（续表）

分　类	OID	说　明
surname	id-at 4	姓
given name	id-at 42	名
initials	id-at 43	首字母缩写
pseudonym	id-at 65	假名
generation qualifier	id-at 44	时代限定符，如老、小、第四代等
email address	pkcs-9 1	电子邮箱

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

pkcs-9 OBJECT IDENTIFIER ::={ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) 9 }

当需要比较两个 issuer 或 subject 是否相同时，应对其包含的所有属性进行比较。针对属性类型相同的属性值，按照以下规则进行比较：

① 采用不同方式编码的属性值代表不同的字符串。如，"Marianne Swanson" 分别采用 PrintableString 和 BMPString 编码后，代表不同的字符串。

② 除 PrintableString 编码方式外，其他编码方式的属性值均大小写相关。可按照二进制对象进行比较。

③ PrintableString 编码方式的属性值大小写无关。如 "Marianne Swanson" 与 "MARIANNE SWANSON"表示相同的字符串。

④ 对于 PrintableString 编码方式的属性值，比较前应删除字符串首尾的所有空格和中间冗余的空格（即将多个连续的空格转换为单个空格）。

5. 证书持有者 subject

subject 用于区分证书持有者。证书持有者的名称或姓名可以包含在 subject 中，也可以包含在 subjectAltName 扩展项中。

subject 格式用 ASN.1 描述与 issuer 相同。

如果证书持有者为 CA 或 CRL 签发者，subject 必须包含一个非空的 DN 项。如果证书持有者名称或姓名只包含在 subjectAltName 扩展项中，subject 必须为一个空的 SEQUENCE，同时 subjectAltName 扩展项必须设置为关键项（critical=TRUE）。当 subject 为非空时，只能包含 X.500 DN 项。同一个 CA 可以为相同的证书持有者签发多个证书，这些证书具有相同的 subject。

subject 包含的主要属性类型与 issuer 相同。此外，subject 还可以包含 EmailAddress 属性。由于 PrintabString 字符集不包括字母“@”，因此 EmailAddress 属性值的编码方式采用 IA5String，包括字母“@”，且 EmailAddress 属性值大小写无关（如 fanfeedback@redsox.com 与 FANFEEDBACK@REDSOX.COM 表示相同的电子邮箱地址）。

6. 证书有效期 validity

validity 用于表示证书有效期，由生效日期和失效日期组成。

validity 格式用 ASN.1 描述如下：

```
Validity ::= SEQUENCE {
```

```
        notBefore       Time,
        notAfter        Time }
Time ::= CHOICE {
        utcTime         UTCTime,
        generalTime     GeneralizedTime }
```

证书有效期可采用两种格式：GeneralizedTime 和 UTCTime。2050 年及之后的日期必须采用 GeneralizedTime 格式，之前的日期可采用 UTCTime 格式。

UTCTime 表示 Universal Time，是一种标准的 ASN.1 时间类型。UTCTime 用 2 位数字表示年份，时间可精确到分或秒。可包含 Z，用于表示 Greenwich Mean Time，也可包含时差。当 validity 中的 notBefore 和 notAfter 采用 UTCTime 格式时，必须采用 Greenwich Mean Time，且必须精确到秒，如 YYMMDDhhmmssZ。当 YY 小于 50 时，年份应该解释为 20YY 年，当 YY 大于或等于 50 时，年份应该解释为 19YY 年。

GeneralizedTime 表示 Generalized Time，也是一种标准的 ASN.1 时间类型。GeneralizedTime 用 4 位数字表示年份。可包含 Z 表示 Greenwich Mean Time，也可包含 Greenwich Mean Time 与本地时间的时差。当 validity 中的 notBefore 和 notAfter 采用 GeneralizedTime 格式时，必须采用 Greenwich Mean Time，且必须精确到秒，如 YYYYMMDDhhmmssZ。

7. 证书持有者公钥 subjectPublicKeyInfo

subjectPublicKeyInfo 表示证书持有者公钥信息。

subjectPublicKeyInfo 格式用 ASN.1 描述如下：

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

8. 证书签发者 ID issuerUniqueID 与证书持有者 ID subjectUniqueID

issuerUniqueID 表示证书签发者的唯一标识，subjectUniqueID 表示证书持有者的唯一标识。

issuerUniqueID 和 subjectUniqueID 格式用 ASN.1 描述如下：

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

issuerUniqueID 和 subjectUniqueID 主要用于兼容 v2 版本证书格式，只能出现在版本 v2 或 v3 格式中，在版本 v1 格式中不允许出现。由于 X.509 数字证书不允许不同的证书持有者使用相同的 DN 项，因此版本 v3 格式中不建议使用 issuerUniqueID 和 subjectUniqueID。

9. 扩展项 extensions

extensions 用于证书信息扩展，可包含多个扩展信息。

extensions 格式用 ASN.1 描述如下：

```
Extension  ::=  SEQUENCE SIZE (1..MAX) OF Extension
Extension  ::=  SEQUENCE  {
    extnID          OBJECT IDENTIFIER,
    critical        BOOLEAN DEFAULT FALSE,
    extnValue       OCTET STRING  }
```

extensions 只能出现在版本 v3 格式中。

每个扩展项都可设置为关键项（critical=TRUE）或非关键项（critical=FALSE）。如果遇到未知的关键扩展项，则必须拒绝该证书；如果遇到未知的非关键扩展项，可以忽略该扩展项。

每个扩展项由一个 OID 和一个 ASN.1 结构组成。OID 赋值给 extnID，ASN.1 编码后的结构赋值给 extnValue。单个证书最多只能包含特定扩展项的单个实例，如最多只能包含一个 AuthorityKeyIdentifier 扩展项。

9.2　标准扩展项

IETF RFC 3280 规定了 X.509 数字证书的标准扩展项和专用互联网扩展项。

9.2.1　标准扩展项（Standard Extensions）

X.509 数字证书的标准扩展项见表 9-4。

表 9-4　X.509 数字证书标准扩展项

/	扩　展　项	OID	critical	说　　明
1	AuthorityKeyIdentifier	id-ce 35	FALSE	证书签发者密钥标识
2	SubjectKeyIdentifier	id-ce 14	TRUE	证书持有者密钥标识
3	KeyUsage	id-ce 15	TRUE	密钥用途
4	PrivateKeyUsagePeriod	id-ce 16	FALSE	私钥有效期
5	CertificatePolicies	id-ce 32		证书策略
6	PolicyMappings	id-ce 33	FALSE	策略映射
7	SubjectAltName	id-ce 17		证书持有者别名
8	IssuerAltName	id-ce 18	FALSE	证书签发者别名
9	SubjectDirectoryAttributes	id-ce 9	FALSE	证书持有者目录属性
10	BasicContraints	id-ce 19		基本限制
11	NameContraints	id-ce 30	TRUE	名称限制
12	PolicyConstraints	id-ce 36		策略限制
13	ExtendedKeyUsage	id-ce 37		扩展密钥用途
14	CRLDistributionPoints	id-ce 31	FALSE	CRL 发布点
15	InhibitAnyPolicy	id-ce 54	TRUE	禁止任意策略
16	FreshestCRL(DeltaCRL DistributionPoint)	id-ce 46	FALSE	最新 CRL 或增量 CRL
17	NetscapeCertType	2.16.840.1. 113730.1.1	FALSE	Netscape 证书类型

注：id-ce OBJECT IDENTIFIER ::=　{ joint-iso-ccitt(2) ds(5) 29 }

id-pkix OBJECT IDENTIFIER ::={ iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) }

1．authorityKeyIdentifier

authorityKeyIdentifier 扩展项用于区分证书签发者（CA）的公钥。当证书签发者拥有

多个公私钥对用于签发用户证书时，必须使用该扩展项。

该扩展项必须设置为非关键项（critical=FALSE）。

authorityKeyIdentifier 格式用 ASN.1 描述如下：

```
id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::=  { id-ce 35 }
authorityKeyIdentifier ::= SEQUENCE {
    keyIdentifier             [0] KeyIdentifier            OPTIONAL,
    authorityCertIssuer       [1] GeneralNames             OPTIONAL,
    authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL  }
KeyIdentifier ::= OCTET STRING
```

authorityKeyIdentifier 基于证书签发者证书（CA 证书）中的内容生成，主要有两种生成方式：基于 subjectKeyIdentifier，以及基于 issuer 和 serialNumber。当基于 subjectKeyIdentifier 生成时，keyIdentifier 通常等于证书签发者证书中的 subjectKeyIdentifier。

2. subjectKeyIdentifier

subjectKeyIdentifier 扩展项用于区分证书持有者的公钥。

该扩展项必须设置为关键项（critical=TRUE）。

subjectKeyIdentifier 格式用 ASN.1 描述如下：

```
id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::=  { id-ce 14 }
SubjectKeyIdentifier ::= KeyIdentifier
```

subjectKeyIdentifier 可以基于公钥产生，两种常用的产生方法如下：

① 将 subjectPublicKey 删除标识(tag)、长度(length)和无用比特个数(number of unused bits)后，使用 SHA1 算法计算获得 160 比特摘要值。subjectKeyIdentifier=160 比特摘要值。

② 同方法①计算获得 160 比特摘要值。subjectKeyIdentifier=4 比特类型（'0100'）+至少 80 比特摘要值。

subjectKeyIdentifier 也可以使用递增的整数来表示。

3. keyUsage

keyUsage 扩展项用于定义证书中的公钥及其对应私钥的用途。当需要限制或约束密钥只能用于部分操作时，可以使用该扩展项。例如，当只允许 RSA 密钥用于验证数据签名，不允许用于验证数字证书或 CRL 中的签名时，需要将 keyUsage 设置为 digitalSignature 或 nonRepudiation；当只允许 RSA 密钥用于密钥管理时，需要将 keyUsage 设置为 keyEncipherment。

该扩展项必须设置为关键项（critical=TRUE）。

keyUsage 格式用 ASN.1 描述如下：

```
id-ce-keyUsage OBJECT IDENTIFIER ::=  { id-ce 15 }
keyUsage ::= BIT STRING {
        digitalSignature        (0),
        nonRepudiation          (1),
        keyEncipherment         (2),
```

```
dataEncipherment        (3),
keyAgreement            (4),
keyCertSign             (5),
cRLSign                 (6),
encipherOnly            (7),
decipherOnly            (8) }
```

其中，digitalSignature 表示数字签名服务，可用于实体身份认证和数据完整性认证，但不可用于签发证书和 CRL。

nonRepudiation 表示抗抵赖服务，可用于操作或交易的抗抵赖，但不可用于证书和 CRL 签发行为的抗抵赖。

keyEncipherment 用于密钥加密。当 RSA 密钥用于密钥管理时，需要将 keyUsage 设置为 keyEncipherment。

dataEncipherment 用于数据加密，但不可用于密钥加密。

keyAgreement 用于密钥协商。如使用 DH 算法密钥进行密钥管理时，需要将 keyUsage 设置为 keyAgreement。

keyCertSign 用于签发和验证数字证书。当 KeyUsage 设置为 keyCertSign 时，需同时设置扩展项 basicConstraints→cA=TRUE。

cRLSign 用于签发和验证 CRL（包括 CRL、增量 CRL、ARL 等）。

encipherOnly 表示只用于数据加密。仅当 keyAgreement 设置时，encipherOnly 才有效，表示密钥只用于密钥协商过程中的数据加密。

decipherOnly 表示只用于数据解密。仅当 keyAgreement 设置时，decipherOnly 才有效，表示密钥只用于密钥协商过程中的数据解密。

4．privateKeyUsagePeriod

privateKeyUsagePeriod 扩展项用于定义私钥有效期，允许私钥有效期不同于证书有效期。该扩展项主要用于限制签名密钥，即与证书对应的私钥不允许在私钥有效期之外进行数字签名操作。

该扩展项必须设置为非关键项（critical=FALSE）。

privateKeyUsagePeriod 格式用 ASN.1 描述如下：

```
id-ce-privateKeyUsagePeriod OBJECT IDENTIFIER ::=  { id-ce 16 }
privateKeyUsagePeriod ::= SEQUENCE {
    notBefore       [0]     GeneralizedTime OPTIONAL,
    notAfter        [1]     GeneralizedTime OPTIONAL }
```

其中，notBefore 和 notAfter 采用 GeneralizedTime 格式。

5．certificatePolicies

certificatePolicies 扩展项可包括多个证书策略；每个证书策略由一个 OID 和多个限定语（qualifier）组成。qualifier 是可选的，但不能与策略的定义或内涵发生冲突。

certificatePolicies 格式用 ASN.1 描述如下：