICATION 33] IMPLICIT SEQUENCE
     {
7F4E   cvbody    [APPLICATION 78] IMPLICIT GermanTBSCVCertificate,
5F37   signature [APPLICATION 55] IMPLICIT OCTET STRING
     }
```

## 2.169 ASN.1 type 'GermanCVExtension'

Source of definition: 'German Gematik/BSI-specific (gemSpec_PKI and Technical Guideline TR-03110, part 3)'

*Please note: There is currently **no** ASN.1 definition in this technical guideline. The content is presented as a bunch of tables, which was converted to this ASN.1 type definition.*

```
 73 GermanCVExtension ::= [APPLICATION 19] IMPLICIT SEQUENCE
    {
 06   extension OBJECT IDENTIFIER,
ANY   content   ANY
    }
```

## 2.170 ASN.1 type 'GermanTBSCVCertificate'

Source of definition: 'German Gematik/BSI-specific (gemSpec_PKI and Technical Guideline TR-03110, part 3)'

*Please note: There is currently **no** ASN.1 definition in this technical guideline. The content is presented as a bunch of tables, which was converted to this ASN.1 type definition.*

```
30 GermanTBSCVCertificate ::= SEQUENCE
   {
5F29 CPI                      [APPLICATION 41] IMPLICIT CertificateProfileIdentifier,
  42 CAR                      [APPLICATION 2] IMPLICIT  OCTET STRING,
7F49 subjectPublicKey         [APPLICATION 73] IMPLICIT CVSubjectPublicKeyInfo,
5F20 CHR                      [APPLICATION 32] IMPLICIT OCTET STRING,
7F4C chat                     [APPLICATION 76] IMPLICIT CertificateHolderAuthorizationTemplate,
5F25 certificateEffectiveDate [APPLICATION 37] IMPLICIT CVCertDate,
5F24 certificateExpirationDate [APPLICATION 36] IMPLICIT CVCertDate,
  65 certificateExtensions    [APPLICATION 5] IMPLICIT  SEQUENCE SIZE (1..MAX) OF GermanCVExtension OPTIONAL
   }
```

## 2.171 ASN.1 type 'HashAlgorithm'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

```
30 HashAlgorithm ::= AlgorithmIdentifier
```

## 2.172 ASN.1 type 'HoldInstructionCode'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
06 HoldInstructionCode ::= OBJECT IDENTIFIER
```

## 2.173 ASN.1 type 'Holder'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 Holder ::= SEQUENCE
   {
A0   baseCertificateID [0] IMPLICIT IssuerSerial     OPTIONAL,
A1   entityName        [1] IMPLICIT GeneralNames     OPTIONAL,
A2   objectDigestInfo  [2] IMPLICIT ObjectDigestInfo OPTIONAL
   }
```

## 2.174 ASN.1 type 'IetfAttrSyntax'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
IetfAttrSyntax ::= SEQUENCE
{
  policyAuthority [0] IMPLICIT GeneralNames       OPTIONAL,
  values                       SEQUENCE OF CHOICE
  {
    octets OCTET STRING,
    oid    OBJECT IDENTIFIER,
    string UTF8String
  }
}
```

## 2.175 ASN.1 type 'InfoTypeAndValue'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
InfoTypeAndValue ::= SEQUENCE
{
  infoType  OBJECT IDENTIFIER,
  infoValue ANY                OPTIONAL
}
```

## 2.176 ASN.1 type 'InhibitAnyPolicy'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
InhibitAnyPolicy ::= SkipCerts
```

## 2.177 ASN.1 type 'IntermediateResponse'

Source of definition: 'LDAP (RFC 4511)'

```
IntermediateResponse ::= [APPLICATION 25] IMPLICIT SEQUENCE
{
  responseName  [0] IMPLICIT LDAPOID      OPTIONAL,
  responseValue [1] IMPLICIT OCTET STRING OPTIONAL
}
```

## 2.178 ASN.1 type 'InvalidityDate'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
InvalidityDate ::= GeneralizedTime
```

## 2.179 ASN.1 type 'IssuerAltName'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
IssuerAltName ::= GeneralNames
```

## 2.180 ASN.1 type 'IssuerAndSerialNumber'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
IssuerAndSerialNumber ::= SEQUENCE
{
  issuer       Name,
  serialNumber CertificateSerialNumber
}
```

## 2.181 ASN.1 type 'IssuerSerial'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 IssuerSerial ::= SEQUENCE
   {
30   issuer    GeneralNames,
02   serial    CertificateSerialNumber,
03   issuerUID UniqueIdentifier        OPTIONAL
   }
```

## 2.182 ASN.1 type 'IssuingDistributionPoint'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 IssuingDistributionPoint ::= SEQUENCE
   {
A0   distributionPoint          [0] IMPLICIT DistributionPointName OPTIONAL,
81   onlyContainsUserCerts      [1] IMPLICIT BOOLEAN               DEFAULT FALSE,
82   onlyContainsCACerts        [2] IMPLICIT BOOLEAN               DEFAULT FALSE,
83   onlySomeReasons            [3] IMPLICIT ReasonFlags           OPTIONAL,
84   indirectCRL                [4] IMPLICIT BOOLEAN               DEFAULT FALSE,
85   onlyContainsAttributeCerts [5] IMPLICIT BOOLEAN               DEFAULT FALSE
   }
```

## 2.183 ASN.1 type 'KEA-Parms-Id'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
04 KEA-Parms-Id ::= OCTET STRING
```

## 2.184 ASN.1 type 'KEKIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 KEKIdentifier ::= SEQUENCE
   {
04   keyIdentifier OCTET STRING,
18   date          GeneralizedTime   OPTIONAL,
30   other         OtherKeyAttribute OPTIONAL
   }
```

## 2.185 ASN.1 type 'KEKRecipientInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 KEKRecipientInfo ::= SEQUENCE
   {
02   version                CMSVersion,
30   kekid                  KEKIdentifier,
30   keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
04   encryptedKey           EncryptedKey
   }
```

## 2.186 ASN.1 type 'KeyAgreeRecipientIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO KeyAgreeRecipientIdentifier ::= CHOICE
    {
30    issuerAndSerialNumber             IssuerAndSerialNumber,
A0    rKeyId                [0] IMPLICIT RecipientKeyIdentifier
    }
```

## 2.187 ASN.1 type 'KeyAgreeRecipientInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 KeyAgreeRecipientInfo ::= SEQUENCE
   {
02   version                              CMSVersion,
A0   originator             [0] EXPLICIT OriginatorIdentifierOrKey,
A1[04]  ukm                  [1] EXPLICIT UserKeyingMaterial                OPTIONAL,
30   keyEncryptionAlgorithm               KeyEncryptionAlgorithmIdentifier,
30   recipientEncryptedKeys               RecipientEncryptedKeys
   }
```

## 2.188 ASN.1 type 'KeyBag'

Source of definition: 'PKCS #12'

```
30 KeyBag ::= PrivateKeyInfo
```

## 2.189 ASN.1 type 'KeyDerivationAlgorithmIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 KeyDerivationAlgorithmIdentifier ::= AlgorithmIdentifier
```

## 2.190 ASN.1 type 'KeyEncryptionAlgorithmIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 KeyEncryptionAlgorithmIdentifier ::= AlgorithmIdentifier
```

## 2.191 ASN.1 type 'KeyGenParameters'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
04 KeyGenParameters ::= OCTET STRING
```

## 2.192 ASN.1 type 'KeyHash'

Source of definition: 'OCSP (RFC 6960)'

```
04 KeyHash ::= OCTET STRING
```

## 2.193 ASN.1 type 'KeyIdentifier'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
04 KeyIdentifier ::= OCTET STRING
```

## 2.194 ASN.1 type 'KeyPurposeId'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
   KeyPurposeId ::= OBJECT IDENTIFIER
06 {
     id-kp-serverAuth(1.3.6.1.5.5.7.3.1),
     id-kp-clientAuth(1.3.6.1.5.5.7.3.2),
     id-kp-codeSigning(1.3.6.1.5.5.7.3.3),
     id-kp-emailProtection(1.3.6.1.5.5.7.3.4),
     id-kp-timeStamping(1.3.6.1.5.5.7.3.8),
     id-kp-OCSPSigning(1.3.6.1.5.5.7.3.9)
   }
```

## 2.195 ASN.1 type 'KeyRecRepContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
    30 KeyRecRepContent ::= SEQUENCE
       {
    30   status                  PKIStatusInfo,
    A0   newSigCert  [0] EXPLICIT CMPCertificate                             OPTIONAL,
A1[30]   caCerts     [1] EXPLICIT SEQUENCE SIZE (1..MAX) OF CMPCertificate   OPTIONAL,
A2[30]   keyPairHist [2] EXPLICIT SEQUENCE SIZE (1..MAX) OF CertifiedKeyPair OPTIONAL
       }
```

## 2.196 ASN.1 type 'KeyTransRecipientInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 KeyTransRecipientInfo ::= SEQUENCE
   {
02   version                CMSVersion,
CHO  rid                    RecipientIdentifier,
30   keyEncryptionAlgorithm KeyEncryptionAlgorithmIdentifier,
04   encryptedKey           EncryptedKey
   }
```

## 2.197 ASN.1 type 'KeyUsage'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
   KeyUsage ::= BIT STRING
03 {
     digitalSignature(0),
     nonRepudiation(1),
     keyEncipherment(2),
     dataEncipherment(3),
     keyAgreement(4),
     keyCertSign(5),
     cRLSign(6),
     encipherOnly(7),
     decipherOnly(8)
   }
```

## 2.198 ASN.1 type 'LDAPAttribute'

Source of definition: 'LDAP (RFC 4511)'

```
30 LDAPAttribute ::= SEQUENCE
   {
04   type AttributeDescription,
31   vals SET SIZE (1..MAX) OF LDAPAttributeValue
   }
```

## 2.199 ASN.1 type 'LDAPAttributeValue'

Source of definition: 'LDAP (RFC 4511)'

```
04 LDAPAttributeValue ::= OCTET STRING
```

## 2.200 ASN.1 type 'LDAPDN'

Source of definition: 'LDAP (RFC 4511)'

```
04 LDAPDN ::= LDAPString
```

## 2.201 ASN.1 type 'LDAPMessage'

Source of definition: 'LDAP (RFC 4511)'

```
30 LDAPMessage ::= SEQUENCE
   {
02   messageID               MessageID,
CHO  protocolOp              CHOICE
     {
60     bindRequest           BindRequest,
61     bindResponse          BindResponse,
42     unbindRequest         UnbindRequest,
63     searchRequest         SearchRequest,
64     searchResEntry        SearchResultEntry,
65     searchResDone         SearchResultDone,
73     searchResRef          SearchResultReference,
66     modifyRequest         ModifyRequest,
67     modifyResponse        ModifyResponse,
68     addRequest            AddRequest,
69     addResponse           AddResponse,
4A     delRequest            DelRequest,
6B     delResponse           DelResponse,
6C     modDNRequest          ModifyDNRequest,
6D     modDNResponse         ModifyDNResponse,
6E     compareRequest        CompareRequest,
6F     compareResponse       CompareResponse,
50     abandonRequest        AbandonRequest,
77     extendedReq           ExtendedRequest,
78     extendedResp          ExtendedResponse,
79     intermediateResponse  IntermediateResponse
     },
A0   controls   [0] IMPLICIT Controls     OPTIONAL
   }
```

## 2.202 ASN.1 type 'LDAPOID'

Source of definition: 'LDAP (RFC 4511)'

```
04 LDAPOID ::= OCTET STRING
```

## 2.203 ASN.1 type 'LDAPResult'

Source of definition: 'LDAP (RFC 4511)'

```
30 LDAPResult ::= SEQUENCE
   {
0A   resultCode                     ENUMERATED
     {
       success(0),
       operationsError(1),
       protocolError(2),
       timeLimitExceeded(3),
       sizeLimitExceeded(4),
       compareFalse(5),
       compareTrue(6),
       authMethodNotSupported(7),
       strongerAuthRequired(8),
       referral(10),
       adminLimitExceeded(11),
       unavailableCriticalExtension(12),
       confidentialityRequired(13),
       saslBindInProgress(14),
       noSuchAttribute(16),
       undefinedAttributeType(17),
       inappropriateMatching(18),
       constraintViolation(19),
       attributeOrValueExists(20),
       invalidAttributeSyntax(21),
       noSuchObject(32),
       aliasProblem(33),
       invalidDNSyntax(34),
       aliasDereferencingProblem(36),
       inappropriateAuthentication(48),
       invalidCredentials(49),
       insufficientAccessRights(50),
       busy(51),
       unavailable(52),
       unwillingToPerform(53),
       loopDetect(54),
       namingViolation(64),
       objectClassViolation(65),
       notAllowedOnNonLeaf(66),
       notAllowedOnRDN(67),
       entryAlreadyExists(68),
       objectClassModsProhibited(69),
       affectsMultipleDSAs(71),
```

```
    other(80)
  },
04  matchedDN                       LDAPDN,
04  diagnosticMessage               LDAPString,
A3  referral          [3] IMPLICIT Referral   OPTIONAL
}
```

## 2.204 ASN.1 type 'LDAPString'

Source of definition: 'LDAP (RFC 4511)'

```
04 LDAPString ::= OCTET STRING
```

## 2.205 ASN.1 type 'LocalPostalAttributes'

Source of definition: 'CRL structures'

```
31 LocalPostalAttributes ::= PDSParameter
```

## 2.206 ASN.1 type 'MacData'

Source of definition: 'PKCS #12'

```
30 MacData ::= SEQUENCE
{
30  mac        DigestInfo,
04  macSalt    OCTET STRING,
02  iterations INTEGER      DEFAULT 1
}
```

## 2.207 ASN.1 type 'MaskGenAlgorithm'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

```
30 MaskGenAlgorithm ::= AlgorithmIdentifier
```

## 2.208 ASN.1 type 'MatchingRuleAssertion'

Source of definition: 'LDAP (RFC 4511)'

```
30 MatchingRuleAssertion ::= SEQUENCE
   {
81   matchingRule [1] IMPLICIT MatchingRuleId       OPTIONAL,
82   type         [2] IMPLICIT AttributeDescription OPTIONAL,
83   matchValue   [3] IMPLICIT AssertionValue,
84   dnAttributes [4] IMPLICIT BOOLEAN              DEFAULT FALSE
   }
```

## 2.209 ASN.1 type 'MatchingRuleId'

Source of definition: 'LDAP (RFC 4511)'

```
04 MatchingRuleId ::= LDAPString
```

## 2.210 ASN.1 type 'MessageAuthenticationCode'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
04 MessageAuthenticationCode ::= OCTET STRING
```

## 2.211 ASN.1 type 'MessageAuthenticationCodeAlgorithm'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 MessageAuthenticationCodeAlgorithm ::= AlgorithmIdentifier
```

## 2.212 ASN.1 type 'MessageDigest'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
04 MessageDigest ::= OCTET STRING
```

## 2.213 ASN.1 type 'MessageID'

Source of definition: 'LDAP (RFC 4511)'

```
02 MessageID ::= INTEGER (0..maxInt)
```

## 2.214 ASN.1 type 'ModifyDNRequest'

Source of definition: 'LDAP (RFC 4511)'

```
6C ModifyDNRequest ::= [APPLICATION 12] IMPLICIT SEQUENCE
   {
04   entry                    LDAPDN,
04   newrdn                   RelativeLDAPDN,
01   deleteoldrdn             BOOLEAN,
80   newSuperior  [0] IMPLICIT LDAPDN         OPTIONAL
   }
```

## 2.215 ASN.1 type 'ModifyDNResponse'

Source of definition: 'LDAP (RFC 4511)'

```
6D ModifyDNResponse ::= [APPLICATION 13] IMPLICIT LDAPResult
```

## 2.216 ASN.1 type 'ModifyRequest'

Source of definition: 'LDAP (RFC 4511)'

```
ModifyRequest ::= [APPLICATION 6] IMPLICIT SEQUENCE
{
  object  LDAPDN,
  changes SEQUENCE OF SEQUENCE
  {
    operation    ENUMERATED
    {
      add(0),
      delete(1),
      replace(2)
    },
    modification PartialAttribute
  }
}
```

## 2.217 ASN.1 type 'ModifyResponse'

Source of definition: 'LDAP (RFC 4511)'

```
ModifyResponse ::= [APPLICATION 7] IMPLICIT LDAPResult
```

## 2.218 ASN.1 type 'Name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
Name ::= CHOICE
{
  rdnSequence RDNSequence
}
```

## 2.219 ASN.1 type 'NameConstraints'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 NameConstraints ::= SEQUENCE
   {
A0   permittedSubtrees [0] IMPLICIT GeneralSubtrees OPTIONAL,
A1   excludedSubtrees  [1] IMPLICIT GeneralSubtrees OPTIONAL
   }
```

## 2.220 ASN.1 type 'NestedMessageContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 NestedMessageContent ::= PKIMessages
```

## 2.221 ASN.1 type 'NetworkAddress'

Source of definition: 'CRL structures'

```
12 NetworkAddress ::= X121Address
```

## 2.222 ASN.1 type 'NoticeReference'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 NoticeReference ::= SEQUENCE
   {
CHO  organization  DisplayText,
30   noticeNumbers SEQUENCE OF INTEGER
   }
```

## 2.223 ASN.1 type 'NumericUserIdentifier'

Source of definition: 'CRL structures'

```
12 NumericUserIdentifier ::= NumericString (SIZE (1..ub-numeric-user-id-length))
```

## 2.224 ASN.1 type 'OCSPRequest'

Source of definition: 'OCSP (RFC 6960)'

```
    30 OCSPRequest ::= SEQUENCE
       {
    30   tbsRequest                     TBSRequest,
A0[30]   optionalSignature [0] EXPLICIT OCSPSignature OPTIONAL
       }
```

## 2.225 ASN.1 type 'OCSPResponse'

Source of definition: 'OCSP (RFC 6960)'

```
    30 OCSPResponse ::= SEQUENCE
       {
    0A   responseStatus              OCSPResponseStatus,
A0[30]   responseBytes  [0] EXPLICIT ResponseBytes      OPTIONAL
       }
```

## 2.226 ASN.1 type 'OCSPResponseStatus'

Source of definition: 'OCSP (RFC 6960)'

```
    OCSPResponseStatus ::= ENUMERATED
0A  {
      successful(0),
      malformedRequest(1),
      internalError(2),
      tryLater(3),
      sigRequired(5),
      unauthorized(6)
    }
```

## 2.227 ASN.1 type 'OCSPSignature'

Source of definition: 'OCSP (RFC 6960)'

```
    30  OCSPSignature ::= SEQUENCE
        {
    30    signatureAlgorithm             AlgorithmIdentifier,
    03    signature                      BIT STRING,
A0[30]    certs              [0] EXPLICIT SEQUENCE OF Certificate OPTIONAL
        }
```

## 2.228 ASN.1 type 'OCSPVersion'

Source of definition: 'OCSP (RFC 6960)'

```
    OCSPVersion ::= INTEGER
02  {
      v1(0)
    }
```

## 2.229 ASN.1 type 'OOBCert'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
CHO OOBCert ::= CMPCertificate
```

## 2.230 ASN.1 type 'OOBCertHash'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
    30 OOBCertHash ::= SEQUENCE
       {
A0[30]   hashAlg [0] EXPLICIT AlgorithmIdentifier OPTIONAL,
A1[30]   certId  [1] EXPLICIT CertId              OPTIONAL,
    03   hashVal              BIT STRING
       }
```

## 2.231 ASN.1 type 'ORAddress'

Source of definition: 'CRL structures'

```
30 ORAddress ::= SEQUENCE
   {
30   built-in-standard-attributes       BuiltInStandardAttributes,
30   built-in-domain-defined-attributes BuiltInDomainDefinedAttributes OPTIONAL,
31   extension-attributes               ExtensionAttributes            OPTIONAL
   }
```

## 2.232 ASN.1 type 'ObjectDigestInfo'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 ObjectDigestInfo ::= SEQUENCE
   {
0A   digestedObjectType ENUMERATED
     {
       publicKey(0),
       publicKeyCert(1),
       otherObjectTypes(2)
     },
06   otherObjectTypeID  OBJECT IDENTIFIER   OPTIONAL,
30   digestAlgorithm    AlgorithmIdentifier,
03   objectDigest       BIT STRING
   }
```

## 2.233 ASN.1 type 'OldCertId'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 OldCertId ::= CertId
```

## 2.234 ASN.1 type 'OptionalValidity'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 OptionalValidity ::= SEQUENCE
   {
A0   notBefore [0] IMPLICIT Time OPTIONAL,
A0   notAfter  [0] IMPLICIT Time OPTIONAL
   }
```

## 2.235 ASN.1 type 'OrganizationName'

Source of definition: 'CRL structures'

```
13 OrganizationName ::= PrintableString (SIZE (1..ub-organization-name-length))
```

## 2.236 ASN.1 type 'OrganizationalUnitName'

Source of definition: 'CRL structures'

```
13 OrganizationalUnitName ::= PrintableString (SIZE (1..ub-organizational-unit-name-length))
```

## 2.237 ASN.1 type 'OrganizationalUnitNames'

Source of definition: 'CRL structures'

```
30 OrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF OrganizationalUnitName
```

## 2.238 ASN.1 type 'OriginatorIdentifierOrKey'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO OriginatorIdentifierOrKey ::= CHOICE
    {
 30   issuerAndSerialNumber              IssuerAndSerialNumber,
 80   subjectKeyIdentifier  [0] IMPLICIT SubjectKeyIdentifier,
 A1   originatorKey         [1] IMPLICIT OriginatorPublicKey
    }
```

## 2.239 ASN.1 type 'OriginatorInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
 30 OriginatorInfo ::= SEQUENCE
    {
 A0   certs [0] IMPLICIT CertificateSet        OPTIONAL,
 A1   crls  [1] IMPLICIT RevocationInfoChoices OPTIONAL
    }
```

## 2.240 ASN.1 type 'OriginatorPublicKey'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
 30 OriginatorPublicKey ::= SEQUENCE
    {
 30   algorithm AlgorithmIdentifier,
 03   publicKey BIT STRING
    }
```

## 2.241 ASN.1 type 'OtherCertificateFormat'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 OtherCertificateFormat ::= SEQUENCE
   {
06   otherCertFormat OBJECT IDENTIFIER,
ANY  otherCert       ANY
   }
```

## 2.242 ASN.1 type 'OtherKeyAttribute'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 OtherKeyAttribute ::= SEQUENCE
   {
06   keyAttrId OBJECT IDENTIFIER,
ANY  keyAttr   ANY
   }
```

## 2.243 ASN.1 type 'OtherPrimeInfo'

Source of definition: 'PKCS #1'

```
30 OtherPrimeInfo ::= SEQUENCE
   {
02   prime       INTEGER,
02   exponent    INTEGER,
02   coefficient INTEGER
   }
```

## 2.244 ASN.1 type 'OtherPrimeInfos'

Source of definition: 'PKCS #1'

```
30 OtherPrimeInfos ::= SEQUENCE SIZE (1..MAX) OF OtherPrimeInfo
```

## 2.245 ASN.1 type 'OtherRecipientInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 OtherRecipientInfo ::= SEQUENCE
   {
06   oriType  OBJECT IDENTIFIER,
ANY  oriValue ANY
   }
```

## 2.246 ASN.1 type 'OtherRevocationInfoFormat'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 OtherRevocationInfoFormat ::= SEQUENCE
   {
06   otherRevInfoFormat OBJECT IDENTIFIER,
ANY  otherRevInfo       ANY
   }
```

## 2.247 ASN.1 type 'P8EncryptedData'

Source of definition: 'PKCS #8'

```
04 P8EncryptedData ::= OCTET STRING
```

## 2.248 ASN.1 type 'PBEParameter'

Source of definition: 'PKCS #5'

```
30 PBEParameter ::= SEQUENCE
   {
04   salt           OCTET STRING (SIZE (8)),
02   iterationCount INTEGER
   }
```

## 2.249 ASN.1 type 'PBES2-params'

Source of definition: 'PKCS #5'

```
30 PBES2-params ::= SEQUENCE
   {
30   keyDerivationFunc AlgorithmIdentifier,
30   encryptionScheme  AlgorithmIdentifier
   }
```

## 2.250 ASN.1 type 'PBKDF2-params'

Source of definition: 'PKCS #5'

```
30 PBKDF2-params ::= SEQUENCE
   {
CHO   salt           CHOICE
      {
04      specified   OCTET STRING,
30      otherSource AlgorithmIdentifier
      },
02    iterationCount INTEGER             (1..MAX),
02    keyLength      INTEGER             (1..MAX) OPTIONAL,
30    prf            AlgorithmIdentifier DEFAULT algid-hmacWithSHA1
   }
```

## 2.251 ASN.1 type 'PBMAC1-params'

Source of definition: 'PKCS #5'

```
30 PBMAC1-params ::= SEQUENCE
   {
30   keyDerivationFunc AlgorithmIdentifier,
30   messageAuthScheme AlgorithmIdentifier
   }
```

## 2.252 ASN.1 type 'PBMParameter'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
PBMParameter ::= SEQUENCE
{
  salt            OCTET STRING,
  owf             AlgorithmIdentifier,
  iterationCount  INTEGER,
  mac             AlgorithmIdentifier
}
```

## 2.253 ASN.1 type 'PDSName'

Source of definition: 'CRL structures'

```
PDSName ::= PrintableString (SIZE (1..ub-pds-name-length))
```

## 2.254 ASN.1 type 'PDSParameter'

Source of definition: 'CRL structures'

```
PDSParameter ::= SET
{
  printable-string PrintableString (SIZE (1..ub-pds-parameter-length)) OPTIONAL,
  teletex-string   TeletexString   (SIZE (1..ub-pds-parameter-length)) OPTIONAL
}
```

## 2.255 ASN.1 type 'PFX'

Source of definition: 'PKCS #12'

```
30 PFX ::= SEQUENCE
   {
02   version  INTEGER
     {
       v3(3)
     },
30   authSafe ContentInfo,
30   macData  MacData     OPTIONAL
   }
```

## 2.256 ASN.1 type 'PKCS12Attribute'

Source of definition: 'PKCS #12'

```
30 PKCS12Attribute ::= Attribute
```

## 2.257 ASN.1 type 'PKCS8ShroudedKeyBag'

Source of definition: 'PKCS #12'

```
30 PKCS8ShroudedKeyBag ::= EncryptedPrivateKeyInfo
```

## 2.258 ASN.1 type 'PKCS9String'

Source of definition: 'PKCS #9'

```
CHO PKCS9String ::= CHOICE
    {
 16   ia5String       IA5String,
CHO   directoryString DirectoryString
    }
```

# 2.259 ASN.1 type 'PKIArchiveOptions'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
CHO PKIArchiveOptions ::= CHOICE
    {
A0    encryptedPrivKey     [0] IMPLICIT CRMFEncryptedKey,
81    keyGenParameters     [1] IMPLICIT KeyGenParameters,
82    archiveRemGenPrivKey [2] IMPLICIT BOOLEAN
    }
```

## 2.260 ASN.1 type 'PKIBody'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
   CHO PKIBody ::= CHOICE
       {
A0[30]   ir         [0] EXPLICIT CertReqMessages,
A1[30]   ip         [1] EXPLICIT CertRepMessage,
A2[30]   cr         [2] EXPLICIT CertReqMessages,
A3[30]   cp         [3] EXPLICIT CertRepMessage,
A4[30]   p10cr      [4] EXPLICIT CertificationRequest,
A5[30]   popdecc    [5] EXPLICIT POPODecKeyChallContent,
A6[30]   popdecr    [6] EXPLICIT POPODecKeyRespContent,
A7[30]   kur        [7] EXPLICIT CertReqMessages,
A8[30]   kup        [8] EXPLICIT CertRepMessage,
A9[30]   krr        [9] EXPLICIT CertReqMessages,
AA[30]   krp       [10] EXPLICIT KeyRecRepContent,
AB[30]   rr        [11] EXPLICIT RevReqContent,
AC[30]   rp        [12] EXPLICIT RevRepContent,
AD[30]   ccr       [13] EXPLICIT CertReqMessages,
AE[30]   ccp       [14] EXPLICIT CertRepMessage,
AF[30]   ckuann    [15] EXPLICIT CAKeyUpdAnnContent,
    B0   cann      [16] EXPLICIT CertAnnContent,
B1[30]   rann      [17] EXPLICIT RevAnnContent,
B2[30]   crlann    [18] EXPLICIT CRLAnnContent,
B3[05]   pkiconf   [19] EXPLICIT PKIConfirmContent,
B4[30]   nested    [20] EXPLICIT NestedMessageContent,
B5[30]   genm      [21] EXPLICIT GenMsgContent,
B6[30]   genp      [22] EXPLICIT GenRepContent,
B7[30]   error     [23] EXPLICIT ErrorMsgContent,
B8[30]   certConf  [24] EXPLICIT CertConfirmContent,
B9[30]   pollReq   [25] EXPLICIT PollReqContent,
BA[30]   pollRep   [26] EXPLICIT PollRepContent
       }
```

## 2.261 ASN.1 type 'PKIConfirmContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
05 PKIConfirmContent ::= NULL
```

## 2.262 ASN.1 type 'PKIFailureInfo'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
PKIFailureInfo ::= BIT STRING
{
  badAlg(0),
  badMessageCheck(1),
  badRequest(2),
  badTime(3),
  badCertId(4),
  badDataFormat(5),
  wrongAuthority(6),
  incorrectData(7),
  missingTimeStamp(8),
  badPOP(9),
  certRevoked(10),
  certConfirmed(11),
  wrongIntegrity(12),
  badRecipientNonce(13),
  timeNotAvailable(14),
  unacceptedPolicy(15),
  unacceptedExtension(16),
  addInfoNotAvailable(17),
  badSenderNonce(18),
  badCertTemplate(19),
  signerNotTrusted(20),
  transactionIdInUse(21),
  unsupportedVersion(22),
  notAuthorized(23),
  systemUnavail(24),
  systemFailure(25),
  duplicateCertReq(26)
}
```

## 2.263 ASN.1 type 'PKIFreeText'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
PKIFreeText ::= SEQUENCE SIZE (1..MAX) OF UTF8String
```

## 2.264 ASN.1 type 'PKIHeader'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
    30 PKIHeader ::= SEQUENCE
       {
    02   pvno                        INTEGER
         {
           cmp1999(1),
           cmp2000(2)
         },
   CHO   sender                      GeneralName,
   CHO   recipient                   GeneralName,
A0[18]   messageTime    [0] EXPLICIT GeneralizedTime                          OPTIONAL,
A1[30]   protectionAlg  [1] EXPLICIT AlgorithmIdentifier                      OPTIONAL,
A2[04]   senderKID      [2] EXPLICIT KeyIdentifier                            OPTIONAL,
A3[04]   recipKID       [3] EXPLICIT KeyIdentifier                            OPTIONAL,
A4[04]   transactionID  [4] EXPLICIT OCTET STRING                             OPTIONAL,
A5[04]   senderNonce    [5] EXPLICIT OCTET STRING                             OPTIONAL,
A6[04]   recipNonce     [6] EXPLICIT OCTET STRING                             OPTIONAL,
A7[30]   freeText       [7] EXPLICIT PKIFreeText                              OPTIONAL,
A8[30]   generalInfo    [8] EXPLICIT SEQUENCE SIZE (1..MAX) OF InfoTypeAndValue OPTIONAL
       }
```

## 2.265 ASN.1 type 'PKIMessage'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
    30 PKIMessage ::= SEQUENCE
       {
    30   header                  PKIHeader,
   CHO   body                    PKIBody,
A0[03]   protection [0] EXPLICIT PKIProtection                          OPTIONAL,
A1[30]   extraCerts [1] EXPLICIT SEQUENCE SIZE (1..MAX) OF CMPCertificate OPTIONAL
       }
```

## 2.266 ASN.1 type 'PKIMessages'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 PKIMessages ::= SEQUENCE SIZE (1..MAX) OF PKIMessage
```

## 2.267 ASN.1 type 'PKIProtection'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
PKIProtection ::= BIT STRING
```

## 2.268 ASN.1 type 'PKIPublicationInfo'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
PKIPublicationInfo ::= SEQUENCE
{
  action   INTEGER
  {
    dontPublish(0),
    pleasePublish(1)
  },
  pubInfos SEQUENCE SIZE (1..MAX) OF SinglePubInfo OPTIONAL
}
```

## 2.269 ASN.1 type 'PKIStatus'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
PKIStatus ::= INTEGER
{
  accepted(0),
  grantedWithMods(1),
  rejection(2),
  waiting(3),
  revocationWarning(4),
  revocationNotification(5),
  keyUpdateWarning(6)
}
```

## 2.270 ASN.1 type 'PKIStatusInfo'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
PKIStatusInfo ::= SEQUENCE
{
  status       PKIStatus,
  statusString PKIFreeText    OPTIONAL,
  failInfo     PKIFailureInfo OPTIONAL
}
```

## 2.271 ASN.1 type 'PKMACValue'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
PKMACValue ::= SEQUENCE
{
  algId AlgorithmIdentifier,
  value BIT STRING
}
```

## 2.272 ASN.1 type 'POPODecKeyChallContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
POPODecKeyChallContent ::= SEQUENCE OF Challenge
```

## 2.273 ASN.1 type 'POPODecKeyRespContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
POPODecKeyRespContent ::= SEQUENCE OF INTEGER
```

## 2.274 ASN.1 type 'POPOPrivKey'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
CHO POPOPrivKey ::= CHOICE
    {
 80   thisMessage       [0] IMPLICIT BIT STRING,
 81   subsequentMessage [1] IMPLICIT SubsequentMessage,
 82   dhMAC             [2] IMPLICIT BIT STRING,
 A3   agreeMAC          [3] IMPLICIT PKMACValue,
 A4   encryptedKey      [4] IMPLICIT EnvelopedData
    }
```

## 2.275 ASN.1 type 'POPOSigningKey'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 POPOSigningKey ::= SEQUENCE
    {
A0   poposkInput         [0] IMPLICIT POPOSigningKeyInput OPTIONAL,
30   algorithmIdentifier             AlgorithmIdentifier,
03   signature                       BIT STRING
    }
```

## 2.276 ASN.1 type 'POPOSigningKeyInput'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 POPOSigningKeyInput ::= SEQUENCE
    {
CHO   authInfo  CHOICE
      {
A0      sender       [0] IMPLICIT GeneralName,
30      publicKeyMAC             PKMACValue
      },
30    publicKey SubjectPublicKeyInfo
    }
```

## 2.277 ASN.1 type 'PartialAttribute'

Source of definition: 'LDAP (RFC 4511)'

```
30 PartialAttribute ::= SEQUENCE
   {
04   type AttributeDescription,
31   vals SET OF LDAPAttributeValue
   }
```

## 2.278 ASN.1 type 'PartialAttributeList'

Source of definition: 'LDAP (RFC 4511)'

```
30 PartialAttributeList ::= SEQUENCE OF PartialAttribute
```

## 2.279 ASN.1 type 'PasswordRecipientInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 PasswordRecipientInfo ::= SEQUENCE
   {
02   version                              CMSVersion,
A0   keyDerivationAlgorithm [0] IMPLICIT KeyDerivationAlgorithmIdentifier OPTIONAL,
30   keyEncryptionAlgorithm              KeyEncryptionAlgorithmIdentifier,
04   encryptedKey                        EncryptedKey
   }
```

## 2.280 ASN.1 type 'Pentanomial'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 Pentanomial ::= SEQUENCE
   {
02   k1 INTEGER,
02   k2 INTEGER,
02   k3 INTEGER
   }
```

## 2.281 ASN.1 type 'PersonalName'

Source of definition: 'CRL structures'

```
31 PersonalName ::= SET
   {
80   surname              [0] IMPLICIT PrintableString (SIZE (1..ub-surname-length)),
81   given-name           [1] IMPLICIT PrintableString (SIZE (1..ub-given-name-length)) OPTIONAL,
82   initials             [2] IMPLICIT PrintableString (SIZE (1..ub-initials-length)) OPTIONAL,
83   generation-qualifier [3] IMPLICIT PrintableString (SIZE (1..ub-generation-qualifier-length)) OPTIONAL
   }
```

## 2.282 ASN.1 type 'PhysicalDeliveryCountryName'

Source of definition: 'CRL structures'

```
CHO PhysicalDeliveryCountryName ::= CHOICE
    {
 12   x121-dcc-code         NumericString   (SIZE (ub-country-name-numeric-length)),
 13   iso-3166-alpha2-code PrintableString (SIZE (ub-country-name-alpha-length))
    }
```

## 2.283 ASN.1 type 'PhysicalDeliveryOfficeName'

Source of definition: 'CRL structures'

```
31 PhysicalDeliveryOfficeName ::= PDSParameter
```

## 2.284 ASN.1 type 'PhysicalDeliveryOfficeNumber'

Source of definition: 'CRL structures'

```
31 PhysicalDeliveryOfficeNumber ::= PDSParameter
```

## 2.285 ASN.1 type 'PhysicalDeliveryOrganizationName'

Source of definition: 'CRL structures'

```
31 PhysicalDeliveryOrganizationName ::= PDSParameter
```

## 2.286 ASN.1 type 'PhysicalDeliveryPersonalName'

Source of definition: 'CRL structures'

```
31 PhysicalDeliveryPersonalName ::= PDSParameter
```

## 2.287 ASN.1 type 'PolicyConstraints'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 PolicyConstraints ::= SEQUENCE
   {
80   requireExplicitPolicy [0] IMPLICIT SkipCerts OPTIONAL,
81   inhibitPolicyMapping  [1] IMPLICIT SkipCerts OPTIONAL
   }
```

## 2.288 ASN.1 type 'PolicyInformation'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 PolicyInformation ::= SEQUENCE
   {
06   policyIdentifier CertPolicyId,
30   policyQualifiers SEQUENCE SIZE (1..MAX) OF PolicyQualifierInfo OPTIONAL
   }
```

## 2.289 ASN.1 type 'PolicyMappings'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 PolicyMappings ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE
   {
06   issuerDomainPolicy  CertPolicyId,
06   subjectDomainPolicy CertPolicyId
   }
```

## 2.290 ASN.1 type 'PolicyQualifierId'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
   PolicyQualifierId ::= OBJECT IDENTIFIER
06 {
     id-qt-cps(1.3.6.1.5.5.7.2.1),
     id-qt-unotice(1.3.6.1.5.5.7.2.2)
   }
```

## 2.291 ASN.1 type 'PolicyQualifierInfo'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 PolicyQualifierInfo ::= SEQUENCE
   {
06   policyQualifierId PolicyQualifierId,
ANY  qualifier         ANY
   }
```

## 2.292 ASN.1 type 'PollRepContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 PollRepContent ::= SEQUENCE OF SEQUENCE
   {
02   certReqId  INTEGER,
02   checkAfter INTEGER,
30   reason     PKIFreeText OPTIONAL
   }
```

## 2.293 ASN.1 type 'PollReqContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 PollReqContent ::= SEQUENCE OF SEQUENCE
   {
02   certReqId INTEGER
   }
```

## 2.294 ASN.1 type 'PostOfficeBoxAddress'

Source of definition: 'CRL structures'

```
31 PostOfficeBoxAddress ::= PDSParameter
```

## 2.295 ASN.1 type 'PostalCode'

Source of definition: 'CRL structures'

```
CHO PostalCode ::= CHOICE
    {
 12   numeric-code   NumericString   (SIZE (1..ub-postal-code-length)),
 13   printable-code PrintableString (SIZE (1..ub-postal-code-length))
    }
```

## 2.296 ASN.1 type 'PosteRestanteAddress'

Source of definition: 'CRL structures'

```
31 PosteRestanteAddress ::= PDSParameter
```

## 2.297 ASN.1 type 'PreferredSignatureAlgorithm'

Source of definition: 'OCSP (RFC 6960)'

```
30 PreferredSignatureAlgorithm ::= SEQUENCE
   {
30   sigIdentifier  AlgorithmIdentifier,
30   certIdentifier AlgorithmIdentifier OPTIONAL
   }
```

## 2.298 ASN.1 type 'PreferredSignatureAlgorithms'

Source of definition: 'OCSP (RFC 6960)'

```
30 PreferredSignatureAlgorithms ::= SEQUENCE OF PreferredSignatureAlgorithm
```

## 2.299 ASN.1 type 'PresentationAddress'

Source of definition: 'CRL structures'

```
    30 PresentationAddress ::= SEQUENCE
       {
A0[04]   pSelector  [0] EXPLICIT OCTET STRING                      OPTIONAL,
A1[04]   sSelector  [1] EXPLICIT OCTET STRING                      OPTIONAL,
A2[04]   tSelector  [2] EXPLICIT OCTET STRING                      OPTIONAL,
A3[31]   nAddresses [3] EXPLICIT SET SIZE (1..MAX) OF OCTET STRING
       }
```

## 2.300 ASN.1 type 'Prime-p'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
02 Prime-p ::= INTEGER
```

## 2.301 ASN.1 type 'PrivateDomainName'

Source of definition: 'CRL structures'

```
CHO PrivateDomainName ::= CHOICE
    {
12    numeric   NumericString   (SIZE (1..ub-domain-name-length)),
13    printable PrintableString (SIZE (1..ub-domain-name-length))
    }
```

## 2.302 ASN.1 type 'PrivateKey'

Source of definition: 'PKCS #8'

```
04 PrivateKey ::= OCTET STRING
```

## 2.303 ASN.1 type 'PrivateKeyInfo'

Source of definition: 'PKCS #8'

```
30 PrivateKeyInfo ::= SEQUENCE
   {
02   version                         INTEGER
     {
       v1(0)
     },
30   privateKeyAlgorithm             AlgorithmIdentifier,
04   privateKey                      PrivateKey,
A0   attributes          [0] IMPLICIT AttributeSet        OPTIONAL
   }
```

## 2.304 ASN.1 type 'PrivateKeyUsagePeriod'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 PrivateKeyUsagePeriod ::= SEQUENCE
   {
80   notBefore [0] IMPLICIT GeneralizedTime OPTIONAL,
81   notAfter  [1] IMPLICIT GeneralizedTime OPTIONAL
   }
```

## 2.305 ASN.1 type 'ProofOfPossession'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
CHO ProofOfPossession ::= CHOICE
    {
 80   raVerified      [0] IMPLICIT NULL,
 A1   signature       [1] IMPLICIT POPOSigningKey,
 A2   keyEncipherment [2] IMPLICIT POPOPrivKey,
 A3   keyAgreement    [3] IMPLICIT POPOPrivKey
    }
```

## 2.306 ASN.1 type 'ProtectedPart'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
 30 ProtectedPart ::= SEQUENCE
    {
 30   header PKIHeader,
CHO   body   PKIBody
    }
```

## 2.307 ASN.1 type 'ProtocolEncrKey'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 ProtocolEncrKey ::= SubjectPublicKeyInfo
```

## 2.308 ASN.1 type 'ProxyInfo'

Source of definition: 'AttributeCertificateVersion1 (RFC 5662)'

```
30 ProxyInfo ::= SEQUENCE OF Targets
```

## 2.309 ASN.1 type 'RC2-CBC-Parameter'

Source of definition: 'PKCS #5'

```
30 RC2-CBC-Parameter ::= SEQUENCE
   {
02   rc2ParameterVersion INTEGER      OPTIONAL,
04   iv                  OCTET STRING (SIZE (8))
   }
```

## 2.310 ASN.1 type 'RC5-CBC-Parameters'

Source of definition: 'PKCS #5'

```
30 RC5-CBC-Parameters ::= SEQUENCE
   {
02   version         INTEGER
     {
       v1-0(16)
     },
02   rounds          INTEGER      (8..127),
02   blockSizeInBits INTEGER      (64..128),
04   iv              OCTET STRING OPTIONAL
   }
```

## 2.311 ASN.1 type 'RDNSequence'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
30 RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
```

## 2.312 ASN.1 type 'RSAES-OAEP-params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

```
      30 RSAES-OAEP-params ::= SEQUENCE
         {
   A0[30]   hashFunc    [0] EXPLICIT AlgorithmIdentifier DEFAULT sha1Identifier,
   A1[30]   maskGenFunc [1] EXPLICIT AlgorithmIdentifier DEFAULT mgf1SHA1Identifier,
   A2[30]   pSourceFunc [2] EXPLICIT AlgorithmIdentifier DEFAULT pSpecifiedEmptyIdentifier
         }
```

## 2.313 ASN.1 type 'RSAPKVersion'

Source of definition: 'PKCS #1'

```
      RSAPKVersion ::= INTEGER
   02 {
        two-prime(0),
        multi(1)
      }
```

## 2.314 ASN.1 type 'RSAPrivateKey'

Source of definition: 'PKCS #1'

```
   30 RSAPrivateKey ::= SEQUENCE
      {
   02   version         RSAPKVersion,
   02   modulus         INTEGER,
   02   publicExponent  INTEGER,
   02   privateExponent INTEGER,
   02   prime1          INTEGER,
   02   prime2          INTEGER,
   02   exponent1       INTEGER,
   02   exponent2       INTEGER,
   02   coefficient     INTEGER,
   30   otherPrimeInfos OtherPrimeInfos OPTIONAL
      }
```

## 2.315 ASN.1 type 'RSAPublicKey'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 RSAPublicKey ::= SEQUENCE
   {
02   modulus         INTEGER,
02   publicExponent  INTEGER
   }
```

## 2.316 ASN.1 type 'RSASSA-PSS-params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

```
    30 RSASSA-PSS-params ::= SEQUENCE
       {
A0[30]   hashAlgorithm    [0] EXPLICIT HashAlgorithm    DEFAULT sha1Identifier,
A1[30]   maskGenAlgorithm [1] EXPLICIT MaskGenAlgorithm DEFAULT mgf1SHA1Identifier,
A2[02]   saltLength       [2] EXPLICIT INTEGER          DEFAULT 20,
A3[02]   trailerField     [3] EXPLICIT TrailerField     DEFAULT trailerFieldBC
       }
```

## 2.317 ASN.1 type 'Rand'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 Rand ::= SEQUENCE
   {
02   int    INTEGER,
CHO  sender GeneralName
   }
```

## 2.318 ASN.1 type 'ReasonFlags'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
ReasonFlags ::= BIT STRING
{
  unused(0),
  keyCompromise(1),
  cACompromise(2),
  affiliationChanged(3),
  superseded(4),
  cessationOfOperation(5),
  certificateHold(6),
  privilegeWithdrawn(7),
  aACompromise(8)
}
```

## 2.319 ASN.1 type 'RecipientEncryptedKey'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
RecipientEncryptedKey ::= SEQUENCE
{
  rid           KeyAgreeRecipientIdentifier,
  encryptedKey  EncryptedKey
}
```

## 2.320 ASN.1 type 'RecipientEncryptedKeys'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
RecipientEncryptedKeys ::= SEQUENCE OF RecipientEncryptedKey
```

## 2.321 ASN.1 type 'RecipientIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO RecipientIdentifier ::= CHOICE
    {
 30   issuerAndSerialNumber              IssuerAndSerialNumber,
 80   subjectKeyIdentifier  [0] IMPLICIT SubjectKeyIdentifier
    }
```

## 2.322 ASN.1 type 'RecipientInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO RecipientInfo ::= CHOICE
    {
 30   ktri               KeyTransRecipientInfo,
 A1   kari  [1] IMPLICIT KeyAgreeRecipientInfo,
 A2   kekri [2] IMPLICIT KEKRecipientInfo,
 A3   pwri  [3] IMPLICIT PasswordRecipientInfo,
 A4   ori   [4] IMPLICIT OtherRecipientInfo
    }
```

## 2.323 ASN.1 type 'RecipientInfos'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 RecipientInfos ::= SET SIZE (1..MAX) OF RecipientInfo
```

## 2.324 ASN.1 type 'RecipientKeyIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 RecipientKeyIdentifier ::= SEQUENCE
   {
04   subjectKeyIdentifier SubjectKeyIdentifier,
18   date                 GeneralizedTime      OPTIONAL,
30   other                OtherKeyAttribute    OPTIONAL
   }
```

## 2.325 ASN.1 type 'Referral'

Source of definition: 'LDAP (RFC 4511)'

```
30 Referral ::= SEQUENCE SIZE (1..MAX) OF URI
```

## 2.326 ASN.1 type 'RegToken'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
0C RegToken ::= UTF8String
```

## 2.327 ASN.1 type 'RelativeDistinguishedName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

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

## 2.328 ASN.1 type 'RelativeLDAPDN'

Source of definition: 'LDAP (RFC 4511)'

```
04 RelativeLDAPDN ::= LDAPString
```

## 2.329 ASN.1 type 'Request'

Source of definition: 'OCSP (RFC 6960)'

```
    30 Request ::= SEQUENCE
       {
    30   reqCert                                  CertID,
A0[30]   singleRequestExtensions [0] EXPLICIT Extensions OPTIONAL
       }
```

## 2.330 ASN.1 type 'ResponderID'

Source of definition: 'OCSP (RFC 6960)'

```
   CHO ResponderID ::= CHOICE
       {
    A1   byName [1] EXPLICIT Name,
A2[04]   byKey  [2] EXPLICIT KeyHash
       }
```

## 2.331 ASN.1 type 'ResponseBytes'

Source of definition: 'OCSP (RFC 6960)'

```
30 ResponseBytes ::= SEQUENCE
   {
06   responseType OBJECT IDENTIFIER,
04   response     OCTET STRING
   }
```

## 2.332 ASN.1 type 'ResponseData'

Source of definition: 'OCSP (RFC 6960)'

```
    30 ResponseData ::= SEQUENCE
       {
A0[02]   version            [0] EXPLICIT Version                    DEFAULT v1,
   CHO   responderID                    ResponderID,
    18   producedAt                     GeneralizedTime,
    30   responses                      SEQUENCE OF SingleResponse,
A1[30]   responseExtensions [1] EXPLICIT Extensions                 OPTIONAL
       }
```

## 2.333 ASN.1 type 'RevAnnContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 RevAnnContent ::= SEQUENCE
   {
02   status          PKIStatus,
30   certId          CertId,
18   willBeRevokedAt GeneralizedTime,
18   badSinceDate    GeneralizedTime,
30   crlDetails      Extensions      OPTIONAL
   }
```

## 2.334 ASN.1 type 'RevDetails'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 RevDetails ::= SEQUENCE
   {
30   certDetails     CertTemplate,
30   crlEntryDetails Extensions   OPTIONAL
   }
```

## 2.335 ASN.1 type 'RevRepContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
    30 RevRepContent ::= SEQUENCE
       {
    30   status                SEQUENCE SIZE (1..MAX) OF PKIStatusInfo,
A0[30]   revCerts [0] EXPLICIT SEQUENCE SIZE (1..MAX) OF CertId          OPTIONAL,
A1[30]   crls     [1] EXPLICIT SEQUENCE SIZE (1..MAX) OF CertificateList OPTIONAL
       }
```

## 2.336 ASN.1 type 'RevReqContent'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

```
30 RevReqContent ::= SEQUENCE OF RevDetails
```

## 2.337 ASN.1 type 'RevocationInfoChoice'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO RevocationInfoChoice ::= CHOICE
    {
 30   crl                CertificateList,
 A1   other [1] IMPLICIT OtherRevocationInfoFormat
    }
```

## 2.338 ASN.1 type 'RevocationInfoChoices'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 RevocationInfoChoices ::= SET OF RevocationInfoChoice
```

## 2.339 ASN.1 type 'RevokedInfo'

Source of definition: 'OCSP (RFC 6960)'

```
    30 RevokedInfo ::= SEQUENCE
       {
    18   revocationTime               GeneralizedTime,
A0[0A]   revocationReason [0] EXPLICIT CRLReason       OPTIONAL
       }
```

## 2.340 ASN.1 type 'RoleSyntax'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 RoleSyntax ::= SEQUENCE
   {
A0   roleAuthority [0] IMPLICIT GeneralNames OPTIONAL,
A1   roleName      [1] IMPLICIT GeneralName
   }
```

## 2.341 ASN.1 type 'SafeBag'

Source of definition: 'PKCS #12'

```
30 SafeBag ::= SEQUENCE
   {
06   bagId                     OBJECT IDENTIFIER,
A0   bagValue      [0] EXPLICIT ANY,
31   bagAttributes             SET OF PKCS12Attribute OPTIONAL
   }
```

## 2.342 ASN.1 type 'SafeContents'

Source of definition: 'PKCS #12'

```
30 SafeContents ::= SEQUENCE OF SafeBag
```

## 2.343 ASN.1 type 'SaslCredentials'

Source of definition: 'LDAP (RFC 4511)'

```
30 SaslCredentials ::= SEQUENCE
   {
04   mechanism   LDAPString,
04   credentials OCTET STRING OPTIONAL
   }
```

## 2.344 ASN.1 type 'SearchRequest'

Source of definition: 'LDAP (RFC 4511)'

```
63 SearchRequest ::= [APPLICATION 3] IMPLICIT SEQUENCE
   {
04   baseObject   LDAPDN,
0A   scope        ENUMERATED
     {
       baseObject(0),
       singleLevel(1),
       wholeSubtree(2)
     },
0A   derefAliases ENUMERATED
     {
       neverDerefAliases(0),
       derefInSearching(1),
       derefFindingBaseObj(2),
       derefAlways(3)
     },
02   sizeLimit    INTEGER            (0..maxInt),
02   timeLimit    INTEGER            (0..maxInt),
01   typesOnly    BOOLEAN,
CHO  filter       Filter,
30   attributes   AttributeSelection
   }
```

## 2.345 ASN.1 type 'SearchResultDone'

Source of definition: 'LDAP (RFC 4511)'

```
65 SearchResultDone ::= [APPLICATION 5] IMPLICIT LDAPResult
```

## 2.346 ASN.1 type 'SearchResultEntry'

Source of definition: 'LDAP (RFC 4511)'

```
64 SearchResultEntry ::= [APPLICATION 4] IMPLICIT SEQUENCE
   {
04   objectName LDAPDN,
30   attributes PartialAttributeList
   }
```

## 2.347 ASN.1 type 'SearchResultReference'

Source of definition: 'LDAP (RFC 4511)'

```
73 SearchResultReference ::= [APPLICATION 19] IMPLICIT SEQUENCE SIZE (1..MAX) OF URI
```

## 2.348 ASN.1 type 'SecretBag'

Source of definition: 'PKCS #12'

```
30 SecretBag ::= SEQUENCE
   {
06   secretTypeId              OBJECT IDENTIFIER,
A0   secretValue  [0] EXPLICIT ANY
   }
```

## 2.349 ASN.1 type 'SecurityCategory'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 SecurityCategory ::= SEQUENCE
   {
80   type  [0] IMPLICIT OBJECT IDENTIFIER,
A1   value [1] EXPLICIT ANY
   }
```

## 2.350 ASN.1 type 'ServiceLocator'

Source of definition: 'OCSP (RFC 6960)'

```
 30 ServiceLocator ::= SEQUENCE
    {
CHO   issuer  Name,
 30   locator AuthorityInfoAccessSyntax
    }
```

## 2.351 ASN.1 type 'Signature'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
03 Signature ::= BIT STRING
```

## 2.352 ASN.1 type 'SignatureAlgorithmIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 SignatureAlgorithmIdentifier ::= AlgorithmIdentifier
```

## 2.353 ASN.1 type 'SignatureValue'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
04 SignatureValue ::= OCTET STRING
```

## 2.354 ASN.1 type 'SignedAttributes'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 SignedAttributes ::= SET SIZE (1..MAX) OF Attribute
```

## 2.355 ASN.1 type 'SignedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 SignedData ::= SEQUENCE
   {
02   version                    CMSVersion,
31   digestAlgorithms           DigestAlgorithmIdentifiers,
30   encapContentInfo           EncapsulatedContentInfo,
A0   certificates     [0] IMPLICIT CertificateSet           OPTIONAL,
A1   crls             [1] IMPLICIT RevocationInfoChoices    OPTIONAL,
31   signerInfos                SignerInfos
   }
```

## 2.356 ASN.1 type 'SignerIdentifier'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO SignerIdentifier ::= CHOICE
    {
 30   issuerAndSerialNumber             IssuerAndSerialNumber,
 80   subjectKeyIdentifier  [0] IMPLICIT SubjectKeyIdentifier
    }
```

## 2.357 ASN.1 type 'SignerInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
30 SignerInfo ::= SEQUENCE
   {
02   version                         CMSVersion,
CHO  sid                             SignerIdentifier,
30   digestAlgorithm                 DigestAlgorithmIdentifier,
A0   signedAttrs        [0] IMPLICIT SignedAttributes             OPTIONAL,
30   signatureAlgorithm              SignatureAlgorithmIdentifier,
04   signature                       SignatureValue,
A1   unsignedAttrs      [1] IMPLICIT UnsignedAttributes           OPTIONAL
   }
```

## 2.358 ASN.1 type 'SignerInfos'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 SignerInfos ::= SET OF SignerInfo
```

## 2.359 ASN.1 type 'SigningTime'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
CHO SigningTime ::= Time
```

## 2.360 ASN.1 type 'SinglePubInfo'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
30 SinglePubInfo ::= SEQUENCE
   {
02   pubMethod    INTEGER
     {
       dontCare(0),
       x500(1),
       web(2),
       ldap(3)
     },
CHO  pubLocation GeneralName OPTIONAL
   }
```

## 2.361 ASN.1 type 'SingleResponse'

Source of definition: 'OCSP (RFC 6960)'

```
    30 SingleResponse ::= SEQUENCE
       {
    30   certID                       CertID,
   CHO   certStatus                   CertStatus,
    18   thisUpdate                   GeneralizedTime,
A0[18]   nextUpdate       [0] EXPLICIT GeneralizedTime OPTIONAL,
A1[30]   singleExtensions [1] EXPLICIT Extensions      OPTIONAL
       }
```

## 2.362 ASN.1 type 'SkipCerts'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
02 SkipCerts ::= INTEGER (0..MAX)
```

## 2.363 ASN.1 type 'StreetAddress'

Source of definition: 'CRL structures'

```
31 StreetAddress ::= PDSParameter
```

## 2.364 ASN.1 type 'SubjectAltName'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 SubjectAltName ::= GeneralNames
```

## 2.365 ASN.1 type 'SubjectDirectoryAttributes'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 SubjectDirectoryAttributes ::= SEQUENCE SIZE (1..MAX) OF Attribute
```

## 2.366 ASN.1 type 'SubjectInfoAccessSyntax'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 SubjectInfoAccessSyntax ::= SEQUENCE SIZE (1..MAX) OF AccessDescription
```

## 2.367 ASN.1 type 'SubjectKeyIdentifier'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
04 SubjectKeyIdentifier ::= KeyIdentifier
```

## 2.368 ASN.1 type 'SubjectPublicKeyInfo'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

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

## 2.369 ASN.1 type 'SubsequentMessage'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
SubsequentMessage ::= INTEGER
{
  encrCert(0),
  challengeResp(1)
}
```

## 2.370 ASN.1 type 'SubstringFilter'

Source of definition: 'LDAP (RFC 4511)'

```
SubstringFilter ::= SEQUENCE
{
  type       AttributeDescription,
  substrings SEQUENCE SIZE (1..MAX) OF CHOICE
  {
    initial [0] IMPLICIT AssertionValue,
    any     [1] IMPLICIT AssertionValue,
    final   [2] IMPLICIT AssertionValue
  }
}
```

## 2.371 ASN.1 type 'SvceAuthInfo'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30  SvceAuthInfo ::= SEQUENCE
    {
CHO   service  GeneralName,
CHO   ident    GeneralName,
04    authInfo OCTET STRING OPTIONAL
    }
```

## 2.372 ASN.1 type 'TBSCertList'

Source of definition: 'CRL structures'

```
    30  TBSCertList ::= SEQUENCE
        {
    02    version                   Version              OPTIONAL,
    30    signature                 AlgorithmIdentifier,
    CHO   issuer                    Name,
    CHO   thisUpdate                Time,
    CHO   nextUpdate                Time                 OPTIONAL,
    30    revokedCertificates       SEQUENCE OF SEQUENCE
          {
    02      userCertificate     CertificateSerialNumber,
    CHO     revocationDate      Time,
    30      crlEntryExtensions  Extensions           OPTIONAL
          } OPTIONAL,
A0[30]    crlExtensions       [0] EXPLICIT Extensions      OPTIONAL
        }
```

## 2.373 ASN.1 type 'TBSCertificate'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
    30 TBSCertificate ::= SEQUENCE
       {
A0[02]   version              [0] EXPLICIT Version                 DEFAULT v1,
    02   serialNumber                   CertificateSerialNumber,
    30   signature                      AlgorithmIdentifier,
   CHO   issuer                         Name,
    30   validity                       Validity,
   CHO   subject                        Name,
    30   subjectPublicKeyInfo           SubjectPublicKeyInfo,
    81   issuerUniqueID           [1] IMPLICIT UniqueIdentifier        OPTIONAL,
    82   subjectUniqueID          [2] IMPLICIT UniqueIdentifier        OPTIONAL,
A3[30]   extensions               [3] EXPLICIT Extensions              OPTIONAL
       }
```

## 2.374 ASN.1 type 'TBSRequest'

Source of definition: 'OCSP (RFC 6960)'

```
    30 TBSRequest ::= SEQUENCE
       {
A0[02]   version            [0] EXPLICIT OCSPVersion         DEFAULT v1,
    A1   requestorName      [1] EXPLICIT GeneralName         OPTIONAL,
    30   requestList                     SEQUENCE OF Request,
A2[30]   requestExtensions  [2] EXPLICIT Extensions          OPTIONAL
       }
```

## 2.375 ASN.1 type 'Target'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
CHO Target ::= CHOICE
    {
 A0   targetName  [0] IMPLICIT GeneralName,
 A1   targetGroup [1] IMPLICIT GeneralName,
 A2   targetCert  [2] IMPLICIT TargetCert
    }
```

## 2.376 ASN.1 type 'TargetCert'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 TargetCert ::= SEQUENCE
   {
30   targetCertificate IssuerSerial,
CHO  targetName        GeneralName      OPTIONAL,
30   certDigestInfo    ObjectDigestInfo OPTIONAL
   }
```

## 2.377 ASN.1 type 'Targets'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 Targets ::= SEQUENCE OF Target
```

## 2.378 ASN.1 type 'TeletexCommonName'

Source of definition: 'CRL structures'

```
14 TeletexCommonName ::= TeletexString (SIZE (1..ub-common-name-length))
```

## 2.379 ASN.1 type 'TeletexDomainDefinedAttribute'

Source of definition: 'CRL structures'

```
30 TeletexDomainDefinedAttribute ::= SEQUENCE
   {
14   type  TeletexString (SIZE (1..ub-domain-defined-attribute-type-length)),
14   value TeletexString (SIZE (1..ub-domain-defined-attribute-value-length))
   }
```

## 2.380 ASN.1 type 'TeletexDomainDefinedAttributes'

Source of definition: 'CRL structures'

```
30 TeletexDomainDefinedAttributes ::= SEQUENCE SIZE (1..ub-domain-defined-attributes) OF TeletexDomainDefinedAttribute
```

## 2.381 ASN.1 type 'TeletexOrganizationName'

Source of definition: 'CRL structures'

```
14 TeletexOrganizationName ::= TeletexString (SIZE (1..ub-organization-name-length))
```

## 2.382 ASN.1 type 'TeletexOrganizationalUnitName'

Source of definition: 'CRL structures'

```
14 TeletexOrganizationalUnitName ::= TeletexString (SIZE (1..ub-organizational-unit-name-length))
```

## 2.383 ASN.1 type 'TeletexOrganizationalUnitNames'

Source of definition: 'CRL structures'

```
30 TeletexOrganizationalUnitNames ::= SEQUENCE SIZE (1..ub-organizational-units) OF TeletexOrganizationalUnitName
```

## 2.384 ASN.1 type 'TeletexPersonalName'

Source of definition: 'CRL structures'

```
31 TeletexPersonalName ::= SET
   {
80   surname              [0] IMPLICIT TeletexString (SIZE (1..ub-surname-length)),
81   given-name           [1] IMPLICIT TeletexString (SIZE (1..ub-given-name-length)) OPTIONAL,
82   initials             [2] IMPLICIT TeletexString (SIZE (1..ub-initials-length)) OPTIONAL,
83   generation-qualifier [3] IMPLICIT TeletexString (SIZE (1..ub-generation-qualifier-length)) OPTIONAL
   }
```

## 2.385 ASN.1 type 'TerminalIdentifier'

Source of definition: 'CRL structures'

```
13 TerminalIdentifier ::= PrintableString (SIZE (1..ub-terminal-id-length))
```

## 2.386 ASN.1 type 'TerminalType'

Source of definition: 'CRL structures'

```
   TerminalType ::= INTEGER (0..ub-integer-options)
02 {
     telex(3),
     teletex(4),
     g3-facsimile(5),
     g4-facsimile(6),
     ia5-terminal(7),
     videotex(8)
   }
```

## 2.387 ASN.1 type 'Time'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO Time ::= CHOICE
    {
 17   utcTime     UTCTime,
 18   generalTime GeneralizedTime
    }
```

## 2.388 ASN.1 type 'TrailerField'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

```
   TrailerField ::= INTEGER
02 {
     trailerFieldBC(1)
   }
```

## 2.389 ASN.1 type 'Trinomial'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
02 Trinomial ::= INTEGER
```

## 2.390 ASN.1 type 'URI'

Source of definition: 'LDAP (RFC 4511)'

```
04 URI ::= LDAPString
```

## 2.391 ASN.1 type 'UTF8Pairs'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

```
0C UTF8Pairs ::= UTF8String
```

## 2.392 ASN.1 type 'UnauthAttributes'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 UnauthAttributes ::= SET SIZE (1..MAX) OF Attribute
```

## 2.393 ASN.1 type 'UnbindRequest'

Source of definition: 'LDAP (RFC 4511)'

```
42 UnbindRequest ::= [APPLICATION 2] IMPLICIT NULL
```

## 2.394 ASN.1 type 'UnformattedPostalAddress'

Source of definition: 'CRL structures'

```
UnformattedPostalAddress ::= SET
{
  printable-address SEQUENCE SIZE (1..ub-pds-physical-address-lines) OF PrintableString (SIZE (1..ub-pds-parameter-length)) OPTIONAL,
  teletex-string    TeletexString                                                    (SIZE (1..ub-unformatted-address-length)) OPTIONAL
}
```

## 2.395 ASN.1 type 'UniqueIdentifier'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
UniqueIdentifier ::= BIT STRING
```

## 2.396 ASN.1 type 'UniquePostalName'

Source of definition: 'CRL structures'

```
UniquePostalName ::= PDSParameter
```

## 2.397 ASN.1 type 'UnknownInfo'

Source of definition: 'OCSP (RFC 6960)'

```
UnknownInfo ::= NULL
```

## 2.398 ASN.1 type 'UnprotectedAttributes'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
UnprotectedAttributes ::= SET SIZE (1..MAX) OF Attribute
```

## 2.399 ASN.1 type 'UnsignedAttributes'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
31 UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute
```

## 2.400 ASN.1 type 'UserKeyingMaterial'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

```
04 UserKeyingMaterial ::= OCTET STRING
```

## 2.401 ASN.1 type 'UserNotice'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

```
30 UserNotice ::= SEQUENCE
   {
30   noticeRef    NoticeReference OPTIONAL,
CHO  explicitText DisplayText     OPTIONAL
   }
```

## 2.402 ASN.1 type 'V2Form'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

```
30 V2Form ::= SEQUENCE
   {
30   issuerName                     GeneralNames     OPTIONAL,
A0   baseCertificateID [0] IMPLICIT IssuerSerial     OPTIONAL,
A1   objectDigestInfo  [1] IMPLICIT ObjectDigestInfo OPTIONAL
   }
```

## 2.403 ASN.1 type 'ValidationParms'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

```
30 ValidationParms ::= SEQUENCE
   {
03   seed        BIT STRING,
02   pgenCounter INTEGER
   }
```

## 2.404 ASN.1 type 'Validity'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
 30 Validity ::= SEQUENCE
    {
CHO   notBefore Time,
CHO   notAfter  Time
    }
```

## 2.405 ASN.1 type 'Version'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
   Version ::= INTEGER
02 {
     v1(0),
     v2(1),
     v3(2)
   }
```

## 2.406 ASN.1 type 'X121Address'

Source of definition: 'CRL structures'

```
12 X121Address ::= NumericString (SIZE (1..ub-x121-address-length))
```

## 2.407 ASN.1 type 'X520CommonName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO X520CommonName ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..ub-common-name)),
 13   printableString PrintableString (SIZE (1..ub-common-name)),
 1C   universalString UniversalString (SIZE (1..ub-common-name)),
 0C   utf8String      UTF8String      (SIZE (1..ub-common-name)),
 1E   bmpString       BMPString       (SIZE (1..ub-common-name))
    }
```

## 2.408 ASN.1 type 'X520LocalityName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO X520LocalityName ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..ub-locality-name)),
 13   printableString PrintableString (SIZE (1..ub-locality-name)),
 1C   universalString UniversalString (SIZE (1..ub-locality-name)),
 0C   utf8String      UTF8String      (SIZE (1..ub-locality-name)),
 1E   bmpString       BMPString       (SIZE (1..ub-locality-name))
    }
```

## 2.409 ASN.1 type 'X520OrganizationName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO X520OrganizationName ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..ub-organization-name)),
 13   printableString PrintableString (SIZE (1..ub-organization-name)),
 1C   universalString UniversalString (SIZE (1..ub-organization-name)),
 0C   utf8String      UTF8String      (SIZE (1..ub-organization-name)),
 1E   bmpString       BMPString       (SIZE (1..ub-organization-name))
    }
```

## 2.410 ASN.1 type 'X520OrganizationalUnitName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO X520OrganizationalUnitName ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..ub-organizational-unit-name)),
 13   printableString PrintableString (SIZE (1..ub-organizational-unit-name)),
 1C   universalString UniversalString (SIZE (1..ub-organizational-unit-name)),
 0C   utf8String      UTF8String      (SIZE (1..ub-organizational-unit-name)),
 1E   bmpString       BMPString       (SIZE (1..ub-organizational-unit-name))
    }
```

## 2.411 ASN.1 type 'X520Pseudonym'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO X520Pseudonym ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..ub-pseudonym)),
 13   printableString PrintableString (SIZE (1..ub-pseudonym)),
 1C   universalString UniversalString (SIZE (1..ub-pseudonym)),
 0C   utf8String      UTF8String      (SIZE (1..ub-pseudonym)),
 1E   bmpString       BMPString       (SIZE (1..ub-pseudonym))
    }
```

## 2.412 ASN.1 type 'X520SerialNumber'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
 13 X520SerialNumber ::= PrintableString (SIZE (1..ub-serial-number))
```

## 2.413 ASN.1 type 'X520StateOrProvinceName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO X520StateOrProvinceName ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..ub-state-name)),
 13   printableString PrintableString (SIZE (1..ub-state-name)),
 1C   universalString UniversalString (SIZE (1..ub-state-name)),
 0C   utf8String      UTF8String      (SIZE (1..ub-state-name)),
 1E   bmpString       BMPString       (SIZE (1..ub-state-name))
    }
```

## 2.414 ASN.1 type 'X520Title'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO X520Title ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..ub-title)),
 13   printableString PrintableString (SIZE (1..ub-title)),
 1C   universalString UniversalString (SIZE (1..ub-title)),
 0C   utf8String      UTF8String      (SIZE (1..ub-title)),
 1E   bmpString       BMPString       (SIZE (1..ub-title))
    }
```

## 2.415 ASN.1 type 'X520countryName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
13 X520countryName ::= PrintableString (SIZE (2))
```

## 2.416 ASN.1 type 'X520dnQualifier'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
13 X520dnQualifier ::= PrintableString
```

## 2.417 ASN.1 type 'X520name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

```
CHO X520name ::= CHOICE
    {
 14   teletexString   TeletexString   (SIZE (1..ub-name)),
 13   printableString PrintableString (SIZE (1..ub-name)),
 1C   universalString UniversalString (SIZE (1..ub-name)),
 0C   utf8String      UTF8String      (SIZE (1..ub-name)),
 1E   bmpString       BMPString       (SIZE (1..ub-name))
    }
```

# 3 ASN.1 value definitions

## 3.1 ASN.1 value 'algid-hmacWithSHA1'

Source of definition: 'PKCS #5'

### 3.1.1 Value definition

```
algid-hmacWithSHA1 AlgorithmIdentifier ::=
{
  algorithm(id-hmacWithSHA1), -- raw value is 1.2.840.113549.2.7
  parameters(nullParameters)  -- original ASN.1 ANY type replaced by 'NULL'
}
```

### 3.1.2 Value DER encoding

```
DER encoding size: 14 bytes

  30 0C 06 08 2A 86 48 86 F7 0D 02 07 05 00
```

## 3.2 ASN.1 value 'ansi-X9-62'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.2.1 Value definition

```
ansi-X9-62 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) 10045 }  -
- raw value is 1.2.840.10045
```

### 3.2.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2A 86 48 CE 3D
```

## 3.3 ASN.1 value 'anyExtendedKeyUsage'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.3.1 Value definition

```
anyExtendedKeyUsage OBJECT IDENTIFIER ::= { id-ce-extKeyUsage 0 }  -
- raw value is 2.5.29.37.0
```

### 3.3.2 Value DER encoding

```
DER encoding size: 6 bytes

  06 04 55 1D 25 00
```

## 3.4 ASN.1 value 'anyPolicy'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.4.1 Value definition

```
anyPolicy OBJECT IDENTIFIER ::= { id-ce-certificatePolicies 0 }  -
- raw value is 2.5.29.32.0
```

### 3.4.2 Value DER encoding

```
DER encoding size: 6 bytes

  06 04 55 1D 20 00
```

## 3.5 ASN.1 value 'bagtypes'

Source of definition: 'PKCS #12'

### 3.5.1 Value definition

```
bagtypes OBJECT IDENTIFIER ::= { pkcs-12 10 1 }  -- raw value is 1.2.840.113549.1.12.10.1
```

### 3.5.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 0C 0A 01
```

## 3.6 ASN.1 value 'c-TwoCurve'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.6.1 Value definition

```
c-TwoCurve OBJECT IDENTIFIER ::= { ellipticCurve characteristicTwo(0) }  -
- raw value is 1.2.840.10045.3.0
```

### 3.6.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 3D 03 00
```

## 3.7 ASN.1 value 'c2onb191v4'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.7.1 Value definition

```
c2onb191v4 OBJECT IDENTIFIER ::= { c-TwoCurve 8 }  -- raw value is 1.2.840.10045.3.0.8
```

### 3.7.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 08
```

## 3.8 ASN.1 value 'c2onb191v5'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.8.1 Value definition

```
c2onb191v5 OBJECT IDENTIFIER ::= { c-TwoCurve 9 }  -- raw value is 1.2.840.10045.3.0.9
```

### 3.8.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 09
```

## 3.9 ASN.1 value 'c2onb239v4'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.9.1 Value definition

```
c2onb239v4 OBJECT IDENTIFIER ::= { c-TwoCurve 14 }  -- raw value is 1.2.840.10045.3.0.14
```

### 3.9.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 0E
```

## 3.10 ASN.1 value 'c2onb239v5'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.10.1 Value definition

```
c2onb239v5 OBJECT IDENTIFIER ::= { c-TwoCurve 15 }  -- raw value is 1.2.840.10045.3.0.15
```

### 3.10.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 0F
```

## 3.11 ASN.1 value 'c2pnb163v1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.11.1 Value definition

```
c2pnb163v1 OBJECT IDENTIFIER ::= { c-TwoCurve 1 }  -- raw value is 1.2.840.10045.3.0.1
```

### 3.11.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 01
```

## 3.12 ASN.1 value 'c2pnb163v2'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.12.1 Value definition

```
c2pnb163v2 OBJECT IDENTIFIER ::= { c-TwoCurve 2 }  -- raw value is 1.2.840.10045.3.0.2
```

### 3.12.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 02
```

## 3.13 ASN.1 value 'c2pnb163v3'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.13.1 Value definition

```
c2pnb163v3 OBJECT IDENTIFIER ::= { c-TwoCurve 3 }  -- raw value is 1.2.840.10045.3.0.3
```

### 3.13.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 03
```

## 3.14 ASN.1 value 'c2pnb176w1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.14.1 Value definition

```
c2pnb176w1 OBJECT IDENTIFIER ::= { c-TwoCurve 4 }  -- raw value is 1.2.840.10045.3.0.4
```

### 3.14.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 04
```

## 3.15 ASN.1 value 'c2pnb208w1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.15.1 Value definition

```
c2pnb208w1 OBJECT IDENTIFIER ::= { c-TwoCurve 10 }  -- raw value is 1.2.840.10045.3.0.10
```

### 3.15.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 0A
```

## 3.16 ASN.1 value 'c2pnb272w1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.16.1 Value definition

```
c2pnb272w1 OBJECT IDENTIFIER ::= { c-TwoCurve 16 }  -- raw value is 1.2.840.10045.3.0.16
```

### 3.16.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 10
```

## 3.17 ASN.1 value 'c2pnb304w1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.17.1 Value definition

```
c2pnb304w1 OBJECT IDENTIFIER ::= { c-TwoCurve 17 }  -- raw value is 1.2.840.10045.3.0.17
```

### 3.17.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 11
```

## 3.18 ASN.1 value 'c2pnb368w1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.18.1 Value definition

```
c2pnb368w1 OBJECT IDENTIFIER ::= { c-TwoCurve 19 }  -- raw value is 1.2.840.10045.3.0.19
```

### 3.18.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 13
```

## 3.19 ASN.1 value 'c2tnb191v1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.19.1 Value definition

```
c2tnb191v1 OBJECT IDENTIFIER ::= { c-TwoCurve 5 }  -- raw value is 1.2.840.10045.3.0.5
```

### 3.19.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 05
```

## 3.20 ASN.1 value 'c2tnb191v2'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.20.1 Value definition

```
c2tnb191v2 OBJECT IDENTIFIER ::= { c-TwoCurve 6 }  -- raw value is 1.2.840.10045.3.0.6
```

### 3.20.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 06
```

## 3.21 ASN.1 value 'c2tnb191v3'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.21.1 Value definition

```
c2tnb191v3 OBJECT IDENTIFIER ::= { c-TwoCurve 7 }  -- raw value is 1.2.840.10045.3.0.7
```

### 3.21.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 07
```

## 3.22 ASN.1 value 'c2tnb239v1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.22.1 Value definition

```
c2tnb239v1 OBJECT IDENTIFIER ::= { c-TwoCurve 11 }  -- raw value is 1.2.840.10045.3.0.11
```

### 3.22.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 0B
```

## 3.23 ASN.1 value 'c2tnb239v2'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.23.1 Value definition

```
c2tnb239v2 OBJECT IDENTIFIER ::= { c-TwoCurve 12 }  -- raw value is 1.2.840.10045.3.0.12
```

### 3.23.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 0C
```

## 3.24 ASN.1 value 'c2tnb239v3'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.24.1 Value definition

```
c2tnb239v3 OBJECT IDENTIFIER ::= { c-TwoCurve 13 }  -- raw value is 1.2.840.10045.3.0.13
```

### 3.24.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 0D
```

## 3.25 ASN.1 value 'c2tnb359v1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.25.1 Value definition

```
c2tnb359v1 OBJECT IDENTIFIER ::= { c-TwoCurve 18 }  -- raw value is 1.2.840.10045.3.0.18
```

### 3.25.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 12
```

## 3.26 ASN.1 value 'c2tnb431r1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.26.1 Value definition

```
c2tnb431r1 OBJECT IDENTIFIER ::= { c-TwoCurve 20 }  -- raw value is 1.2.840.10045.3.0.20
```

### 3.26.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 00 14
```

## 3.27 ASN.1 value 'certTypes'

Source of definition: 'PKCS #9'

### 3.27.1 Value definition

```
certTypes OBJECT IDENTIFIER ::= { pkcs-9 22 }  -- raw value is 1.2.840.113549.1.9.22
```

### 3.27.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 16
```

## 3.28 ASN.1 value 'characteristic-two-field'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.28.1 Value definition

```
characteristic-two-field OBJECT IDENTIFIER ::= { id-fieldType 2 }  -
- raw value is 1.2.840.10045.1.2
```

### 3.28.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 3D 01 02
```

## 3.29 ASN.1 value 'common-name'

Source of definition: 'CRL structures'

### 3.29.1 Value definition

```
common-name INTEGER ::= 1
```

### 3.29.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 01
```

## 3.30 ASN.1 value 'crlTypes'

Source of definition: 'PKCS #9'

### 3.30.1 Value definition

```
crlTypes OBJECT IDENTIFIER ::= { pkcs-9 23 }  -- raw value is 1.2.840.113549.1.9.23
```

### 3.30.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 17
```

## 3.31 ASN.1 value 'des-EDE3-CBC'

Source of definition: 'PKCS #5'

### 3.31.1 Value definition

```
des-EDE3-CBC OBJECT IDENTIFIER ::= { encryptionAlgorithm 7 }  -
- raw value is 1.2.840.113549.3.7
```

### 3.31.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 03 07
```

## 3.32 ASN.1 value 'desCBC'

Source of definition: 'PKCS #5'

### 3.32.1 Value definition

```
desCBC OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) oiw(14) secsig(3) algorithms(2) 7 }  -- raw value is 1.3.14.3.2.7
```

### 3.32.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 0E 03 02 07
```

## 3.33 ASN.1 value 'dhpublicnumber'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.33.1 Value definition

```
dhpublicnumber OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-
x942(10046) number-type(2) 1 }  -- raw value is 1.2.840.10046.2.1
```

### 3.33.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 3E 02 01
```

## 3.34 ASN.1 value 'digestAlgorithm'

Source of definition: 'PKCS #5'

### 3.34.1 Value definition

```
digestAlgorithm OBJECT IDENTIFIER ::= { rsadsi 2 }  -- raw value is 1.2.840.113549.2
```

### 3.34.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 86 F7 0D 02
```

## 3.35 ASN.1 value 'ecdsa-with-SHA1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.35.1 Value definition

```
ecdsa-with-SHA1 OBJECT IDENTIFIER ::= { id-ecSigType 1 }  -- raw value is 1.2.840.10045.4.1
```

### 3.35.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 3D 04 01
```

## 3.36 ASN.1 value 'ecdsa-with-SHA224'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.36.1 Value definition

```
ecdsa-with-SHA224 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-
62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }  -- raw value is 1.2.840.10045.4.3.1
```

### 3.36.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 04 03 01
```

## 3.37 ASN.1 value 'ecdsa-with-SHA256'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.37.1 Value definition

```
ecdsa-with-SHA256 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-
62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }  -- raw value is 1.2.840.10045.4.3.2
```

### 3.37.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 04 03 02
```

## 3.38 ASN.1 value 'ecdsa-with-SHA384'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.38.1 Value definition

```
ecdsa-with-SHA384 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-
62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }  -- raw value is 1.2.840.10045.4.3.3
```

### 3.38.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 04 03 03
```

## 3.39 ASN.1 value 'ecdsa-with-SHA512'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.39.1 Value definition

```
ecdsa-with-SHA512 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-
62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }  -- raw value is 1.2.840.10045.4.3.4
```

### 3.39.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 04 03 04
```

## 3.40 ASN.1 value 'ellipticCurve'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.40.1 Value definition

```
ellipticCurve OBJECT IDENTIFIER ::= { ansi-X9-62 curves(3) }  -
- raw value is 1.2.840.10045.3
```

### 3.40.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 2A 86 48 CE 3D 03
```

## 3.41 ASN.1 value 'emptyString'

Source of definition: 'PKCS #1'

### 3.41.1 Value definition

```
emptyString EncodingParameters ::= ''H
```

### 3.41.2 Value DER encoding

```
DER encoding size: 2 bytes

  04 00
```

## 3.42 ASN.1 value 'encryptionAlgorithm'

Source of definition: 'PKCS #5'

### 3.42.1 Value definition

```
encryptionAlgorithm OBJECT IDENTIFIER ::= { rsadsi 3 }  -- raw value is 1.2.840.113549.3
```

### 3.42.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 86 F7 0D 03
```

## 3.43 ASN.1 value 'extended-network-address'

Source of definition: 'CRL structures'

### 3.43.1 Value definition

```
extended-network-address INTEGER ::= 22
```

### 3.43.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 16
```

## 3.44 ASN.1 value 'extension-OR-address-components'

Source of definition: 'CRL structures'

### 3.44.1 Value definition

```
extension-OR-address-components INTEGER ::= 12
```

### 3.44.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 0C
```

## 3.45 ASN.1 value 'extension-physical-delivery-address-components'

Source of definition: 'CRL structures'

### 3.45.1 Value definition

```
extension-physical-delivery-address-components INTEGER ::= 15
```

### 3.45.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 0F
```

## 3.46 ASN.1 value 'gnBasis'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.46.1 Value definition

```
gnBasis OBJECT IDENTIFIER ::= { id-characteristic-two-basis 1 }  -
- raw value is 1.2.840.10045.1.2.3.1
```

### 3.46.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 CE 3D 01 02 03 01
```

## 3.47 ASN.1 value 'holdInstruction'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.47.1 Value definition

```
holdInstruction OBJECT IDENTIFIER ::= { joint-iso-itu-t(2) member-
body(2) us(840) x9cm(10040) 2 }  -- raw value is 2.2.840.10040.2
```

### 3.47.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 52 86 48 CE 38 02
```

## 3.48 ASN.1 value 'id-DHBasedMac'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

### 3.48.1 Value definition

```
id-DHBasedMac OBJECT IDENTIFIER ::= { 1 2 840 113533 7 66 30 }  -
- raw value is 1.2.840.113533.7.66.30
```

### 3.48.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F6 7D 07 42 1E
```

## 3.49 ASN.1 value 'id-Ed25519'

Source of definition: 'Edwards Curve Algorithms (RFC 8410)'

### 3.49.1 Value definition

```
id-Ed25519 OBJECT IDENTIFIER ::= { id-edwards-curve-algs 112 }  -- raw value is 1.3.101.112
```

### 3.49.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 2B 65 70
```

## 3.50 ASN.1 value 'id-Ed448'

Source of definition: 'Edwards Curve Algorithms (RFC 8410)'

### 3.50.1 Value definition

```
id-Ed448 OBJECT IDENTIFIER ::= { id-edwards-curve-algs 113 }  -- raw value is 1.3.101.113
```

### 3.50.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 2B 65 71
```

## 3.51 ASN.1 value 'id-PBES2'

Source of definition: 'PKCS #5'

### 3.51.1 Value definition

```
id-PBES2 OBJECT IDENTIFIER ::= { pkcs-5 13 }  -- raw value is 1.2.840.113549.1.5.13
```

### 3.51.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 0D
```

## 3.52 ASN.1 value 'id-PBKDF2'

Source of definition: 'PKCS #5'

### 3.52.1 Value definition

```
id-PBKDF2 OBJECT IDENTIFIER ::= { pkcs-5 12 }  -- raw value is 1.2.840.113549.1.5.12
```

### 3.52.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 0C
```

## 3.53 ASN.1 value 'id-PBMAC1'

Source of definition: 'PKCS #5'

### 3.53.1 Value definition

```
id-PBMAC1 OBJECT IDENTIFIER ::= { pkcs-5 14 }  -- raw value is 1.2.840.113549.1.5.14
```

### 3.53.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 0E
```

## 3.54 ASN.1 value 'id-PasswordBasedMac'

Source of definition: 'Certificate Management Protocol (CMP, RFC 4210)'

### 3.54.1 Value definition

```
id-PasswordBasedMac OBJECT IDENTIFIER ::= { 1 2 840 113533 7 66 13 }  -
- raw value is 1.2.840.113533.7.66.13
```

### 3.54.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F6 7D 07 42 0D
```

## 3.55 ASN.1 value 'id-RSAES-OAEP'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.55.1 Value definition

```
id-RSAES-OAEP OBJECT IDENTIFIER ::= { pkcs-1 7 }  -- raw value is 1.2.840.113549.1.1.7
```

### 3.55.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 07
```

## 3.56 ASN.1 value 'id-RSASSA-PSS'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.56.1 Value definition

```
id-RSASSA-PSS OBJECT IDENTIFIER ::= { pkcs-1 10 }  -- raw value is 1.2.840.113549.1.1.10
```

### 3.56.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 0A
```

## 3.57 ASN.1 value 'id-X25519'

Source of definition: 'Edwards Curve Algorithms (RFC 8410)'

### 3.57.1 Value definition

```
id-X25519 OBJECT IDENTIFIER ::= { id-edwards-curve-algs 110 }  -- raw value is 1.3.101.110
```

### 3.57.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 2B 65 6E
```

## 3.58 ASN.1 value 'id-X448'

Source of definition: 'Edwards Curve Algorithms (RFC 8410)'

### 3.58.1 Value definition

```
id-X448 OBJECT IDENTIFIER ::= { id-edwards-curve-algs 111 }  -- raw value is 1.3.101.111
```

### 3.58.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 2B 65 6F
```

## 3.59 ASN.1 value 'id-aca'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.59.1 Value definition

```
id-aca OBJECT IDENTIFIER ::= { id-pkix 10 }  -- raw value is 1.3.6.1.5.5.7.10
```

### 3.59.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2B 06 01 05 05 07 0A
```

## 3.60 ASN.1 value 'id-aca-accessIdentity'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.60.1 Value definition

```
id-aca-accessIdentity OBJECT IDENTIFIER ::= { id-aca 2 }  -
- raw value is 1.3.6.1.5.5.7.10.2
```

### 3.60.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 0A 02
```

## 3.61 ASN.1 value 'id-aca-authenticationInfo'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.61.1 Value definition

```
id-aca-authenticationInfo OBJECT IDENTIFIER ::= { id-aca 1 }  -
- raw value is 1.3.6.1.5.5.7.10.1
```

### 3.61.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 0A 01
```

## 3.62 ASN.1 value 'id-aca-chargingIdentity'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.62.1 Value definition

```
id-aca-chargingIdentity OBJECT IDENTIFIER ::= { id-aca 3 }  -
- raw value is 1.3.6.1.5.5.7.10.3
```

### 3.62.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 0A 03
```

## 3.63 ASN.1 value 'id-aca-encAttrs'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.63.1 Value definition

```
id-aca-encAttrs OBJECT IDENTIFIER ::= { id-aca 6 }  -- raw value is 1.3.6.1.5.5.7.10.6
```

### 3.63.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 0A 06
```

## 3.64 ASN.1 value 'id-aca-group'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.64.1 Value definition

```
id-aca-group OBJECT IDENTIFIER ::= { id-aca 4 }  -- raw value is 1.3.6.1.5.5.7.10.4
```

### 3.64.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 0A 04
```

## 3.65 ASN.1 value 'id-ad'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.65.1 Value definition

```
id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }  -- raw value is 1.3.6.1.5.5.7.48
```

### 3.65.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2B 06 01 05 05 07 30
```

## 3.66 ASN.1 value 'id-ad-calssuers'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.66.1 Value definition

```
id-ad-caIssuers OBJECT IDENTIFIER ::= { id-ad 2 }  -- raw value is 1.3.6.1.5.5.7.48.2
```

### 3.66.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 30 02
```

## 3.67 ASN.1 value 'id-ad-caRepository'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.67.1 Value definition

```
id-ad-caRepository OBJECT IDENTIFIER ::= { id-ad 5 }  -- raw value is 1.3.6.1.5.5.7.48.5
```

### 3.67.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 30 05
```

## 3.68 ASN.1 value 'id-ad-ocsp'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.68.1 Value definition

```
id-ad-ocsp OBJECT IDENTIFIER ::= { id-ad 1 }  -- raw value is 1.3.6.1.5.5.7.48.1
```

### 3.68.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 30 01
```

## 3.69 ASN.1 value 'id-ad-timeStamping'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.69.1 Value definition

```
id-ad-timeStamping OBJECT IDENTIFIER ::= { id-ad 3 }  -- raw value is 1.3.6.1.5.5.7.48.3
```

### 3.69.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 30 03
```

## 3.70 ASN.1 value 'id-at'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.70.1 Value definition

```
id-at OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 4 }  -- raw value is 2.5.4
```

### 3.70.2 Value DER encoding

```
DER encoding size: 4 bytes

  06 02 55 04
```

## 3.71 ASN.1 value 'id-at-clearance'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.71.1 Value definition

```
id-at-clearance OBJECT IDENTIFIER ::= { joint-iso-
ccitt(2) ds(5) attributeType(4) clearance(55) }  -- raw value is 2.5.4.55
```

### 3.71.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 37
```

## 3.72 ASN.1 value 'id-at-commonName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.72.1 Value definition

```
id-at-commonName AttributeType ::= { id-at 3 }  -- raw value is 2.5.4.3
```

### 3.72.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 03
```

## 3.73 ASN.1 value 'id-at-countryName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.73.1 Value definition

```
id-at-countryName AttributeType ::= { id-at 6 }  -- raw value is 2.5.4.6
```

### 3.73.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 06
```

## 3.74 ASN.1 value 'id-at-dnQualifier'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.74.1 Value definition

```
id-at-dnQualifier AttributeType ::= { id-at 46 }  -- raw value is 2.5.4.46
```

### 3.74.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 2E
```

## 3.75 ASN.1 value 'id-at-generationQualifier'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.75.1 Value definition

```
id-at-generationQualifier AttributeType ::= { id-at 44 }  -- raw value is 2.5.4.44
```

### 3.75.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 2C
```

## 3.76 ASN.1 value 'id-at-givenName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.76.1 Value definition

```
id-at-givenName AttributeType ::= { id-at 42 }  -- raw value is 2.5.4.42
```

### 3.76.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 2A
```

## 3.77 ASN.1 value 'id-at-initials'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.77.1 Value definition

```
id-at-initials AttributeType ::= { id-at 43 }  -- raw value is 2.5.4.43
```

### 3.77.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 2B
```

## 3.78 ASN.1 value 'id-at-localityName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.78.1 Value definition

```
id-at-localityName AttributeType ::= { id-at 7 }  -- raw value is 2.5.4.7
```

### 3.78.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 07
```

## 3.79 ASN.1 value 'id-at-name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.79.1 Value definition

```
id-at-name AttributeType ::= { id-at 41 }  -- raw value is 2.5.4.41
```

### 3.79.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 29
```

## 3.80 ASN.1 value 'id-at-organizationName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.80.1 Value definition

```
id-at-organizationName AttributeType ::= { id-at 10 }  -- raw value is 2.5.4.10
```

### 3.80.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 0A
```

## 3.81 ASN.1 value 'id-at-organizationalUnitName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.81.1 Value definition

```
id-at-organizationalUnitName AttributeType ::= { id-at 11 }  -- raw value is 2.5.4.11
```

### 3.81.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 0B
```

## 3.82 ASN.1 value 'id-at-pseudonym'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.82.1 Value definition

```
id-at-pseudonym AttributeType ::= { id-at 65 }  -- raw value is 2.5.4.65
```

### 3.82.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 41
```

## 3.83 ASN.1 value 'id-at-role'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.83.1 Value definition

```
id-at-role OBJECT IDENTIFIER ::= { id-at 72 }  -- raw value is 2.5.4.72
```

### 3.83.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 48
```

## 3.84 ASN.1 value 'id-at-serialNumber'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.84.1 Value definition

```
id-at-serialNumber AttributeType ::= { id-at 5 }  -- raw value is 2.5.4.5
```

### 3.84.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 05
```

## 3.85 ASN.1 value 'id-at-stateOrProvinceName'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.85.1 Value definition

```
id-at-stateOrProvinceName AttributeType ::= { id-at 8 }  -- raw value is 2.5.4.8
```

### 3.85.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 08
```

## 3.86 ASN.1 value 'id-at-surname'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.86.1 Value definition

```
id-at-surname AttributeType ::= { id-at 4 }  -- raw value is 2.5.4.4
```

### 3.86.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 04
```

## 3.87 ASN.1 value 'id-at-title'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.87.1 Value definition

```
id-at-title AttributeType ::= { id-at 12 }  -- raw value is 2.5.4.12
```

### 3.87.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 04 0C
```

## 3.88 ASN.1 value 'id-ce'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.88.1 Value definition

```
id-ce OBJECT IDENTIFIER ::= { joint-iso-ccitt(2) ds(5) 29 }  -- raw value is 2.5.29
```

### 3.88.2 Value DER encoding

```
DER encoding size: 4 bytes

  06 02 55 1D
```

## 3.89 ASN.1 value 'id-ce-authorityKeyIdentifier'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.89.1 Value definition

```
id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 35 }  -- raw value is 2.5.29.35
```

### 3.89.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 23
```

## 3.90 ASN.1 value 'id-ce-basicConstraints'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.90.1 Value definition

```
id-ce-basicConstraints OBJECT IDENTIFIER ::= { id-ce 19 }  -- raw value is 2.5.29.19
```

### 3.90.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 13
```

## 3.91 ASN.1 value 'id-ce-cRLDistributionPoints'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.91.1 Value definition

```
id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::= { id-ce 31 }  -- raw value is 2.5.29.31
```

### 3.91.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 1F
```

## 3.92 ASN.1 value 'id-ce-cRLNumber'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.92.1 Value definition

```
id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }  -- raw value is 2.5.29.20
```

### 3.92.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 14
```

## 3.93 ASN.1 value 'id-ce-cRLReasons'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.93.1 Value definition

```
id-ce-cRLReasons OBJECT IDENTIFIER ::= { id-ce 21 }  -- raw value is 2.5.29.21
```

### 3.93.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 15
```

## 3.94 ASN.1 value 'id-ce-certificateIssuer'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.94.1 Value definition

```
id-ce-certificateIssuer OBJECT IDENTIFIER ::= { id-ce 29 }  -- raw value is 2.5.29.29
```

### 3.94.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 1D
```

## 3.95 ASN.1 value 'id-ce-certificatePolicies'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.95.1 Value definition

```
id-ce-certificatePolicies OBJECT IDENTIFIER ::= { id-ce 32 }  -- raw value is 2.5.29.32
```

### 3.95.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 20
```

## 3.96 ASN.1 value 'id-ce-deltaCRLIndicator'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.96.1 Value definition

```
id-ce-deltaCRLIndicator OBJECT IDENTIFIER ::= { id-ce 27 }  -- raw value is 2.5.29.27
```

### 3.96.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 1B
```

## 3.97 ASN.1 value 'id-ce-extKeyUsage'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.97.1 Value definition

```
id-ce-extKeyUsage OBJECT IDENTIFIER ::= { id-ce 37 }  -- raw value is 2.5.29.37
```

### 3.97.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 25
```

## 3.98 ASN.1 value 'id-ce-freshestCRL'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.98.1 Value definition

```
id-ce-freshestCRL OBJECT IDENTIFIER ::= { id-ce 46 }  -- raw value is 2.5.29.46
```

### 3.98.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 2E
```

## 3.99 ASN.1 value 'id-ce-holdInstructionCode'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.99.1 Value definition

```
id-ce-holdInstructionCode OBJECT IDENTIFIER ::= { id-ce 23 }  -- raw value is 2.5.29.23
```

### 3.99.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 17
```

## 3.100 ASN.1 value 'id-ce-inhibitAnyPolicy'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.100.1 Value definition

```
id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::= { id-ce 54 }  -- raw value is 2.5.29.54
```

### 3.100.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 36
```

## 3.101 ASN.1 value 'id-ce-invalidityDate'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.101.1 Value definition

```
id-ce-invalidityDate OBJECT IDENTIFIER ::= { id-ce 24 }  -- raw value is 2.5.29.24
```

### 3.101.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 18
```

## 3.102 ASN.1 value 'id-ce-issuerAltName'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.102.1 Value definition

```
id-ce-issuerAltName OBJECT IDENTIFIER ::= { id-ce 18 }  -- raw value is 2.5.29.18
```

### 3.102.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 12
```

## 3.103 ASN.1 value 'id-ce-issuingDistributionPoint'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.103.1 Value definition

```
id-ce-issuingDistributionPoint OBJECT IDENTIFIER ::= { id-ce 28 }  -
- raw value is 2.5.29.28
```

### 3.103.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 1C
```

## 3.104 ASN.1 value 'id-ce-keyUsage'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.104.1 Value definition

```
id-ce-keyUsage OBJECT IDENTIFIER ::= { id-ce 15 }  -- raw value is 2.5.29.15
```

### 3.104.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 0F
```

## 3.105 ASN.1 value 'id-ce-nameConstraints'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.105.1 Value definition

```
id-ce-nameConstraints OBJECT IDENTIFIER ::= { id-ce 30 }  -- raw value is 2.5.29.30
```

### 3.105.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 1E
```

## 3.106 ASN.1 value 'id-ce-policyConstraints'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.106.1 Value definition

```
id-ce-policyConstraints OBJECT IDENTIFIER ::= { id-ce 36 }  -- raw value is 2.5.29.36
```

### 3.106.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 24
```

## 3.107 ASN.1 value 'id-ce-policyMappings'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.107.1 Value definition

```
id-ce-policyMappings OBJECT IDENTIFIER ::= { id-ce 33 }  -- raw value is 2.5.29.33
```

### 3.107.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 21
```

## 3.108 ASN.1 value 'id-ce-privateKeyUsagePeriod'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.108.1 Value definition

```
id-ce-privateKeyUsagePeriod OBJECT IDENTIFIER ::= { id-ce 16 }  -- raw value is 2.5.29.16
```

### 3.108.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 10
```

## 3.109 ASN.1 value 'id-ce-subjectAltName'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.109.1 Value definition

```
id-ce-subjectAltName OBJECT IDENTIFIER ::= { id-ce 17 }  -- raw value is 2.5.29.17
```

### 3.109.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 11
```

## 3.110 ASN.1 value 'id-ce-subjectDirectoryAttributes'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.110.1 Value definition

```
id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::= { id-ce 9 }  -
- raw value is 2.5.29.9
```

### 3.110.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 09
```

## 3.111 ASN.1 value 'id-ce-subjectKeyIdentifier'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.111.1 Value definition

```
id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 14 }  -- raw value is 2.5.29.14
```

### 3.111.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 0E
```

## 3.112 ASN.1 value 'id-ce-targetInformation'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.112.1 Value definition

```
id-ce-targetInformation OBJECT IDENTIFIER ::= { id-ce 55 }  -- raw value is 2.5.29.55
```

### 3.112.2 Value DER encoding

```
DER encoding size: 5 bytes

  06 03 55 1D 37
```

## 3.113 ASN.1 value 'id-characteristic-two-basis'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.113.1 Value definition

```
id-characteristic-two-basis OBJECT IDENTIFIER ::= { characteristic-two-
field basisType(3) }  -- raw value is 1.2.840.10045.1.2.3
```

### 3.113.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 01 02 03
```

## 3.114 ASN.1 value 'id-contentType'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.114.1 Value definition

```
id-contentType OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }  -- raw value is 1.2.840.113549.1.9.3
```

### 3.114.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 03
```

## 3.115 ASN.1 value 'id-countersignature'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.115.1 Value definition

```
id-countersignature OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 6 }  -- raw value is 1.2.840.113549.1.9.6
```

### 3.115.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 06
```

## 3.116 ASN.1 value 'id-ct'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.116.1 Value definition

```
id-ct OBJECT IDENTIFIER ::= { id-smime 1 }  -- raw value is 1.2.840.113549.1.9.16.1
```

### 3.116.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 10 01
```

# 3.117 ASN.1 value 'id-ct-authData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

## 3.117.1 Value definition

```
id-ct-authData OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 2 }  -
- raw value is 1.2.840.113549.1.9.16.1.2
```

## 3.117.2 Value DER encoding

```
DER encoding size: 13 bytes

  06 0B 2A 86 48 86 F7 0D 01 09 10 01 02
```

# 3.118 ASN.1 value 'id-ct-contentInfo'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

## 3.118.1 Value definition

```
id-ct-contentInfo OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) ct(1) 6 }  -
- raw value is 1.2.840.113549.1.9.16.1.6
```

## 3.118.2 Value DER encoding

```
DER encoding size: 13 bytes

  06 0B 2A 86 48 86 F7 0D 01 09 10 01 06
```

# 3.119 ASN.1 value 'id-ct-encKeyWithID'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

## 3.119.1 Value definition

```
id-ct-encKeyWithID OBJECT IDENTIFIER ::= { id-ct 21 }  -
- raw value is 1.2.840.113549.1.9.16.1.21
```

## 3.119.2 Value DER encoding

```
DER encoding size: 13 bytes

  06 0B 2A 86 48 86 F7 0D 01 09 10 01 15
```

## 3.120 ASN.1 value 'id-data'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.120.1 Value definition

```
id-data OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 1 }  -- raw value is 1.2.840.113549.1.7.1
```

### 3.120.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 07 01
```

## 3.121 ASN.1 value 'id-digestedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.121.1 Value definition

```
id-digestedData OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 5 }  -- raw value is 1.2.840.113549.1.7.5
```

### 3.121.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 07 05
```

## 3.122 ASN.1 value 'id-domainComponent'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.122.1 Value definition

```
id-domainComponent AttributeType ::= { 0 9 2342 19200300 100 1 25 }  -
- raw value is 0.9.2342.19200300.100.1.25
```

### 3.122.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 09 92 26 89 93 F2 2C 64 01 19
```

## 3.123 ASN.1 value 'id-dsa'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.123.1 Value definition

```
id-dsa OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) x9-
57(10040) x9algorithm(4) 1 }  -- raw value is 1.2.840.10040.4.1
```

### 3.123.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 38 04 01
```

## 3.124 ASN.1 value 'id-dsa-with-sha1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.124.1 Value definition

```
id-dsa-with-sha1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) x9-
57(10040) x9algorithm(4) 3 }  -- raw value is 1.2.840.10040.4.3
```

### 3.124.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 38 04 03
```

## 3.125 ASN.1 value 'id-dsa-with-sha224'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.125.1 Value definition

```
id-dsa-with-sha224 OBJECT IDENTIFIER ::= { joint-iso-
ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) algorithms(4) id-dsa-with-
sha2(3) 1 }  -- raw value is 2.16.840.1.101.3.4.3.1
```

### 3.125.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 60 86 48 01 65 03 04 03 01
```

## 3.126 ASN.1 value 'id-dsa-with-sha256'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.126.1 Value definition

```
id-dsa-with-sha256 OBJECT IDENTIFIER ::= { joint-iso-
ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) algorithms(4) id-dsa-with-
sha2(3) 2 }  -- raw value is 2.16.840.1.101.3.4.3.2
```

### 3.126.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 60 86 48 01 65 03 04 03 02
```

## 3.127 ASN.1 value 'id-ecDH'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.127.1 Value definition

```
id-ecDH OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) schemes(1) ecdh(12) }  -- raw value is 1.3.132.1.12
```

### 3.127.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 01 0C
```

## 3.128 ASN.1 value 'id-ecMQV'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.128.1 Value definition

```
id-ecMQV OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) schemes(1) ecmqv(13) }  -- raw value is 1.3.132.1.13
```

### 3.128.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 01 0D
```

## 3.129 ASN.1 value 'id-ecPublicKey'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.129.1 Value definition

```
id-ecPublicKey OBJECT IDENTIFIER ::= { id-publicKeyType 1 }  -
- raw value is 1.2.840.10045.2.1
```

### 3.129.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 3D 02 01
```

## 3.130 ASN.1 value 'id-ecSigType'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.130.1 Value definition

```
id-ecSigType OBJECT IDENTIFIER ::= { ansi-X9-62 signatures(4) }  -
- raw value is 1.2.840.10045.4
```

### 3.130.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 2A 86 48 CE 3D 04
```

## 3.131 ASN.1 value 'id-edwards-curve-algs'

Source of definition: 'Edwards Curve Algorithms (RFC 8410)'

### 3.131.1 Value definition

```
id-edwards-curve-algs OBJECT IDENTIFIER ::= { 1 3 101 }  -- raw value is 1.3.101
```

### 3.131.2 Value DER encoding

```
DER encoding size: 4 bytes

  06 02 2B 65
```

## 3.132 ASN.1 value 'id-emailAddress'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.132.1 Value definition

```
id-emailAddress AttributeType ::= { pkcs-9 1 }  -- raw value is 1.2.840.113549.1.9.1
```

### 3.132.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 01
```

## 3.133 ASN.1 value 'id-encryptedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.133.1 Value definition

```
id-encryptedData OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 6 }  -- raw value is 1.2.840.113549.1.7.6
```

### 3.133.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 07 06
```

## 3.134 ASN.1 value 'id-envelopedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.134.1 Value definition

```
id-envelopedData OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 3 }  -- raw value is 1.2.840.113549.1.7.3
```

### 3.134.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 07 03
```

## 3.135 ASN.1 value 'id-fieldType'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.135.1 Value definition

```
id-fieldType OBJECT IDENTIFIER ::= { ansi-X9-62 fieldType(1) }  -
- raw value is 1.2.840.10045.1
```

### 3.135.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 2A 86 48 CE 3D 01
```

## 3.136 ASN.1 value 'id-hmacWithSHA1'

Source of definition: 'PKCS #5'

### 3.136.1 Value definition

```
id-hmacWithSHA1 OBJECT IDENTIFIER ::= { digestAlgorithm 7 }  -
- raw value is 1.2.840.113549.2.7
```

### 3.136.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 02 07
```

## 3.137 ASN.1 value 'id-holdinstruction-callissuer'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.137.1 Value definition

```
id-holdinstruction-callissuer OBJECT IDENTIFIER ::= { holdInstruction 2 }  -
- raw value is 2.2.840.10040.2.2
```

### 3.137.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 52 86 48 CE 38 02 02
```

## 3.138 ASN.1 value 'id-holdinstruction-none'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.138.1 Value definition

```
id-holdinstruction-none OBJECT IDENTIFIER ::= { holdInstruction 1 }  -
- raw value is 2.2.840.10040.2.1
```

### 3.138.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 52 86 48 CE 38 02 01
```

## 3.139 ASN.1 value 'id-holdinstruction-reject'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.139.1 Value definition

```
id-holdinstruction-reject OBJECT IDENTIFIER ::= { holdInstruction 3 }  -
- raw value is 2.2.840.10040.2.3
```

### 3.139.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 52 86 48 CE 38 02 03
```

## 3.140 ASN.1 value 'id-keyExchangeAlgorithm'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.140.1 Value definition

```
id-keyExchangeAlgorithm OBJECT IDENTIFIER ::= { 2 16 840 1 101 2 1 1 22 }  -
- raw value is 2.16.840.1.101.2.1.1.22
```

### 3.140.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 60 86 48 01 65 02 01 01 16
```

## 3.141 ASN.1 value 'id-kp'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.141.1 Value definition

```
id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }  -- raw value is 1.3.6.1.5.5.7.3
```

### 3.141.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2B 06 01 05 05 07 03
```

## 3.142 ASN.1 value 'id-kp-OCSPSigning'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.142.1 Value definition

```
id-kp-OCSPSigning OBJECT IDENTIFIER ::= { id-kp 9 }  -- raw value is 1.3.6.1.5.5.7.3.9
```

### 3.142.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 03 09
```

## 3.143 ASN.1 value 'id-kp-clientAuth'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.143.1 Value definition

```
id-kp-clientAuth OBJECT IDENTIFIER ::= { id-kp 2 }  -- raw value is 1.3.6.1.5.5.7.3.2
```

### 3.143.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 03 02
```

## 3.144 ASN.1 value 'id-kp-codeSigning'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.144.1 Value definition

```
id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }  -- raw value is 1.3.6.1.5.5.7.3.3
```

### 3.144.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 03 03
```

## 3.145 ASN.1 value 'id-kp-emailProtection'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.145.1 Value definition

```
id-kp-emailProtection OBJECT IDENTIFIER ::= { id-kp 4 }  -- raw value is 1.3.6.1.5.5.7.3.4
```

### 3.145.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 03 04
```

## 3.146 ASN.1 value 'id-kp-serverAuth'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.146.1 Value definition

```
id-kp-serverAuth OBJECT IDENTIFIER ::= { id-kp 1 }  -- raw value is 1.3.6.1.5.5.7.3.1
```

### 3.146.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 03 01
```

# 3.147 ASN.1 value 'id-kp-timeStamping'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

## 3.147.1 Value definition

```
id-kp-timeStamping OBJECT IDENTIFIER ::= { id-kp 8 }  -- raw value is 1.3.6.1.5.5.7.3.8
```

## 3.147.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 03 08
```

# 3.148 ASN.1 value 'id-md2'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.148.1 Value definition

```
id-md2 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) digestAlgorithm(2) 2 }  -- raw value is 1.2.840.113549.2.2
```

## 3.148.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 02 02
```

# 3.149 ASN.1 value 'id-md5'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.149.1 Value definition

```
id-md5 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) digestAlgorithm(2) 5 }  -- raw value is 1.2.840.113549.2.5
```

## 3.149.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 02 05
```

## 3.150 ASN.1 value 'id-messageDigest'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.150.1 Value definition

```
id-messageDigest OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }  -- raw value is 1.2.840.113549.1.9.4
```

### 3.150.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 04
```

## 3.151 ASN.1 value 'id-mgf1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.151.1 Value definition

```
id-mgf1 OBJECT IDENTIFIER ::= { pkcs-1 8 }  -- raw value is 1.2.840.113549.1.1.8
```

### 3.151.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 08
```

## 3.152 ASN.1 value 'id-pSpecified'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.152.1 Value definition

```
id-pSpecified OBJECT IDENTIFIER ::= { pkcs-1 9 }  -- raw value is 1.2.840.113549.1.1.9
```

### 3.152.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 09
```

## 3.153 ASN.1 value 'id-pe'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.153.1 Value definition

```
id-pe OBJECT IDENTIFIER ::= { id-pkix 1 }  -- raw value is 1.3.6.1.5.5.7.1
```

### 3.153.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2B 06 01 05 05 07 01
```

## 3.154 ASN.1 value 'id-pe-aaControls'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.154.1 Value definition

```
id-pe-aaControls OBJECT IDENTIFIER ::= { id-pe 6 }  -- raw value is 1.3.6.1.5.5.7.1.6
```

### 3.154.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 01 06
```

## 3.155 ASN.1 value 'id-pe-ac-auditIdentity'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.155.1 Value definition

```
id-pe-ac-auditIdentity OBJECT IDENTIFIER ::= { id-pe 4 }  -- raw value is 1.3.6.1.5.5.7.1.4
```

### 3.155.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 01 04
```

## 3.156 ASN.1 value 'id-pe-ac-proxying'

Source of definition: 'PKIXAttributeCertificate 2008 (RFC 5755)'

### 3.156.1 Value definition

```
id-pe-ac-proxying OBJECT IDENTIFIER ::= { id-pe 10 }  -- raw value is 1.3.6.1.5.5.7.1.10
```

### 3.156.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 01 0A
```

## 3.157 ASN.1 value 'id-pe-authorityInfoAccess'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.157.1 Value definition

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }  -
- raw value is 1.3.6.1.5.5.7.1.1
```

### 3.157.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 01 01
```

## 3.158 ASN.1 value 'id-pe-subjectInfoAccess'

Source of definition: 'PKIX1Implicit88 (RFC 5280)'

### 3.158.1 Value definition

```
id-pe-subjectInfoAccess OBJECT IDENTIFIER ::= { id-pe 11 }  -
- raw value is 1.3.6.1.5.5.7.1.11
```

### 3.158.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 01 0B
```

## 3.159 ASN.1 value 'id-pkip'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.159.1 Value definition

```
id-pkip OBJECT IDENTIFIER ::= { id-pkix 5 }  -- raw value is 1.3.6.1.5.5.7.5
```

### 3.159.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2B 06 01 05 05 07 05
```

## 3.160 ASN.1 value 'id-pkix'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.160.1 Value definition

```
id-pkix OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) }  -
- raw value is 1.3.6.1.5.5.7
```

### 3.160.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 2B 06 01 05 05 07
```

## 3.161 ASN.1 value 'id-pkix-ocsp'

Source of definition: 'OCSP (RFC 6960)'

### 3.161.1 Value definition

```
id-pkix-ocsp OBJECT IDENTIFIER ::= { id-ad-ocsp }  -- raw value is 1.3.6.1.5.5.7.48.1
```

### 3.161.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 30 01
```

## 3.162 ASN.1 value 'id-pkix-ocsp-archive-cutoff'

Source of definition: 'OCSP (RFC 6960)'

### 3.162.1 Value definition

```
id-pkix-ocsp-archive-cutoff OBJECT IDENTIFIER ::= { id-pkix-ocsp 6 }  -
- raw value is 1.3.6.1.5.5.7.48.1.6
```

### 3.162.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 06
```

## 3.163 ASN.1 value 'id-pkix-ocsp-basic'

Source of definition: 'OCSP (RFC 6960)'

### 3.163.1 Value definition

```
id-pkix-ocsp-basic OBJECT IDENTIFIER ::= { id-pkix-ocsp 1 }  -
- raw value is 1.3.6.1.5.5.7.48.1.1
```

### 3.163.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 01
```

## 3.164 ASN.1 value 'id-pkix-ocsp-crl'

Source of definition: 'OCSP (RFC 6960)'

### 3.164.1 Value definition

```
id-pkix-ocsp-crl OBJECT IDENTIFIER ::= { id-pkix-ocsp 3 }  -
- raw value is 1.3.6.1.5.5.7.48.1.3
```

### 3.164.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 03
```

## 3.165 ASN.1 value 'id-pkix-ocsp-extended-revoke'

Source of definition: 'OCSP (RFC 6960)'

### 3.165.1 Value definition

```
id-pkix-ocsp-extended-revoke OBJECT IDENTIFIER ::= { id-pkix-ocsp 9 }  -
- raw value is 1.3.6.1.5.5.7.48.1.9
```

### 3.165.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 09
```

## 3.166 ASN.1 value 'id-pkix-ocsp-nocheck'

Source of definition: 'OCSP (RFC 6960)'

### 3.166.1 Value definition

```
id-pkix-ocsp-nocheck OBJECT IDENTIFIER ::= { id-pkix-ocsp 5 }  -
- raw value is 1.3.6.1.5.5.7.48.1.5
```

### 3.166.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 05
```

## 3.167 ASN.1 value 'id-pkix-ocsp-nonce'

Source of definition: 'OCSP (RFC 6960)'

### 3.167.1 Value definition

```
id-pkix-ocsp-nonce OBJECT IDENTIFIER ::= { id-pkix-ocsp 2 }  -
- raw value is 1.3.6.1.5.5.7.48.1.2
```

### 3.167.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 02
```

## 3.168 ASN.1 value 'id-pkix-ocsp-pref-sig-algs'

Source of definition: 'OCSP (RFC 6960)'

### 3.168.1 Value definition

```
id-pkix-ocsp-pref-sig-algs OBJECT IDENTIFIER ::= { id-pkix-ocsp 8 }  -
- raw value is 1.3.6.1.5.5.7.48.1.8
```

### 3.168.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 08
```

## 3.169 ASN.1 value 'id-pkix-ocsp-response'

Source of definition: 'OCSP (RFC 6960)'

### 3.169.1 Value definition

```
id-pkix-ocsp-response OBJECT IDENTIFIER ::= { id-pkix-ocsp 4 }  -
- raw value is 1.3.6.1.5.5.7.48.1.4
```

### 3.169.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 04
```

## 3.170 ASN.1 value 'id-pkix-ocsp-service-locator'

Source of definition: 'OCSP (RFC 6960)'

### 3.170.1 Value definition

```
id-pkix-ocsp-service-locator OBJECT IDENTIFIER ::= { id-pkix-ocsp 7 }  -
- raw value is 1.3.6.1.5.5.7.48.1.7
```

### 3.170.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 30 01 07
```

## 3.171 ASN.1 value 'id-pkix2'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.171.1 Value definition

```
id-pkix2 OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 }  -- raw value is 1.3.6.1.5.5.7
```

### 3.171.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 2B 06 01 05 05 07
```

## 3.172 ASN.1 value 'id-pkix3'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.172.1 Value definition

```
id-pkix3 OBJECT IDENTIFIER ::= { 1 three 6 1 5 5 7 }  -- raw value is 1.3.6.1.5.5.7
```

### 3.172.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 2B 06 01 05 05 07
```

## 3.173 ASN.1 value 'id-publicKeyType'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.173.1 Value definition

```
id-publicKeyType OBJECT IDENTIFIER ::= { ansi-X9-62 keyType(2) }  -
- raw value is 1.2.840.10045.2
```

### 3.173.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 2A 86 48 CE 3D 02
```

## 3.174 ASN.1 value 'id-qt'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.174.1 Value definition

```
id-qt OBJECT IDENTIFIER ::= { id-pkix 2 }  -- raw value is 1.3.6.1.5.5.7.2
```

### 3.174.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2B 06 01 05 05 07 02
```

## 3.175 ASN.1 value 'id-qt-cps'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.175.1 Value definition

```
id-qt-cps OBJECT IDENTIFIER ::= { id-qt 1 }  -- raw value is 1.3.6.1.5.5.7.2.1
```

### 3.175.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 02 01
```

## 3.176 ASN.1 value 'id-qt-unotice'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.176.1 Value definition

```
id-qt-unotice OBJECT IDENTIFIER ::= { id-qt 2 }  -- raw value is 1.3.6.1.5.5.7.2.2
```

### 3.176.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 02 02
```

## 3.177 ASN.1 value 'id-regCtrl'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.177.1 Value definition

```
id-regCtrl OBJECT IDENTIFIER ::= { id-pkip 1 }  -- raw value is 1.3.6.1.5.5.7.5.1
```

### 3.177.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 05 01
```

## 3.178 ASN.1 value 'id-regCtrl-authenticator'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.178.1 Value definition

```
id-regCtrl-authenticator OBJECT IDENTIFIER ::= { id-regCtrl 2 }  -
- raw value is 1.3.6.1.5.5.7.5.1.2
```

### 3.178.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 05 01 02
```

## 3.179 ASN.1 value 'id-regCtrl-oldCertID'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.179.1 Value definition

```
id-regCtrl-oldCertID OBJECT IDENTIFIER ::= { id-regCtrl 5 }  -
- raw value is 1.3.6.1.5.5.7.5.1.5
```

### 3.179.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 05 01 05
```

# 3.180 ASN.1 value 'id-regCtrl-pkiArchiveOptions'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

## 3.180.1 Value definition

```
id-regCtrl-pkiArchiveOptions OBJECT IDENTIFIER ::= { id-regCtrl 4 }  -
- raw value is 1.3.6.1.5.5.7.5.1.4
```

## 3.180.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 05 01 04
```

# 3.181 ASN.1 value 'id-regCtrl-pkiPublicationInfo'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

## 3.181.1 Value definition

```
id-regCtrl-pkiPublicationInfo OBJECT IDENTIFIER ::= { id-regCtrl 3 }  -
- raw value is 1.3.6.1.5.5.7.5.1.3
```

## 3.181.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 05 01 03
```

# 3.182 ASN.1 value 'id-regCtrl-protocolEncrKey'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

## 3.182.1 Value definition

```
id-regCtrl-protocolEncrKey OBJECT IDENTIFIER ::= { id-regCtrl 6 }  -
- raw value is 1.3.6.1.5.5.7.5.1.6
```

## 3.182.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 05 01 06
```

## 3.183 ASN.1 value 'id-regCtrl-regToken'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.183.1 Value definition

```
id-regCtrl-regToken OBJECT IDENTIFIER ::= { id-regCtrl 1 }  -
- raw value is 1.3.6.1.5.5.7.5.1.1
```

### 3.183.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 05 01 01
```

## 3.184 ASN.1 value 'id-regInfo'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.184.1 Value definition

```
id-regInfo OBJECT IDENTIFIER ::= { id-pkip 2 }  -- raw value is 1.3.6.1.5.5.7.5.2
```

### 3.184.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 05 02
```

## 3.185 ASN.1 value 'id-regInfo-certReq'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.185.1 Value definition

```
id-regInfo-certReq OBJECT IDENTIFIER ::= { id-regInfo 2 }  -
- raw value is 1.3.6.1.5.5.7.5.2.2
```

### 3.185.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 05 02 02
```

# 3.186 ASN.1 value 'id-regInfo-utf8Pairs'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

## 3.186.1 Value definition

```
id-regInfo-utf8Pairs OBJECT IDENTIFIER ::= { id-regInfo 1 }  -
- raw value is 1.3.6.1.5.5.7.5.2.1
```

## 3.186.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2B 06 01 05 05 07 05 02 01
```

# 3.187 ASN.1 value 'id-sha1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

## 3.187.1 Value definition

```
id-sha1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) oiw(14) secsig(3) algorithms(2) 26 }  -- raw value is 1.3.14.3.2.26
```

## 3.187.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 0E 03 02 1A
```

# 3.188 ASN.1 value 'id-sha224'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.188.1 Value definition

```
id-sha224 OBJECT IDENTIFIER ::= { joint-iso-itu-
t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 4 }
 -- raw value is 2.16.840.1.101.3.4.2.4
```

## 3.188.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 60 86 48 01 65 03 04 02 04
```

## 3.189 ASN.1 value 'id-sha256'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.189.1 Value definition

```
id-sha256 OBJECT IDENTIFIER ::= { joint-iso-itu-
t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
 -- raw value is 2.16.840.1.101.3.4.2.1
```

### 3.189.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 60 86 48 01 65 03 04 02 01
```

## 3.190 ASN.1 value 'id-sha384'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.190.1 Value definition

```
id-sha384 OBJECT IDENTIFIER ::= { joint-iso-itu-
t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 }
 -- raw value is 2.16.840.1.101.3.4.2.2
```

### 3.190.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 60 86 48 01 65 03 04 02 02
```

## 3.191 ASN.1 value 'id-sha512'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.191.1 Value definition

```
id-sha512 OBJECT IDENTIFIER ::= { joint-iso-itu-
t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }
 -- raw value is 2.16.840.1.101.3.4.2.3
```

### 3.191.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 60 86 48 01 65 03 04 02 03
```

## 3.192 ASN.1 value 'id-signedData'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.192.1 Value definition

```
id-signedData OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs7(7) 2 }  -- raw value is 1.2.840.113549.1.7.2
```

### 3.192.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 07 02
```

## 3.193 ASN.1 value 'id-signingTime'

Source of definition: 'CMS 2004 (Cryptographic Message Syntax, RFC 5652)'

### 3.193.1 Value definition

```
id-signingTime OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 5 }  -- raw value is 1.2.840.113549.1.9.5
```

### 3.193.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 05
```

## 3.194 ASN.1 value 'id-smime'

Source of definition: 'Certificate Request Message Format (CRMF, RFC 4211)'

### 3.194.1 Value definition

```
id-smime OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9) 16 }  -- raw value is 1.2.840.113549.1.9.16
```

### 3.194.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 10
```

## 3.195 ASN.1 value 'ietf-at'

Source of definition: 'PKCS #9'

### 3.195.1 Value definition

```
ietf-at OBJECT IDENTIFIER ::= { 1 3 6 1 5 5 7 9 }  -- raw value is 1.3.6.1.5.5.7.9
```

### 3.195.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2B 06 01 05 05 07 09
```

## 3.196 ASN.1 value 'local-postal-attributes'

Source of definition: 'CRL structures'

### 3.196.1 Value definition

```
local-postal-attributes INTEGER ::= 21
```

### 3.196.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 15
```

## 3.197 ASN.1 value 'maxInt'

Source of definition: 'LDAP (RFC 4511)'

### 3.197.1 Value definition

```
maxInt INTEGER ::= 2147483647
```

### 3.197.2 Value DER encoding

```
DER encoding size: 6 bytes

  02 04 7F FF FF FF
```

# 3.198 ASN.1 value 'md2'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

## 3.198.1 Value definition

```
md2 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) digestAlgorithm(2) 2 }  -- raw value is 1.2.840.113549.2.2
```

## 3.198.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 02 02
```

# 3.199 ASN.1 value 'md2WithRSAEncryption'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

## 3.199.1 Value definition

```
md2WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 2 }  -
- raw value is 1.2.840.113549.1.1.2
```

## 3.199.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 02
```

# 3.200 ASN.1 value 'md5'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

## 3.200.1 Value definition

```
md5 OBJECT IDENTIFIER ::= { iso(1) member-
body(2) us(840) rsadsi(113549) digestAlgorithm(2) 5 }  -- raw value is 1.2.840.113549.2.5
```

## 3.200.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 02 05
```

## 3.201 ASN.1 value 'md5WithRSAEncryption'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.201.1 Value definition

```
md5WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 4 }  -
- raw value is 1.2.840.113549.1.1.4
```

### 3.201.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 04
```

## 3.202 ASN.1 value 'mgf1SHA1Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.202.1 Value definition

```
mgf1SHA1Identifier AlgorithmIdentifier ::=
{
  algorithm(id-mgf1),         -- raw value is 1.2.840.113549.1.1.8
  parameters(sha1Identifier) -- original ASN.1 ANY type replaced by 'AlgorithmIdentifier'
}
```

### 3.202.2 Value DER encoding

```
DER encoding size: 24 bytes

  30 16 06 09 2A 86 48 86 F7 0D 01 01 08 30 09 06
  05 2B 0E 03 02 1A 05 00
```

## 3.203 ASN.1 value 'mgf1SHA224Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.203.1 Value definition

```
mgf1SHA224Identifier AlgorithmIdentifier ::=
{
  algorithm(id-mgf1),           -- raw value is 1.2.840.113549.1.1.8
  parameters(sha224Identifier) -- original ASN.1 ANY type replaced by 'AlgorithmIdentifier'
}
```

### 3.203.2 Value DER encoding

```
DER encoding size: 28 bytes

  30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06
  09 60 86 48 01 65 03 04 02 04 05 00
```

## 3.204 ASN.1 value 'mgf1SHA256Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.204.1 Value definition

```
mgf1SHA256Identifier AlgorithmIdentifier ::=
{
  algorithm(id-mgf1),           -- raw value is 1.2.840.113549.1.1.8
  parameters(sha256Identifier) -- original ASN.1 ANY type replaced by 'AlgorithmIdentifier'
}
```

### 3.204.2 Value DER encoding

```
DER encoding size: 28 bytes

  30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06
  09 60 86 48 01 65 03 04 02 01 05 00
```

## 3.205 ASN.1 value 'mgf1SHA384Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.205.1 Value definition

```
mgf1SHA384Identifier AlgorithmIdentifier ::=
{
  algorithm(id-mgf1),           -- raw value is 1.2.840.113549.1.1.8
  parameters(sha384Identifier) -- original ASN.1 ANY type replaced by 'AlgorithmIdentifier'
}
```

### 3.205.2 Value DER encoding

```
DER encoding size: 28 bytes

  30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06
  09 60 86 48 01 65 03 04 02 02 05 00
```

## 3.206 ASN.1 value 'mgf1SHA512Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.206.1 Value definition

```
mgf1SHA512Identifier AlgorithmIdentifier ::=
{
  algorithm(id-mgf1),          -- raw value is 1.2.840.113549.1.1.8
  parameters(sha512Identifier) -- original ASN.1 ANY type replaced by 'AlgorithmIdentifier'
}
```

### 3.206.2 Value DER encoding

```
DER encoding size: 28 bytes

  30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30 0D 06
  09 60 86 48 01 65 03 04 02 03 05 00
```

## 3.207 ASN.1 value 'nullOctetString'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.207.1 Value definition

```
nullOctetString OCTET STRING ::= ''H
```

### 3.207.2 Value DER encoding

```
DER encoding size: 2 bytes

  04 00
```

## 3.208 ASN.1 value 'nullParameters'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.208.1 Value definition

```
nullParameters NULL ::=   -- value of type NULL cannot be printed
```

### 3.208.2 Value DER encoding

```
DER encoding size: 2 bytes

  05 00
```

## 3.209 ASN.1 value 'pSpecifiedEmptyIdentifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.209.1 Value definition

```
pSpecifiedEmptyIdentifier AlgorithmIdentifier ::=
{
  algorithm(id-pSpecified),    -- raw value is 1.2.840.113549.1.1.9
  parameters(nullOctetString) -- original ASN.1 ANY type replaced by 'OCTET STRING'
}
```

### 3.209.2 Value DER encoding

```
DER encoding size: 15 bytes

  30 0D 06 09 2A 86 48 86 F7 0D 01 01 09 04 00
```

## 3.210 ASN.1 value 'pbeWithMD2AndDES-CBC'

Source of definition: 'PKCS #5'

### 3.210.1 Value definition

```
pbeWithMD2AndDES-CBC OBJECT IDENTIFIER ::= { pkcs-5 1 }  -
- raw value is 1.2.840.113549.1.5.1
```

### 3.210.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 01
```

## 3.211 ASN.1 value 'pbeWithMD2AndRC2-CBC'

Source of definition: 'PKCS #5'

### 3.211.1 Value definition

```
pbeWithMD2AndRC2-CBC OBJECT IDENTIFIER ::= { pkcs-5 4 }  -
- raw value is 1.2.840.113549.1.5.4
```

### 3.211.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 04
```

## 3.212 ASN.1 value 'pbeWithMD5AndDES-CBC'

Source of definition: 'PKCS #5'

### 3.212.1 Value definition

```
pbeWithMD5AndDES-CBC OBJECT IDENTIFIER ::= { pkcs-5 3 }  -
- raw value is 1.2.840.113549.1.5.3
```

### 3.212.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 03
```

## 3.213 ASN.1 value 'pbeWithMD5AndRC2-CBC'

Source of definition: 'PKCS #5'

### 3.213.1 Value definition

```
pbeWithMD5AndRC2-CBC OBJECT IDENTIFIER ::= { pkcs-5 6 }  -
- raw value is 1.2.840.113549.1.5.6
```

### 3.213.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 06
```

## 3.214 ASN.1 value 'pbeWithSHA1AndDES-CBC'

Source of definition: 'PKCS #5'

### 3.214.1 Value definition

```
pbeWithSHA1AndDES-CBC OBJECT IDENTIFIER ::= { pkcs-5 10 }  -
- raw value is 1.2.840.113549.1.5.10
```

### 3.214.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 0A
```

## 3.215 ASN.1 value 'pbeWithSHA1AndRC2-CBC'

Source of definition: 'PKCS #5'

### 3.215.1 Value definition

```
pbeWithSHA1AndRC2-CBC OBJECT IDENTIFIER ::= { pkcs-5 11 }  -
- raw value is 1.2.840.113549.1.5.11
```

### 3.215.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 05 0B
```

## 3.216 ASN.1 value 'pbeWithSHAAnd128BitRC2-CBC'

Source of definition: 'PKCS #12'

### 3.216.1 Value definition

```
pbeWithSHAAnd128BitRC2-CBC OBJECT IDENTIFIER ::= { pkcs-12PbeIds 5 }  -
- raw value is 1.2.840.113549.1.12.1.5
```

### 3.216.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 0C 01 05
```

## 3.217 ASN.1 value 'pbeWithSHAAnd128BitRC4'

Source of definition: 'PKCS #12'

### 3.217.1 Value definition

```
pbeWithSHAAnd128BitRC4 OBJECT IDENTIFIER ::= { pkcs-12PbeIds 1 }  -
- raw value is 1.2.840.113549.1.12.1.1
```

### 3.217.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 0C 01 01
```

## 3.218 ASN.1 value 'pbeWithSHAAnd2-KeyTripleDES-CBC'

Source of definition: 'PKCS #12'

### 3.218.1 Value definition

```
pbeWithSHAAnd2-KeyTripleDES-CBC OBJECT IDENTIFIER ::= { pkcs-12PbeIds 4 }  -
- raw value is 1.2.840.113549.1.12.1.4
```

### 3.218.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 0C 01 04
```

## 3.219 ASN.1 value 'pbeWithSHAAnd3-KeyTripleDES-CBC'

Source of definition: 'PKCS #12'

### 3.219.1 Value definition

```
pbeWithSHAAnd3-KeyTripleDES-CBC OBJECT IDENTIFIER ::= { pkcs-12PbeIds 3 }  -
- raw value is 1.2.840.113549.1.12.1.3
```

### 3.219.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 0C 01 03
```

## 3.220 ASN.1 value 'pbeWithSHAAnd40BitRC4'

Source of definition: 'PKCS #12'

### 3.220.1 Value definition

```
pbeWithSHAAnd40BitRC4 OBJECT IDENTIFIER ::= { pkcs-12PbeIds 2 }  -
- raw value is 1.2.840.113549.1.12.1.2
```

### 3.220.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 0C 01 02
```

## 3.221 ASN.1 value 'pbewithSHAAnd40BitRC2-CBC'

Source of definition: 'PKCS #12'

### 3.221.1 Value definition

```
pbewithSHAAnd40BitRC2-CBC OBJECT IDENTIFIER ::= { pkcs-12PbeIds 6 }  -
- raw value is 1.2.840.113549.1.12.1.6
```

### 3.221.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 0C 01 06
```

## 3.222 ASN.1 value 'pds-name'

Source of definition: 'CRL structures'

### 3.222.1 Value definition

```
pds-name INTEGER ::= 7
```

### 3.222.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 07
```

## 3.223 ASN.1 value 'physical-delivery-country-name'

Source of definition: 'CRL structures'

### 3.223.1 Value definition

```
physical-delivery-country-name INTEGER ::= 8
```

### 3.223.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 08
```

## 3.224 ASN.1 value 'physical-delivery-office-name'

Source of definition: 'CRL structures'

### 3.224.1 Value definition

```
physical-delivery-office-name INTEGER ::= 10
```

### 3.224.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 0A
```

## 3.225 ASN.1 value 'physical-delivery-office-number'

Source of definition: 'CRL structures'

### 3.225.1 Value definition

```
physical-delivery-office-number INTEGER ::= 11
```

### 3.225.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 0B
```

## 3.226 ASN.1 value 'physical-delivery-organization-name'

Source of definition: 'CRL structures'

### 3.226.1 Value definition

```
physical-delivery-organization-name INTEGER ::= 14
```

### 3.226.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 0E
```

## 3.227 ASN.1 value 'physical-delivery-personal-name'

Source of definition: 'CRL structures'

### 3.227.1 Value definition

```
physical-delivery-personal-name INTEGER ::= 13
```

### 3.227.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 0D
```

## 3.228 ASN.1 value 'pkcs'

Source of definition: 'PKCS #5'

### 3.228.1 Value definition

```
pkcs OBJECT IDENTIFIER ::= { rsadsi pkcs(1) }  -- raw value is 1.2.840.113549.1
```

### 3.228.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 86 F7 0D 01
```

## 3.229 ASN.1 value 'pkcs-1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.229.1 Value definition

```
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 1 }  -
- raw value is 1.2.840.113549.1.1
```

### 3.229.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 01 01
```

## 3.230 ASN.1 value 'pkcs-12'

Source of definition: 'PKCS #12'

### 3.230.1 Value definition

```
pkcs-12 OBJECT IDENTIFIER ::= { pkcs 12 }  -- raw value is 1.2.840.113549.1.12
```

### 3.230.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 01 0C
```

## 3.231 ASN.1 value 'pkcs-12PbeIds'

Source of definition: 'PKCS #12'

### 3.231.1 Value definition

```
pkcs-12PbeIds OBJECT IDENTIFIER ::= { pkcs-12 1 }  -- raw value is 1.2.840.113549.1.12.1
```

### 3.231.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 0C 01
```

## 3.232 ASN.1 value 'pkcs-5'

Source of definition: 'PKCS #5'

### 3.232.1 Value definition

```
pkcs-5 OBJECT IDENTIFIER ::= { pkcs 5 }  -- raw value is 1.2.840.113549.1.5
```

### 3.232.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 01 05
```

## 3.233 ASN.1 value 'pkcs-9'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.233.1 Value definition

```
pkcs-9 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 9 }  -
- raw value is 1.2.840.113549.1.9
```

### 3.233.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 01 09
```

## 3.234 ASN.1 value 'pkcs-9-at'

Source of definition: 'PKCS #9'

### 3.234.1 Value definition

```
pkcs-9-at OBJECT IDENTIFIER ::= { pkcs-9 25 }  -- raw value is 1.2.840.113549.1.9.25
```

### 3.234.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 19
```

## 3.235 ASN.1 value 'pkcs-9-at-challengePassword'

Source of definition: 'PKCS #9'

### 3.235.1 Value definition

```
pkcs-9-at-challengePassword OBJECT IDENTIFIER ::= { pkcs-9 7 }  -
- raw value is 1.2.840.113549.1.9.7
```

### 3.235.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 07
```

## 3.236 ASN.1 value 'pkcs-9-at-contentType'

Source of definition: 'PKCS #9'

### 3.236.1 Value definition

```
pkcs-9-at-contentType OBJECT IDENTIFIER ::= { pkcs-9 3 }  -
- raw value is 1.2.840.113549.1.9.3
```

### 3.236.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 03
```

## 3.237 ASN.1 value 'pkcs-9-at-counterSignature'

Source of definition: 'PKCS #9'

### 3.237.1 Value definition

```
pkcs-9-at-counterSignature OBJECT IDENTIFIER ::= { pkcs-9 6 }  -
- raw value is 1.2.840.113549.1.9.6
```

### 3.237.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 06
```

## 3.238 ASN.1 value 'pkcs-9-at-countryOfCitizenship'

Source of definition: 'PKCS #9'

### 3.238.1 Value definition

```
pkcs-9-at-countryOfCitizenship OBJECT IDENTIFIER ::= { ietf-at 4 }  -
- raw value is 1.3.6.1.5.5.7.9.4
```

### 3.238.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 09 04
```

## 3.239 ASN.1 value 'pkcs-9-at-countryOfResidence'

Source of definition: 'PKCS #9'

### 3.239.1 Value definition

```
pkcs-9-at-countryOfResidence OBJECT IDENTIFIER ::= { ietf-at 5 }  -
- raw value is 1.3.6.1.5.5.7.9.5
```

### 3.239.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 09 05
```

## 3.240 ASN.1 value 'pkcs-9-at-dateOfBirth'

Source of definition: 'PKCS #9'

### 3.240.1 Value definition

```
pkcs-9-at-dateOfBirth OBJECT IDENTIFIER ::= { ietf-at 1 }  -
- raw value is 1.3.6.1.5.5.7.9.1
```

### 3.240.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 09 01
```

## 3.241 ASN.1 value 'pkcs-9-at-emailAddress'

Source of definition: 'PKCS #9'

### 3.241.1 Value definition

```
pkcs-9-at-emailAddress OBJECT IDENTIFIER ::= { pkcs-9 1 }  -
- raw value is 1.2.840.113549.1.9.1
```

### 3.241.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 01
```

## 3.242 ASN.1 value 'pkcs-9-at-encryptedPrivateKeyInfo'

Source of definition: 'PKCS #9'

### 3.242.1 Value definition

```
pkcs-9-at-encryptedPrivateKeyInfo OBJECT IDENTIFIER ::= { pkcs-9-at 2 }  -
- raw value is 1.2.840.113549.1.9.25.2
```

### 3.242.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 19 02
```

## 3.243 ASN.1 value 'pkcs-9-at-extendedCertificateAttributes'

Source of definition: 'PKCS #9'

### 3.243.1 Value definition

```
pkcs-9-at-extendedCertificateAttributes OBJECT IDENTIFIER ::= { pkcs-9 9 }  -
- raw value is 1.2.840.113549.1.9.9
```

### 3.243.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 09
```

## 3.244 ASN.1 value 'pkcs-9-at-extensionRequest'

Source of definition: 'PKCS #9'

### 3.244.1 Value definition

```
pkcs-9-at-extensionRequest OBJECT IDENTIFIER ::= { pkcs-9 14 }  -
- raw value is 1.2.840.113549.1.9.14
```

### 3.244.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 0E
```

## 3.245 ASN.1 value 'pkcs-9-at-friendlyName'

Source of definition: 'PKCS #9'

### 3.245.1 Value definition

```
pkcs-9-at-friendlyName OBJECT IDENTIFIER ::= { pkcs-9 20 }  -
- raw value is 1.2.840.113549.1.9.20
```

### 3.245.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 14
```

## 3.246 ASN.1 value 'pkcs-9-at-gender'

Source of definition: 'PKCS #9'

### 3.246.1 Value definition

```
pkcs-9-at-gender OBJECT IDENTIFIER ::= { ietf-at 3 }  -- raw value is 1.3.6.1.5.5.7.9.3
```

### 3.246.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 09 03
```

## 3.247 ASN.1 value 'pkcs-9-at-localKeyId'

Source of definition: 'PKCS #9'

### 3.247.1 Value definition

```
pkcs-9-at-localKeyId OBJECT IDENTIFIER ::= { pkcs-9 21 }  -
- raw value is 1.2.840.113549.1.9.21
```

### 3.247.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 15
```

# 3.248 ASN.1 value 'pkcs-9-at-messageDigest'

Source of definition: 'PKCS #9'

## 3.248.1 Value definition

```
pkcs-9-at-messageDigest OBJECT IDENTIFIER ::= { pkcs-9 4 }  -
- raw value is 1.2.840.113549.1.9.4
```

## 3.248.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 04
```

# 3.249 ASN.1 value 'pkcs-9-at-pkcs15Token'

Source of definition: 'PKCS #9'

## 3.249.1 Value definition

```
pkcs-9-at-pkcs15Token OBJECT IDENTIFIER ::= { pkcs-9-at 1 }  -
- raw value is 1.2.840.113549.1.9.25.1
```

## 3.249.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 19 01
```

# 3.250 ASN.1 value 'pkcs-9-at-pkcs7PDU'

Source of definition: 'PKCS #9'

## 3.250.1 Value definition

```
pkcs-9-at-pkcs7PDU OBJECT IDENTIFIER ::= { pkcs-9-at 5 }  -
- raw value is 1.2.840.113549.1.9.25.5
```

## 3.250.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 19 05
```

## 3.251 ASN.1 value 'pkcs-9-at-placeOfBirth'

Source of definition: 'PKCS #9'

### 3.251.1 Value definition

```
pkcs-9-at-placeOfBirth OBJECT IDENTIFIER ::= { ietf-at 2 }  -
- raw value is 1.3.6.1.5.5.7.9.2
```

### 3.251.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2B 06 01 05 05 07 09 02
```

## 3.252 ASN.1 value 'pkcs-9-at-randomNonce'

Source of definition: 'PKCS #9'

### 3.252.1 Value definition

```
pkcs-9-at-randomNonce OBJECT IDENTIFIER ::= { pkcs-9-at 3 }  -
- raw value is 1.2.840.113549.1.9.25.3
```

### 3.252.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 19 03
```

## 3.253 ASN.1 value 'pkcs-9-at-sequenceNumber'

Source of definition: 'PKCS #9'

### 3.253.1 Value definition

```
pkcs-9-at-sequenceNumber OBJECT IDENTIFIER ::= { pkcs-9-at 4 }  -
- raw value is 1.2.840.113549.1.9.25.4
```

### 3.253.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 19 04
```

## 3.254 ASN.1 value 'pkcs-9-at-signingDescription'

Source of definition: 'PKCS #9'

### 3.254.1 Value definition

```
pkcs-9-at-signingDescription OBJECT IDENTIFIER ::= { pkcs-9 13 }  -
- raw value is 1.2.840.113549.1.9.13
```

### 3.254.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 0D
```

## 3.255 ASN.1 value 'pkcs-9-at-signingTime'

Source of definition: 'PKCS #9'

### 3.255.1 Value definition

```
pkcs-9-at-signingTime OBJECT IDENTIFIER ::= { pkcs-9 5 }  -
- raw value is 1.2.840.113549.1.9.5
```

### 3.255.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 05
```

## 3.256 ASN.1 value 'pkcs-9-at-smimeCapabilities'

Source of definition: 'PKCS #9'

### 3.256.1 Value definition

```
pkcs-9-at-smimeCapabilities OBJECT IDENTIFIER ::= { pkcs-9 15 }  -
- raw value is 1.2.840.113549.1.9.15
```

### 3.256.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 0F
```

## 3.257 ASN.1 value 'pkcs-9-at-unstructuredAddress'

Source of definition: 'PKCS #9'

### 3.257.1 Value definition

```
pkcs-9-at-unstructuredAddress OBJECT IDENTIFIER ::= { pkcs-9 8 }  -
- raw value is 1.2.840.113549.1.9.8
```

### 3.257.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 08
```

## 3.258 ASN.1 value 'pkcs-9-at-unstructuredName'

Source of definition: 'PKCS #9'

### 3.258.1 Value definition

```
pkcs-9-at-unstructuredName OBJECT IDENTIFIER ::= { pkcs-9 2 }  -
- raw value is 1.2.840.113549.1.9.2
```

### 3.258.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 02
```

## 3.259 ASN.1 value 'pkcs-9-at-userPKCS12'

Source of definition: 'PKCS #9'

### 3.259.1 Value definition

```
pkcs-9-at-userPKCS12 OBJECT IDENTIFIER ::= { 2 16 840 1 113730 3 1 216 }  -
- raw value is 2.16.840.1.113730.3.1.216
```

### 3.259.2 Value DER encoding

```
DER encoding size: 13 bytes

  06 0B 60 86 48 01 86 F8 42 03 01 81 58
```

# 3.260 ASN.1 value 'pkcs-9-mo'

Source of definition: 'PKCS #9'

## 3.260.1 Value definition

```
pkcs-9-mo OBJECT IDENTIFIER ::= { pkcs-9 0 }  -- raw value is 1.2.840.113549.1.9.0
```

## 3.260.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 00
```

# 3.261 ASN.1 value 'pkcs-9-mr'

Source of definition: 'PKCS #9'

## 3.261.1 Value definition

```
pkcs-9-mr OBJECT IDENTIFIER ::= { pkcs-9 27 }  -- raw value is 1.2.840.113549.1.9.27
```

## 3.261.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 1B
```

# 3.262 ASN.1 value 'pkcs-9-mr-caseIgnoreMatch'

Source of definition: 'PKCS #9'

## 3.262.1 Value definition

```
pkcs-9-mr-caseIgnoreMatch OBJECT IDENTIFIER ::= { pkcs-9-mr 1 }  -
- raw value is 1.2.840.113549.1.9.27.1
```

## 3.262.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 1B 01
```

## 3.263 ASN.1 value 'pkcs-9-mr-signingTimeMatch'

Source of definition: 'PKCS #9'

### 3.263.1 Value definition

```
pkcs-9-mr-signingTimeMatch OBJECT IDENTIFIER ::= { pkcs-9-mr 2 }  -
- raw value is 1.2.840.113549.1.9.27.2
```

### 3.263.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 1B 02
```

## 3.264 ASN.1 value 'pkcs-9-oc'

Source of definition: 'PKCS #9'

### 3.264.1 Value definition

```
pkcs-9-oc OBJECT IDENTIFIER ::= { pkcs-9 24 }  -- raw value is 1.2.840.113549.1.9.24
```

### 3.264.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 18
```

## 3.265 ASN.1 value 'pkcs-9-oc-naturalPerson'

Source of definition: 'PKCS #9'

### 3.265.1 Value definition

```
pkcs-9-oc-naturalPerson OBJECT IDENTIFIER ::= { pkcs-9-oc 2 }  -
- raw value is 1.2.840.113549.1.9.24.2
```

### 3.265.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 18 02
```

## 3.266 ASN.1 value 'pkcs-9-oc-pkcsEntity'

Source of definition: 'PKCS #9'

### 3.266.1 Value definition

```
pkcs-9-oc-pkcsEntity OBJECT IDENTIFIER ::= { pkcs-9-oc 1 }  -
- raw value is 1.2.840.113549.1.9.24.1
```

### 3.266.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 18 01
```

## 3.267 ASN.1 value 'pkcs-9-sx'

Source of definition: 'PKCS #9'

### 3.267.1 Value definition

```
pkcs-9-sx OBJECT IDENTIFIER ::= { pkcs-9 26 }  -- raw value is 1.2.840.113549.1.9.26
```

### 3.267.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 1A
```

## 3.268 ASN.1 value 'pkcs-9-sx-pkcs9String'

Source of definition: 'PKCS #9'

### 3.268.1 Value definition

```
pkcs-9-sx-pkcs9String OBJECT IDENTIFIER ::= { pkcs-9-sx 1 }  -
- raw value is 1.2.840.113549.1.9.26.1
```

### 3.268.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 1A 01
```

## 3.269 ASN.1 value 'pkcs-9-sx-signingTime'

Source of definition: 'PKCS #9'

### 3.269.1 Value definition

```
pkcs-9-sx-signingTime OBJECT IDENTIFIER ::= { pkcs-9-sx 2 }  -
- raw value is 1.2.840.113549.1.9.26.2
```

### 3.269.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 1A 02
```

## 3.270 ASN.1 value 'pkcs-9-ub-challengePassword'

Source of definition: 'PKCS #9'

### 3.270.1 Value definition

```
pkcs-9-ub-challengePassword INTEGER ::= pkcs-9-ub-pkcs9String
```

### 3.270.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.271 ASN.1 value 'pkcs-9-ub-emailAddress'

Source of definition: 'PKCS #9'

### 3.271.1 Value definition

```
pkcs-9-ub-emailAddress INTEGER ::= pkcs-9-ub-pkcs9String
```

### 3.271.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.272 ASN.1 value 'pkcs-9-ub-friendlyName'

Source of definition: 'PKCS #9'

### 3.272.1 Value definition

```
pkcs-9-ub-friendlyName INTEGER ::= pkcs-9-ub-pkcs9String
```

### 3.272.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.273 ASN.1 value 'pkcs-9-ub-match'

Source of definition: 'PKCS #9'

### 3.273.1 Value definition

```
pkcs-9-ub-match INTEGER ::= pkcs-9-ub-pkcs9String
```

### 3.273.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.274 ASN.1 value 'pkcs-9-ub-pkcs9String'

Source of definition: 'PKCS #9'

### 3.274.1 Value definition

```
pkcs-9-ub-pkcs9String INTEGER ::= 255
```

### 3.274.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.275 ASN.1 value 'pkcs-9-ub-placeOfBirth'

Source of definition: 'PKCS #9'

### 3.275.1 Value definition

```
pkcs-9-ub-placeOfBirth INTEGER ::= ub-name
```

### 3.275.2 Value DER encoding

```
DER encoding size: 5 bytes

  02 03 00 80 00
```

## 3.276 ASN.1 value 'pkcs-9-ub-pseudonym'

Source of definition: 'PKCS #9'

### 3.276.1 Value definition

```
pkcs-9-ub-pseudonym INTEGER ::= ub-name
```

### 3.276.2 Value DER encoding

```
DER encoding size: 5 bytes

  02 03 00 80 00
```

## 3.277 ASN.1 value 'pkcs-9-ub-signingDescription'

Source of definition: 'PKCS #9'

### 3.277.1 Value definition

```
pkcs-9-ub-signingDescription INTEGER ::= pkcs-9-ub-pkcs9String
```

### 3.277.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.278 ASN.1 value 'pkcs-9-ub-unstructuredAddress'

Source of definition: 'PKCS #9'

### 3.278.1 Value definition

```
pkcs-9-ub-unstructuredAddress INTEGER ::= pkcs-9-ub-pkcs9String
```

### 3.278.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.279 ASN.1 value 'pkcs-9-ub-unstructuredName'

Source of definition: 'PKCS #9'

### 3.279.1 Value definition

```
pkcs-9-ub-unstructuredName INTEGER ::= pkcs-9-ub-pkcs9String
```

### 3.279.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.280 ASN.1 value 'post-office-box-address'

Source of definition: 'CRL structures'

### 3.280.1 Value definition

```
post-office-box-address INTEGER ::= 18
```

### 3.280.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 12
```

## 3.281 ASN.1 value 'postal-code'

Source of definition: 'CRL structures'

### 3.281.1 Value definition

```
postal-code INTEGER ::= 9
```

### 3.281.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 09
```

## 3.282 ASN.1 value 'poste-restante-address'

Source of definition: 'CRL structures'

### 3.282.1 Value definition

```
poste-restante-address INTEGER ::= 19
```

### 3.282.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 13
```

## 3.283 ASN.1 value 'ppBasis'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.283.1 Value definition

```
ppBasis OBJECT IDENTIFIER ::= { id-characteristic-two-basis 3 }  -
- raw value is 1.2.840.10045.1.2.3.3
```

### 3.283.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 CE 3D 01 02 03 03
```

## 3.284 ASN.1 value 'prime-field'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.284.1 Value definition

```
prime-field OBJECT IDENTIFIER ::= { id-fieldType 1 }  -- raw value is 1.2.840.10045.1.1
```

### 3.284.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 3D 01 01
```

## 3.285 ASN.1 value 'prime192v1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.285.1 Value definition

```
prime192v1 OBJECT IDENTIFIER ::= { primeCurve 1 }  -- raw value is 1.2.840.10045.3.1.1
```

### 3.285.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 01
```

## 3.286 ASN.1 value 'prime192v2'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.286.1 Value definition

```
prime192v2 OBJECT IDENTIFIER ::= { primeCurve 2 }  -- raw value is 1.2.840.10045.3.1.2
```

### 3.286.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 02
```

## 3.287 ASN.1 value 'prime192v3'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.287.1 Value definition

```
prime192v3 OBJECT IDENTIFIER ::= { primeCurve 3 }  -- raw value is 1.2.840.10045.3.1.3
```

### 3.287.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 03
```

## 3.288 ASN.1 value 'prime239v1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.288.1 Value definition

```
prime239v1 OBJECT IDENTIFIER ::= { primeCurve 4 }  -- raw value is 1.2.840.10045.3.1.4
```

### 3.288.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 04
```

## 3.289 ASN.1 value 'prime239v2'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.289.1 Value definition

```
prime239v2 OBJECT IDENTIFIER ::= { primeCurve 5 }  -- raw value is 1.2.840.10045.3.1.5
```

### 3.289.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 05
```

## 3.290 ASN.1 value 'prime239v3'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.290.1 Value definition

```
prime239v3 OBJECT IDENTIFIER ::= { primeCurve 6 }  -- raw value is 1.2.840.10045.3.1.6
```

### 3.290.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 06
```

## 3.291 ASN.1 value 'prime256v1'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.291.1 Value definition

```
prime256v1 OBJECT IDENTIFIER ::= { primeCurve 7 }  -- raw value is 1.2.840.10045.3.1.7
```

### 3.291.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 07
```

## 3.292 ASN.1 value 'primeCurve'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.292.1 Value definition

```
primeCurve OBJECT IDENTIFIER ::= { ellipticCurve prime(1) }  -
- raw value is 1.2.840.10045.3.1
```

### 3.292.2 Value DER encoding

```
DER encoding size: 9 bytes

  06 07 2A 86 48 CE 3D 03 01
```

## 3.293 ASN.1 value 'rSAES-OAEP-Default-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.293.1 Value definition

```
rSAES-OAEP-Default-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSAES-OAEP),              -- raw value is 1.2.840.113549.1.1.7
  parameters(rSAES-OAEP-Default-Params) -- original ASN.1 ANY type replaced by 'RSAES-OAEP-
params'
}
```

### 3.293.2 Value DER encoding

```
DER encoding size: 15 bytes

  30 0D 06 09 2A 86 48 86 F7 0D 01 01 07 30 00
```

## 3.294 ASN.1 value 'rSAES-OAEP-Default-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.294.1 Value definition

```
rSAES-OAEP-Default-Params RSAES-OAEP-params ::=
{
  hashFunc(sha1Identifier),              -- matches default value, absent
  maskGenFunc(mgf1SHA1Identifier),       -- matches default value, absent
  pSourceFunc(pSpecifiedEmptyIdentifier) -- matches default value, absent
}
```

### 3.294.2 Value DER encoding

```
DER encoding size: 2 bytes

  30 00
```

# 3.295 ASN.1 value 'rSAES-OAEP-SHA224-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.295.1 Value definition

```
rSAES-OAEP-SHA224-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSAES-OAEP),            -- raw value is 1.2.840.113549.1.1.7
  parameters(rSAES-OAEP-SHA224-Params) -- original ASN.1 ANY type replaced by 'RSAES-OAEP-
params'
}
```

## 3.295.2 Value DER encoding

```
DER encoding size: 62 bytes

  30 3C 06 09 2A 86 48 86 F7 0D 01 01 07 30 2F A0
  0F 30 0D 06 09 60 86 48 01 65 03 04 02 04 05 00
  A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30
  0D 06 09 60 86 48 01 65 03 04 02 04 05 00
```

# 3.296 ASN.1 value 'rSAES-OAEP-SHA224-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.296.1 Value definition

```
rSAES-OAEP-SHA224-Params RSAES-OAEP-params ::=
{
  hashFunc(sha224Identifier),
  maskGenFunc(mgf1SHA224Identifier),
  pSourceFunc(pSpecifiedEmptyIdentifier) -- matches default value, absent
}
```

## 3.296.2 Value DER encoding

```
DER encoding size: 49 bytes

  30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02
  04 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01
  01 08 30 0D 06 09 60 86 48 01 65 03 04 02 04 05
  00
```

# 3.297 ASN.1 value 'rSAES-OAEP-SHA256-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.297.1 Value definition

```
rSAES-OAEP-SHA256-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSAES-OAEP),            -- raw value is 1.2.840.113549.1.1.7
  parameters(rSAES-OAEP-SHA256-Params) -- original ASN.1 ANY type replaced by 'RSAES-OAEP-
params'
}
```

## 3.297.2 Value DER encoding

```
DER encoding size: 62 bytes

  30 3C 06 09 2A 86 48 86 F7 0D 01 01 07 30 2F A0
  0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00
  A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30
  0D 06 09 60 86 48 01 65 03 04 02 01 05 00
```

# 3.298 ASN.1 value 'rSAES-OAEP-SHA256-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.298.1 Value definition

```
rSAES-OAEP-SHA256-Params RSAES-OAEP-params ::=
{
  hashFunc(sha256Identifier),
  maskGenFunc(mgf1SHA256Identifier),
  pSourceFunc(pSpecifiedEmptyIdentifier) -- matches default value, absent
}
```

## 3.298.2 Value DER encoding

```
DER encoding size: 49 bytes

  30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02
  01 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01
  01 08 30 0D 06 09 60 86 48 01 65 03 04 02 01 05
  00
```

# 3.299 ASN.1 value 'rSAES-OAEP-SHA384-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.299.1 Value definition

```
rSAES-OAEP-SHA384-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSAES-OAEP),            -- raw value is 1.2.840.113549.1.1.7
  parameters(rSAES-OAEP-SHA384-Params) -- original ASN.1 ANY type replaced by 'RSAES-OAEP-
params'
}
```

## 3.299.2 Value DER encoding

```
DER encoding size: 62 bytes

  30 3C 06 09 2A 86 48 86 F7 0D 01 01 07 30 2F A0
  0F 30 0D 06 09 60 86 48 01 65 03 04 02 02 05 00
  A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30
  0D 06 09 60 86 48 01 65 03 04 02 02 05 00
```

# 3.300 ASN.1 value 'rSAES-OAEP-SHA384-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.300.1 Value definition

```
rSAES-OAEP-SHA384-Params RSAES-OAEP-params ::=
{
  hashFunc(sha384Identifier),
  maskGenFunc(mgf1SHA384Identifier),
  pSourceFunc(pSpecifiedEmptyIdentifier) -- matches default value, absent
}
```

## 3.300.2 Value DER encoding

```
DER encoding size: 49 bytes

  30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02
  02 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01
  01 08 30 0D 06 09 60 86 48 01 65 03 04 02 02 05
  00
```

# 3.301 ASN.1 value 'rSAES-OAEP-SHA512-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.301.1 Value definition

```
rSAES-OAEP-SHA512-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSAES-OAEP),            -- raw value is 1.2.840.113549.1.1.7
  parameters(rSAES-OAEP-SHA512-Params) -- original ASN.1 ANY type replaced by 'RSAES-OAEP-
params'
}
```

## 3.301.2 Value DER encoding

```
DER encoding size: 62 bytes

  30 3C 06 09 2A 86 48 86 F7 0D 01 01 07 30 2F A0
  0F 30 0D 06 09 60 86 48 01 65 03 04 02 03 05 00
  A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30
  0D 06 09 60 86 48 01 65 03 04 02 03 05 00
```

# 3.302 ASN.1 value 'rSAES-OAEP-SHA512-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.302.1 Value definition

```
rSAES-OAEP-SHA512-Params RSAES-OAEP-params ::=
{
  hashFunc(sha512Identifier),
  maskGenFunc(mgf1SHA512Identifier),
  pSourceFunc(pSpecifiedEmptyIdentifier) -- matches default value, absent
}
```

## 3.302.2 Value DER encoding

```
DER encoding size: 49 bytes

  30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02
  03 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01
  01 08 30 0D 06 09 60 86 48 01 65 03 04 02 03 05
  00
```

# 3.303 ASN.1 value 'rSASSA-PSS-Default-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.303.1 Value definition

```
rSASSA-PSS-Default-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSASSA-PSS),             -- raw value is 1.2.840.113549.1.1.10
  parameters(rSASSA-PSS-Default-Params) -- original ASN.1 ANY type replaced by 'RSASSA-PSS-
params'
}
```

## 3.303.2 Value DER encoding

```
DER encoding size: 15 bytes

  30 0D 06 09 2A 86 48 86 F7 0D 01 01 0A 30 00
```

# 3.304 ASN.1 value 'rSASSA-PSS-Default-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.304.1 Value definition

```
rSASSA-PSS-Default-Params RSASSA-PSS-params ::=
{
  hashAlgorithm(sha1Identifier),        -- matches default value, absent
  maskGenAlgorithm(mgf1SHA1Identifier), -- matches default value, absent
  saltLength(20),                       -- matches default value, absent
  trailerField(trailerFieldBC)          -- matches default value, absent
}
```

## 3.304.2 Value DER encoding

```
DER encoding size: 2 bytes

  30 00
```

# 3.305 ASN.1 value 'rSASSA-PSS-SHA224-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.305.1 Value definition

```
rSASSA-PSS-SHA224-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSASSA-PSS),            -- raw value is 1.2.840.113549.1.1.10
  parameters(rSASSA-PSS-SHA224-Params) -- original ASN.1 ANY type replaced by 'RSASSA-PSS-
params'
}
```

## 3.305.2 Value DER encoding

```
DER encoding size: 62 bytes

  30 3C 06 09 2A 86 48 86 F7 0D 01 01 0A 30 2F A0
  0F 30 0D 06 09 60 86 48 01 65 03 04 02 04 05 00
  A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30
  0D 06 09 60 86 48 01 65 03 04 02 04 05 00
```

# 3.306 ASN.1 value 'rSASSA-PSS-SHA224-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.306.1 Value definition

```
rSASSA-PSS-SHA224-Params RSASSA-PSS-params ::=
{
  hashAlgorithm(sha224Identifier),
  maskGenAlgorithm(mgf1SHA224Identifier),
  saltLength(20),                      -- matches default value, absent
  trailerField(trailerFieldBC)         -- matches default value, absent
}
```

## 3.306.2 Value DER encoding

```
DER encoding size: 49 bytes

  30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02
  04 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01
  01 08 30 0D 06 09 60 86 48 01 65 03 04 02 04 05
  00
```

# 3.307 ASN.1 value 'rSASSA-PSS-SHA256-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.307.1 Value definition

```
rSASSA-PSS-SHA256-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSASSA-PSS),            -- raw value is 1.2.840.113549.1.1.10
  parameters(rSASSA-PSS-SHA256-Params) -- original ASN.1 ANY type replaced by 'RSASSA-PSS-
params'
}
```

## 3.307.2 Value DER encoding

```
DER encoding size: 62 bytes

  30 3C 06 09 2A 86 48 86 F7 0D 01 01 0A 30 2F A0
  0F 30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00
  A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30
  0D 06 09 60 86 48 01 65 03 04 02 01 05 00
```

# 3.308 ASN.1 value 'rSASSA-PSS-SHA256-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.308.1 Value definition

```
rSASSA-PSS-SHA256-Params RSASSA-PSS-params ::=
{
  hashAlgorithm(sha256Identifier),
  maskGenAlgorithm(mgf1SHA256Identifier),
  saltLength(20),                      -- matches default value, absent
  trailerField(trailerFieldBC)         -- matches default value, absent
}
```

## 3.308.2 Value DER encoding

```
DER encoding size: 49 bytes

  30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02
  01 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01
  01 08 30 0D 06 09 60 86 48 01 65 03 04 02 01 05
  00
```

# 3.309 ASN.1 value 'rSASSA-PSS-SHA384-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.309.1 Value definition

```
rSASSA-PSS-SHA384-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSASSA-PSS),            -- raw value is 1.2.840.113549.1.1.10
  parameters(rSASSA-PSS-SHA384-Params) -- original ASN.1 ANY type replaced by 'RSASSA-PSS-
params'
}
```

## 3.309.2 Value DER encoding

```
DER encoding size: 62 bytes

  30 3C 06 09 2A 86 48 86 F7 0D 01 01 0A 30 2F A0
  0F 30 0D 06 09 60 86 48 01 65 03 04 02 02 05 00
  A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30
  0D 06 09 60 86 48 01 65 03 04 02 02 05 00
```

# 3.310 ASN.1 value 'rSASSA-PSS-SHA384-Params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.310.1 Value definition

```
rSASSA-PSS-SHA384-Params RSASSA-PSS-params ::=
{
  hashAlgorithm(sha384Identifier),
  maskGenAlgorithm(mgf1SHA384Identifier),
  saltLength(20),                      -- matches default value, absent
  trailerField(trailerFieldBC)         -- matches default value, absent
}
```

## 3.310.2 Value DER encoding

```
DER encoding size: 49 bytes

  30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02
  02 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01
  01 08 30 0D 06 09 60 86 48 01 65 03 04 02 02 05
  00
```

# 3.311 ASN.1 value 'rSASSA-PSS-SHA512-Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.311.1 Value definition

```
rSASSA-PSS-SHA512-Identifier AlgorithmIdentifier ::=
{
  algorithm(id-RSASSA-PSS),             -- raw value is 1.2.840.113549.1.1.10
  parameters(rSSASSA-PSS-SHA512-params) -- original ASN.1 ANY type replaced by 'RSASSA-PSS-
params'
}
```

## 3.311.2 Value DER encoding

```
DER encoding size: 62 bytes

  30 3C 06 09 2A 86 48 86 F7 0D 01 01 0A 30 2F A0
  0F 30 0D 06 09 60 86 48 01 65 03 04 02 03 05 00
  A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01 01 08 30
  0D 06 09 60 86 48 01 65 03 04 02 03 05 00
```

# 3.312 ASN.1 value 'rSSASSA-PSS-SHA512-params'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.312.1 Value definition

```
rSSASSA-PSS-SHA512-params RSASSA-PSS-params ::=
{
  hashAlgorithm(sha512Identifier),
  maskGenAlgorithm(mgf1SHA512Identifier),
  saltLength(20),                       -- matches default value, absent
  trailerField(trailerFieldBC)          -- matches default value, absent
}
```

## 3.312.2 Value DER encoding

```
DER encoding size: 49 bytes

  30 2F A0 0F 30 0D 06 09 60 86 48 01 65 03 04 02
  03 05 00 A1 1C 30 1A 06 09 2A 86 48 86 F7 0D 01
  01 08 30 0D 06 09 60 86 48 01 65 03 04 02 03 05
  00
```

## 3.313 ASN.1 value 'rc2CBC'

Source of definition: 'PKCS #5'

### 3.313.1 Value definition

```
rc2CBC OBJECT IDENTIFIER ::= { encryptionAlgorithm 2 }  -- raw value is 1.2.840.113549.3.2
```

### 3.313.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 03 02
```

## 3.314 ASN.1 value 'rc5-CBC-PAD'

Source of definition: 'PKCS #5'

### 3.314.1 Value definition

```
rc5-CBC-PAD OBJECT IDENTIFIER ::= { encryptionAlgorithm 9 }  -
- raw value is 1.2.840.113549.3.9
```

### 3.314.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 86 F7 0D 03 09
```

## 3.315 ASN.1 value 'rsaEncryption'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.315.1 Value definition

```
rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1 }  -- raw value is 1.2.840.113549.1.1.1
```

### 3.315.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 01
```

## 3.316 ASN.1 value 'rsadsi'

Source of definition: 'PKCS #5'

### 3.316.1 Value definition

```
rsadsi OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) }  -
- raw value is 1.2.840.113549
```

### 3.316.2 Value DER encoding

```
DER encoding size: 8 bytes

  06 06 2A 86 48 86 F7 0D
```

## 3.317 ASN.1 value 'sdsiCertificate'

Source of definition: 'PKCS #12'

### 3.317.1 Value definition

```
sdsiCertificate OBJECT IDENTIFIER ::= { certTypes 2 }  -
- raw value is 1.2.840.113549.1.9.22.2
```

### 3.317.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 16 02
```

## 3.318 ASN.1 value 'secp192r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.318.1 Value definition

```
secp192r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-
62(10045) curves(3) prime(1) 1 }  -- raw value is 1.2.840.10045.3.1.1
```

### 3.318.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 01
```

## 3.319 ASN.1 value 'secp224r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.319.1 Value definition

```
secp224r1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 33 }  -- raw value is 1.3.132.0.33
```

### 3.319.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 21
```

## 3.320 ASN.1 value 'secp256r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.320.1 Value definition

```
secp256r1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-
62(10045) curves(3) prime(1) 7 }  -- raw value is 1.2.840.10045.3.1.7
```

### 3.320.2 Value DER encoding

```
DER encoding size: 10 bytes

  06 08 2A 86 48 CE 3D 03 01 07
```

## 3.321 ASN.1 value 'secp384r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.321.1 Value definition

```
secp384r1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 34 }  -- raw value is 1.3.132.0.34
```

### 3.321.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 22
```

## 3.322 ASN.1 value 'secp521r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.322.1 Value definition

```
secp521r1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 35 }  -- raw value is 1.3.132.0.35
```

### 3.322.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 23
```

## 3.323 ASN.1 value 'sect163k1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.323.1 Value definition

```
sect163k1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 1 }  -- raw value is 1.3.132.0.1
```

### 3.323.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 01
```

## 3.324 ASN.1 value 'sect163r2'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.324.1 Value definition

```
sect163r2 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 15 }  -- raw value is 1.3.132.0.15
```

### 3.324.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 0F
```

## 3.325 ASN.1 value 'sect233k1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.325.1 Value definition

```
sect233k1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 26 }  -- raw value is 1.3.132.0.26
```

### 3.325.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 1A
```

## 3.326 ASN.1 value 'sect233r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.326.1 Value definition

```
sect233r1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 27 }  -- raw value is 1.3.132.0.27
```

### 3.326.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 1B
```

## 3.327 ASN.1 value 'sect283k1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.327.1 Value definition

```
sect283k1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 16 }  -- raw value is 1.3.132.0.16
```

### 3.327.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 10
```

# 3.328 ASN.1 value 'sect283r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.328.1 Value definition

```
sect283r1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 17 }  -- raw value is 1.3.132.0.17
```

## 3.328.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 11
```

# 3.329 ASN.1 value 'sect409k1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.329.1 Value definition

```
sect409k1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 36 }  -- raw value is 1.3.132.0.36
```

## 3.329.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 24
```

# 3.330 ASN.1 value 'sect409r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.330.1 Value definition

```
sect409r1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 37 }  -- raw value is 1.3.132.0.37
```

## 3.330.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 25
```

## 3.331 ASN.1 value 'sect571k1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.331.1 Value definition

```
sect571k1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 38 }  -- raw value is 1.3.132.0.38
```

### 3.331.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 26
```

## 3.332 ASN.1 value 'sect571r1'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.332.1 Value definition

```
sect571r1 OBJECT IDENTIFIER ::= { iso(1) identified-
organization(3) certicom(132) curve(0) 39 }  -- raw value is 1.3.132.0.39
```

### 3.332.2 Value DER encoding

```
DER encoding size: 7 bytes

  06 05 2B 81 04 00 27
```

## 3.333 ASN.1 value 'sha1Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.333.1 Value definition

```
sha1Identifier AlgorithmIdentifier ::=
{
  algorithm(id-sha1),         -- raw value is 1.3.14.3.2.26
  parameters(nullParameters) -- original ASN.1 ANY type replaced by 'NULL'
}
```

### 3.333.2 Value DER encoding

```
DER encoding size: 11 bytes

  30 09 06 05 2B 0E 03 02 1A 05 00
```

## 3.334 ASN.1 value 'sha1WithRSAEncryption'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.334.1 Value definition

```
sha1WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 5 }  -
- raw value is 1.2.840.113549.1.1.5
```

### 3.334.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 05
```

## 3.335 ASN.1 value 'sha224Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.335.1 Value definition

```
sha224Identifier AlgorithmIdentifier ::=
{
  algorithm(id-sha224),       -- raw value is 2.16.840.1.101.3.4.2.4
  parameters(nullParameters) -- original ASN.1 ANY type replaced by 'NULL'
}
```

### 3.335.2 Value DER encoding

```
DER encoding size: 15 bytes

  30 0D 06 09 60 86 48 01 65 03 04 02 04 05 00
```

## 3.336 ASN.1 value 'sha224WithRSAEncryption'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.336.1 Value definition

```
sha224WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 14 }  -
- raw value is 1.2.840.113549.1.1.14
```

### 3.336.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 0E
```

# 3.337 ASN.1 value 'sha256Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.337.1 Value definition

```
sha256Identifier AlgorithmIdentifier ::=
{
  algorithm(id-sha256),       -- raw value is 2.16.840.1.101.3.4.2.1
  parameters(nullParameters) -- original ASN.1 ANY type replaced by 'NULL'
}
```

## 3.337.2 Value DER encoding

```
DER encoding size: 15 bytes

  30 0D 06 09 60 86 48 01 65 03 04 02 01 05 00
```

# 3.338 ASN.1 value 'sha256WithRSAEncryption'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.338.1 Value definition

```
sha256WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 11 }  -
- raw value is 1.2.840.113549.1.1.11
```

## 3.338.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 0B
```

# 3.339 ASN.1 value 'sha384Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.339.1 Value definition

```
sha384Identifier AlgorithmIdentifier ::=
{
  algorithm(id-sha384),       -- raw value is 2.16.840.1.101.3.4.2.2
  parameters(nullParameters) -- original ASN.1 ANY type replaced by 'NULL'
}
```

## 3.339.2 Value DER encoding

```
DER encoding size: 15 bytes

  30 0D 06 09 60 86 48 01 65 03 04 02 02 05 00
```

# 3.340 ASN.1 value 'sha384WithRSAEncryption'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

## 3.340.1 Value definition

```
sha384WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 12 }  -
- raw value is 1.2.840.113549.1.1.12
```

## 3.340.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 0C
```

## 3.341 ASN.1 value 'sha512Identifier'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.341.1 Value definition

```
sha512Identifier AlgorithmIdentifier ::=
{
  algorithm(id-sha512),       -- raw value is 2.16.840.1.101.3.4.2.3
  parameters(nullParameters) -- original ASN.1 ANY type replaced by 'NULL'
}
```

### 3.341.2 Value DER encoding

```
DER encoding size: 15 bytes

  30 0D 06 09 60 86 48 01 65 03 04 02 03 05 00
```

## 3.342 ASN.1 value 'sha512WithRSAEncryption'

Source of definition: 'PKIX1Algorithms2008 (RFC 5480)'

### 3.342.1 Value definition

```
sha512WithRSAEncryption OBJECT IDENTIFIER ::= { pkcs-1 13 }  -
- raw value is 1.2.840.113549.1.1.13
```

### 3.342.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 01 0D
```

## 3.343 ASN.1 value 'smime'

Source of definition: 'PKCS #9'

### 3.343.1 Value definition

```
smime OBJECT IDENTIFIER ::= { pkcs-9 16 }  -- raw value is 1.2.840.113549.1.9.16
```

### 3.343.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 86 F7 0D 01 09 10
```

## 3.344 ASN.1 value 'street-address'

Source of definition: 'CRL structures'

### 3.344.1 Value definition

```
street-address INTEGER ::= 17
```

### 3.344.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 11
```

## 3.345 ASN.1 value 'teletex-common-name'

Source of definition: 'CRL structures'

### 3.345.1 Value definition

```
teletex-common-name INTEGER ::= 2
```

### 3.345.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 02
```

## 3.346 ASN.1 value 'teletex-domain-defined-attributes'

Source of definition: 'CRL structures'

### 3.346.1 Value definition

```
teletex-domain-defined-attributes INTEGER ::= 6
```

### 3.346.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 06
```

## 3.347 ASN.1 value 'teletex-organization-name'

Source of definition: 'CRL structures'

### 3.347.1 Value definition

```
teletex-organization-name INTEGER ::= 3
```

### 3.347.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 03
```

## 3.348 ASN.1 value 'teletex-organizational-unit-names'

Source of definition: 'CRL structures'

### 3.348.1 Value definition

```
teletex-organizational-unit-names INTEGER ::= 5
```

### 3.348.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 05
```

## 3.349 ASN.1 value 'teletex-personal-name'

Source of definition: 'CRL structures'

### 3.349.1 Value definition

```
teletex-personal-name INTEGER ::= 4
```

### 3.349.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 04
```

## 3.350 ASN.1 value 'terminal-type'

Source of definition: 'CRL structures'

### 3.350.1 Value definition

```
terminal-type INTEGER ::= 23
```

### 3.350.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 17
```

## 3.351 ASN.1 value 'three'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.351.1 Value definition

```
three INTEGER ::= 3
```

### 3.351.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 03
```

## 3.352 ASN.1 value 'tpBasis'

Source of definition: 'PKIX1Algortihms88 (RFC 3279)'

### 3.352.1 Value definition

```
tpBasis OBJECT IDENTIFIER ::= { id-characteristic-two-basis 2 }  -
- raw value is 1.2.840.10045.1.2.3.2
```

### 3.352.2 Value DER encoding

```
DER encoding size: 11 bytes

  06 09 2A 86 48 CE 3D 01 02 03 02
```

## 3.353 ASN.1 value 'ub-common-name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.353.1 Value definition

```
ub-common-name INTEGER ::= 64
```

### 3.353.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 40
```

## 3.354 ASN.1 value 'ub-common-name-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.354.1 Value definition

```
ub-common-name-length INTEGER ::= 64
```

### 3.354.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 40
```

## 3.355 ASN.1 value 'ub-country-name-alpha-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.355.1 Value definition

```
ub-country-name-alpha-length INTEGER ::= 2
```

### 3.355.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 02
```

## 3.356 ASN.1 value 'ub-country-name-numeric-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.356.1 Value definition

```
ub-country-name-numeric-length INTEGER ::= 3
```

### 3.356.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 03
```

## 3.357 ASN.1 value 'ub-domain-defined-attribute-type-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.357.1 Value definition

```
ub-domain-defined-attribute-type-length INTEGER ::= 8
```

### 3.357.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 08
```

## 3.358 ASN.1 value 'ub-domain-defined-attribute-value-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.358.1 Value definition

```
ub-domain-defined-attribute-value-length INTEGER ::= 128
```

### 3.358.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 80
```

## 3.359 ASN.1 value 'ub-domain-defined-attributes'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.359.1 Value definition

```
ub-domain-defined-attributes INTEGER ::= 4
```

### 3.359.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 04
```

## 3.360 ASN.1 value 'ub-domain-name-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.360.1 Value definition

```
ub-domain-name-length INTEGER ::= 16
```

### 3.360.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 10
```

## 3.361 ASN.1 value 'ub-e163-4-number-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.361.1 Value definition

```
ub-e163-4-number-length INTEGER ::= 15
```

### 3.361.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 0F
```

## 3.362 ASN.1 value 'ub-e163-4-sub-address-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.362.1 Value definition

```
ub-e163-4-sub-address-length INTEGER ::= 40
```

### 3.362.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 28
```

## 3.363 ASN.1 value 'ub-emailaddress-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.363.1 Value definition

```
ub-emailaddress-length INTEGER ::= 255
```

### 3.363.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 FF
```

## 3.364 ASN.1 value 'ub-extension-attributes'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.364.1 Value definition

```
ub-extension-attributes INTEGER ::= 256
```

### 3.364.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 01 00
```

## 3.365 ASN.1 value 'ub-generation-qualifier-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.365.1 Value definition

```
ub-generation-qualifier-length INTEGER ::= 3
```

### 3.365.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 03
```

## 3.366 ASN.1 value 'ub-given-name-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.366.1 Value definition

```
ub-given-name-length INTEGER ::= 16
```

### 3.366.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 10
```

## 3.367 ASN.1 value 'ub-initials-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.367.1 Value definition

```
ub-initials-length INTEGER ::= 5
```

### 3.367.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 05
```

## 3.368 ASN.1 value 'ub-integer-options'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.368.1 Value definition

```
ub-integer-options INTEGER ::= 256
```

### 3.368.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 01 00
```

## 3.369 ASN.1 value 'ub-locality-name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.369.1 Value definition

```
ub-locality-name INTEGER ::= 128
```

### 3.369.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 80
```

## 3.370 ASN.1 value 'ub-match'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.370.1 Value definition

```
ub-match INTEGER ::= 128
```

### 3.370.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 80
```

## 3.371 ASN.1 value 'ub-name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.371.1 Value definition

```
ub-name INTEGER ::= 32768
```

### 3.371.2 Value DER encoding

```
DER encoding size: 5 bytes

  02 03 00 80 00
```

## 3.372 ASN.1 value 'ub-numeric-user-id-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.372.1 Value definition

```
ub-numeric-user-id-length INTEGER ::= 32
```

### 3.372.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 20
```

## 3.373 ASN.1 value 'ub-organization-name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.373.1 Value definition

```
ub-organization-name INTEGER ::= 64
```

### 3.373.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 40
```

## 3.374 ASN.1 value 'ub-organization-name-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.374.1 Value definition

```
ub-organization-name-length INTEGER ::= 64
```

### 3.374.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 40
```

## 3.375 ASN.1 value 'ub-organizational-unit-name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.375.1 Value definition

```
ub-organizational-unit-name INTEGER ::= 64
```

### 3.375.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 40
```

## 3.376 ASN.1 value 'ub-organizational-unit-name-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.376.1 Value definition

```
ub-organizational-unit-name-length INTEGER ::= 32
```

### 3.376.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 20
```

## 3.377 ASN.1 value 'ub-organizational-units'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.377.1 Value definition

```
ub-organizational-units INTEGER ::= 4
```

### 3.377.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 04
```

## 3.378 ASN.1 value 'ub-pds-name-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.378.1 Value definition

```
ub-pds-name-length INTEGER ::= 16
```

### 3.378.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 10
```

## 3.379 ASN.1 value 'ub-pds-parameter-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.379.1 Value definition

```
ub-pds-parameter-length INTEGER ::= 30
```

### 3.379.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 1E
```

## 3.380 ASN.1 value 'ub-pds-physical-address-lines'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.380.1 Value definition

```
ub-pds-physical-address-lines INTEGER ::= 6
```

### 3.380.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 06
```

## 3.381 ASN.1 value 'ub-postal-code-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.381.1 Value definition

```
ub-postal-code-length INTEGER ::= 16
```

### 3.381.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 10
```

## 3.382 ASN.1 value 'ub-pseudonym'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.382.1 Value definition

```
ub-pseudonym INTEGER ::= 128
```

### 3.382.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 80
```

## 3.383 ASN.1 value 'ub-serial-number'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.383.1 Value definition

```
ub-serial-number INTEGER ::= 64
```

### 3.383.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 40
```

## 3.384 ASN.1 value 'ub-state-name'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.384.1 Value definition

```
ub-state-name INTEGER ::= 128
```

### 3.384.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 80
```

## 3.385 ASN.1 value 'ub-surname-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.385.1 Value definition

```
ub-surname-length INTEGER ::= 40
```

### 3.385.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 28
```

## 3.386 ASN.1 value 'ub-terminal-id-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.386.1 Value definition

```
ub-terminal-id-length INTEGER ::= 24
```

### 3.386.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 18
```

## 3.387 ASN.1 value 'ub-title'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.387.1 Value definition

```
ub-title INTEGER ::= 64
```

### 3.387.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 40
```

## 3.388 ASN.1 value 'ub-unformatted-address-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.388.1 Value definition

```
ub-unformatted-address-length INTEGER ::= 180
```

### 3.388.2 Value DER encoding

```
DER encoding size: 4 bytes

  02 02 00 B4
```

## 3.389 ASN.1 value 'ub-x121-address-length'

Source of definition: 'PKIX1Explicit88 (RFC 5280)'

### 3.389.1 Value definition

```
ub-x121-address-length INTEGER ::= 16
```

### 3.389.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 10
```

## 3.390 ASN.1 value 'unformatted-postal-address'

Source of definition: 'CRL structures'

### 3.390.1 Value definition

```
unformatted-postal-address INTEGER ::= 16
```

### 3.390.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 10
```

## 3.391 ASN.1 value 'unique-postal-name'

Source of definition: 'CRL structures'

### 3.391.1 Value definition

```
unique-postal-name INTEGER ::= 20
```

### 3.391.2 Value DER encoding

```
DER encoding size: 3 bytes

  02 01 14
```

# 3.392 ASN.1 value 'x509Certificate'

Source of definition: 'PKCS #12'

## 3.392.1 Value definition

```
x509Certificate OBJECT IDENTIFIER ::= { certTypes 1 }  -
- raw value is 1.2.840.113549.1.9.22.1
```

## 3.392.2 Value DER encoding

```
DER encoding size: 12 bytes

  06 0A 2A 86 48 86 F7 0D 01 09 16 01
```

# A Appendix

## A.1 <TODO>

The document in-hand does not have an appendix yet.

### A.1.1 <TODO>