```
id-ce-certificatePolicies OBJECT IDENTIFIER ::=    { id-ce 32 }
anyPolicy OBJECT IDENTIFIER ::= { id-ce-certificate-policies 0 }
certificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation
PolicyInformation ::= SEQUENCE {
     policyIdentifier     CertPolicyId,
     policyQualifiers     SEQUENCE SIZE (1..MAX) OF
                PolicyQualifierInfo OPTIONAL }
CertPolicyId ::= OBJECT IDENTIFIER
PolicyQualifierInfo ::= SEQUENCE {
     policyQualifierId    PolicyQualifierId,
     qualifier            ANY DEFINED BY policyQualifierId }
id-qt            OBJECT IDENTIFIER ::=    { id-pkix 2 }
id-qt-cps        OBJECT IDENTIFIER ::=    { id-qt 1 }
id-qt-unotice    OBJECT IDENTIFIER ::=    { id-qt 2 }
PolicyQualifierId ::= OBJECT IDENTIFIER ( id-qt-cps | id-qt-unotice )
Qualifier ::= CHOICE {
     cPSuri               CPSuri,
     userNotice           UserNotice }
CPSuri ::= IA5String
UserNotice ::= SEQUENCE {
     noticeRef            NoticeReference OPTIONAL,
     explicitText         DisplayText OPTIONAL}
NoticeReference ::= SEQUENCE {
     organization         DisplayText,
     noticeNumbers        SEQUENCE OF INTEGER }
DisplayText ::= CHOICE {
     ia5String            IA5String          (SIZE (1..200)),
     visibleString        VisibleString    (SIZE (1..200)),
     bmpString            BMPString          (SIZE (1..200)),
     utf8String           UTF8String         (SIZE (1..200)) }
```

其中，策略限定语类型（qualifier type）主要包括 2 类：CPS Pointer 和 User Notice。

CPS Pointer 表示 CPS 指针，包含一个 URL，可链接到 CA 中心发布的 CPS（Certification Practice Statement）。

User Notice 表示用户通知内容，应用系统应显示给用户阅读，可由 2 个可选字段组成：noticeRef 和 explicitText。noticeRef 包含组织名称和通知编号，应用系统可据此获得通知内容（例如，以文件形式保存所有通知，通过编号查找文件并获得通知内容），并显示给用户阅读。explicitText 包含文本内容，最大长度不应超过 200 字符。当 noticeRef 和 explicitText 同时存在时，应优先使用 noticeRef；如无法通过 noticeRef 获得通知内容，则使用 explicitText。

6. policyMappings

policyMappings 扩展项只用于 CA 证书，可包含多对 OID，每对 OID 由 issuerDomainPolicy

和 subjectDomainPolicy 组成，表示 issuer 域的证书策略 issuerDomainPolicy 等同于 subject 域的证书策略 subjectDomainPolicy。该扩展项中不允许包含证书策略 anyPolicy。

该扩展项必须设置为非关键项（critical=FALSE）。

policyMappings 格式用 ASN.1 描述如下：

```
id-ce-policyMappings OBJECT IDENTIFIER ::=  { id-ce 33 }
PolicyMappings ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
    issuerDomainPolicy      CertPolicyId,
    subjectDomainPolicy     CertPolicyId }
```

7．subjectAltName

subjectAltName 扩展项表示证书持有者的别名，可包含多个。别名形式包括电子邮箱、DNS 名称、IP 地址、URI 等，其中 DNS 名称也可以使用 subject 中的 DN 项 domainComponent 表示。

当 subject 为空时，该扩展项必须设置为关键项（critical=TRUE）。

subjectAltName 格式用 ASN.1 描述如下：

```
id-ce-subjectAltName OBJECT IDENTIFIER ::=  { id-ce 17 }
subjectAltName ::= GeneralNames
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
GeneralName ::= CHOICE {
    otherName                   [0]     OtherName,
    rfc822Name                  [1]     IA5String,
    dNSName                     [2]     IA5String,
    x400Address                 [3]     ORAddress,
    directoryName               [4]     Name,
    ediPartyName                [5]     EDIPartyName,
    uniformResourceIdentifier   [6]     IA5String,
    iPAddress                   [7]     OCTET STRING,
    registeredID                [8]     OBJECT IDENTIFIER }
OtherName ::= SEQUENCE {
    type-id     OBJECT IDENTIFIER,
    value       [0] EXPLICIT ANY DEFINED BY type-id }
EDIPartyName ::= SEQUENCE {
    nameAssigner            [0]     DirectoryString OPTIONAL,
    partyName               [1]     DirectoryString }
```

当 subjectAltName 包含电子邮箱时，格式必须符合 rfc822Name 类型（RFC 822 规范）。

当 subjectAltName 包含 IP 地址时，格式必须采用网络字节序和 LSB（least significant bit）方式，且 IP 地址字节与 ASN.1 编码后的 OCTET 一一对应。对于 IPv4（RFC 791 规范），必须包含 4 个字节；对于 IPv6（RFC 1883 规范），必须包含 16 个字节。

当 subjectAltName 包含 DNS 名称时，格式必须符合 dNSName 类型（RFC 1034 规范）。

当 subjectAltName 包含 URI 地址时，格式必须符合 uniformResourceIdentifier 类型（RFC

1738 规范），不允许使用相对地址，只能使用绝对地址。在 URI 地址中，只有模式名（scheme name，如 http）和主机名（hostname，如 www.sina.com）大小写无关，其他组成部分均大小写相关。

当 subjectAltName 包含 DN 项时，格式必须符合 directoryName 类型，且同一证书持有者必须具有唯一性。

8. issuerAltName

issuerAltName 扩展项表示证书签发者的别名，可包含多个。具体要求同 subjectAltName。该扩展项必须设置为非关键项（critical=FALSE）。

issuerAltName 格式用 ASN.1 描述如下：

```
id-ce-issuerAltName OBJECT IDENTIFIER ::=  { id-ce 18 }
issuerAltName ::= GeneralNames
```

9. subjectDirectoryAttributes

subjectDirectoryAttributes 扩展项可包含证书持有者的目录属性。

该扩展项必须设置为非关键项（critical=FALSE）。

subjectDirectoryAttributes 格式用 ASN.1 描述如下：

```
id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::=  { id-ce 9 }
subjectDirectoryAttributes ::= SEQUENCE SIZE (1..MAX) OF Attribute
```

10. basicConstraints

basicContraints 扩展项用于区分证书持有者是否是 CA。如果是 CA，则限制其认证路径的最大长度。

当用于终端实体证书时，该扩展项可以设置为关键项或非关键项。当用于签发用户证书的 CA 证书时，该扩展项必须设置为关键项（critical=TRUE）。当 CA 证书不用于签发用户证书，只用于签发 CRL 时，该扩展项可以设置为关键项或非关键项。

basicContraints 格式用 ASN.1 描述如下：

```
id-ce-basicConstraints OBJECT IDENTIFIER ::=  { id-ce 19 }
basicConstraints ::= SEQUENCE {
    cA                      BOOLEAN DEFAULT FALSE,
    pathLenConstraint       INTEGER (0..MAX) OPTIONAL }
```

其中，cA 表示该证书是否是 CA。如果 cA 设置为 FALSE，则 keyUsage 扩展项不能包含 keyCertSign。

仅当 cA 设置为 TRUE，且 keyUsage 扩展项包含 keyCertSign 时，pathLenConstraint 才有效，表示该 CA 证书之后认证路径中非自签名 CA 证书的最大数目（即认证路径或信任链中，该 CA 证书和终端实体证书之间的非自签名证书的最大数目）。pathLenConstraint 出现时必须大于或等于 0，当等于 0 时表示该 CA 证书不能签发下级 CA 证书，只能签发终端实体（End Entity）证书；如果 pathLenConstraint 没有出现，表明认证路径的长度没有限制。

11．nameConstraints

nameContraints 扩展项只用于 CA 证书，包含一个命名空间，用于限制认证路径中后续证书中的 subject 内容和 subjectAltName 扩展项。

该扩展项必须设置为关键项（critical=TRUE）。

nameContraints 格式用 ASN.1 描述如下：

```
id-ce-nameConstraints OBJECT IDENTIFIER ::=    { id-ce 30 }
nameConstraints ::= SEQUENCE {
    permittedSubtrees          [0]      GeneralSubtrees OPTIONAL,
    excludedSubtrees           [1]      GeneralSubtrees OPTIONAL }
GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree
GeneralSubtree ::= SEQUENCE {
    base                              GeneralName,
    minimum              [0]      BaseDistance DEFAULT 0,
    maximum              [1]      BaseDistance OPTIONAL }
BaseDistance ::= INTEGER (0..MAX)
```

其中，permittedSubtrees 表示允许的名称范围，excludedSubtrees 表示无效的名称范围。permittedSubtrees 和 excludedSubtrees 可包含一个或多个命名子树；每个命名子树定义为 GeneralName 类型，可以采用多种形式，如 URI、电子邮箱、DNS、IP 地址等。

如果采用 URI 形式，该扩展项只用于限制名称的主机部分，可以设定一个主机或域名。如果该扩展项以“.”开始，则表示该域名可以扩展子域；如 abc.xyz.com 和 abc.def.xyz.com 都属于“.xyz.com”扩展，但 xyz.com 不属于“.xyz.com”扩展。如果该扩展项不以“.”开始，则表示特定主机，不允许任何扩展，如 foo.bar.com 就不能扩展。

如果采用电子邮箱形式，该扩展项可以设定一个特定邮箱、一个特定主机的所有邮箱或一个域名范围的所有邮箱。若需设定一个特定邮箱，则直接使用完整的电子邮箱地址，如 root@xyz.com。若需设定一个特定主机的所有邮箱，则应使用主机名，如 xyz.com 表示主机 xyz.com 上的所有邮箱地址。如需设定一个域名范围的所有邮箱，应使用以“.”开始的域名，如.xyz.com 表示 xyz.com 域范围内的所有邮箱地址，但不包括主机 xyz.com 上的邮箱地址。

如果采用 DNS 形式，该扩展项可直接使用域名，如 foo.bar.com；该域名扩展后的任何新域名均满足要求。如 www.foo.bar.com 是 foo.bar.com 的扩展，但 foo1.bar.com 就不是。

如果采用 IP 地址形式，该扩展项必须使用 CIDR 格式（即“地址+掩码”，RFC 1519 规范），用于表示 IP 地址范围。对于 IPv4 地址，应编码成 8 个 OCTET；如 C 类地址 10.9.8.0，CIDR 表示为 10.9.8.0/255.255.255.0，编码后为 0A 09 08 00 FF FF FF 00。对于 IPv6，应编码成 32 个 OCTET。

12．policyConstraints

policyContraints 扩展项只用于 CA 证书，用于禁止策略映射，或用于要求认证路径中所有证书必须包含一个认可的策略 ID（policy identifier）。

该扩展项可以设置为关键项或非关键项。

policyContraints 格式用 ASN.1 描述如下：

```
id-ce-policyConstraints OBJECT IDENTIFIER ::=  { id-ce 36 }
policyConstraints ::= SEQUENCE {
    requireExplicitPolicy            [0] SkipCerts OPTIONAL,
    inhibitPolicyMapping              [1] SkipCerts OPTIONAL }
SkipCerts ::= INTEGER (0..MAX)
```

其中，如果 inhibitPolicyMapping 存在，其值 *n* 表示认证路径中该证书后面允许策略映射的证书数目，也就是说，认证路径中从该证书后的第 *n*+1 个证书开始不再允许策略映射。例如，inhibitPolicyMapping 为 1 表示认证路径中，该证书签发的下级证书允许策略映射，但其他后续证书不允许策略映射。

如果 requireExplicitPolicy 存在，其值 *m* 表示认证路径中该证书后面不需要显性策略（explicit policy）的证书数目，也就是说，认证路径中从该证书后的第 *m*+1 个证书开始需要显性策略。当需要一个显性策略时，应在 certificatePolicis 扩展项中包含一个认可的策略 ID。

13. extendedKeyUsage

extendedKeyUsage 扩展项用于表示证书中公钥及其对应私钥的一个或多个用途，是 keyUsage 扩展项中基本用途的替代或补充。通常，该扩展项只用于终端实体（end entity）证书。

该扩展项可以设置为关键项或非关键项，由证书签发者决定。当设置为 anyExtendedKeyUsage 时，该扩展项应该设置为非关键项（critical=FALSE）。

extendedKeyUsage 格式用 ASN.1 描述如下：

```
id-ce-extKeyUsage OBJECT IDENTIFIER ::= { id-ce 37 }
ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId
KeyPurposeId ::= OBJECT IDENTIFIER
```

当 keyUsage 和 extendedKeyUsage 同时存在时，必须分别进行处理，该证书只能用于 keyUsage 和 extendedKeyUsage 同时允许的用途。如果 keyUsage 和 extendedKeyUsage 所定义的用途完全互斥，没有同时允许的用途，则该证书被认为无效，不能用于任何目的。

常用的扩展密钥用途用 ASN.1 描述如下：

```
anyExtendedKeyUsage OBJECT IDENTIFIER ::= { id-ce-extKeyUsage 0 }
id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }
id-kp-serverAuth              OBJECT IDENTIFIER ::= { id-kp 1 }
id-kp-clientAuth              OBJECT IDENTIFIER ::= { id-kp 2 }
id-kp-codeSigning             OBJECT IDENTIFIER ::= { id-kp 3 }
id-kp-emailProtection         OBJECT IDENTIFIER ::= { id-kp 4 }
id-kp-timeStamping            OBJECT IDENTIFIER ::= { id-kp 8 }
id-kp-OCSPSigning             OBJECT IDENTIFIER ::= { id-kp 9 }
```