表 9-8　数字证书国内通用扩展项

/	扩　展　项	OID	是否关键项	说　　明
1	IdentifyCode	1.2.156.10260.4.1.1	FALSE	个人身份标识码
2	InsuranceNumber	1.2.156.10260.4.1.2	FALSE	个人社会保险号
3	ICRegistrationNumber	1.2.156.10260.4.1.3	FALSE	企业工商注册号
4	OrganizationCode	1.2.156.10260.4.1.4	FALSE	企业组织机构代码
5	TaxationNumber	1.2.156.10260.4.1.5	FALSE	企业税号

1．identifyCode

identifyCode 扩展项用于表示个人的身份标识号码。该扩展项应该设置为非关键项（critical=FALSE）。

identifyCode 格式用 ASN.1 描述如下：

```
id-IdentifyCode    OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.1 }
identifyCode    ::=    CHOICE {
    residenterCardNumber          [0] PrintableString OPTIONAL,
    militaryOfficerCardNumber     [1] UTF8String OPTIONAL,
    passportNumber                [2] PrintableString OPTIONAL    }
```

其中，residenterCardNumber 表示身份证号码，militaryOfficerCardNumber 表示军官证号码，passportNumber 表示护照号码。

2．insuranceNumber

insuranceNumber 扩展项用于表示个人的社会保险号码。该扩展项应该设置为非关键项（critical=FALSE）。

insuranceNumber 格式用 ASN.1 描述如下：

```
id-InsuranceNumber    OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.2 }
insuranceNumber    ::=    PrintableString
```

3．iCRegistrationNumber

iCRegistrationNumber 扩展项用于表示企业的工商注册号码。该扩展项应该设置为非关键项（critical=FALSE）。

iCRegistrationNumber 格式用 ASN.1 描述如下：

```
id-ICRegistrationNumber    OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.3 }
iCRegistrationNumber    ::=    PrintableString
```

4．organizationCode

organizationCode 扩展项用于表示企业的组织机构代码。该扩展项应该设置为非关键项（critical=FALSE）。

organizationCode 格式用 ASN.1 描述如下：

```
id-OrganizationCode    OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.4 }
organizationCode    ::=    PrintableString
```

5．taxationNumber

taxationNumber 扩展项用于表示企业税号码。该扩展项应该设置为非关键项（critical=FALSE）。

taxationNumber 格式用 ASN.1 描述如下：

```
id-TaxationNumber    OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.5 }
taxationNumber    ::=    PrintableString
```

第 10 章　数字证书分类

为适应复杂的应用场景，在实际应用中，通常需要将证书进行分类。有些分类方式 X.509 格式已经支持，但有些分类方式 X.509 格式本身并不支持，需要通过其他方式来识别。

证书通常可分为两大类：根据证书持有者分类和根据密钥分类。

10.1　根据证书持有者分类

1．根据证书持有者是否为 CA 进行分类

根据证书持有者是否为 CA，可将证书分为 2 类：CA 证书和用户证书。CA 证书可以给用户或其他 CA 签发证书，用户证书不允许给其他用户或 CA 签发证书。

X.509 格式中通过扩展项 BasicConstraints 来区分这 2 类证书。当其中的 cA 项为 TRUE 时表示 CA 证书，为 FALSE 时表示用户证书。

BasicConstraints 扩展项格式用 ASN.1 描述如下：

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

2．按照证书持有者类型进行分类

根据证书持有者类型，通常将证书分为几类：个人证书、单位证书和系统证书等。

个人证书是 CA 系统给个人签发的证书，代表个人身份。证书中需要包含个人信息（如姓名、身份证、E-mail、电话等）和个人的公钥。

单位证书是 CA 系统给机构或组织等签发的证书，代表单位身份。证书中需要包含单位信息（如名称、组织机构代码、E-mail、联系人等）和单位的公钥。

系统证书是 CA 系统给软件系统或设备系统等签发的证书，代表系统身份。证书中需要包含系统信息（如 IP 地址、域名等）和系统的公钥。系统证书又包括 Web 服务器证书、域控制器证书、VPN 设备证书、OCSP 服务器证书、时间戳服务器证书等。

X.509 格式本身并不支持这种分类，通常通过在 Subject 中增加 DN 项进行区分，如可增加 OU=PERSON 表示个人证书，OU=UNIT 表示单位证书等。为保持证书内容的统一性，扩展项 KeyUsage、ExtKeyUsage 必须设置合适的值。

10.2　根据密钥分类

1．根据密钥对产生方式进行分类

根据密钥对的产生方式，可将证书分为 2 类：签名证书和加密证书。

签名证书及私钥只用于签名验签，不能用于加密解密。为保证该密钥对的唯一性，该密钥对必须由用户端密码模块产生和保存，在证书签发过程中 CA 中心并不知道其私钥，只对其公钥进行操作。

加密证书及私钥只用于加密解密，不能用于签名验签。为实现密钥恢复或行业监管，该密钥对必须由 CA 中心产生，并回送给用户端密码模块保存。CA 中心同时保存该密钥对，必要时可恢复该密钥对。

X.509 格式本身并不支持这种分类；通常通过存储位置或应用系统进行区分。为保持证书内容的统一性，扩展项 KeyUsage、ExtKeyUsage 必须设置合适的值。

KeyUsage 中已经定义的类型如下。

① digitalSignature：表示数字签名；
② nonRepudiation：表示不可抵赖；
③ keyEncipherment：表示密钥加密；
④ dataEncipherment：表示数据加密；
⑤ keyAgreement：表示密钥协商；
⑥ keyCertSign：表示证书签名；
⑦ cRLSign：表示 CRL 签名；
⑧ encipherOnly：表示只用于加密；
⑨ decipherOnly：表示只用于解密。

2．根据证书用途进行分类

根据证书用途，通常将证书分为 SSL 服务器证书、SSL 客户端证书、代码签名证书、Email 证书、时间戳服务器证书、OCSP 服务器证书等。SSL 证书只用于 SSL/TLS 应用，Email 证书只用于安全电子邮件，代码签名证书只用于对代码进行签名验签。

X.509 格式中通过扩展项 ExtKeyUsage 来区分这几类证书。为保持证书内容的统一性，扩展项 KeyUsage 必须设置合适的值。

ExtKeyUsage 中已经定义的类型如下。

① id-kp-serverAuth：用于 SSL/TLS Web 服务器身份认证；
② id-kp-clientAuth：用于 SSL/TLS Web 客户端身份认证；
③ id-kp-codeSigning：用于对可下载的执行代码进行签名；
④ id-kp-emailProtection：用于保护 E-mail；
⑤ id-kp-timeStamping：用于将对象摘要值与时间绑定；
⑥ id-kp-OCSPSigning：用于对 OCSP 响应包进行签名。

第 11 章　私钥与证书存储方式

公钥无需保密，包含在数字证书中，并以数字证书形式对外公开发布，由数字证书的安全机制来保证公钥的完整性和真实性。

私钥必须保密，有多种存储方式，且不同的存储方式安全性不同。

通常将密码算法运算、密钥存储及产生的装置称为密码模块。密码模块又可分为软件密码模块和硬件密码模块。

11.1　证书保存形式

11.1.1　DER 文件形式

数字证书按照 Certificate 类型进行 DER 编码后，以二进制形式保存为文件。

当证书采用 DER 文件形式保存时，常用的文件后缀为 der 或 crt。

例如，用户 ZHANG San 的数字证书内容显示如图 11-1 所示，其中序列号=1174（0x0496），证书签发者 DN=“CN = Virtual CA，C = CN”，证书持有者 DN=“CN = ZHANG San，OU = Person，C = CN”，证书有效期=20130222000000-20160222000000。

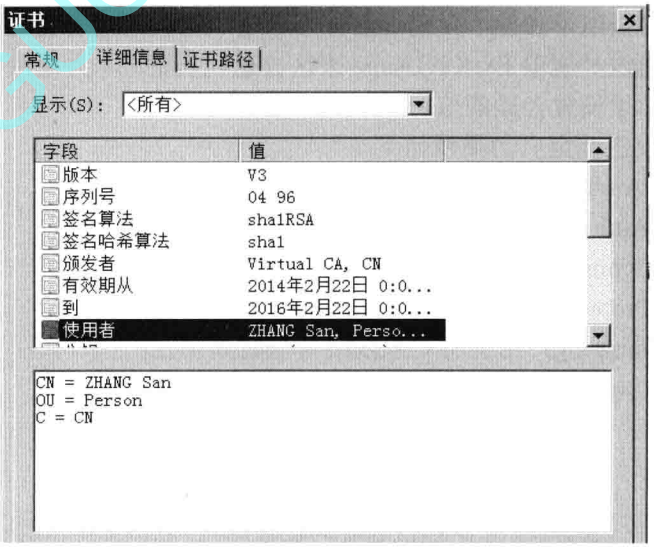

图 11-1　数字证书内容

该数字证书 DER 编码后的文件大小为 752 字节，具体二进制值如表 11-1 所示，其中，每行显示 16 个字节，每行最前面 4 个数字表示该行第 1 个字节的地址序号（从 0 开始）。