



中华人民共和国密码行业标准

GM/T 0015—2023

代替 GM/T 0015—2012

数 字 证 书 格 式

Digital certificate format

2023-12-04 发布

2024-06-01 实施

国家密码管理局 发 布

目 次

前言 III

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 数字证书与 CRL 2

 5.1 概述 2

 5.2 数字证书格式 2

 5.3 CRL 格式 18

附录 A（规范性） 证书结构 23

附录 B（规范性） 证书的结构实例 25

附录 C（规范性） 证书内容表 27

附录 D（资料性） SM2 数字证书示例 45

参考文献 49

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GM/T 0015—2012《基于 SM2 密码算法的数字证书格式规范》。与 GM/T 0015—2012 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 增加了规范性引用文件 GB/T 16262.1(见 5.2.1)、GB/T 17969.1(见 5.2.4.2.5)、GB/T 16264.8(见 5.2.3.6 和 5.2.4.2.1)、GB/T 25069(见第 3 章)和 GM/Z 4001(见第 3 章)，删除了 PKCS#7 的引用(见第 2 章，2012 年版的第 2 章)；
- b) 删除了术语“数字证书”“证书撤销列表”“CA 证书”“终端实体证书”(见 2012 年版的 3.1、3.2、3.3、3.4)；
- c) 删除了 5.1 概述的中表述不清的内容(见 5.1，2012 年版的 5.1)；
- d) 更改了“ISO/IEC 9594-2:2001”的描述为“GB/T 16264.8—2005”(见 5.2.3.6，2012 年版的 5.2.3.6)；
- e) 更改了 5.2.4.2.1 中的综述，其中 6 个扩展定义的 OID 应遵循 GM/T 0006 而不是 GB/T 16264.8(见 5.2.4.2.1，2012 年版的 5.2.4.2.1)；
- f) 更改了 keyIdentifier 的描述(见 5.2.4.2.2，2012 年版的 5.2.4.2.2)；
- g) 更改了个人身份标识码的定义(见 5.2.4.2.18，2012 年版的 5.2.4.2.18)；
- h) 增加了“统一社会信用代码”(见 5.2.4.2.23)；
- i) 更改了证书颁发者描述(见 5.3.4.7.3，2012 年版的 5.3.4.7.3)，并增加了描述“本扩展应是关键的”(见 5.3.4.7.3，2012 年版的 5.3.4.7.3)；
- j) 更改了扩展域中 keyusage 的关键度(见表 A.3，2012 年版的 A.3)；
- k) 增加了 UniformSocialCreditIdentifier 统一社会信用号(见表 A.3)；
- l) 增加了密钥使用(KeyUsage)项(见表 B.1 和表 B.2)；
- m) 增加了 SAN 主体替换名称(subjectalternativenam)(见表 B.2)；
- n) 删除了 SHA-1 算法(见 2012 年版的附录 C)；
- o) 更改了附录 D 的名称，删除了 RSA 数字证书编码的举例(见附录 D，2012 年版的附录 D)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由密码行业标准化技术委员会提出并归口。

本文件起草单位：格尔软件股份有限公司、北京数字认证股份有限公司、北京海泰方圆科技股份有限公司、广东省电子商务认证有限公司、上海智巡密码检测技术有限公司、无锡江南信息安全工程技术中心、上海市数字证书认证中心有限公司、长春吉大正元信息技术股份有限公司、中电科网络安全科技股份有限公司、兴唐通信科技有限公司、北京华大智宝电子系统有限公司、山东得安信息技术有限公司、山东大学、北京国脉信安科技有限公司、国家信息安全工程技术研究中心、国家密码管理局商用密码检测中心。

本文件主要起草人：刘平、郑强、谭武征、李述胜、柳增寿、赵敏、梁宁宁、韩玮、封维端、刘承、赵丽丽、李元正、徐强、王妮娜、陈跃、孔凡玉、马洪富、袁峰、李志伟。

本文件及其所代替文件的历次版本发布情况为：

- 2012 年首次发布为 GM/T 0015—2012；
- 本次为第一次修订。

数字证书格式

1 范围

本文件规定了数字证书和证书撤销列表的基本结构,描述了数字证书和证书撤销列表中的各数据项内容。

本文件适用于数字证书认证系统的研发、数字证书认证机构的运营以及基于数字证书的安全应用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 16262.1 信息技术 抽象语法记法 (ASN.1) 第1部分:基本记法规范

GB/T 16264.8 信息技术 开放系统互连 目录 第8部分:公钥和属性证书框架

GB/T 17969.1 信息技术 开放系统互连 (OSI) 登记机构的操作规程 第1部分:一般规程和国际对象标识符树的顶级弧

GB/T 25069 信息安全技术 术语

GM/T 0006 密码应用标识规范

GM/T 0009 SM2 密码算法使用规范

GM/T 0010 SM2 密码算法加密签名消息语法规范

GM/Z 4001 密码术语

3 术语和定义

GB/T 25069 和 GM/Z 4001 界定的术语和定义适用于本文件。

4 缩略语

下列缩略语适用于本文件。

CA:证书认证机构(Certification Authority)

CRL:证书撤销列表(Certificate Revocation List)

DIT:目录信息树系统(Directory Information Tree)

DNS:域名系统(Domain Name System)

OID:对象标识符(Object ID)

PKI:公钥基础设施(Public Key Infrastructure)

URI:统一资源标识符(Uniform Resource Identifier)

5 数字证书与 CRL

5.1 概述

数字证书具有以下特性：

- 数字证书可通过证书认证机构的公钥进行有效性验证；
- 数字证书不可被篡改和伪造。

证书认证机构通过对信息集合的签名来生成用户证书，信息集合包括可甄别的用户名、公钥以及一个可选的包含用户附加信息的唯一性标识符。唯一性标识符可是诸如对象标识符、证书、日期或是说明有关可辨别用户名的有效性的证书的其他形式。具体地说，如果一个用户证书的可辨别名为 A，唯一性标识符为 UA，并且该证书是由名为 CA，其唯一性标识符为 UCA 的认证机构生成的，则用户证书具有下列的形式： $CA\langle A \rangle = CA\{V, SN, AI, CA, UCA, A, UA, Ap, T^A\}$ ，这里 V 为证书版本；SN 为证书序列号；AI 为签发证书使用的算法标识符；UCA 为 CA 的可选的唯一性标识符；UA 为用户 A 的可选的唯一性标识符；Ap 为用户 A 的公钥； T^A 表示证书的有效期。

CRL 是 CA 对撤销的证书而签发的一个列表文件，该文件可用于应用系统鉴别用户证书的有效性。

5.2 数字证书格式

5.2.1 综述

本文件按照 GB/T 16262.1 的特定编码规则 (DER) 对下列证书项中的各项信息进行编码，组成特定的证书数据结构。ASN.1 DER 编码是关于每个元素的标记、长度和值的编码系统。

5.2.2 基本证书域的数据结构

数字证书的基本数据结构如下：

```
Certificate ::= SEQUENCE {
    tbsCertificate      TBSCertificate,
    signatureAlgorithm   AlgorithmIdentifier,
    signatureValue       BIT STRING }
TBSCertificate ::= SEQUENCE {
    version              [0] EXPLICIT Version DEFAULT v1,
    serialNumber          CertificateSerialNumber,
    signature             AlgorithmIdentifier,
    issuer                Name,
    validity              Validity,
    subject               Name,
    subjectPublicKeyInfo  SubjectPublicKeyInfo,
    issuerUniqueID        [1] IMPLICIT UniqueIdentifier OPTIONAL,
                        ——如果出现，version 应是 v2 或者 v3
    subjectUniqueID       [2] IMPLICIT UniqueIdentifier OPTIONAL,
                        ——如果出现，version 应是 v2 或者 v3
    extensions            [3] EXPLICIT Extensions OPTIONAL 扩展项
                        ——如果出现，version 应是 v3
```

```

}
Version ::= INTEGER { v1(0), v2(1), v3(2) }
CertificateSerialNumber ::= INTEGER
Validity ::= SEQUENCE {
    notBefore      Time,
    notAfter       Time }
Time ::= CHOICE {
    utcTime        UTCTime,
    generalTime    GeneralizedTime }
UniqueIdentifier ::= BIT STRING
SubjectPublicKeyInfo ::= SEQUENCE {
    algorithm       AlgorithmIdentifier,
    subjectPublicKey BIT STRING }
Extensions ::= SEQUENCE SIZE (1..MAX) OF Extension
Extension ::= SEQUENCE {
    extnID          OBJECT IDENTIFIER,
    critical         BOOLEAN DEFAULT FALSE,
    extnValue        OCTET STRING }

```

上述的证书数据结构由 `tbsCertificate`、`signatureAlgorithm` 和 `signatureValue` 三个域构成。这些域的含义如下所述。

- `tbsCertificate` 域包含了主体名称和颁发者名称、主体的公钥、证书的有效期以及其他相关信息。
- `signatureAlgorithm` 域包含了证书签发机构签发该证书所使用的密码算法标识符。其 ASN.1 结构如下：

```

AlgorithmIdentifier ::= SEQUENCE {
    algorithm    OBJECT IDENTIFIER,
    parameters  ANY DEFINED BY algorithm OPTIONAL }

```

其中 `algorithm` 是算法标识符，标识了具体的算法。`parameters` 是可选参数，依赖于所标识的算法。该域中 `algorithm` 标识的算法应与 `tbsCertificate` 域中 `signature` 标识的签名算法相同。如果签名算法为 SM2，则 `parameters` 的值为空。

- `signatureValue` 域包含了对 `tbsCertificate` 域进行数字签名的结果。采用 ASN.1 DER 编码的 `tbsCertificate` 域作为数字签名的输入，签名的结果按照 ASN.1 BITSTRING 类型编码，并保存在 `signatureValue` 域内。如果签名算法为 SM2 密码算法，则签名数据格式应遵循 GM/T 0009。

5.2.3 TBSCertificate 数据结构

5.2.3.1 版本 (Version)

本项描述了编码证书的版本号。

5.2.3.2 序列号 (Serial number)

本项描述了证书序列号，证书序列号是 CA 分配给所签发证书的用于唯一标识该数字证书的一个正整数。序列号最大长度为 20 个八比特字节。

5.2.3.3 签名算法(Signature)

本项包含 CA 签发该证书所使用的密码算法的标识符,这个算法标识符应与证书 signatureAlgorithm 域中项的算法标识符相同。可选参数的内容依赖算法标识符所标识的具体算法。本项可支持用户定义的签名算法。

5.2.3.4 颁发者(Issuer)

本项标识了进行证书签名和证书颁发的实体。它应包含一个非空的甄别名称(DN——distinguished name)。该项被定义为 Name 类型,其 ASN.1 的结构如下。

```

Name ::= CHOICE { RDNSequence }
RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
RelativeDistinguishedName ::= SET OF AttributeTypeAndValue
AttributeTypeAndValue ::= SEQUENCE {
    type AttributeType,
    value AttributeValue }
AttributeType ::= OBJECT IDENTIFIER
AttributeValue ::= ANY DEFINED BY AttributeType
DirectoryString ::= CHOICE {
    teletexString      TeletexString (SIZE (1..MAX)),
    printableString    PrintableString (SIZE (1..MAX)),
    universalString    UniversalString (SIZE (1..MAX)),
    utf8String         UTF8String (SIZE (1..MAX)),
    bmpString          BMPString (SIZE (1..MAX)) }

```

Name 是由一些属性及相应的值组成的层次结构,如“国家=C”。其中 AttributeValue 项的类型是由 AttributeType 确定的,通常它是一个 DirectoryString 类型。

DirectoryString 类型定义可取值范围包括 PrintableString, TeletexString, BMPString, UTF8String 和 UniversalString 类型。UTF8String 是首选的编码类型。

5.2.3.5 有效期(Validity)

5.2.3.5.1 概述

证书有效期是一个时间段,在这个时间段内,CA 担保对证书状态的相关信息维护。该项是证书有效期的起始时间(notBefore)和证书有效期的终止时间(notAfter)两个时间值的序列(SEQUENCE)。NotBefore 和 notAfter 这两个时间都可作为 UTCTime 类型或者 GeneralizedTime 类型进行编码。

5.2.3.5.2 编码类型要求

在 2049 年之前(包括 2049 年)颁发的证书,时间值应采用 UTCTime 类型编码,在 2050 年之后颁发的证书,时间值应采用 GeneralizedTime 类型编码。

5.2.3.5.3 世界时间(UTCTime)

本项是为国际应用设立的一个标准 ASN.1 类型,在这里只有本地时间是不够的。UTCTime 包含 Z(用于 Zulu,或格林威治标准时间)或时间差。

在本文件中,UTCTime 值应使用格林威治标准时间(Zulu)表示,其年份使用最低两位,并且应包含秒,即时间格式为 YYMMDDHHMMSSZ。系统对年字段(YY)应作如下解释:

当 YY 大于或等于 50,年字段应解释为 19YY;当 YY 小于 50,年应解释为 20YY。

5.2.3.5.4 通用时间类型(GeneralizedTime)

本项是一个标准 ASN.1 类型,表示时间的可变精确度。GeneralizedTime 字段能包含一个本地和格林威治标准时间之间的时间差。

本文件中,GeneralizedTime 值应使用格林威治标准时间表示,且应包含秒,即时间格式为 YYYYMMDDHHMMSSZ。GeneralizedTime 值中秒的取值为整数。

5.2.3.6 主体(Subject)

本项描述了与主体公钥信息项中的公钥相对应的实体。本项可出现在主体项和/或主体可选替换名称扩展项中。如果主体是一个 CA,那么主体项应是一个非空的与颁发者项的内容相匹配的甄别名称。如果主体的命名信息只出现在主体替换名称扩展项中,那么主体名称应是一个空序列,且主体替换名称扩展项应被标记为关键的。

当主体项非空时,这个项应包含一个甄别名称。一个 CA 认证的每个主体实体的甄别名称应是唯一的。一个 CA 可为同一个主体实体以相同的甄别名称签发多个证书。

主体项结构定义应符合 GB/T 16264.8 中对名字类型的要求。

5.2.3.7 主体公钥信息(Subject Public Key Info)

本项包含证书公钥和相应的公钥算法。公钥算法使用算法标识符 AlgorithmIdentifier 结构表示。

当公钥算法为 SM2 时,AlgorithmIdentifier 结构定义应遵循 GM/T 0010;当公钥算法为 RSA 时,AlgorithmIdentifier 结构定义见 RFC8017。

5.2.3.8 颁发者唯一标识符(issuerUniqueID)

本项用来处理颁发者名称的重用问题。对于不同的颁发者,颁发者唯一标识符不同。在 v1 版本中,符合本文件的 CA 在颁发证书时,证书中应不包含本项,但应用在解析证书过程中,若存在包含本扩展项的证书,应能正确解析该项的值。

5.2.3.9 主体唯一标识符(subjectUniqueID)

本项用来处理主体名称的重用问题。对于不同的主体,主体唯一标识符不同。在 v1 版本中,符合本文件的 CA 在颁发证书时,证书中应不包含本项,但应用在解析证书过程中,若存在包含本扩展项的证书,应能正确解析该项的值。

5.2.3.10 扩展项(extensions)

本项是一个或多个证书扩展的序列(SEQUENCE),其内容和数据结构见 5.2.4。

5.2.4 证书扩展域及其数据结构

5.2.4.1 证书扩展

证书的扩展包括标准扩展项和专用扩展项。扩展由三部分组成,分别是扩展类型、扩展关键度和扩展项值。扩展关键度可定义成关键的或非关键的,表明一个证书的使用者是否可忽略该扩展项。证书的应用系统如果不能识别关键的扩展时,应拒绝接受该证书,如果不能识别非关键的扩展,则可忽略该

扩展项的信息。

本条定义一些标准的扩展项。应特别注意的是,在实际应用过程中,如果采用了关键的扩展,可能导致在一些通用的应用中无法使用该证书。

每个扩展项包括一个对象标识符 OID 和一个 ASN.1 结构。当证书中出现一个扩展时,OID 作为 extnID 项出现,其对应的 ASN.1 编码结构就是八比特字符串 extnValue 的值。一个证书中特定的扩展应只出现一次。一个扩展中包含一个布尔型的值用来表示该扩展的关键性,其缺省值为 FALSE,即非关键的。

CA 应支持颁发机构密钥标识符、主体密钥标识符、基本限制、密钥用法和证书策略扩展,其他的扩展是可选的。如果 CA 签发的证书中的主体项为空序列,该 CA 就应支持主体可替换名称扩展。CA 也可支持本文件定义之外的其他的扩展,但如果这些扩展被定义为关键的,则可能会给互操作性带来障碍。

应用应至少能识别下列扩展:密钥用法、证书策略、主体替换名称、基本限制、名称限制、策略限制和扩展的密钥用途。另外,宜支持颁发机构密钥标识符、主体密钥标识符以及策略映射扩展。

5.2.4.2 标准扩展

5.2.4.2.1 综述

本条定义数字证书的标准证书扩展,其中,扩展 5.2.4.2.2 到扩展 5.2.4.2.17 共 16 个扩展中定义的 OID 应遵循 GB/T 16264.8。这些 OID 都是 id-ce 的成员,其定义如下:

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

扩展 5.2.4.2.18 到扩展 5.2.4.2.23 共 6 个扩展定义的 OID 应遵循 GM/T 0006。

5.2.4.2.2 颁发机构密钥标识符(authorityKeyIdentifier)

本项提供了一种方式,以识别与证书签名私钥相应的公钥。当颁发者由于有多个密钥共存或由于发生变化而具有多个签名密钥时使用该扩展。颁发机构密钥标识符可基于 CA 证书中的主体密钥标识符或基于颁发者的名称和序列号。

CA 产生的所有证书应包括颁发机构密钥标识符扩展的 keyIdentifier 项,以便于证书链的建立。CA 以“自签”(self-signed)证书形式发放其公钥时,可省略认证机构密钥标识符。此时,主体和认证机构密钥标识符是完全相同的。

本项既可用作证书扩展亦可用作 CRL 扩展。本项标识用来验证在证书或 CRL 上签名的公开密钥。它能辨别同一 CA 使用的不同密钥(例如,在密钥更新发生时)。本项定义如下:

id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::= { id-ce 35 }

AuthorityKeyIdentifier ::= SEQUENCE {

keyIdentifier [0] KeyIdentifier OPTIONAL,

authorityCertIssuer [1] GeneralNames OPTIONAL,

authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }

(WITH COMPONENTS { ..., authorityCertIssuer PRESENT, authorityCertSerialNumber PRESENT } |

WITH COMPONENTS { ..., authorityCertIssuer ABSENT, authorityCertSerialNumber ABSENT })

KeyIdentifier ::= OCTET STRING。

KeyIdentifier 项的值应从用于证实证书签名的公钥导出或用产生唯一值的方法导出。公开密钥的密钥标识符 KeyIdentifier 可采用下述两种通用的方法之一生成。

- a) keyIdentifier 由 BIT STRING subjectPublicKey 值(不包括标签、长度和未使用的比特个数的编码)的 SM3 杂凑值中最低位的 160 比特组成。
- b) keyIdentifier 由 0100 加上后跟的 BIT STRING subjectPublicKey 值(不包括标签、长度和未使用的比特个数的编码)的 SM3 杂凑值中最低位的 60 比特组成。

此密钥可通过 keyIdentifier 字段中的密钥标识符来标识,也可通过此密钥的证书标识(使用 authorityCertIssuer 字段中的证书颁发者或 authorityCertSerialNumber 字段中的证书序列号)来标识,或者可通过密钥标识符和此密钥的证书标识来标识。如果使用两种标识形式,证书或 CRL 的颁发者应保证它们是一致的。对于颁发机构的包含扩展的证书或 CRL 的所有密钥标识符而言,每个密钥标识符应是唯一的。支持此扩展的实现不必处理 authorityCertIssuer 字段中的所有名字形式。

证书认证机构指定或者自动产生证书序列号,这样颁发者和证书序列号相结合就唯一地标识了一份证书。

除自签证书之外,所有的证书应包含本扩展,而且要包含 keyIdentifier 项。如果证书的颁发者的证书有主体密钥标识符扩展,则本扩展中 keyIdentifier 项应与颁发者的证书中 SubjectKeyIdentifier 扩展的值一致,如果证书的颁发者的证书没有主体密钥标识符扩展,则可使用文中介绍的两种方法之一来产生。

本扩展应是非关键的。

5.2.4.2.3 主体密钥标识符(subjectKeyIdentifier)

本项提供一种识别包含有一个特定公钥的方法。此扩展标识了被认证的公开密钥。它能区分同一主体使用的不同密钥。此项定义如下:

id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::= {id-ce 14}

SubjectKeyIdentifier ::= KeyIdentifier

对于使用密钥标识符的主体的各个密钥而言,每一个密钥标识符均应是唯一的。此扩展项总是非关键的。

所有的 CA 证书应包括本扩展,而且 CA 签发证书时应把 CA 证书中本扩展的值赋给终端实体证书颁发者密钥标识符扩展中的 KeyIdentifier 项。CA 证书的主体密钥标识符应从公钥或生成唯一值的方法中导出。终端实体证书的主体密钥标识符应从公钥中导出。从公钥中生成密钥标识符,应使用 5.2.4.2.2 中的两种通用方法之一。

5.2.4.2.4 密钥用法(keyUsage)

本项指示已认证的公开密钥用于何种用途,该项定义如下:

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) }

KeyUsage 类型中的用法如下:

- a) digitalSignature: 验证下列 b)、f) 或 g) 所标识的用途之外的数字签名;
- b) nonRepudiation: 验证用来提供抗抵赖服务的数字签名, 这种服务防止签名实体不实地拒绝某种行为(不包括如 f) 或 g) 中的证书或 CRL 签名);
- c) keyEncipherment: 加密密钥或其他安全信息, 例如用于密钥传输;
- d) dataEncipherment: 加密用户数据, 但不包括上面 c) 中的密钥或其他安全信息;
- e) keyAgreement: 用作公开密钥协商密钥;
- f) keyCertSign: 验证证书的 CA 签名;
- g) cRLSign: 验证 CRL 的 CA 签名;
- h) encipherOnly: 当本位与已设置的 keyAgreement 位一起使用时, 公开密钥协商密钥仅用于加密数据(本位与已设置的其他密钥用法位一起使用的含义未定义);
- i) decipherOnly: 当本位与已设置的 keyAgreement 位一起使用时, 公开密钥协商密钥仅用于解密数据(本位与已设置的其他密钥用法位一起使用的含义未定义)。

keyCertSign 只用于 CA 证书。如果 KeyUsage 被置为 keyCertSign 和基本限制扩展存在于同一证书之中, 那么, basicConstraints 扩展的 cA 字段的值应被置为 TRUE。CA 还可使用 keyUsag 扩展中定义的其他密钥用法位, 例如, 提供鉴别和在线管理事务完整性的 digitalSignature。

若未设置 keyAgreement 位, 则不定义 encipherOnly 位的含义。若设置 encipherOnly 位, 且 keyAgreement 位也被设置时, 主体公钥可只用于加密数据, 同时执行密钥协议。

若未设置 keyAgreement 位, 则不定义 decipherOnly 位的含义。若设置 decipherOnly 位, 且 keyAgreement 位也被设置时, 主体公钥可只用于解密数据, 同时执行密钥协议。

所有的 CA 证书应包括本扩展, 而且应包含 keyCertSign 这一用法。此扩展可定义为关键的或非关键的, 由证书签发者选择。

如果此扩展标记为关键的, 那么该证书应只用于相应密钥用法位置为“1”的用途。

如果此扩展标记为非关键的, 那么它指明此密钥的预期用途或多种用途, 并可用于查找具有多密钥/证书的实体的正确密钥/证书。它是一个建议项, 并不意指此密钥的用法限于指定的用途。置为“0”的位指明此密钥不是预期的这一用途。如果所有位均为“0”, 它指明此密钥预期用于所列用途之外的某种用途。

在应用中, 使用该扩展项对证书类型进行区别, 当设置了 c)、d)、e) 位中的一位时, 表示该证书为加密证书; 当设置了 a)、b) 位中的一位时, 表示该证书为签名证书。

5.2.4.2.5 扩展密钥用途(extKeyUsage)

本项指明已验证的公开密钥可用于一种用途或多种用途, 它们可作为对密钥用法扩展项中指明的基本用途的补充或替代。此项定义如下:

id-ce-extKeyUsage OBJECT IDENTIFIER :: {id-ce 37}

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

KeyPurposeId ::= OBJECT IDENTIFIER

密钥的用途可由有此需要的任何组织定义。用来标识密钥用途的客体标识符应按照 GB/T 17969.1 要求来分配。

由证书签发者确定此扩展是关键的或非关键的。

如果此扩展标记为关键的, 那么, 此证书应只用于所指示的用途之一。

如果此扩展标记为非关键的, 那么, 它指明此密钥的预期用途或一些用途, 并可用于查找多密钥/证书的实体的正确密钥/证书。它是一个建议项, 并不表示认证机构将此密钥的用法限于所指示的用途。然而, 进行应用的证书应指明特定的用途, 以便证书为此应用接受。

如果证书包含关键的密钥用途项和关键的扩展密钥项, 那么, 两个项应独立地处理, 并且证书应只

用于与两个项一致的用途。如果没有与两个项一致的用途,那么,此证书不能用于任何用途。

本文件定义下列密钥用途:

id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }

id-kp-serverAuth OBJECT IDENTIFIER ::= { id-kp 1 }

——TLS Web server 鉴别

——Key usage 可设置为 digitalSignature, keyEncipherment 或 keyAgreement

id-kp-clientAuth OBJECT IDENTIFIER ::= { id-kp 2 }

——TLS Web server 鉴别

——Key usage 可设置为 digitalSignature 和/或 keyAgreement

id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }

——可下载执行代码的签名

——Key usage 可设置为 digitalSignature

id-kp-emailProtection OBJECT IDENTIFIER ::= { id-kp 4 }

——E-mail 保护

——Key usage 可设置为 digitalSignature, nonRepudiation 和/或 (keyEncipherment 或 keyAgreement)

id-kp-timeStamping OBJECT IDENTIFIER ::= { id-kp 8 }

——将对象的 Hash 与同一时间源提供的时间绑定

——Key usage 可设置为 digitalSignature, nonRepudiation

id-kp-OCSPSigning OBJECT IDENTIFIER ::= { id-kp 9 }

——OCSP 应答签名

——Key usage 可设置为 digitalSignature, nonRepudiation

5.2.4.2.6 私有密钥使用期(privateKeyUsagePeriod)

本项指明与已验证的公开密钥相对应的私有密钥的使用期限。它仅用于数字签名密钥。此项定义如下:

id-ce-privateKeyUsagePeriod OBJECT IDENTIFIER ::= { id-ce 16 }

PrivateKeyUsagePeriod ::= SEQUENCE {

notBefore [0] GeneralizedTime OPTIONAL,

notAfter [1] GeneralizedTime OPTIONAL }

notBefore 字段指明私有密钥可能用于签名的最早时间。如果没有 notBefore 字段,那么不提供有关私有密钥有效使用期何时开始的信息。notAfter 字段指明私有密钥可用于签名的最迟时间。如果没有 notAfter 字段,那么,不提供有关私有密钥有效使用期何时结束的信息。

这个扩展应标记为非关键。

注 1: 私有密钥有效使用期可与证书有效性周期指明的已验证的公开密钥有效性不同。就数字签名密钥而言,签名的私有密钥使用期一般比验证公开密钥的时间短。

注 2: 数字签名的验证者想要检查直到验证时刻此密钥是否未被撤销,则在验证时,对公开密钥的有效证书方需存在。在公开密钥的证书期满之后,签名验证者不能依赖 CRL 所通知的协议。

5.2.4.2.7 证书策略(certificatePolicies)

本项列出了由颁发的 CA 所认可的证书策略,这些策略适用于证书以及关于这些证书策略的任选的限定符信息。

证书策略扩展包含了一系列策略信息条目,每个条目都由一个 OID 和一个可选的限定条件组成。

这个可选的限定条件不应改变策略的定义。

在用户证书中,这些策略信息条目描述了证书发放所依据的策略以及证书的应用目的;在 CA 证书中,这些策略条目指定了包含这个证书的验证路径的策略集合。具有特定策略需求的应用系统应拥有它们将接受的策略的列表,并把证书中的策略 OID 与该列表进行比较。如果该扩展是关键的,则应能解释该扩展(包括选择性限定语),否则应拒绝该证书。如果 CA 不希望限制该证书的证书路径上的策略集合,可使用一个特别的 anyPolicy 策略。

为了提高互操作性,本文件策略信息条目中宜只包含一个 OID,如果一个 OID 不够,宜使用本条定义的限定语。

```
id-ce-certificatePolicies OBJECT IDENTIFIER ::= { id-ce 32 }
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 }
——policyQualifierIds for Internet policy qualifiers
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 {
    visibleString        VisibleString (SIZE (1 .. 200)),
    bmpString            BMPString (SIZE (1 .. 200)),
    utf8String           UTF8String (SIZE (1 .. 200)) }
```

本项定义了两种策略限定语:CPS Pointer 和 User Notice 限定语,以供证书策略制定者和证书签发者使用。

CPS Pointer 限定语包含一个 CA 发布的 CPS(Certification Practice Statement),指示字的形式为 URI。

User Notice 有两种可选字段:noticeRef 字段和 explicitText 字段。noticeRef 字段命名一个组织,并通过记数识别该组织所做的一个专用文本声明。explicitText 字段在证书内直接包括文本声明,该字段是一个最多含有 200 个字符的文本。如果 noticeRef 和 explicitText 选项都在同一个限定语

中,且如果应用软件可找出由 noticeRef 选项指明的通知文本,则应展示该文本,否则应展示 explicitText 的值。

5.2.4.2.8 策略映射(policyMappings)

本扩展仅用于 CA 证书。它列出一个或多个 OID 对,每对包括一个 issuerDomainPolicy 和一个 subjectDomainPolicy。这种成对形式表明,发行方 CA 认为其 issuerDomainPolicy 与主体 CA 的 subjectDomainPolicy 是等效的。发行方 CA 的用户可为某应用接收一个 issuerDomainPolicy。策略映射告知发行方 CA 的用户,哪些同 CA 有关的策略可与他们接收到的策略是等效的。此项定义如下:

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

策略不会被映射到或来自特殊的值 anyPolicy。

该扩展可由 CA 和/或应用支持。证书签发者宜将该扩展选择为关键的,否则一个证书用户就不能正确解释发布的 CA 设定的规则。

5.2.4.2.9 主体替换名称(subjectAltName)

本项包含一个或多个可选替换名供实体使用,CA 把该实体与认证的公开密钥绑定在一起。

主体替换名称扩展允许把附加身份加到证书的主体上。所定义的选项包括因特网电子邮件地址、DNS 名称、IP 地址和统一资源标识符(URI)。还有一些纯本地定义的选项,可包括多名称形式和每个名称形式的多个范例。当这样的身份被附加到一个证书中时,应使用主体选择名称或颁发者选择名称扩展。由于主体可选替换名被认为是与公钥绑在一起的,主体可选替换名的所有部分应由 CA 认证。此项定义如下:

```
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 }
GeneralName 类型中可替换的值是下列各种形式的名称:
```

- otherName 是按照 OTHER-NAME 信息客体类别实例定义的任一种形式的名称；
- rfc822Name 是 Internet 电子邮件地址；
- dNSName 是 Internet 域名；
- x400Address 是 O/R 地址；
- directoryName 是目录名称；
- ediPartyName 是通信的电子数据交换双方之间商定的形式名称；nameAssigner 成分标识了分配 partyName 中唯一名称值的机构；
- uniformResourceIdentifier 是用于 WWW 的 UniformResourceIdentifier, RFC 1738 中定义的 URL 语法和编码规则；
- IPAddress 是用二进制串表示的 Internet Protocol 地址；
- registeredID 是对注册的客体分配的标识符。

CA 不应签发带有 subjectAltNames 却包含空 GeneralName 项的证书。如果证书中的唯一主体身份是一个替换名称格式(如一个电子邮件地址),则主体的甄别名应是一个空序列,且主体替换名称扩展应存在,且应标识为关键的。如果出现主体替换名称扩展,则序列应至少包含一个条目。

对 GeneralName 类型中使用的每个名称形式,应有一个名称注册系统,以保证所使用的任何名称能向证书颁发者和证书使用者无歧义地标识一个主体。

此扩展可是关键的或非关键的,由证书签发者选择。不要求支持此扩展的实现能处理所有名称形式。如果此扩展标记为关键的,至少应能识别和处理存在的名称形式之一,否则,应认为此证书无效。除先前的限制以外,允许证书使用系统忽略具有不能识别的或不被支持的名称形式的任何名称。倘若证书的主体项包含了无歧义标识主体的目录名称,此项标记宜为非关键的。如果存在此扩展并标记为关键的,证书的 subject 项可包含空名称,在此情况下,主体只能用此扩展中的名称或一些扩展名称来标识。

5.2.4.2.10 颁发者替换名称(issuerAltName)

此项包含一个或多个替换名称(可使用多种名称形式中的任一个),以供证书或 CRL 颁发者使用。此项定义如下:

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

IssuerAltName ::= GeneralNames

此项可是关键的或非关键的,由证书或 CRL 颁发者选择。如果此扩展标记为关键的,那么至少应能识别和处理存在的名称形式之一,否则,应认为此证书无效。另外,应忽略不能识别的名称或不能被支持的名称格式。倘若证书或 CRL 的颁发者项包含了一个明确标识颁发机构的目录名称,此项标记宜为非关键的。

如果存在此扩展,并标记为关键的,证书或 CRL 的 issuer 项可包含空名称(例如,对应可甄别名的一个“0”序列),在此情况下,颁发者只能用名称或此扩展中的一些名称来标识。

5.2.4.2.11 主体目录属性(subjectDirectoryAttributes)

本项为证书主体传送其期望的任何目录属性值。此项定义如下:

id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::= { id-ce 9 }

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

AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute

该扩展总标记为非关键的。

5.2.4.2.12 基本限制(basicConstraints)

本扩展项用来标识证书的主体是否是一个 CA,通过该 CA 可能存在的认证路径有多长。此项定义

如下：

```
id-ce-basicConstraints OBJECT IDENTIFIER ::= { id-ce 19 }
BasicConstraintsSyntax ::= SEQUENCE {
    cA                               BOOLEAN DEFAULT FALSE,
    pathLenConstraint                INTEGER (0..MAX) OPTIONAL }
CA 字段标识此公钥证书是否可用来验证证书签名。
```

pathLenConstraint 字段仅在 cA 设置为 TRUE 时才有意义。它给出此证书之后认证路径中最多的 CA 证书数目。0 值表明在路径中只应签发终端实体证书。pathLenConstraint 字段出现时应大于或等于 0。如果在认证路径的任何证书中未出现 pathLenConstraint 字段，则对认证路径的允许长度没有限制。

CA 证书中应包括本扩展，而且应标记为关键的。

如果此扩展存在，并标记为关键的，那么：

- 如果 cA 字段的值置为 FALSE，则密钥用法不能包含 keyCertSign 这一用法，其公开密钥不能用来验证证书签名；
- 如果 cA 字段的值置为 TRUE，并且 pathLenConstraint 存在，则证书使用系统应检查被处理的认证路径是否与 pathLenConstraint 的值一致。

注：为限制一证书主体只是一个终端实体，颁发者在扩展中只包含一个空 SEQUENCE 值的扩展项。

5.2.4.2.13 名称限制(nameConstraints)

本项应只用于 CA 证书，它指示了一个名称空间，在此空间设置了认证路径中后续证书中的所有主体名称。此项定义如下：

```
id-ce-nameConstraints OBJECT IDENTIFIER ::= { id-ce 30 }
NameConstraintsSyntax ::= 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)
```

如果存在 permittedSubtrees 和 excludedSubtrees 字段，则它们每个都规定一个或多个命名子树，每个由此子树的根的名称或以任选处于其子树内的任意节点名称来定义，子树范围是一个由上界和/或下界限定的区域。如果 permittedSubtrees 存在，在主体 CA 和认证路径中下级 CA 颁发的所有证书中，只有那些在子树中具有与 permittedSubtrees 字段规定主体名称相同的证书才是可接受的。如果 excludedSubtrees 存在，在主体 CA 或认证路径中后继的 CA 颁发的所有证书中，同 excludedSubtrees 规定主体名称相同的任何证书都是不可接受的。如果 permittedSubtrees 和 excludedSubtrees 都存在并且名称空间重叠，则优先选用排斥声明 excludedSubtrees。

通过 GeneralName 字段定义的命名格式，应将那些具有良好定义的分层结构的名称形式用于这些字段，Directory Name 名称形式满足这种要求；使用这些命名格式命名的子树对应于 DIT 子树。在应用中不应检查和识别所有可能的命名格式。如果此扩展标记为关键项，并且证书使用中不能识别用于 base 项的命名格式，应视同遇到未识别的关键项扩展那样来处理此证书。如果此扩展标记为非关键的，并且证书使用中不能识别用于 base 项的命名格式，那么，可忽略此子树规范。当证书主体具有同一

名称形式的多个名称时(在 directory Name 名称形式情况下,包括证书主体项中的名称,如果非“0”),那么,应检验所有这些名称。

可对主体名称或主体替换名称进行限制。只有当确定的名称格式出现时才应用限制。如果证书中没有类型的名称,则证书是可接受的。当对于命名格式限制的一致性测试证书主体名称时,即使扩展中标识为非关键项也应予以处理。

minimum 字段规定了子树内这一区域的上边界。最后的命名形式在规定的级别之上的所有名称不包含在此区域内。等于“0”的 minimum 值对应于此基部,即子树的顶节点。例如,如果 minimum 置为“1”,则命名子树不包含根节点而只包含下级节点。

maximun 字段规定了子树内这一区域的下边界。最后的命名形式在规定的级别之下所有名称不包含在此区域内。最大值“0”对应于此基部,即子树的顶。不存在的 maximun 字段指出不应把下限值施加到子树内的此区域上。例如,如果 maximun 置为“1”,那么,命名子树不包含除子树根节点及其直接下级外的所有节点。

此扩展宜标记为关键项,否则,证书用户不能检验认证路径中的后续证书是否位于签发 CA 指定的命名域中。

如果此扩展存在,并标记为关键的,则证书用户系统应检验所处理的认证路径与此扩展中的值是否一致。

本文件中,任何名称格式都不使用最小和最大字段,最小数总为 0,最大数总是空缺的。

5.2.4.2.14 策略限制(policyConstraints)

策略限制扩展用于向 CA 颁发的证书中。本扩展以两种方式限制路径确认。它可用来禁止策略映射或要求路径中的每个证书包含一个认可的策略标示符。本项定义如下:

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

如果 requireExplicitPolicy 字段存在,并且证书路径包含一个由指定 CA(包含此扩展信息的 CA 或是认证路径中后续 CA)签发的证书,所有在此路径中的证书都应在证书扩展项中包含合适的策略标识符。合适的策略标识符是由用户在证书策略中定义的标识符,或声明通过策略映射与其等价的策略的标识符。

如果 inhibitPolicyMapping 字段存在,它表明在认证路径中从所指定 CA(包含此扩展信息的 CA 或是认证路径中后续 CA)开始直到认证路径结束为止的所有证书中,不准许策略映射。

SkipCerts 类型的值表示在某个限制成为有效之前,应在认证路径中跳过的证书的个数。

此扩展由证书签发者选择是关键的还是非关键的。证书签发者宜标记为关键的。

5.2.4.2.15 证书撤销列表分发点(CRLDistributionPoints)

证书撤销列表分发点扩展用来标识如何获得 CRL 信息,本扩展仅作为证书扩展使用。它可用于认证机构证书,终端实体公钥证书中。本项指定了 CRL 分发点或证书用户的查阅点以确定证书是否已被撤销。证书用户能从可用分发点获得一个 CRL,或者它可从认证机构目录项获得当前完整的 CRL。

该项定义如下:

```
id-ce-CRLDistributionPoints OBJECT IDENTIFIER ::= { id-ce 31 }
cRLDistributionPoits ::= { CRLDistPointsSyntax}
CRLDistPointsSyntax ::= 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 ::= BITSTRING{
    unused                     (0),
    keyCompromise              (1),
    CACompromise               (2),
    affiliationChanged         (3),
    superseded                  (4),
    cessationOfOperation       (5),
    certificateHold             (6)}

```

distributionPoint 字段标识如何能获得 CRL 的位置。如果此字段缺省,分发点名称默认为 CRL 颁发者的名称。

当使用 fullName 或应用默认时,分发点名称可有多种名称形式。同一名称应存在于颁发 CRL 的分发点扩展的 distributionPoint 字段中。证书使用系统可只处理分发点提供的诸多名称形式中的一种。如果不能处理某一分发点的任何名称形式,但能从另一个信任源得到必要的撤销信息,例如,另一个分发点或 CA 目录项,则证书应用系统仍能使用该证书。

如果 CRL 分发点被赋予一个属于 CRL 颁发者的目录名称的目录名,则应只使用 nameRelativeToCRLIssuer 字段。此时,nameRelativeToCRLIssuer 字段是以 CRL 颁发者目录名称相对的可甄别名。

reasons 字段指明由此 CRL 所包含的撤销原因。如果没有 reasons 字段,相应的 CRL 分发点发布应只包含此证书项的 CRL,而不包含撤销原因。否则,reasons 值指明相应的 CRL 分发点所包含的那些撤销原因。

cRLIssuer 字段标识颁发和签署 CRL 的机构。如果没有此字段,CRL 颁发者的名称默认为证书签发者的名称。

此扩展可是关键的或非关键的,由证书颁发者选择,该扩展宜设置为非关键的,但 CA 和应用应支持该扩展。

如果该扩展标记为关键,CA 则要保证分发点包含所用的撤销原因代码 keyCompromise 和/或 cACompromise。若没有首先从一个包含了原因代码 keyCompromise (对终端实体证书)或 cACompromise(对 CA 证书)的指定的分发点检索和核对 CRL,证书使用系统应不使用该证书。在分发点条目为所有撤销原因代码和由 CA(包括作为关键扩展的 cRLDistributionPoint)发布的 CRL 信息的项中,CA 不应在 CA 条目发布一个完整的 CRL。

如果此扩展标记为非关键的,当证书使用系统未能识别此扩展项类型时,则只有在下列情况中,该系统使用此证书:

- 它能从 CA 获得一份完整 CRL 并检查它(通过在 CRL 中设有发布点扩展项来指示最近的 CRL 是完整的);
- 根据本地策略不要求撤销检查;
- 用其他手段完成撤销检查。

注:证书撤销列表 CRL 的应用,见 RFC 5280。

5.2.4.2.16 限制所有策略(**inhibitAnyPolicy**)

本扩展指定了一个限制,它指出了对于从指定 CA(包含这个扩展的证书的主体 CA,或是认证路径中后继认证机构 CA)开始的认证路径中的所有证书的证书策略与 anyPolicy 都是不匹配的。

id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::= {id-ce 54}

InhibitAnyPolicy ::= SkipCerts

SkipCerts ::= INTEGER(0..MAX)

本扩展由证书颁发者选择关键项还是非关键项。宜标记为关键项,否则证书用户可能不能正确地解释认证机构 CA 设定的规则。

5.2.4.2.17 最新证书撤销列表(**freshestCRL**)

最新证书撤销列表扩展用于标识如何获取增量证书撤销列表。

id-ce-CRL freshestCRL OBJECT IDENTIFIER ::= {id-ce 46}

reshestCRL ::= {CRLDistPointsSyntax}

根据证书颁发者的选择,这个扩展可是关键的,也可是非关键的。如果最新的 CRL 扩展是关键的,那么证书使用者在使用证书之前,应首先使用最新 CRL 来验证该证书。如果 freshestCRL 被标记为不关键的,证书使用者可使用本地方法来决定是否检查最新的 CRL。

5.2.4.2.18 个人身份标识码(**identifyCode**)

个人身份号码用于表示个人身份证件的号码,其定义如下:

id-IdentifyCode OBJECT IDENTIFIER ::= {1.2.156.10260.4.1.1.1}

residentifierCardNumber ::= PrintableString

residentifierCardNumber —— 身份证号码

此扩展项标记为非关键的。

id-IdentifyCode OBJECT IDENTIFIER ::= {1.2.156.10260.4.1.1.2}

passportNumber ::= UTF8String

passportNumber —— 护照号码

此扩展项标记为非关键的。

5.2.4.2.19 个人社会保险号(**insuranceNumber**)

个人社会保险号扩展项用于表示个人社会保险号码,其定义如下:

ID-InsuranceNumber OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.2 }

InsuranceNumber ::= PrintableString

此扩展项标记为非关键的。

5.2.4.2.20 企业工商注册号(**iCRegistrationNumber**)

企业工商注册号扩展项用于表示企业工商注册号,其定义如下:

ID-ICRegistrationNumber OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.3 }

ICRegistrationNumber ::= PrintableString

此扩展项标记为非关键的。

5.2.4.2.21 企业组织机构代码(**organizationCode**)

企业组织机构代码号扩展项用于表示企业组织机构代码,其定义如下:

ID-OrganizationCode OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.4 }

OrganizationCode ::= PrintableString

此扩展项标记为非关键的。

5.2.4.2.22 企业税号(taxationNumber)

企业税号扩展项用于表示企业税号码,其定义如下:

ID-TaxationNumber OBJECT IDENTIFIER ::= { 1.2.156.10260.4.1.5 }

TaxationNumber ::= PrintableString

此扩展项标记为非关键的。

5.2.4.2.23 统一社会信用代码(UniformSocialCreditIdentifier)

统一社会信用号扩展项用于每一个法人和其他组织在全国范围内唯一的,终身不变的法定身份识别码,其定义如下:

ID-UniformSocialCreditIdentifier OBJECT IDENTIFIER ::= { 1.2.156.10260.4.4 }

UniformSocialCreditIdentifier ::= PrintableString

此扩展项标记为非关键的。

5.2.4.3 专用因特网扩展(privateInternetExtensions)

5.2.4.3.1 综述

本条定义了两个应用于因特网公钥基础结构的新扩展,用于应用来识别支持 CA 的在线验证服务。其对象标识符如下:

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

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

每个扩展是一个 IA5String 值的序列,每个值分别代表一个 URI。URI 直接确定信息的位置和格式以及获得信息的方式。

5.2.4.3.2 机构信息访问(authorityInfoAccess)

本扩展项描述了包含该扩展的证书的签发者如何访问 CA 的信息以及服务。包括在线验证服务和 CA 策略数据。该扩展可在用户证书和 CA 证书中,且应为非关键的。

id-pe- authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }

AuthorityInfoAccessSyntax ::=

SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE {

 accessMethod OBJECT IDENTIFIER,

 accessLocation GeneralName }

id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }

id-ad-caIssuers OBJECT IDENTIFIER ::= { id-ad 2 }

id-ad-ocsp OBJECT IDENTIFIER ::= { id-ad 1 }

序列 AuthorityInfoAccessSyntax 表示颁发含有该扩展的证书的 CA 附加信息格式和位置。信息的类型和格式由 accessMethod 字段说明;信息的位置由 accessLocation 字段说明。检索机制可由 ac-

cessMethod 表明或由 accessLocaion 说明。

定义用于 accessMethod 的两个 OID, id-ad-caIssuers 和 id-ad-ocsp。id-ad-caIssuers 用于获取 CA 证书, id-ad-ocsp 用于获取 OCSP 服务地址。

当 id-ad-caIssuers 以 accessInfoType 出现时, accessLocaion 字段说明参考的描述服务器及获得参考描述的访问协议。AccessLocaion 字段定义为 GeneralName, 它可有几种形式: 当信息可通过 http, ftp 或 ldap 获得时, accessLocaion 应是一个 uniformResourceIdentifier 类型。当信息可通过目录访问协议获得时, accessLocaion 应是一个 directoryName 类型。当信息可通过电子邮件获得时, accessLocaion 应是一个 rfc822Name 类型。

5.2.4.3.3 主体信息访问(subjectInformationAccess)

本扩展描述了证书主体如何访问信息和服务。如果主体是 CA, 则包括证书验证服务和 CA 策略的数据。主体是用户, 则包括提供的服务的类型以及如何访问它们, 在这种情况下, 扩展域/项中的内容在所支持的服务的协议的说明中定义。这个扩展项应被定义为非关键的。

id-pe-SubjectInformationAccess OBJECT IDENTIFIER ::= { id-pe 11 }

SubjectInfoAccessSyntax ::=

SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE {

accessMethod OBJECT IDENTIFIER,

accessLocation GeneralName }

5.3 CRL 格式

5.3.1 综述

本文件按照 GB/T 16262.1 中定义的特定编码规则(DER)对下列证书撤销列表项中的各项信息进行编码, 组成特定的证书撤销列表数据结构。

5.3.2 CRL 的数据结构

CRL 数据结构的 ASN.1 编码形式如下:

CertificateList ::= SEQUENCE {

tbsCertList TBSCertList,

signatureAlgorithm AlgorithmIdentifier,

signatureValue BIT STRING

}

TBSCertList ::= SEQUENCE {

version Version OPTIONAL,
——如果出现, 应是 v2

signature AlgorithmIdentifier,

issuer Name,

thisUpdate Time,

nextUpdate Time OPTIONAL,

revokedCertificates SEQUENCE OF SEQUENCE {

userCertificate CertificateSerialNumber,

revocationDate Time,

```

        crlEntryExtensions      Extensions OPTIONAL
                                ——如果出现,version 应是 v2
    } OPTIONAL,
    crlExtensions                [0] EXPLICIT Extensions OPTIONAL
                                ——如果出现,version 应是 v2
}

```

上述的 CRL 数据结构由 tbsCertList、signatureAlgorithm 和 signatureValue 三个域构成。这些域的含义如下所述。

- tbsCertList 域包含了版本、签名算法、颁发者、生效日期、下次更新日期、被撤销的证书列表和 CRL 的扩展项。
- signatureAlgorithm 域包含 CA 签发该 CRL 所使用的算法标识符。一个算法标识符的 ASN.1 编码形式如下：

```

AlgorithmIdentifier ::= SEQUENCE
{
    algorithm      OBJECT IDENTIFIER,
    parameters    ANY DEFINED BY algorithm OPTIONAL
}

```

其中 algorithm 是算法标识符,标识了具体的算法。parameters 是可选参数,依赖于所标识的算法。该域中 algorithm 标识的算法应与 tbsCertList 域中 signature 标识的签名算法相同。如果签名算法为 SM2,则 parameters 的值为空。

- signatureValue 域包含了对 tbsCertList 域进行数字签名的结果。采用 ASN.1 DER 编码的 tbsCertList 域作为数字签名的输入,签名的结果按照 ASN.1 BITSTRING 类型编码,并保存在 CRL 签名值域内。如果签名算法为 SM2 密码算法,则签名数据格式应遵循 GM/T 0009。

5.3.3 TBSCertList 数据结构

5.3.3.1 版本(version)

本可选项描述了编码 CRL 的版本号。如果 crlExtensions 项存在,则此项应存在,且其值应是 v2 (用整数 1 表示)。

5.3.3.2 签名算法(signature)

本项包含 CA 签发该 CRL 所使用的密码算法的标识符,这个算法标识符应与 CertificateList 中 signatureAlgorithm 项的算法标识符相同。

5.3.3.3 颁发者(issuer)

本项标识了签名和颁发 CRL 的实体。它应包含一个非空的甄别名称(DN——distinguished name)。该项被定义为 Name 类型。

issuer 的编码规则同 5.2.3.4。

5.3.3.4 生效日期(thisUpdate)

本项标明了 CRL 的颁发日期,使用 UTCTime 或 GeneralizedTime 类型编码。

在 2049 年之前(包括 2049 年)颁发的 CRL,时间值应采用 UTCTime 类型编码,在 2050 年之后颁发的 CRL,时间值应采用 GeneralizedTime 类型编码。

UTCTime 的编码规则同 5.2.3.5.3。

GeneralizedTime 的编码规则同 5.2.3.5.4。

5.3.3.5 下次更新日期(nextUpdate)

本项标明了下一次 CRL 将要发布的时间。下一次 CRL 可在此时间前签发,但不能晚于此时间签发。使用 UTCTime 或 GeneralizedTime 编码。

CRL 颁发者应在签发的 CRL 中包含 nextUpdate 项。

对于在 2049 年之前(包括 2049 年)颁发的 CRL,应将时间编码为 UTCTime 类型;在 2050 年之后颁发的 CRL,应将时间编码为 GeneralizedTime 类型。

UTCTime 的编码规则同 5.2.3.5.3。

GeneralizedTime 的编码规则同 5.2.3.5.4。

5.3.3.6 被撤销的证书列表(Revoked Certificates)

本项表明被撤销证书的序列号、撤销时间和证书撤销列表条目扩展项。

当没有被撤销的证书时,此项不存在,否则应在本项中包含被撤销证书的序列号,并标明撤销的日期。

5.3.3.7 扩展项(crlExtensions)

本项只可在 v2 版本的 CRL 中出现。本项由一个或多个 CRL 扩展的序列组成。

crlExtensions 在 5.3.4 描述。

5.3.4 CRL 扩展项

5.3.4.1 颁发机构密钥标识符(authorityKeyIdentifier)

本项提供了一种识别与 CRL 签名私钥相应的公钥的方式。当颁发者拥有多个密钥或由于发生变化而具有多个签名密钥时,使用该扩展。

5.3.4.2 颁发者替换名称(issuerAltName)

本项包含一个或多个替换名称,以供 CRL 颁发者使用。

本扩展项应为非关键的。

5.3.4.3 证书撤销列表号(crlNumber)

对于 CRL 颁发者,在其依次颁发的一系列 CRL 中,本项表示的值可构成一个单调递增序列。本项可让用户方便地确定一个特定的 CRL 何时取代另一个 CRL。证书撤销列表号宜支持区分完整 CRL 和增量 CRL。本项是一个非关键的 CRL 扩展。

如果 CRL 颁发者在一个特定范围内除了生成完整 CRL 之外,还生成了增量 CRL,完整 CRL 和增量 CRL 应采用同一个编号。如果完整 CRL 和增量 CRL 在同一时间被颁发,它们应使用相同的证书撤销列表号,并提供相同的撤销信息。

如果 CRL 颁发者在一个特定范围内的不同时间生成两个 CRL(可能是两个完整 CRL,或两个增量 CRL,或一个完整 CRL 和一个增量 CRL),即两个 CRL 的 thisUpdate 域不同,此时这两个 CRL 不能使用相同的证书撤销列表号。

CRL 验证者应能处理 20 个字节长的证书撤销列表号。CRL 颁发者应使用不大于 20 字节长的证书撤销列表号。

id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }

CRLNumber ::= INTEGER (0..MAX)

5.3.4.4 增量证书撤销列表指示(delta CRL Indicator)

本项用于标识一个 CRL 是增量 CRL。增量 CRL 包含上次发布之后要新添加的证书撤销信息,而不是将所有的撤销信息包含在一个完整 CRL 里。本项应标记成关键。

本项扩展包含一个类型为 BaseCRLNumber 的值。证书撤销列表号标识了此增量 CRL 使用的起始基准 CRL。CRL 颁发者应以完整 CRL 形式颁发基准 CRL,增量 CRL 中应包含所有的更新撤销信息。增量 CRL 和参考基准 CRL 的组合等效于完整 CRL。

id-ce-deltaCRLIndicator OBJECT IDENTIFIER ::= { id-ce 27 }

BaseCRLNumber ::= CRLNumber

5.3.4.5 颁发分发点(issuing Distribution Point)

本项表示一个特定 CRL 的分发点和范围,以及 CRL 中是否仅包含了用户证书的撤销信息、CA 证书的撤销信息或者一系列的原因代码。本项应标记成关键。

id-ce-issuingDistributionPoint OBJECT IDENTIFIER ::= { id-ce 28 }

IssuingDistributionPoint ::= SEQUENCE {

distributionPoint	[0] DistributionPointName OPTIONAL,
onlyContainsUserCerts	[1] BOOLEAN DEFAULT FALSE,
onlyContainsCACerts	[2] BOOLEAN DEFAULT FALSE,
onlySomeReasons	[3] ReasonFlags OPTIONAL,
indirectCRL	[4] BOOLEAN DEFAULT FALSE,
onlyContainsAttributeCerts	[5] BOOLEAN DEFAULT FALSE }

5.3.4.6 最新证书撤销列表(freshest CRL)

本项标识完整 CRL 中的增量 CRL 信息如何获取。本项应标记成非关键。此项不在增量 CRL 中出现。

本项的格式同 5.2.4.2.15,但应略去其中的 reasons 和 cRLIssuer 域。

id-ce-freshestCRL OBJECT IDENTIFIER ::= { id-ce 46 }

FreshestCRL ::= CRLDistributionPoints

5.3.4.7 证书撤销列表条目(CRL Entry)

5.3.4.7.1 原因代码(reason Code)

本项表明证书撤销的原因,应标记为非关键扩展。

原因代码 removeFromCRL (8)仅用于增量 CRL。其他原因代码可用于任意 CRL。

id-ce-cRLReasons OBJECT IDENTIFIER ::= { id-ce 21 }

——reasonCode ::= { CRLReason }

CRLReason ::= ENUMERATED {

unspecified	(0),
keyCompromise	(1),
cACompromise	(2),
affiliationChanged	(3),

superseded	(4),
cessationOfOperation	(5),
certificateHold	(6),
——7 不使用	
removeFromCRL	(8),
privilegeWithdrawn	(9),
aACompromise	(10) }

5.3.4.7.2 撤销时间(**invalidity Date**)

本项表示确认或怀疑私钥泄露或证书失效的时间,应标记为非关键扩展。

本项包含的 GeneralizedTime 应使用格林威治标准时间,应按照 5.2.3.5.3 的要求表示。

id-ce-invalidityDate OBJECT IDENTIFIER ::= { id-ce 24 }

InvalidityDate ::= GeneralizedTime

5.3.4.7.3 证书颁发者(**certificate Issuer**)

本项用于间接 CRL,表示证书的颁发者名。如果在间接 CRL 中,第一个条目不包含本扩展,则证书颁发者是 CRL 颁发者,后续的条目如果不包含本扩展,则证书颁发者是前一条目的证书颁发者。

本项应标记为关键扩展。

id-ce-certificateIssuer OBJECT IDENTIFIER ::= { id-ce 29 }

CertificateIssuer ::= GeneralNames

本文件附录 A 中规定了证书的结构,附录 B 中规定了数字证书的结构实例,并规定了数据项是否为关键项,附录 C 中规定了目前通用的数字证书结构,附录 D 中提供了数字证书的编码示例。

附录 A
(规范性)
证书结构

A.1 证书构成

证书的构成见表 A.1。

表 A.1 证书结构

基本证书域(TBSCertificate)
签名算法域(signatureAlgorithm)
签名值域(signatureValue)

A.2 基本证书域

基本证书域见表 A.2。

表 A.2 基本证书域

项名称	描述	备注
version	版本	
serialNumber	序列号	
signature	签名算法	
issuer	颁发者	
validity	有效日期	
Subject	主体	—
subjectPublicKeyInfo	主体公钥信息	—
issuerUniqueID	颁发者唯一标识符	本文件中不使用
subjectUniqueID	主体唯一标识符	本文件中不使用
extensions	扩展项	按本文件的扩展项进行定义,见 A.3

A.3 标准的扩展域

标准的扩展域见表 A.3。

表 A.3 标准的扩展域

名称	描述	关键度
authorityKeyIdentifier	颁发机构密钥标识符	非关键
subjectKeyIdentifier	主体密钥标识符	非关键
keyUsage	密钥用法	关键

表 A.3 标准的扩展域 (续)

名称	描述	关键度
extKeyUsage	扩展密钥用途	如果密钥的用法只限于所指示的用途时标记为关键,否则标记为非关键
privateKeyUsagePeriod	私有密钥使用期	非关键
certificatePolicies	证书策略	非关键
policyMappings	策略映射	如果证书用户需要正确解释发布的 CA 设定的规则时标识为关键,否则标识为非关键
subjectAltName	主体可选替换名称	非关键
issuerAltName	颁发者可选替换名称	非关键
subjectDirectoryAttributes	主体目录属性	非关键
basicConstraints	基本限制	CA 证书标记为关键,终端实体证书标记为非关键
nameConstraints	名称限制	如果证书用户系统应检验所处理的认证路径与此扩展中的值是否一致时标记为关键,否则标记为非关键
policyConstraints	策略限制	如果证书用户需要正确地解释认证机构 CA 设定的规则时标识为关键,否则标识为非关键
CRLDistributionPoints	CRL 分发点	非关键
inhibitAnyPolicy	限制所有策略	如果证书用户需要正确地解释认证机构 CA 设定的规则时标识为关键,否则标识为非关键
freshestCRL	最新的 CRL	非关键
authorityInfoAccess	机构信息访问	非关键
SubjectInformationAccess	主体信息访问	非关键
IdentifyCardNumber	个人身份标识码	非关键
InsuranceNumber	个人社会保险号	非关键
ICRegistrationNumber	企业工商注册号	非关键
OrganizationCode	企业组织机构代码	非关键
TaxationNumeber	企业税号	非关键
UniformSocialCreditIdentifier	统一社会信用代码	非关键

附 录 B
(规范性)
证书的结构实例

B.1 用户证书的结构实例

用户证书的结构实例见表 B.1。

表 B.1 用户证书的结构实例

版本(version)	
序列号(serialNumber)	
签名算法(signature)	
颁发者(issuer)	
有效期(Validity)	起始有效期
	终止有效期
主体(subject)	国家(countryName)
	省份(stateOrProvinceName)
	地市(localityName)
	组织名称(organizationName)
	机构名称(organizationalUnitName)
	用户名称(CommonName)
主体公钥信息(subjectPublicKeyInfo)	
颁发机构的密钥标识(authorityKeyIdentifier)	
主体密钥标识符 subjectKeyIdentifier	
密钥用法(KeyUsage)	
CRL 分发点 CRLDistributionPoints	

B.2 服务器证书的结构实例

服务器证书的结构实例见表 B.2。

表 B.2 服务器证书的结构实例

版本(version)	
序列号(serialNumber)	
签名算法(signature)	
颁发者(issuer)	
有效期(Validity)	起始有效期
	终止有效期
主体(subject)	国家(countryName)
	省份(stateOrProvinceName)
	地市(localityName)
	组织名称(organizationName)
	机构名称(organizationalUnitName)
	服务器名称(CommonName)
主体公钥信息(subjectPublicKeyInfo)	
颁发机构的密钥标识(authorityKeyIdentifier)	
主体密钥标识符(subjectKeyIdentifier)	
密钥用法(KeyUsage)	
SAN 主体替换名称(subjectAlternativeName)	
CRL 分发点(CRLDistributionPoints)	

附 录 C

(规范性)

证书内容表

C.1 通则

本附录定义了一系列证书内容表。每个表定义了一个特别类型证书或证书撤销列表的证书内容。并且在签发者属性中,包含了在 PKI 体系中被广泛支持的可选特征。在实际应用中,证书和证书撤销列表中可包括局部应用中非关键扩展信息,但是 PKI 客户端可不去处理这些额外信息。另外,对于未列在工作表中的关键扩展,不应在 PKI 证书或证书撤销列表内容中使用。

证书内容表包括以下内容。

- a) 自签名 CA 证书内容表,即根证书内容工作表,定义了自签名证书强制和可选的内容。当确认一个信任根时,PKI 体系中的 CA 发布自签名证书。
- b) 二级 CA 证书内容表,定义了二级 CA 证书的强制和可选内容。
- c) 终端实体签名证书内容表,定义了 CA 颁发的实体签名证书的强制和可选内容,其对象是一终端实体,其私钥用于签名,其公钥用于验证签名,该证书的密钥对签发时在客户端生成,为用户所私有,其私钥在终端介质中应不能导出。
- d) 终端实体加密证书内容表,它定义了由 PKI 体系中 CA 颁发的实体加密证书的强制和可选内容。其公钥用于加密数据,私钥用于解密数据。密钥由密钥管理中心(KM)分发,其生命周期受密钥管理中心控制,在证书有效期内,在介质损坏的情况下,可通过正常的流程通过 CA 中心进行恢复。
- e) 证书撤销列表内容表,其定义了由证书撤销列表签发者发布的证书撤销列表的强制和可选内容。

对于终端实体签名证书和加密证书,它们应总是成对出现,其生命周期由 CA 中心进行管理。对于既用作签名,又用于加密的单张终端实体证书,由于其安全和可管理性存在问题,因此不宜使用。

C.2 自签名 CA 证书内容表

自签名 CA 证书内容表见表 C.1。

表 C.1 基本证书域结构

域	关键项标识	值	描述
Certificate	—	—	—
signature	—	—	—
AlgorithmIdentifier	—	—	应与 signatureAlgorithm 域匹配
algorithm	—	选择下列算法	
		1.2.156.10197.1.501	SM3WithSM2Encryption
		1.2.840.113549.1.1.11	sha256WithRSAEncryption
parameters	—	NULL	当为 SM2 密码算法时,此项不需要
tbsCertificate	—	—	待签名内容
version	—	2	整数 2 用于版本 3 证书

表 C.1 基本证书域结构（续）

域	关键项标识	值	描述
serialNumber	—	INTEGER	唯一正整数, 见 5.2.3.2
issuer	—	—	—
Name	—	—	应与主题 DN 一致
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	见 5.2.3.4
validity	—	—	—
NotBefore	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
NotAfter	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
subject	—	—	—
Name	—	—	应与主题 DN 一致
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	见 5.2.3.4
subjectPublicKeyInfo	—	—	—
algorithm	—	—	—
AlgorithmIdentifier	—	—	公钥算法, RSA 公钥或椭圆曲线公钥
algorithm	—	1.2.840.113549.1.1.1	RSA
		1.2.840.10045.2.1	Id-ecPublicKey
		1.2.156.10197.1.301	SM2 椭圆曲线公钥密码算法
parameters	—	NULL	RSA
	—	ECPublicKeySpec	当使用 SM2 密码算法时, 为 SM2 密码算法曲线的 OID

表 C.1 基本证书域结构 (续)

域	关键项标识	值	描述
subjectPublicKey	—	BIT STRING	对 RSA 算法, 模长至少应是 2048 位, 对 SM2 算法, 公钥至少 256 位
必须的扩展	—	—	—
subjectKeyIdentifier	FALSE	—	主题密钥标识符, 用于证书路径查询
keyIdentifier	—	OCTET STRING	公钥值的 SM3 哈希算法摘要
subjectInfoAccess	FALSE	—	对象信息存储包括一系列访问方法。只有一种存储方法被定义为 CA 证书中
AccessDescription	—	—	—
accessMethod	—	id-ad-caRepository (1.3.6.1.5.5.7.48.5)	自签名证书至少要包括存储方法一个实例, 这种存储方法包括 URI 名字形成 LDAP 访问目录服务器的指定位置。证书也可包括 URI 名字形成指定 HTTP 访问 WEB 服务器。每一个 URI 应指向 CA 证书的位置
accessLocation	—	—	—
GeneralName	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
basicConstraints	TRUE	—	—
cA	—	TRUE	—
KeyUsage	TRUE	—	—
数字签名(digitalSignature)	—	0	—
防抵赖(nonRepudiation)	—	0	—
密钥加密(keyEncipherment)	—	0	—
数据加密(dataEncipherment)	—	0	—
密钥协议(keyAgreement)	—	0	—
证书签发(KeyCertSign)	—	1	—
黑名单签名(CRLSign)	—	1	—
仅加密(encipherOnly)	—	0	—
仅解密(decipherOnly)	—	0	—
可选扩展	—	—	—
issuerAltName	—	—	任何名字类型都可以, 但只有最常用的名称才在这里加入

表 C.1 基本证书域结构 (续)

域	关键项标识	值	描述
GeneralNames	—	—	—
GeneralName	—	—	—
rfc822Name	—	IA5String	PKI 管理机构的电子邮件地址

C.3 下级 CA 证书内容表

下级 CA 证书内容表见表 C.2。

表 C.2 下级 CA 证书内容表

域	关键项标识	值	描述
Certificate	—	—	—
signature	—	—	—
AlgorithmIdentifier	—	—	应与 signatureAlgorithm 域匹配
algorithm	—	选择下列算法	algorithm
		1.2.156.10197.1.501	SM3WithSM2Encryption
		1.2.840.113549.1.1.11	sha256WithRSAEncryption
parameters	—	NULL	当为 SM2 算法时,此项不需要
tbsCertificate	—	—	待签名内容
version	—	2	整数 2 用于版本 3 证书
serialNumber	—	INTEGER	唯一正整数
issuer	—	—	—
Name	—	—	应与发行者主题 DN 一致
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
validity	—	—	—
NotBefore	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
NotAfter	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)

表 C.2 下级 CA 证书内容表 (续)

域	关键项标识	值	描述
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
subject	—	—	—
Name	—	—	—
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
subjectPublicKeyInfo	—	—	—
algorithm	—	—	—
AlgorithmIdentifier	—	—	公钥算法, RSA 公钥或椭圆曲线公钥
algorithm	—	1.2.840.113549.1.1.1	RSA
		1.2.840.10045.2.1	Id-ecPublicKey
		1.2.156.10197.1.301	SM2 椭圆曲线公钥密码算法
parameters	—	NULL	RSA
		ECPublicKeySpec	SM2 算法曲线的 OID
subjectPublicKey	—	BIT STRING	对 RSA 算法, 模长至少应是 2048 位, 对 SM2 算法, 公钥至少 256 位
必须的扩展	—	—	—
authorityKeyIdentifier	FALSE	—	签发者密钥标识符
keyIdentifier	—	OCTET STRING	签发者公钥值的 SM3 摘要值
subjectKeyIdentifier	FALSE	—	主题密钥标识符用于证书路径查询
keyIdentifier	—	OCTET STRING	公钥值的 SM3 哈希算法摘要
basicConstraints	TRUE	—	—
CA	—	TRUE	—
KeyUsage	TRUE	—	—
数字签名(digitalSignature)	—	0	—
防抵赖(nonRepudiation)	—	0	—
密钥加密(keyEncipherment)	—	0	—
数据加密(dataEncipherment)	—	0	—
密钥协议(keyAgreement)	—	0	—
证书签发(KeyCertSign)	—	1	—

表 C.2 下级 CA 证书内容表 (续)

域	关键项标识	值	描述
黑名单签名(CRLSign)	—	1	—
仅加密(encipherOnly)	—	0	—
仅解密(decipherOnly)	—	—	—
certificatePolicies	—	—	—
PolicyInformation	—	—	—
policyIdentifier	—	OID	The inclusion of policy qualifiers is discouraged
CRLDistributionPoints	—	—	—
DistributionPoint	—	—	—
distributionPoint	—	—	—
DistributionPointName	—	—	—
fullName	—	—	—
GeneralNames	—	—	—
GeneralName	—	—	—
directoryName	—	—	—
Name	—	—	—
RDNSSequence	—	—	—
RelativeDistinguished	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
uniformResourceIdentifier	—	—	采用“ldap:”或者“http://”形式
authorityInfoAccess	FALSE	—	—
AccessDescription	—	—	访问方法一
accessMethod	—	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	—
accessLocation	—	—	—
GeneralName	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
AccessDescription	—	—	访问方法二
accessMethod	—	id-ad-ocsp (1.3.6.1.5.5.7.48.1)	—
accessLocation	—	—	—
GeneralName	—	—	—

表 C.2 下级 CA 证书内容表 (续)

域	关键项标识	值	描述
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
subjectInfoAccess	FALSE	—	对象信息存储包括一系列访问方法。只有一种存储方法被定义为 CA 证书中
AccessDescription	—	—	—
accessMethod	—	id-ad-caRepository (1.3.6.1.5.5.7.48.5)	自签名证书至少要包括存储方法一个实例,这种存储方法包括 URI 名字形成 LDAP 访问目录服务器的指定位置。证书也可包括 URI 名字形成指定 HTTP 访问 WEB 服务器。每一个 URI 应指向 CA 证书的位置
accessLocation	—	—	—
GeneralName	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
可选扩展	—	—	—
issuerAltName	FALSE	—	任何名字类型都可以,但只有最通用的名称才在这里加入
GeneralNames	—	—	—
GeneralName	—	—	—
rfc822Name	—	IA5String	PKI 管理机构的电子邮件地址
FreshestCRL	FALSE	—	使用增量黑名单方式才有此扩展
DistributionPoint	—	—	—
distributionPoint	—	—	—
DistributionPointName	—	—	—
fullName	—	—	—
GeneralNames	—	—	—
GeneralName	—	—	—
directoryName	—	—	—
Name	—	—	—
RDNSSequence	—	—	—
RelativeDistinguished	—	—	—
AttributeTypeAndV	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式

C.4 终端实体签名证书内容表

终端实体签名证书内容表见表 C.3。

表 C.3 终端实体签名证书内容表

域	关键项标识	值	描述
Certificate	—	—	—
signature	—	—	—
AlgorithmIdentifier	—	—	应与 signatureAlgorithm 域匹配
algorithm	—	1.2.156.10197.1.501	选择下列算法 SM3WithSM2Encryption
		1.2.840.113549.1.1.11	sha256WithRSAEncryption
parameters	—	NULL	—
tbsCertificate	—	—	待签名内容
version	—	2	整数 2 用于版本 3 证书
serialNumber	—	INTEGER	唯一正整数
issuer	—	—	—
Name	—	—	应与发行者主题 DN 一致
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
validity	—	—	—
NotBefore	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
NotAfter	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
subject	—	—	—
Name	—	—	—
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—

表 C.3 终端实体签名证书内容表 (续)

域	关键项标识	值	描述
AttributeType	—	OID	—
AttributeValue	—	—	—
subjectPublicKeyInfo	—	—	—
algorithm	—	—	—
AlgorithmIdentifier	—	—	公钥算法, RSA 公钥或椭圆曲线公钥
algorithm	—	1.2.840.113549.1.1.1	RSA
		1.2.840.10045.2.1	Id-ecPublicKey
		1.2.156.10197.1.301	SM2 椭圆曲线公钥密码算法
parameters	—	NULL	RSA
		ECPublicKeySpec	SM2 算法曲线的 OID
subjectPublicKey	—	BIT STRING	对 RSA 算法, 模长至少应是 2048 位, 对 SM2 算法, 公钥至少 256 位
必须的扩展	—	—	—
authorityKeyIdentifier	FALSE	—	签发者密钥标识符
keyIdentifier	—	OCTET 字符串	签发者公钥值的 SM3 哈希算法摘要
subjectKeyIdentifier	FALSE	—	主题密钥标识符, 用于证书路径查询
keyIdentifier	—	OCTET 字符串	公钥值的 SM3 哈希算法摘要
KeyUsage	TRUE	—	—
数字签名(digitalSignature)	—	1	—
防抵赖(nonRepudiation)	—	1	—
密钥加密(keyEncipherment)	—	0	—
数据加密(dataEncipherment)	—	0	—
密钥协议(keyAgreement)	—	0	—
证书签发(KeyCertSign)	—	0	—
黑名单签名(CRLSign)	—	0	—
仅加密(encipherOnly)	—	0	—
仅解密(decipherOnly)	—	—	—
certificatePolicies	FALSE	—	—
PolicyInformation	—	—	—
policyIdentifier	—	OID	The inclusion of policy qualifiers is discouraged

表 C.3 终端实体签名证书内容表 (续)

域	关键项标识	值	描述
CRLDistributionPoints	—	—	—
DistributionPoint	—	—	—
distributionPoint	—	—	—
DistributionPointName	—	—	—
fullName	—	—	—
GeneralNames	—	—	—
GeneralName	—	—	—
directoryName	—	—	—
Name	—	—	—
RDNSequence	—	—	—
RelativeDistinguished	—	—	—
AttributeTypeAndV	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
authorityInfoAccess	FALSE	—	—
AccessDescription	—	—	访问方法一
accessMethod	—	id-ad-caIssuers (1.3.6.1.5.5.7.48.2)	—
accessLocation	—	—	—
GeneralName	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
AccessDescription	—	—	访问方法二
accessMethod	—	id-ad-ocsp (1.3.6.1.5.5.7.48.1)	—
accessLocation	—	—	—
GeneralName	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
可选扩展	—	—	—
extKeyUsage	BOOLEAN	—	扩展密钥用法
KeyPurposeId	—	OID	—
issuerAltName	FALSE	—	任何名字类型都可以,但只有最通用的被名称才在这里加入
GeneralNames	—	—	—

表 C.3 终端实体签名证书内容表（续）

域	关键项标识	值	描述
GeneralName	---	---	---
rfc822Name	---	IA5String	PKI 管理机构的电子邮件地址
subjectAltName	FALSE	---	---
GeneralNames	---	---	---
GeneralName	---	---	---
rfc822Name	---	IA5String	---
dNSName	---	IA5String	---
iPAddress	---	IA5String	---
directoryName	---	---	---
Name	---	---	---
RDNSSequence	---	---	---
RelativeDistinguished	---	---	---
AttributeTypeAndV	---	---	---
AttributeType	---	OID	---
AttributeValue	---	---	---
FreshestCRL	FALSE	---	使用增量黑名单方式才有此扩展
DistributionPoint	---	---	---
distributionPoint	---	---	---
DistributionPointName	---	---	---
fullName	---	---	---
GeneralNames	---	---	---
GeneralName	---	---	---
directoryName	---	---	---
Name	---	---	---
RDNSSequence	---	---	---
RelativeDistinguished	---	---	---
AttributeTypeAndV	---	---	---
AttributeType	---	OID	---
AttributeValue	---	---	---
uniformResourceIdentifier	---	---	采用“ldap://”或者“http://”形式

C.5 终端实体加密证书内容表

终端实体加密证书内容表见表 C.4。

表 C.4 终端实体加密证书内容表

域	关键项标识	值	描述
Certificate	—	—	—
signature	—	—	—
AlgorithmIdentifier	—	—	应与 signatureAlgorithm 域匹配
algorithm	—	选择下列算法	
		1.2.156.10197.1.501	SM3WithSM2Encryption
		1.2.840.113549.1.1.11	sha256WithRSAEncryption
parameters	—	NULL	—
tbsCertificate	—	—	待签名内容
version	—	2	整数 2 用于版本 3 证书
serialNumber	—	INTEGER	唯一正整数
issuer	—	—	—
Name	—	—	应与发行者主题 DN 一致
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
validity	—	—	—
NotBefore	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
NotAfter	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
subject	—	—	—
Name	—	—	—
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
subjectPublicKeyInfo	—	—	—

表 C.4 终端实体加密证书内容表 (续)

域	关键项标识	值	描述
algorithm	---	---	---
AlgorithmIdentifier	---	---	公钥算法, RSA 公钥或椭圆曲线公钥
algorithm	---	1.2.840.113549.1.1.1	RSA
		1.2.840.10045.2.1	Id-ecPublicKey
		1.2.156.10197.1.301	SM2 椭圆曲线公钥密码算法
parameters	---	NULL	RSA
		ECPublicKeySpec	SM2 算法曲线的 OID
subjectPublicKey	---	BIT STRING	对 RSA 算法, 模长至少应是 2048 位, 对 SM2 算法, 公钥至少 256 位
必须的扩展	---	---	---
authorityKeyIdentifier	FALSE	---	签发者密钥标识符
keyIdentifier	---	OCTET 字符串	签发者公钥值的 SM3 哈希算法摘要
subjectKeyIdentifier	FALSE	---	主题密钥标识符, 用于证书路径查询
keyIdentifier	---	OCTET 字符串	公钥值的 SM3 哈希算法摘要
KeyUsage	TRUE	---	---
数字签名 (digitalSignature)	---	0	---
防抵赖 (nonRepudiation)	---	0	---
密钥加密 (keyEncipherment)	---	1	---
数据加密 (dataEncipherment)	---	1	---
密钥协议 (keyAgreement)	---	1	---
证书签发 (KeyCertSign)	---	0	---
黑名单签名 (CRLSign)	---	0	---
仅加密 (encipherOnly)	---	0	---
仅解密 (decipherOnly)	---	0	---
certificatePolicies	FALSE	---	---
PolicyInformation	---	---	---
policyIdentifier	---	OID	The inclusion of policy qualifiers is discouraged
CRLDistributionPoints	---	---	---
DistributionPoint	---	---	---
distributionPoint	---	---	---

表 C.4 终端实体加密证书内容表 (续)

域	关键项标识	值	描述
DistributionPointName	—	—	—
fullName	—	—	—
GeneralNames	—	—	—
GeneralName	—	—	—
directoryName	—	—	—
Name	—	—	—
RDNSequence	—	—	—
RelativeDistinguished	—	—	—
AttributeTypeAndV	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
authorityInfoAccess	FALSE	—	—
AccessDescription	—	—	访问方法一
accessMethod	—	ad-ad-caIssuers (1.3.6.1.5.5.7.48.2)	—
accessLocation	—	—	—
GeneralName	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
AccessDescription	—	—	访问方法二
accessLocation	—	—	—
GeneralName	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
可选扩展	—	—	—
extKeyUsage	BOOLEAN	—	扩展密钥用法
KeyPurposeId	—	OID	—
issuerAltName	FALSE	—	任何名字类型都可以,但只有最通用的被名称才在这里加入
GeneralNames	—	—	—
GeneralName	—	—	—
rfc822Name	—	IA5String	PKI 管理机构的电子邮件地址
subjectAltName	FALSE	—	—
GeneralNames	—	—	—
GeneralName	—	—	—

表 C.4 终端实体加密证书内容表 (续)

域	关键项标识	值	描述
rfc822Name	---	IA5String	---
dNSName	---	IA5String	---
iPAddress	---	IA5String	---
directoryName	---	---	---
Name	---	—	---
RDNSequence	---	—	---
RelativeDistinguished	---	---	---
AttributeTypeAndV	---	—	---
AttributeType	---	OID	---
AttributeValue	---	---	---
FreshestCRL	FALSE	---	使用增量黑名单方式才有此扩展
DistributionPoint	---	---	---
distributionPoint	---	---	---
DistributionPointName	---	---	---
fullName	---	---	---
GeneralNames	---	---	---
GeneralName	---	---	---
directoryName	---	---	---
Name	---	---	---
RDNSequence	---	---	---
RelativeDistinguished	---	---	---
AttributeTypeAndV	---	---	---
AttributeType	---	OID	---
AttributeValue	---	---	---
uniformResourceIdentifier	---	---	采用“ldap://”或者“http://”形式

C.6 证书撤销列表内容表

证书撤销列表内容表见表 C.5。

表 C.5 证书撤销列表内容表

域	关键项标识	值	描述
CertificateList	—	—	—
signature	—	—	—
AlgorithmIdentifier	—	—	应与 signatureAlgorithm 域匹配
algorithm	—	选择下列算法	
		1.2.156.10197.1.501	SM3WithSM2Encryption
		1.2.840.113549.1.1.11	sha256WithRSAEncryption
parameters	—	NULL	—
tbsCertList	—	—	待签名内容
version	—	2	版本 2(整数 1)
issuer	—	—	—
Name	—	—	应与发行者主题 DN 一致
RDNSequence	—	—	—
RelativeDistinguishedName	—	—	—
AttributeTypeAndValue	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
thisUpdate	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
nextUpdate	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
revokedCertificates	—	—	—
userCertificate	—	INTEGER	被撤销证书的序列号
revocationDate	—	—	—
Time	—	—	—
UtcTime	—	YYMMDDHHMMSSZ	用于 2049 之前的年份(含 2049)
generalTime	—	YYYYMMDDHHMMSSZ	用于 2049 之后的年份
crlEntryExtensions	—	—	—
Extensions	—	—	—
reasonCode	FALSE	—	废除原因

表 C.5 证书撤销列表内容表 (续)

域	关键项标识	值	描述
CRLReason	---	---	主要使用的原因包括:keyCompromise 密钥泄露、CACompromise CA 泄露、affiliationChanged、superseded 或 cessationOfOperation。如果废除原因未知,则无此扩展项。removeFromCRL 只能用于增量 CRL 中,关于证书冻结 certificateHold 不宜使用
invalidityDate	FALSE	---	---
GeneralizedTime	---	YYYYMMDDHHMMSSZ	---
certificateIssuer	FALSE	---	---
GeneralNames	---	---	---
GeneralName	---	---	---
rfc822Name	---	IA5String	PKI 管理机构的电子邮件地址
crlExtensions	---	---	---
Extensions	---	---	---
authorityKeyIdentifier	FALSE	---	签发者密钥标识符
keyIdentifier	---	OCTET 字符串	签发者公钥值的 SM3 哈希算法摘要
issuerAltName	FALSE	---	可为任意名字类型,应为最通用的名称才在这里加入
GeneralNames	---	---	---
GeneralName	---	---	---
rfc822Name	---	IA5String	PKI 管理机构的电子邮件地址
CRLNumber	FALSE	INTEGER	单调递增序列,所有的 CRL 都应包含这一项
issuingDistributionPoint	TRUE	OCTET 字符串	本项出现在分块 CRL 中,若 CRL 覆盖所有发行者签发的证书,则无需包含此项。不宜使用间接 CRL 或不能覆盖所有原因码的 CRL
distributionPoint	---	---	---
DistributionPointName	---	---	使用在分块 CRL 中,应与证书中的发布点扩展值一致
fullName	---	---	---
GeneralNames	---	---	---
GeneralName	---	---	---

表 C.5 证书撤销列表内容表 (续)

域	关键项标识	值	描述
directoryName	—	—	—
Name	—	—	—
RDNSequence	—	—	—
RelativeDistinguished	—	—	—
AttributeTypeAndV	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
uniformResourceIdentifier	—	IA5String	采用“ldap://”或者“http://”形式
onlyContainsUserCerts	—	BOOLEAN	如果设置为真,则本 CRL 只覆盖实体证书。(注意:如果本值为真,同时覆盖了所有实体证书,则 distributionPoint 可以忽略)
onlyContainsCACerts	—	BOOLEAN	如果设置为真,则本 CRL 只覆盖 CA 证书。(注意:如果本值为真,同时覆盖了所有 CA 证书,则 distributionPoint 可以忽略)
IndirectCRL	—	FALSE	本文件不宜使用间接 CRL,如果本 CRL 包含了非本 CRL 发行者所颁发的证书,这一项应设置为真
FreshestCRL	FALSE	—	在启用增量方式时,包含此项
DistributionPoint	—	—	—
distributionPoint	—	—	—
DistributionPointName	—	—	—
fullName	—	—	—
GeneralNames	—	—	—
GeneralName	—	—	—
directoryName	—	—	—
Name	—	—	—
RDNSequence	—	—	—
RelativeDistinguished	—	—	—
AttributeTypeAndV	—	—	—
AttributeType	—	OID	—
AttributeValue	—	—	—
uniformResourceIdentifier	—	—	采用“ldap://”或者“http://”形式
deltaCRLIndicator	TRUE	—	本扩展项只出现在增量 CRL 中
BaseCRLNumber	—	INTEGER	指向基 CRL

附 录 D
(资料性)
SM2 数字证书示例

以下内容将以 X.509 版本 3 证书为例,证书包含下列信息:

- a) the serial number is 64 57 00 b7 00 00 02 f6 (dec is 7230248512745636598);
- b) the serial number is 64 57 00 b7 00 00 02 f6 (dec is 7230248512745636598);
- c) the issuer's distinguished name is CN=OSCCA SM2 CA, C=CN;
- d) and the subject's distinguished name is CN=用户名字, OU=部门名称, O=组织名称, S=省份名称, C=CN;
- e) the certificate was issued on March 22, 2011 and expired on March 29, 2014;
- f) the certificate contains a 256 bit EC SM2 public key;
- g) the certificate is an end entity certificate (not a CA certificate);
- h) the certificate include an authority key identifier ,subject KeyIdentifier and basic constraints extensions;
- i) the certificate includes a critical key usage extension specifying the public is intended for generation of digital signatures;
- j) the certificate include a extend key usage extensions。

```

0000 30 200 : SEQUENCE {
0004 30 1A5: SEQUENCE {
0008 A0 3: [0] {
000A 02 1: INTEGER 2
: }
000D 02 8: INTEGER
: 64 57 00 B7 00 00 02 F6
0017 30 C: SEQUENCE {
0019 06 8: OBJECT IDENTIFIER '1 2 156 10197 1 501'
0023 05 0:
: }
0025 30 24 : SEQUENCE {
0027 31 15 : SET {
0029 30 13 : SEQUENCE {
002B 06 3: OBJECT IDENTIFIER commonName (2 5 4 3)
0030 13 C: UTF8String 'OSCCA SM2 CA'
: }
: }
003E 31 B: SET {
0040 30 9: SEQUENCE {
0042 06 3: OBJECT IDENTIFIER countryName (2 5 4 6)
0047 13 2: PrintableString 'CN'
: }

```

```

:      }
:      }
004B 30 1E : SEQUENCE {
004D 17 D :   UTCTime '110322074444Z'
005C 17 D :   UTCTime '140329074400Z'
:      }
006B 30 52 : SEQUENCE {
006D 31 15 :   SET {
006F 30 13 :     SEQUENCE {
0071 06 3 :       OBJECT IDENTIFIER commonName (2 5 4 3)
0076 0C C :       UTF8String '用户名字'
:       }
:     }
0084 31 15 :   SET {
0086 30 13 :     SEQUENCE {
0088 06 3 :       OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
008D 0C C :       UTF8String '部门名称'
:       }
:     }
009B 31 15 :   SET {
009D 30 13 :     SEQUENCE {
009F 06 3 :       OBJECT IDENTIFIER organizationName (2 5 4 10)
00A4 0C C :       UTF8String '组织名称'
:       }
:     }
00B2 31 B :   SET {
00B4 30 9 :     SEQUENCE {
00B6 06 3 :       OBJECT IDENTIFIER countryName (2 5 4 6)
00BB 13 2 :       PrintableString 'CN'
:       }
:     }
00BF 30 59 : SEQUENCE {
00C1 30 13 :   SEQUENCE {
00C3 06 7 :     OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1)
00CC 06 8 :     OBJECT IDENTIFIER '1 2 156 10197 1 301'
:     }
00D6 03 42 : BIT STRING 0 unused bits
:      04 97 0A 71 9B CC 02 B4 6E E9 CC DF 59 2F 59 0B
:      2D C7 5A AC B1 C7 B9 45 55 FE 07 E2 70 B3 83 9A
:      4B EB 4C 37 A3 AD 5E FF BF 23 39 0C AD 36 9A EC
:      58 B2 92 32 A0 CA 30 29 6F 0F F1 F8 35 F1 52 F6
:      76

```

```

:      }
011A A3 90 :      [3] {
011D 30 8D:      SEQUENCE {
0120 30 C:      SEQUENCE {
0122 06 3 :      OBJECT IDENTIFIER basicConstraints (2 5 29 19)
0127 04 5 :      OCTET STRING
:      30 03 01 01 00
:      }
012E 30 1D:      SEQUENCE {
0130 06 3 :      OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
0135 04 16 :      OCTET STRING
:      30 14 06 08 2B 06 01 05 05 07 03 02 06 08 2B 06
:      01 05 05 07 03 04
:      }
014D 30 B:      SEQUENCE {
014F 06 3 :      OBJECT IDENTIFIER keyUsage (2 5 29 15)
0154 04 4 :      OCTET STRING
:      03 02 00 C0
:      }
015A 30 11:      SEQUENCE {
015C 06 9:      OBJECT IDENTIFIER
:      netscape-cert-type (2 16 840 1 113730 1 1)
0167 04 4 :      OCTET STRING
:      03 02 00 80
:      }
016D 30 1F:      SEQUENCE {
016F 06 3 :      OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
0174 04 18 :      OCTET STRING
:      30 16 80 14 8E 7B 6D F4 CB 16 BC 42 79 80 22 80
:      92 49 97 1C EA BD D3 E5
:      }
018E 30 1D:      SEQUENCE {
0190 06 3 :      OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
0195 04 16 :      OCTET STRING
:      04 14 1E 99 F3 37 A8 7E 1F 5D C8 B5 C4 D9 F6 94
:      2E A6 9C 24 9F 31
:      }
:      }
:      }
:      }
01AD 30 C:      SEQUENCE {
01AF 06 8 :      OBJECT IDENTIFIER '1 2 156 10197 1 501'
01B9 05 0 :

```



