其中，anyExtendedKeyUsage 表示所有用途。id-kp-serverAuth 表示 Web 服务器 SSL/TLS 身份认证，等同于 keyUsage 中的 digitalSignature、keyEncipherment、keyAgreement。id-kp-clientAuth 表示 Web 客户端 SSL/TLS 身份认证，等同于 keyUsage 中的 digitalSignature、keyAgreement。id-kp-codeSigning 表示可执行程序的代码签名，等同于 keyUsage 中的 digitalSignature。id-kp-emailProtection 表示电子邮件保护，等同于 keyUsage 中的 digitalSignature、nonRepudiation、keyEncipherment 或 keyAgreement。id-kp-timeStamping 表示时间戳，即将某对象摘要值与时间绑定，等同于 keyUsage 中的 digitalSignature、nonRepudiation。id-kp-OCSPSigning 表示 OCSP 响应包签名，等同于 keyUsage 中的 digitalSignature、nonRepudiation。

### 14．cRLDistributionPoints

cRLDistributionPoints 扩展项用于确定如何获得 CRL 信息。

该扩展项应该设置为非关键项（critical=FALSE）。

cRLDistributionPoints 格式用 ASN.1 描述如下：

```
id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::=  { id-ce 31 }
cRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint
DistributionPoint ::= SEQUENCE {
    distributionPoint       [0]     DistributionPointName OPTIONAL,
    reasons                 [1]     ReasonFlags OPTIONAL,
    cRLIssuer               [2]     GeneralNames OPTIONAL }
DistributionPointName ::= CHOICE {
    fullName                [0]     GeneralNames,
    nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }
ReasonFlags ::= BIT STRING {
    unused                  (0),
    keyCompromise           (1),    --表示密钥泄露
    cACompromise            (2),    --表示 CA 泄露
    affiliationChanged      (3),    --表示关系变更
    superseded              (4),    --表示废弃
    cessationOfOperation    (5),    --表示操作中止
    certificateHold         (6),    --表示证书冻结
    privilegeWithdrawn      (7),    --表示权限撤销
    aACompromise            (8) }   --表示 AA 泄露
```

其中，DistributionPoint 类型不能只包含 reasons 字段，distributionPoint 和 cRLIssuer 字段至少包含一个。如果证书签发者不是 CRL 签发者，则 cRLIssuer 字段必须存在，且必须包含 CRL 签发者的 DN 名称。如果证书签发者也是 CRL 签发者，则 cRLIssuer 字段必须忽略，distributionPoint 字段必须存在。

distributionPoint 定义为 DistributionPointName 类型。如果 distributionPoint 包含多个名称值（GeneralNames），则每个名称表示一种方法或机制，不同方法或机制能获取相同的 CRL，如 LDAP 和 HTTP。如果 distributionPoint 只包含单个值（nameRelativeToCRLIssuer），

则表示 DN 项的一部分；只需将其附加到 CRL 签发者或证书签发者的 X.500 DN 名称后即可获得 CRL 发布点名称；如果 DistributionPoint 中的 cRLIssuer 存在，则使用 CRL 签发者 cRLIssuer，否则使用证书签发者。

### 15. inhibitAnyPolicy

inhibitAnyPolicy 扩展项只用于 CA 证书，用于表示认证路径中哪些证书允许 anyPolicy 策略（OID 为 2.5.29.32.0）。

该扩展项应该设置为关键项（critical=TRUE）。

inhibitAnyPolicy 格式用 ASN.1 描述如下：

```
id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::=  { id-ce 54 }
inhibitAnyPolicy ::= SkipCerts
SkipCerts ::= INTEGER (0..MAX)
```

其中，SkipCerts 表示认证路径中该证书后面允许 anyPolicy 策略的证书数目，也就是说，认证路径中从该证书后的第 SkipCerts+1 个证书开始不再允许 anyPolicy 策略。例如，SkipCerts 为 1 表示认证路径中该证书签发的下级证书允许 anyPolicy 策略，但其他后续证书不允许 anyPolicy 策略。

### 16. freshestCRL（Delta CRL Distribution Point）

freshestCRL 扩展项用于确定如何获取增量 CRL 信息。该扩展项格式与 cRLDistributionPoints 扩展项完全一致。

该扩展项应该设置为非关键项（critical=FALSE）。

freshestCRL 格式用 ASN.1 描述如下：

```
id-ce-freshestCRL OBJECT IDENTIFIER ::=  { id-ce 46 }
FreshestCRL ::= CRLDistributionPoints
```

### 17. netscapeCertType

netscapeCertType 扩展项表示 Netscape 证书类型，用于定义证书中公钥及其对应私钥的一个或多个用途，与 extendedKeyUsage 扩展项的功能类似。

该扩展项必须设置为非关键项（critical=FALSE）。

netscapeCertType 格式用 ASN.1 描述如下：

```
id-NetscapeCertType OBJECT IDENTIFIER ::= { 2.16.840.1.113730.1.1 }
netscapeCertType ::= BIT STRING {
        SSLClient               (0),
        SSLServer               (1),
        S/MIME                  (2),
        Object Signing          (3),
        Reserved                (4),
        SSL CA                  (5),
        S/MIME CA               (6),
        Object Signing CA       (7) }
```

### 9.2.2　专用互联网扩展项

X.509 数字证书的专用互联网扩展项（Private Internet Extensions）见表 9-5。

表 9-5　X.509 数字证书专用互联网扩展项

| / | 扩　展　项 | OID | critical | 说　　明 |
|---|---|---|---|---|
| 1 | AuthorityInfoAccess | id-pe 1 | FALSE | 证书签发者信息访问 |
| 2 | SubjectInfoAccess | id-pe 11 | FALSE | 证书持有者信息访问 |

注：id-pe OBJECT IDENTIFIER ::= { id-pkix 1 }

#### 1．authorityInfoAccess

authorityInfoAccess 扩展项用于确定如何访问证书签发者（CA）的信息和服务，如在线验证服务、CA 策略数据（不包含 CRL 访问地址，对于 CRL 访问地址应使用 cRLDistributionPoints 扩展项）等。

该扩展项可以用于 CA 证书，也可以用于终端实体（End Entity）证书，但必须设置为非关键项（critical=FALSE）。

authorityInfoAccess 格式用 ASN.1 描述如下：

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }
authorityInfoAccessSyntax::= SEQUENCE SIZE (1..MAX) OF AccessDescription
AccessDescription   ::=   SEQUENCE {
    accessMethod            OBJECT IDENTIFIER,
    accessLocation          GeneralName   }
```

其中，accessMethod 字段表示信息格式和类型，accessLocation 字段表示信息地址。访问机制或方式可由 accessMethod 确定，也可由 accessLocation 确定。

常用的 accessMethod 用 ASN.1 描述如下：

```
id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }
id-ad-caIssuers OBJECT IDENTIFIER ::= { id-ad 2 }
id-ad-ocsp OBJECT IDENTIFIER ::= { id-ad 1 }
```

当 accessMethod 为 id-ad-ocsp 时，accessLocation 表示 OCSP 服务器地址，通过 OCSP 服务可获得当前证书的作废状态。

当 accessMethod 为 id-ad-caIssuers 时，accessLocation 表示服务器地址和访问协议，可获得参考描述（referenced description）信息。accessLocation 定义为 GeneralName 类型，可以采用多种形式。当通过 http、ftp 或 ldap 方式访问信息时，accessLocation 必须为 URI。当通过 DAP（Directory Access Protocol）方式访问信息时，accessLocation 必须为目录名称 directoryName，且该目录名称入口应在 crossCertificatePair 属性中包含 CA 证书。当通过 email 方式访问信息时，accessLocation 必须为 rfc822Name。

#### 2．subjectInfoAccess

subjectInfoAccess 扩展项用于确定如何访问证书持有者的信息和服务。如果证书持有

者 subject 是 CA，信息和服务包括证书验证服务、CA 策略数据等；如果证书持有者是终端实体（End Entity），则描述服务类型和访问方法。

该扩展项可以用于 CA 证书，也可以用于终端实体证书，但必须设置为非关键项（critical=FALSE）。

subjectInfoAccess 格式用 ASN.1 描述如下：

```
id-pe-subjectInfoAccess OBJECT IDENTIFIER ::= { id-pe 11 }
subjectInfoAccessSyntax ::= SEQUENCE SIZE (1..MAX) OF AccessDescription
AccessDescription  ::=  SEQUENCE {
    accessMethod          OBJECT IDENTIFIER,
    accessLocation        GeneralName  }
```

其中，accessMethod 字段表示信息格式和类型，accessLocation 字段表示信息地址。访问机制或方式可由 accessMethod 确定，也可由 accessLocation 确定。

常用的 accessMethod 用 ASN.1 描述如下：

```
id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }
id-ad-caRepository OBJECT IDENTIFIER ::= { id-ad 5 }
id-ad-timeStamping OBJECT IDENTIFIER ::= { id-ad 3 }
```

当证书持有者 subject 是 CA 时，accessMethod 可以使用 id-ad-caRepository，表示该 CA 通过 repository 发布其签发的证书和 CRL。accessLocation 定义为 GeneralName 类型，可以采用多种形式。当通过 http、ftp 或 ldap 方式访问信息时，accessLocation 必须为 URI；当通过 DAP（Directory Access Protocol）方式访问信息时，accessLocation 必须为目录名称 directoryName；当通过 email 方式访问信息时，accessLocation 必须为 rfc822Name。

当证书持有者采用 TSP 协议提供时间戳服务时，accessMethod 可以使用 id-ad-timeStamping。当通过 http、ftp 或 ldap 方式访问时间戳服务时，accessLocation 必须为 URI。当通过 email 方式访问时间戳服务时，accessLocation 必须为 rfc822Name。当通过 TCP/IP 方式访问时间戳服务时，accessLocation 可以采用域名或 IP 地址。

## 9.3 国内扩展项

### 9.3.1 卫生系统专用扩展项

《卫生系统数字证书格式规范》规定了卫生系统数字证书的专用扩展项，见表 9-6。

表 9-6 卫生系统数字证书专用扩展项

| / | 扩 展 项 | OID | critical | 说 明 |
|---|---|---|---|---|
| 1 | SubjectUniqueID | 自行定义 | FALSE | 证书持有者唯一标识 |

#### 1. subjectUniqueID

subjectUniqueID 扩展项代表一个证书持有者身份的唯一编码（实体唯一标识），在业务系统中，本标识可与应用系统内的用户账号一一关联，从而用于实现证书用户与系统用

户的绑定。该扩展项 OID 由各电子认证服务机构自行申请和定义。

对于终端实体证书，该扩展项必须签发，该项应为非关键扩展项。

subjectUniqueID 的编码规范如下：

用户编号（变长）+“@”+CA 编号（4 位）+证件类型代码（2 位）+安全标识（1 位）+证件号码（变长）

其中，用户编号是一个证书持有者的证书序号，建议用户编号采用阿拉伯数字。例如一个企业申请 2 个证书，则第一张证书的用户编号为 1，第 2 张证书的用户编号为 2，依次类推。

CA 编号应为 CA 机构的《电子认证服务许可证》上“许可证编号”的后四位数字。

证件类型代码是证书用户申请数字证书使用的关键证件的编码，证书类型和号码类型的代码如表 9-7 所示。

表 9-7　证书类型与证件类型代码对应表

| 证 书 类 型 | 办理证书时可使用的证件名称 | 证件类型代码 |
|---|---|---|
| 内部机构证书 | 组织机构代码/工商营业执照/税务登记证/其他 | JJ/GS/SW/QT |
| 内部工作人员证书 | 身份证/军官证/护照/回乡证/其他 | SF/JG/HZ/HX/QT |
| 内部设备证书 | 组织机构代码/工商营业执照/税务登记证/其他 | JJ/GS/SW/QT |
| 外部机构证书 | 组织机构代码/工商营业执照/税务登记证/其他 | JJ/GS/SW/QT |
| 个人证书 | 身份证/军官证/护照/回乡证/其他 | SF/JG/HZ/HX/QT |
| 外部设备证书 | 组织机构代码/工商营业执照/税务登记证/其他 | JJ/GS/SW/QT |

安全标识使用 1 位数字代表不同含义，其意义如下：

0：代表其后的“证件号码”为明文格式签发；

1：代表其后的“证件号码”为 Base64 编码格式签发；

用户根据不同的证书类型，应提供不同的证件办理数字证书。

例如，个人证书办理时提供的证件为身份证，身份证号码为：342222197205053618，CA 机构编号为 1001，该 CA 中心为用户签发的第一张数字证书的实体唯一标识应为：

① 安全标识为 0 时的值应为：1@1001SF0342222197205053618

② 安全标识为 1 时的值应为：1@1001SF1MzQyMjIyMTk3MjA1MDUzNjE4，其中 SF1 后面的内容为 Base64(342222197205053618)的结果。

对于机构证书，如果提供组织机构代码证件号码为：123456789，CA 机构编号为 1001，该 CA 中心为用户签发的第一张数字证书的实体唯一标识应为：

① 安全标识为 0 时的值应为：1@1001JJ0123456789

② 安全标识为 1 时的值应为：1@1001JJ1MTIzNDU2Nzg5，其中 JJ1 后面的内容为 Base64(123456789)结果。

实体唯一标识数据总长度不应超过 128 字节，属性编码应使用 UTF8String。

### 9.3.2　国内通用扩展项

《基于 SM2 密码算法的数字证书格式规范》规定了数字证书的国内通用扩展项，见表 9-8。