信息安全技术 数字证书格式

Information security technology - digital certificate format

（征求意见稿）

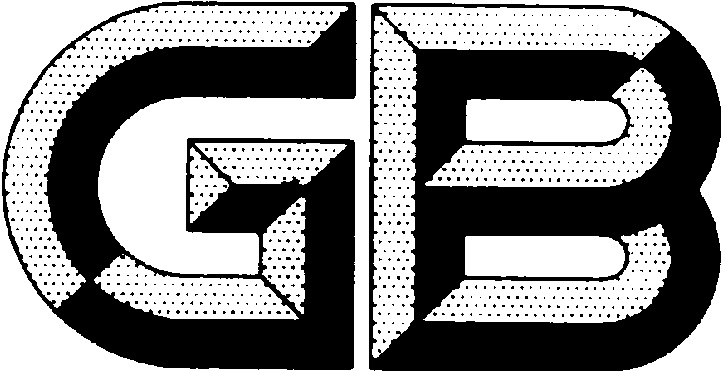
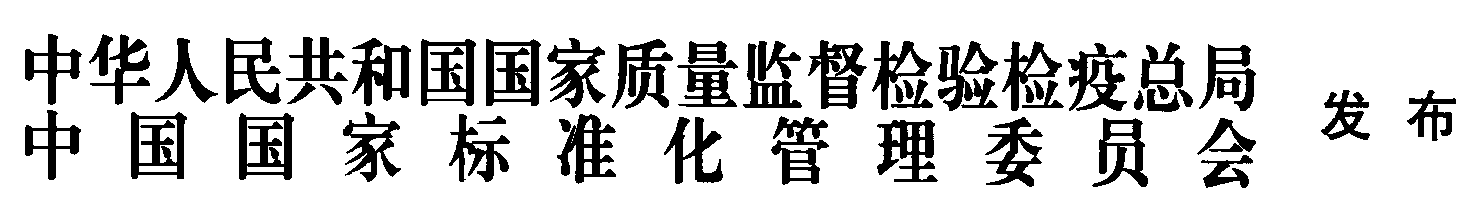
2016-06

ICS35.040**.**

L 80

XXXX-XX-XX实施

XXXX-XX-XX发布



中华人民共和国国家标准

GB/TXXXX—XXXX

目 次

[前 言 II](#_Toc453505314)

[引 言 III](#_Toc453505315)

[1 范围 1](#_Toc453505317)

[2 规范性引用文件 1](#_Toc453505318)

[3 术语和定义 1](#_Toc453505319)

[4 缩略语 2](#_Toc453505327)

[5 数字证书与CRL 2](#_Toc453505328)

[5.1 概述 2](#_Toc453505329)

[5.2 数字证书格式 3](#_Toc453505330)

[5.2.1 基本证书域的数据结构 3](#_Toc453505331)

[5.2.2TBSCertificate及其数据结构 4](#_Toc453505332)

[5.2.3 证书扩展域及其数据结构 7](#_Toc453505333)

[5.3 CRL格式 21](#_Toc453505334)

[6 算法技术的支持 25](#_Toc453505335)

[附　录　A 证书的结构 26](#_Toc453505336)

[附　录　B （规范性附录） 证书的结构实例 28](#_Toc453505337)

[附　录　C （资料性附录） 数字证书编码举例 29](#_Toc453505338)

[附　录　D （规范性附录） 证书撤销列表内容表 37](#_Toc453505339)

[附　录　E （资料性附录） 算法技术支持 40](#_Toc453505340)

前 言

本标准按照GB/T 1.1—2009给出的规则编写。

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这些专利的责任。

本标准由国家密码管理局提出。

本标准由全国信息安全标准化技术委员会（SAC/TC260）归口。

本标准主要根据Internet工程任务组（IETF）的RFC 2459文件制定，并结合我国数字证书应用的特点进行相应的扩充和调整。

本标准的附录A为规范性附录。

本标准的附录B为资料性附录。

本标准的附录C为资料性附录。

本标准的附录D为资料性附录。

本标准起草单位：上海格尔软件股份有限公司、北京海泰方圆科技有限公司、北京数字认证股份有限公司、无锡江南信息安全工程技术中心、成都卫士通信息产业股份有限公司、上海市数字证书认证中心有限公司、兴唐通信科技有限公司、山东得安信息技术有限公司、国家信息安全工程技术研究中心。

本标准主要起草人：郑强、蒋红宇、傅大鹏、李元正、韩玮、徐明翼、王妮娜、孔凡玉、袁锋。

本标准责任专家：刘平。

引 言

信息技术和网络技术极大地促进了社会的经济、科技、文化、教育和管理等各个方面的发展。互联网使地域和空间的距离进一步缩小，将地球变成了一个小小的村落。人们在享受信息化带来的众多好处的同时，也面临着日益突出的信息安全问题。在一个完全开放的网络环境下，如何建立一个真实、有效的身份信任体制已成为全球普遍关注的问题之一。人们从现实世界进入由网络构筑的虚拟世界时，面临的主要问题就是如何确认各自的身份、建立彼此间的信任关系以及保证信息的真实性、完整性、机密性和不可否认性。公钥基础设施（PKI）则是利用公钥理论和技术提供信息安全服务的基础设施，是目前有效解决开放网络环境中信息安全问题的关键技术。

PKI以公钥理论为基础，综合应用数据加密、密钥管理、数字签名及身份鉴别等技术，为开放网络环境内实体的鉴别、证书管理、数字签名、数据加密和信息安全服务（即机密性、真实性、完整性、不可否认性等）提供了所需的基础技术。PKI可以提供会话保密、身份鉴别、信息完整性、访问控制、源不可否认、目的不可否认、安全通信、密钥恢复和安全时间戳等九项信息安全功能所需要的服务。利用PKI，人们可以方便地建立和维护一个可信的网络计算环境，无需直接见面就能够确认彼此的身份，安全地进行信息交换。目前，以PKI为核心的网络身份认证体系和信息加密技术已成为业界广泛认同的一种构造网络身份信任体制的重要方式，并将成为我国信息安全保障体系中极其重要的组成部分之一。

数字证书是PKI的关键要素之一，是传送和处理实体身份鉴别信息的重要载体。国际标准化组织（ISO）和国际电信联盟（ITU）分别在国际标准ISO/IEC 9594-8和ITU-T X.509中对数字证书的基本格式进行规定,并简称为X.509证书。X.509证书成为Internet网上身份认证的基础性标准而得到广泛的使用， X.509证书已用于包括安全电子邮件（SEmail）、IP安全（IPsec）、安全套接层（SSL）、安全电子交易（SET）等许多网络安全协议中。虽然，ISO/IEC 9594-8规定了数字证书的基本格式，但是未对数字证书的扩展项进行明确规定。随着我国商用密码算法的越来越多的被使用，且数字证书应用领域的不断扩大，统一国内数字证书格式成为各界的共识。

信息技术 安全技术 公钥基础设施   
数字证书格式

范围

本标准规定了中国数字证书的基本结构，并对数字证书中的各数据项内容进行了描述。本标准规定了一些标准的证书扩展域，并对每个扩展域的结构进行了定义，特别是增加了一些专门面向国内应用的扩充项。建议在今后的应用中应按照本标准的规定使用这些扩充项。本标准还对证书中所应支持的签名算法、哈希函数、公开密钥算法进行了描述，另外在附录C中列举了中国目前通用的数字证书结构,附录zD中提供了证书DER编码供参考。

本标准适用于国内数字证书认证机构、数字证书认证系统的开发商以及基于数字证书的安全应用开发商来设计和处理各类数字证书。

本标准推荐的数字证书格式可以同RFC2459,ISO/IEC/ITU X.509 v3推荐的数字证书格式通用。

规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 16264.8—200× 信息技术 开放系统互连 目录 公钥和属性证书框架。

RFC2459：1999，互联网X.509公钥基础设施证书和CRL轮廓。

ITU-T X.680（1994）│ISO/IEC 8824-1：1994，信息技术-抽象语法记法1（ASN.1）：基本记法规范。

ITU-T X.681（1994）│ISO/IEC 8824-2：1994，信息技术-抽象语法记法1（ASN.1）：客体信息规范。

ITU-T X.682（1994）│ISO/IEC 8824-3：1994，信息技术-抽象语法记法1（ASN.1）：约束规范。

ITU-T X.683（1994）│ISO/IEC 8824-4：1994，信息技术-抽象语法记法1（ASN.1）：ASN.1规范参数化。

ITU-T X.690（1994）│ISO/IEC 8825-1：1994，信息技术-ASN.1编码规则：基本编码规则（BER）的规范，正规编码规则（CER）和可辨别编码规则（DER）。

术语和定义

下列定义适用于本标准。

公开密钥基础设施（PKI） public Key Infrastructure

支持公钥管理体制的基础设施，提供鉴别、加密、完整性和不可否认性服务。

公开密钥证书 Public Key Certificate

用户的公钥连同其他信息，并由发布该证书的证书认证机构的私钥进行加密使其不可伪造。

证书撤销列表（CRL） Certificate Revocation List

一个已标识的列表，它指定了一套证书颁发者确认为无效的证书。除了普通CRL外，还定义了一些特殊的CRL类型用于覆盖特殊领域的CRLs。

证书序列号 Certificate Serial Number

在CA颁发的证书范围内为每个证书分配的一个整数值。此整数值对于该CA所颁发的每一张证书必须是唯一的。

证书认证机构(CA) Certification Authority

受用户信任,负责创建和分配证书的权威机构。证书认证机构也可以为用户创建密钥。

证书撤销列表分发点 CRL Distribution Point

一个CRL的目录项或其他CRL分发源,通过CRL分发点分发的CRL可以只含有某个CA所颁发的证书全集中的某个子集的撤销项，也可以包括有多个CA的撤销项。

数字证书（或证书） Digital Certificate

数字证书是由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行数字签名的一个可信的数字化文件。数字证书包含有公开密钥拥有者的信息、公开密钥，签名算法和CA的数字签名。

缩略语

下列缩略语适用于本标准：

CA 证书认证机构

CRL 证书撤销列表

DIT 目录信息树系统

OID 对象标识符

PKI 公钥基础设施

数字证书与CRL

概述

数字证书具有以下的特性：

任何能够获得和使用认证机构公钥的用户都可以恢复认证机构所认证的公钥。

除了认证机构，没有其他机构能够更改证书,证书是不可伪造的。

由于证书是不可伪造的，所以可以通过将其放置在目录中来发布，而不需要以后特意去保护它们。

1——尽管在DIT中使用唯一性名称来明确定义CA，但这并不意味着CA组织和DIT之间有任何联系。

认证机构通过对信息集合的签名来生成用户证书，信息集合包括可辨别的用户名、公钥以及一个可选的包含用户附加信息的唯一性标识符（unique identifier）。唯一性标识符内容的确切格式这里未做规定，而留给认证机构(CA)去定义。唯一性标识符可以是诸如对象标识符、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它形式。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<<A>>=CA{V，SN，AI，CA，UCA，A，UA，Ap，TA}

这里V为证书版本；SN为证书序列号；AI为用来签署证书的算法标识符；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；TA表示证书的有效期，由两个日期组成，两者之间的时间段即是证书的有效期。证书有效期是一个时间区间，在这个时间区间里，CA必须保证维护该证书的状态信息，也就是发布有关撤销的信息数据。由于假定TA在不小于24小时的周期内变化，要求系统以格林威治时间（Coordinated Universal Time）为基准时间。证书上的签名可被任何知道CA公钥CAp的用户用来验证证书的有效性。

数字证书格式

本标准采用GB/T 16262系列标准的特定编码规则(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。

5.2.1 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 DEFAUT v1,

serialNumber CertificateSerialNumber,

signature AlgorithmIdentifier,

issuer Name,

validity Validity,

subject Name,

subjectPublicKeyInfo SubjectPublicKeyInfo,

issuerUniqueID [1] IMPLICIT UniqueIdentifier OPTIONAL,

-- 如果出现，version必须是v2或者v3

subjectUniqueID [2] IMPLICIT Unique Identifier OPTIONAL,

-- 如果出现，version必须是v2或者v3

extensions [3] EXPLICIT Extensions OPTIONAL 扩展项

-- 如果出现, version 必须是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：

tbsCertificate域包含了主体名称和签发者名称、主体的公钥、证书的有效期以及其它的相关信息。

signatureAlgorithm域包含证书签发机构签发该证书所使用的密码算法的标识符。一个算法标识符的ASN.1结构如下：

AlgorithmIdentifier ::= SEQUENCE {

algorithm OBJECT IDENTIFIER,

parameters ANY DEFINED BY algorithm OPTIONAL }

算法标识符用来标识一个密码算法，其中的OBJECT IDENTIFIER 部分标识了具体的算法(如 DSA with SHA-1)。其中可选参数的内容完全依赖于所标识的算法。该域的算法标识符必须与tbsCertificate中的signature标识的签名算法项相同。

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作为数字签名的输入，而签名的结果则按照ASN.1编码成BIT STRING类型并保存在证书签名值域内。

5.2.2TBSCertificate及其数据结构

TBSCertificate包含了证书结构中前十个项的信息。这些信息主要有主体和签发者的名称、主体的公钥、有效期、版本号和序列号，有些TBSCertificate还可以包含可选的唯一标识符项和扩展项。本节的下述段落描述这些项的语法和语义。

5.2.2.1 版本 Version

本项描述了编码证书的版本号。

5.2.2.2 序列号 Serial number

序列号是CA分配给每个证书的一个正整数，一个CA签发的每张证书的序列号必须是唯一的（这样，通过签发者的名字和序列号就可以唯一地确定一张证书），CA 必须保证序列号是非负整数。序列号可以是长整数，证书用户必须能够处理长达20个8比特字节的序列号值。CA必须确保不使用大于20个8比特字节的序列号。

5.2.2.3 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，这个算法标识符必须与证书中signatureAlgorithm项的算法标识符相同。可选参数的内容完全依赖所标识的具体算法，可以支持用户定义的签名算法。

5.2.2.4 颁发者 Issuer

本项标识了证书签名和证书颁发的实体。它必须包含一个非空的甄别名称（DN-distinguished name）。该项被定义为X.501的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描述了由一些属性组成的层次结构的名称，如国家名、相应的值,如“国家=CN”。其中AttributeValue部分的类型是由AttributeType确定的，通常它是一个DirectoryString类型。

DirectoryString类型被定义为PrintableString, TeletexString, BMPString, UTF8String和UniversalString类型之一。UTF8String 编码是首选的编码，在2003年12月31日之后签发的证书必须使用UTF8String 格式对DirectoryString项进行编码。在此之前，必须采用下面的方式之一进行编码：

如果PrintableString字符集足够，该串可以采用PrintableString类型进行编码；

如果(a)的条件不满足, 但BMPString类型的字符集满足要求，该串可以采用BMPString类型进行编码；

如果上述条件都不满足，则必须表示成UTF8String类型。如果满足（a）和（b），CA仍可以选择把数据串表示为UTF8String类型。

关于本项应用的更详细说明，可参照RFC2459 4.1.2.4[RFC2459]。

5.2.2.5 有效期 Validity

证书有效期是一个时间段，在这个时间段内，CA担保它将维护关于证书状态的信息。该项被表示成一个具有两个时间值的SEQUENCE类型数据：证书有效期的起始时间(notBefore)和证书有效期的终止时间(notAfter)。NotBefore和 notAfter这两个时间都可以作为UTCTime类型或者GeneralizedTime类型进行编码。

5.2.2.5.1 编码类型要求

遵循本标准的CA在2049年之前（包括2049年）必须将该时间编码为UTCTime类型，在2050年之后，编码为GeneralizedTime类型。

5.2.2.5.2 世界时间 UTCTime

世界时间（universal time）类型，UTCTime，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通过两个低位数确定年，时间精确到一分钟或一秒钟。UTCTime包含Z（用于Zulu，或格林威治标准时间）或时间差。

在本标准中，UTCTime值必须用格林威治标准时间（Zulu）表示，并且必须包含秒，即使秒的数值为零（即时间格式为YYMMDDHHMMSSZ）。系统对年字段（YY）必须如下解释：

当YY大于等于50，年应解释为19YY；当YY不到50，年应解释为20YY。

5.2.2.5.3通用时间类型 GeneralizedTime

通用时间类型，GeneralizedTime，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。

本标准中，GeneralizedTime值必须用格林威治标准时间表示，且必须包含秒，即使秒的数值为零（即时间格式为YYYYMMDDHHMMSSZ）。GeneralizedTime值绝不能包含小数秒（fractional seconds）。

5.2.2.6 主体 Subject

主体项描述了与主体公钥项中的公钥相对应的实体。主体名称可以出现在主体项和/或主体可选替换名称扩展项中（subjectAltName）。如果主体是一个CA，那么主体项必须是一个非空的与签发者项的内容相匹配的甄别名称（distinguished name）。如果主体的命名信息只出现在主体可选替换名称扩展项中（例如密钥只与一个Email地址或者URL绑定），那么主体名称必须是一个空序列，且主体可选替换名称扩展项必须被标识成关键的。

当主体项非空时，这个项必须包含一个X.500的甄别名称（DN）,一个CA认证的每个主体实体的甄别名称必须是唯一的。一个CA可以为同一个主体实体以相同的甄别名称签发多个证书。

主体名称扩展项被定义成ISO/IEC 9594-2:2001的名字类型。

关于本项应用的更详细说明，可参照RFC2459 4.1.2.6[RFC2459]。

5.2.2.7 主体公钥信息 Subject Public Key Info

本项用来标识公钥和相应的公钥算法。公钥算法使用算法标识符AlgorithmIdentifier结构来表示。

当公钥算法为RSA时，AlgorithmIdentifier结构定义参见PKCS#7；当公钥算法为SM2时，AlgorithmIdentifier结构定义参见GM/T CCCCC。

5.2.2.8 颁发者唯一标识符issuerUniqueID

该项主要用来处理主体或者颁发者名称的重用问题。本标准建议不同的实体名称不要重用， Internet网的证书不要使用唯一标识符。遵循本标准的证书签发机构应不生成带有颁发者唯一标识符的证书，但是在应用过程中应该能够解析这个项并进行对比。

5.2.2.9 主体唯一标识符subjectUniqueID

该项主要用来处理主体名称的重用问题，本标准建议对不同的实体名称不要重用，并且不建议使用此项，遵循本标准的证书签发机构应不生成带有主体唯一标识符的证书，但是在应用过程中应该能够解析唯一标识符并进行对比。

5.2.2.10 扩展项extensions

若出现，该项则是一个或多个证书扩展的序列（SEQUENCE），其内容和数据结构在5.2.3中定义。

5.2.3 证书扩展域及其数据结构

5.2.3.1 证书扩展

本标准定义的证书扩展项提供了把一些附加属性同用户或公钥相关联的方法以及证书结构的管理方法。数字证书允许定义标准扩展项和专用扩展项。每个证书中的扩展可以定义成关键性的和非关键性的。一个扩展含有三部分，他们分别是扩展类型、扩展关键度和扩展项值。扩展关键度（extension criticality）告诉一个证书的使用者是否可以忽略某一扩展类型。证书的应用系统如果不能识别关键的扩展时，必须拒绝接受该证书，如果不能识别非关键的扩展，则可以忽略该扩展项的信息。

本节定义一些标准的扩展项。需要特别注意的是，在实际应用过程中，如果采用了关键性的扩展，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8比特字符串extnValue的值。一个特定的证书中特定的扩展只可出现一次。例如，一个证书只可以包含一个认证机构密钥标识符扩展。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。每个扩展的正文指出了关键性项的可接收的值。

遵循本标准的CA必须支持密钥标识符、基本限制、密钥用法和证书策略等扩展。如果CA签发的证书中的主体项为空序列，该CA就必须支持主体可替换名称扩展。其它的扩展是可选的。CA还可以支持本标准定义之外的其它的扩展。证书的签发者必须注意，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。

遵循本标准的应用必须至少能够识别下列扩展：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法。另外，本标准建议还能支持认证机构（authority）和主体密钥标识符（subject key identifier）以及策略映射扩展。

5.2.3.2 标准扩展

本节定义数字证书的标准证书扩展，每个扩展与GB/T 16264.8-200X中定义的一个OID相关。这些OID都是id-ce的成员，其定义如下：

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

5.2.3.1 颁发机构密钥标识符authorityKeyIdentifier

颁发机构密钥标识符扩展提供了一种方式，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。识别可基于发行方证书中的主体密钥标识符或基于颁发者的名称和序列号。

相应CA产生的所有证书应包括authorityKeyIdentifier扩展的keyIdentifier项，以便于链的建立。CA以“自签”（self-signed ）证书形式发放其公钥时，可以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 OBJECTIDENTIFIER ::= {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生成：

1. keyIdentifier由BIT STRING subjectPublicKey值的160-bit SHA1（不安全了是不是换25？）哈希值组成（去掉标签、长度和不使用的字节数目）。
2. keyIdentifier 由0100加上后跟的BIT STRING subjectPublicKey值的SHA -1（不安全了是不是换25？）哈希值中最低位的60比特组成。

此密钥可以通过keyIdentifier字段中的密钥标识符来标识，也可以通过此密钥的证书的标识（给出authorityCertIssur字段中的证书颁发者以及authorityCertSerialNumber字段中的证书序列号）来标识，或者可以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，那么，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，每个密钥标识符应该是唯一的。不要求支持此扩展的实现能够处理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，所有的证书必须包含本扩展，而且要包含keyIdentifier项。如果证书的颁发者的证书有SubjectKeyIdetifier扩展，则本扩展中keyIdentifier项必须与颁发者的证书的SubjectKeyIdetifier扩展的值一致，如果证书的颁发者的证书没有SubjectKeyIdetifier扩展，则可以使用文中介绍的两种方法之一来产生。

结构中的keyIdentifier,authorityCertSerialNumber建议为必选，但本扩展必须是非关键的。

5.2.3.2 主体密钥标识符subjectKeyIdentifier

主体密钥标识符扩展提供一种识别包含有一个特定公钥的证书的方法。此扩展标识了被认证的公开密钥。它能够区分同一主体使用的不同密钥（例如，当密钥更新发生时）。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标识符而言，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证书必须包括本扩展；而且CA签发证书时必须把CA证书中本扩展的值赋给终端实体证书AuthorityKeyIdentifier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。有两种通用的方法从公钥中生成密钥标识符（见 5.2.3.2.1）。

5.2.3.3 密钥用法keyUsage

此扩展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：

1. digitalSignature:验证下列b)、f)或g）所标识的用途之外的数字签名；
2. 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）。
3. keyEncipherment：加密密钥或其它安全信息，例如用于密钥传输。
4. 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。
5. keyAgreement：用作公开密钥协商密钥。
6. keyCertSign:验证证书的CA签名。
7. CRLSign：验证CRL的CA签名。
8. EncipherOnly：当本比特与已设置的keyAgreement比特一起使用时，公开密钥协商密钥仅用于加密数据（本比特与已设置的其他密钥用法比特一起使用的含义未定义）。
9. DecipherOnly: 当本比特与已设置的keyAgreement比特一起使用时，公开密钥协商密钥仅用于解密数据（本比特与已设置的其他密钥用法比特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，此扩展的CA成分的值应被置为TRUE。CA还可使用keyUsag中定义的其他密钥用法比特，例如，提供鉴别和在线管理事务完整性的digitalSignature。

若缺少keyAgreement比特，则不定义encipherOnly比特的含义。若确定encipherOnly比特，且keyAgreement比特也被确定时，主体公钥可只用于加密数据，同时执行密钥协议。

若缺少keyAgreement比特，则不定义decipherOnly比特的含义。若确定decipherOnly比特，且keyAgreement比特也被确定时，主体公钥可只用于脱密数据，同时执行密钥协议。

所有的CA证书必须包括本扩展，而且必须包含keyertSign这一用法。此扩展可以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比特置为“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的用途或多种用途，并可用于查找具有多密钥/证书的实体的正确密钥/证书。它是一个咨询项，并不意指此密钥的用法限于指定的用途。置为“0”的比特指明此密钥不是预期的这一用途。如果所有比特均为“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的进行区别，当设置了c)、d)、h)、i)比特中的一位时，表示该证书为加密证书；当设置了a)、b)比特中的一位时，表示该证书为签名证书。

5.2.3.4 扩展密钥用途extKeyUsage

此项指明已验证的公开密钥可以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 17969.1-2000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。它是一个咨询项，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，进行应用的证书仍然可以要求指明特定的用途，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。

本标准定义下列密钥用途：

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

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

-- TLS Web server 鉴别

-- Key usage 可以设置为digitalSignature， keyEncipherment或keyAgreement

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

-- TLS Web server 鉴别

-- Key usage 可以设置为digitalSignature和/或keyAgreement

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

-- 可下载执行代码的签名

-- Key usage 可以设置为digitalSignature

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

-- E-mail 保护

-- Key usage可以设置为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 可以设置为digitalSignature，nonRepudiation

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

-- OCSP 应答签名

-- Key usage 可以设置为digitalSignature，nonRepudiation

5.2.3.5 私有密钥使用期privateKeyUsagePeriod

此扩展指明与已验证的公开密钥相对应的私有密钥的使用期限。它只能用于数字签名密钥。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日期和时间。如果没有notBefere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以用于签名的最迟日期和时间。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。

这个扩展总是为非关键的。

1：私有密钥有效使用期可以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。

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，例如，由于密钥泄露，那么，在验证时，对公开密钥而言的有效证方应仍存在。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

5.2.3.6 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，每个条目都有一个OID和一个可选的限定条件。这个可选的限定条件不要改变策略的定义。

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该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，则路径有效性软件必须能够解释该扩展（包括选择性限定语），否则必须拒绝该证书。

为了提高互操作性，本标准建议策略信息条目中只包含一个OID，如果一个OID不够，建议使用本节定义的限定语。

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)) }

本标准定义了两种策略限定语，以供证书策略制定者和证书签发者使用。限定语类型为CPS Pointer和User Notice限定语。

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字段命名一个团体，并通过记数识别该团体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字符的串。如果noticeRef和explicitText选项都在同一个限定语中，且如果应用软件可以找出由noticeRef选项指明的通知文本，则应展示该文本，否则应展示explicitText串。

5.2.3.7 策略映射policyMappings

本扩展只用于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的用户可以为某应用接收一个issuerDomainPolicy。策略映射告知发行方CA的用户，哪些同CA有关的策略可以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。证书签发者可以将该扩展选择为关键或非关键的。本标准推荐为关键的，否则一个证书用户就不能正确解释发布的CA设定的规则。

1：政策映射的一个例子如下：美国政府可有一个称之为加拿大贸易的政策，加拿大政府可有一个称之为美国贸易的政策。当两个政策可有区别地被标识并被定义时，两国政府之间可有个协定：就相关的用途，在两个政策所隐含的规则之内，允许认证路径延伸过境。

2：政策映射意味着作出有关决策时会耗费显著的管理开销和涉及相当大的劳动和委任人员。一般而言，最好的办法是同意使用比应用政策映射更广的全球的公共政策。在上述例子中，美国，加拿大和墨西哥同意一项公共政策，用于北美贸易那将是最好的。

3：预计政策映射实际上只能用于政策声明非常简单的有限环境。

5.2.3.8 主体可选替换名称subjectAltName

本项包含一个或多个可选替换名（可使用多种名称形式中的任一个）供实体使用， CA把该实体与认证的公开密钥绑定在一起。

主体可选替换名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。可以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，必须使用主体选择名称或颁发者选择名称扩展。由于主体可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必须由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是按照Internet RFC822定义的Internet电子邮件地址；
* dNSName 是按照RFC 1034定义的Internet域名；
* x400Address是按照GB/T 16284.4- 1996定义的O/R地址；
* directoryName是按照ITU-T Rec. X.501 | ISO/IEC 9594-2:2001定义的目录名称；
* 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是按照Internet RFC1630定义的用于WWW的UniformRAesourceIdentifier,RFC1738中定义的URL语法和编码规则；
* iPAddress是按照Internet RFC791定义的用二进制串表示的Internet Protocol地址；
* registeredID是按照GB/T17969.1-2000对注册的客体分配的标识符。

CA不得签发带有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选择名称格式（如一个电子邮件地址），则主体的甄别名必须是空的（一个空序列），且subjectAltName扩展必须存在。如果主体字段包括一个空序列，则subjectAltName扩展必须标识为关键性的。如果出现subjectAltName扩展，则序列必须至少包含一个条目。

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实体。

此扩展可以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，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。除先前的限制以外，允许证书使用系统不理睬具有不能识别的或不被支持的名称形式的任何名称。倘若，证书的主体项包含无二义地标识主体的目录名称，推荐将此项标记为非关键的。

1：TYPE-IDENTIFIER类别的使用在ITU-T Rec.x.681|ISO/IEC 8824-2的附录A和C中描述。

2：如果存在此扩展并标记为关键的，证书的subject项可以包含空名称（例如，相关可甄别名的一个“0”序列），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。

3：进一步说明可参考RFC2459 4.2.1.7[RFC2459]

5.2.3.9 颁发者可选替换名称issuerAltName

此项包含一个或多个可选替换名称（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

此扩展可以是关键的或非关键的，由证书或CRL颁发者选择。不要求支持此扩展的实际应用能处理所有名称形式。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。除先前的限制以外，允许证书使用系统不理睬具有不能识别的或不支持的名称形式的任何名称。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，推荐将此项标记为非关键的。

如果存在此扩展，并标记为关键的，证书或CRL的issuer项可以包含空名称（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。签发者可选替换名称必须按5.2.3.2.8节的说明进行编码。

5.2.3.10 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

该扩展总是非关键的。

5.2.3.11 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值表明在路径中只可以向终端实体签发证书，而不可以签发下级CA证书。PathLenConstraint字段出现时必须大于或等于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证书中必须必须包括本扩展，而且必须是关键的，否则，未被授权为CA的实体可以签发证书，同时证书使用系统会在不知情的情况下使用这样的证书。

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，其公开密钥应不能用来验证证书签名；

——如果CA字段的值置为TRUE，并且pathLen Constraint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。

1：如果此扩展不存在或标记为非关键项的并且未被证书使用系统认可，该证书被系统视为终端用户证书，并且不能用来验证证书签名。

2：为限制一证书主体只是一个端实体，即，不是CA，颁发者可以在扩展中只包含一个空SEQUENCE值的扩展项。

5.2.3.12 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，则他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，由主体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，由主体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PermittedSutrees和excluded Subtrees都存在并且名称空间重叠，则优先选用排斥声明（exclusion statement）。

通过GeneralName字段定义的命名格式，需要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。在应用中不需要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，可以不理睬此子树规范。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，对与此名称形式的名称限制一致性而言应检验所有这些名称。

可以对主体名称或主体选择名称进行限制。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，则证书是可以接受的。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”（默认）的minimum值对应于此基部（base），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（base），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。

本标准建议将它标记为关键项，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。

本标准中，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。

5.2.3.13 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。它可以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签发的证书，所有在此路径中的证书都有必要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。指定的CA指包含此扩展信息的认证机构（如果requireExplicitpolicy的值为“0”）或是认证路径中后续认证机构CA（由非“0”值指示的）。

如果inhibitploicyMapping字段存在，它表明在认证路径中从所指定的CA开始直到认证路径结束为止的所有证书中，不允许策略映射。指定的CA指包含此扩展信息的认证机构（如果inhibitPolicyMapping的值为“0”）或是认证路径中后续认证机构CA（由非“0”值指示的）。

SkipCerts类型的值表示在某一限制成为有效之前应在认证路径中需要跳过的证书的个数。

此扩展由证书签发者选择是关键的还是非关键的。本标准建议它标记为关键的，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。

5.2.3.14 证书撤销列表分发点CRLDistributionPoints

CRL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，终端实体公钥证书以及属性证书中。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，或者它可以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] DistributionPointNameOPTIONAL，  
 reasons [1] ReasonFlagsOPTIONAL，  
 cRLIssuer [2] GeneralNamesOPTIONAL}  
  
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字段标识如何能够获得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替代名称或应用默认时，分发点名称可以有多种名称形式。同一名称（至少用其名称形式之一）应存在于颁发CRL的分发点扩展的distrubutionPoint字段中。不要求证书使用系统能处理所有名称形式。它可以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，若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分发点被赋于一个直接从属于CRL颁发者的目录名称的目录名，则只能使用nameRelativeToCRLIssuer字段。此时，nameRelativeToCRLIssuer字段传送与CRL颁发者目录名称有关的可甄别名。

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分发点发布包含此证书（如果此证书已被撤销）的项的CRL，而不管撤销原因。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。

此扩展可以是关键的或非关键的，由证书颁发者选择，建议该扩展设置为非关键的，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，证书使用系统将不使用该证书。在分配点为所有撤销原因代码和由CA（包括作为关键扩展的CRLDistributionPoint）发布的所有证书分配CRL信息的项中，CA不需要在CA项发布一个完整的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；或

用其他手段完成撤销检查。

1：一个以上的CRL分发者对应一个证书CRL签发者是可能的。这些CRL分发者和签发CA的协调是CA策略的一个方面。

2:证书撤销列表CRL的应用,请参照RFC2459 第5章, January 1999。

5.2.3.15 限制所有策略inhibitAnyPolicy

本扩展指定了一个限制，它指出了任何策略，对于从指定CA开始的认证路径中的所有证书的证书策略，都认为不是显式匹配。指定的CA要么是包含这个扩展的证书的主体CA（如果inhitanyPolicy值为0），要么是认证路径（由非0值指定）中后继认证机构CA。

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。建议它标记为关键项，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。

5.2.3.16 最新证书撤销列表 freshestCRL

最新CRL扩展只被作为证书扩展使用，或在发给认证机构和用户的证书中使用。该项标识了CRL，对CRL来说证书用户应包含最新的撤销信息（例如：最新的dCRL）。

该项定义如下：

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

freshestCRL::={CRLDistPointsSyntax}

根据证书颁发者的选择，这个扩展可能是关键的，也可能是非关键的。如果最新的CRL扩展是关键的，那么证书使用系统不使用没有首先进行撤销和核对的最新CRL的证书。如果扩展被标记为不关键的，证书使用系统能使用本地方法来决定是否需要检查最新的CRL。

5.2.3.17 个人身份标识码 IdentifyCode

个人身份证号码用于表示个人身份证件的号码，其定义如下：

id-IdentifyCode OBJECT IDENTIFIER ::={1.2.86.11.7.1}

IdentifyCode ::=SET {

residenterCardNumber [0] PrintableString OPTIONAL,

militaryOfficerCardNumber [1] UTF8String OPTIONAL,

passportNumber [2] PrintableString OPTIONAL,

...

}

此扩展项标记为非关键的。

5.2.3.18 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 ::={ 1.2.86.11.7.2 }

InsuranceNumber::= PrintableString  
此扩展项标记为非关键的。

5.2.3.19 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码，其定义如下：

ID-ICRegistrationNumber OBJECT IDENTIFIER ::={ 1.2.86.11.7.4 }

ICRegistrationNumber::= PrintableString

此扩展项标记为非关键的。

5.2.3.20 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 ::={ 1.2.86.11.7.3 }

OrganizationCode::= PrintableString

此扩展项标记为非关键的。

5.2.3.21 企业税号 TaxationNumeber

企业税号扩展项用于表示企业税号码，其定义如下：

ID- TaxationNumeber OBJECT IDENTIFIER ::={ 1.2.86.11.7. 5 }

TaxationNumeber::= PrintableString

此扩展项标记为非关键的。

5.2.3.22专用因特网扩展 PrivateInternetExtensions id-pkix

本节定义了两个应用于因特网公钥基础结构（PKI）的新扩展，用于指导应用以识别一个支持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。

5.2.3.23 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。该扩展可包括在用户证书和CA证书中，且必须为非关键的。

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AuthorityInforAccessSyntax中的每个入口描述有关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。检索机制可以由accessMethod表明或由acessLocaion说明。

本标准定义用于accessMethod的一个OID。当附加的信息列出了发行证书的CA高于发行该扩展的证书CA时，使用id-ad-caIssuers OID。

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

5.2.3.24 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策略数据，主体是用户，则描述了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。这个扩展项必须被定义为非关键的。

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

SubjectInfoAccessSyntax ::=

SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE {

accessMethod OBJECT IDENTIFIER,

accessLocation GeneralName }

* 1. CRL格式

本标准采用GB/T 16262系列标准的特定编码规则（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。ASN.1 DER 编码是关于每个元素的标记、长度和值的编码系统。CRL数据结构的ASN.1描述如下：

CertificateList ::= SEQUENCE {

tbsCertList TBSCertList,

signatureAlgorithm AlgorithmIdentifier,

signatureValue BIT STRING

}

TBSCertList ::= SEQUENCE {

version Version OPTIONAL,

--如果出现，必须是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必须是v2

} OPTIONAL,

crlExtensions [0] EXPLICIT Extensions OPTIONAL

-- 如果出现，version必须是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：

* tbsCertList域包含了主体名称和颁发者名称、颁发日期、撤销的证书信息和CRL的扩展信息。
* 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结构如下：

AlgorithmIdentifier ::= SEQUENCE

{

algorithm OBJECT IDENTIFIER,

parameters ANY DEFINED BY algorithm OPTIONAL

}

算法标识符用来标识一个密码算法，其中的OBJECT IDENTIFIER 部分标识了具体的算法。其中可选参数的内容完全依赖于所标识的算法。该域的算法标识符必须与tbsCertList中的signature标识的签名算法项相同。如果签名算法为SM2，无参数。

* 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作为数字签名的输入，而签名的结果则按照ASN.1编码成BIT STRING类型并保存在CRL签名值域内。如果签名算法为SM2，SM2密码算法签名数据格式参见GM/T BBBBB。
  + 1. TBSCertList 及其数据结构

TBSCertList主要包含了版本号、颁发者、生效日期、下次更新日期、签名算法、签发机构密钥标识符、撤销的证书信息。有些TBSCertList还可以包含可选的扩展项。本条的下述段落描述这些项的语法和语义。

* + - 1. 版本 version

本可选项描述了编码CRL的版本号。如果使用了Extensions 项，则此项必须存在，且其值必须是version 2（用整数1表示）。

* + - 1. 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，这个算法标识符必须与CertificateList 中signatureAlgorithm项的算法标识符相同。使用国家密码管理主管部门审核批准的相关算法。

* + - 1. 颁发者 issuer

本项标识了签名和颁发CRL的实体。它必须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。

* + - 1. 生效日期 thisUpdate

本项标明了CRL的颁发日期，使用UTCTime or GeneralizedTime编码。

遵循本标准的CRL颁发者在2049年之前（包括2049年）必须将该时间编码为UTCTime类型，在2050年之后，编码为GeneralizedTime类型。

UTCTime的编码规则同。

GeneralizedTime的编码规则同。

* + - 1. 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可以在此时间前签发，但不能晚于此时间签发。使用UTCTime or GeneralizedTime编码。

遵循本标准的CRL颁发者必须在签发的CRL中包含nextUpdate项。

遵循本标准的CRL颁发者在2049年之前（包括2049年）必须将该时间编码为UTCTime类型，在2050年之后，编码为GeneralizedTime类型。

UTCTime的编码规则同。

GeneralizedTime的编码规则同。

* + - 1. 被撤销的证书列表 Revoked Certificates

该域标明被撤销的证书序列号、撤销时间和撤销原因。

如果没有被撤销的证书，此项不存在。否则，列出被撤销证书的序列号，并指定撤销的日期。

crlEntryExtensions在描述。

* + - 1. 扩展项 crlExtensions

该域只可在version 2出现。如果出现，此项由一个或多个CRL扩展的序列组成。

crlExtensions在5.3.2 描述。

* + 1. CRL扩展项及其数据结构
       1. 颁发机构密钥标识符 authorityKeyIdentifier

颁发机构密钥标识符扩展提供了一种方式，以识别与CRL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。识别可基于颁发者的主体密钥标识符或基于颁发者的名称和序列号。

* + - 1. 颁发者替换名称 issuerAltName

本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CRL颁发者使用。

* + - 1. 证书撤销列表号 crlNumber

证书撤销列表号是一个非关键的CRL扩展，表示在给定的CRL颁发者和CRL范围内一个单调递增序列。这个扩展可以让用户方便地确定一个特定的CRL何时取代另一个CRL。证书撤销列表号也支持鉴别一个附件的完整CRL和增量CRL。

如果CRL颁发者在一个特定范围内除了生成完整CRL外，还生成增量CRL，完整CRL和增量CRL必须共享同一个编号序列。如果完整CRL和增量CRL在同一时间颁发，它们必须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（两个完整CRL，两个增量CRL，或者一个完整CRL和一个增量CRL），这两个CRL不能使用相同的证书撤销列表号。也就是说，如果两个CRL的thisUpdate域不同，证书撤销列表号必须不同。

CRL号可以使用长整数。CRL验证者必须能够处理20字节的证书撤销列表号。遵循本标准的CRL颁发者不使用大于20字节的证书撤销列表号。

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

CRLNumber ::= INTEGER (0..MAX)

* + - 1. 增量证书撤销列表指示 Delta CRL Indicator

增量证书撤销列表指示是一个关键CRL扩展，表明一个CRL是增量CRL。增量CRL包含上次发布之后的撤销信息，而不是将所有的撤销信息包含在一个完整CRL里。在一些环境里使用增量CRL可以显著减少网络流量和处理时间。

增量证书撤销列表指示扩展包含一个类型为BaseCRLNumber的单一值。证书撤销列表号标识了此增量CRL使用的起始CRL。遵循本标准的CRL颁发者必须将参考基准CRL颁发为完整CRL。增量CRL包含所有的更新撤销状态。增量CRL和参考基准CRL的组合与完整CRL是等效的。

当遵循本标准的CRL颁发者生成增量CRL，此增量CRL必须包含一个关键的增量证书撤销列表指示扩展项。

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

BaseCRLNumber ::= CRLNumber

* + - 1. 颁发分发点 Issuing Distribution Point

颁发分发点是一个关键CRL扩展，表明一个特定CRL的分发点和范围，还表明这个CRL是否只包含了用户证书的撤销、CA证书的撤销或者一系列的原因代码。

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 }

* + - 1. 最新证书撤销列表 Freshest CRL

最新证书撤销列表扩展项表明完整CRl的增量CRL信息如何获取。遵循本标准的CRL颁发者必须将此项标记成非关键。此项不在增量CRL中出现。

最新证书撤销列表扩展项的格式和数字证书的cRLDistributionPoints扩展项相同。参考5.2.3.2.16。但是，该最新证书撤销列表扩展项中分发点域是有意义的；同时Reasons和cRLIssuer域必须略去。

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

FreshestCRL ::= CRLDistributionPoints

* + - 1. 证书撤销列表条目 CRL Entry
         1. 原因代码 Reason Code

原因代码为非关键扩展，表明证书撤销的原因。

代码removeFromCRL (8)只用于增量CRL。其它代码可以用于任意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) }

* + - * 1. 撤销时间 Invalidity Date

撤销时间是个非关键扩展，表明知道或怀疑私钥泄露或证书失效的时间。

该域包含的GeneralizedTime必须使用格林威治标准时间，必须按照的要求表示。

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

InvalidityDate ::= GeneralizedTime

* + - * 1. 证书颁发者 Certificate Issuer

如果存在，证书颁发者扩展包含一个或多个和CRL条目对应的，从证书的颁发者域和/或颁发者替换名称域得到的名字。

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

CertificateIssuer ::= GeneralNames

算法技术的支持

国际上的数字证书可支持多种密码算法，如SHA-1，签名算法RSA等。在国内，数字证书还可以支持国家密码管理局公布的SM2和SM3等算法。参见附录D。

证书的结构

A.1 证书构成

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

A.2 基本证书域

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 项名称 | 描述 | 备注 |
|  | version | 版本号 |  |
|  | 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 | 本标准中不使用 |
|  | subjectUniqueID | 主体唯一标识符 | 本标准中不使用 |
|  | extensions | 扩展项 | 按本标准的扩展项进行定义，参考B3。 |

A.3 标准的扩展域

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 名称 | 描述 | 关键度 |
|  | authorityKeyIdentifier | 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 | 双证书标记为关键，单证书标记为非关键 |
|  | 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 |
|  | id-pkix | 私有的 Internet 扩展 | 非关键 |
|  | authorityInfoAccess | 机构信息访问 | 非关键 |
|  | SubjectInformationAccess | 主体信息访问 | 非关键 |
|  | IdentifyCardNumber | 个人身份证号码 | 非关键 |
|  | InuranceNumber | 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 |

（规范性附录）  
证书的结构实例

B.1 用户证书的结构实例

|  |  |
| --- | --- |
| 版本号（version） | |
| 证书序列号（serialNumber） | |
| 签名算法标识符（signature） | |
| 颁发者名称（issuer） | |
| 有效期（validity） | 起始有效期 |
| 终止有效期 |
| 主体名称（subject） | countryName国家 |
| stateOrProvinceName省份 |
| localityName地市 |
| organizationName组织名称 |
| organizationalUnitName机构名称 |
| CommanName 用户名称 |
| 主体公钥信息（subjectPublicKeyInfo） | |
| 颁发机构的密钥标识authorityKeyIdentifier | |
| 主体密钥标识符subjiectKeyIdentifier | |
| CRL分发点CRLDistributionPoints | |

B.2 服务器证书的结构实例

|  |  |
| --- | --- |
| 版本号（version） | |
| 证书序列号（serialNumber） | |
| 签名算法标识符（signature） | |
| 颁发者名称（issuer） | |
| 有效期（validity） | 起始有效期 |
| 终止有效期 |
| 主体名称（subject） | countryName国家 |
| stateOrProvinceName省份 |
| localityName地市 |
| organizationName组织名称 |
| organizationalUnitName机构名称 |
| CommanName 服务器名称 |
| 主体公钥信息（subjectPublicKeyInfo） | |
| 颁发机构的密钥标识(authorityKeyIdentifier) | |
| 主体密钥标识符(subjiectKeyIdentifier) | |
| CRL分发点(CRLDistributionPoints) | |

（资料性附录）  
数字证书编码举例

C.1 RSA数字证书编码

这部分将以X.509版本3证书为例，证书包含下列信息：

（a） the serial number is 6565422187515605500000000000000000000;

（b） the certificate is signed with RSA and the sha1 hash algorithm;

（c） the issuer's distinguished name is CN=Certificate Center; 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 August 7, 2003 and expired on August 6,2004;

（f） the certificate contains a 1024 bit RSA public key;

（g） the certificate is an end entity certificate （not a CA certificate）;

（h） the certificate includes an alternative subject name ,is URL;

（i） the certificate include an authority key identifier ,subject KeyIdentifier and basic constraints extensions;

（j） the certificate includes a critical key usage extension specifying the public is intended for generation of digital signatures.

（k） the certificate include a extend key usage extensions;

（l） the certificate include a crl distributionpoints extensions;

0000 30 82 04 16 1046: SEQUENCE

0004 30 82 02 FE 766: . SEQUENCE

0008 a0 03 3: . . [0]

0010 02 01 1: . . . INTEGER 2

: 02

0013 02 10 16: . . INTEGER 6565422187515605500000000000000000000

:04 F0 74 4E 3D 72 65 06 C4 92 77 0A 5E 71 F1 5B

0031 30 0D 13: . . SEQUENCE

0033 06 09 9: . . . OID 1.2.840.113549.1.1.5

sha1withRSAEncryption

:2a 86 48 86 f7 0d 01 01 05

0044 05 00 0: . . . NULL

0046 30 2A 42: . . SEQUENCE

0048 31 0B 11: . . . SET

0050 30 09 9: . . . . SEQUENCE

0052 06 03 3: . . . . . OID 2.5.4.6: C countryName

: 55 04 06

0057 13 02 2: . . . . . PrintableString 'CN'

: 43 4E

0061 31 1B 27: . . . SET

0063 30 19 25: . . . . SEQUENCE

0065 06 03 3: . . . . . OID 2.5.4.3: CN

: 55 04 03

0070 13 12 18: . . . . . PrintableString 'Certificate Center'

: 43 65 72 74 69 66 69 63 61 74 65 20 43 65 6E 74 65 72

0090 30 1E 30: . . SEQUENCE

0092 17 0D 13: . . . UTCTime '030807063811Z'

: 30 33 30 38 30 37 30 36 33 38 31 31 5A

0107 17 0D 13: . . . UTCTime '040806063811Z'

: 30 34 30 38 30 36 30 36 31 38 31 31 5A

0122 30 7A 122: . . SEQUENCE

0124 31 1F 31: . . . SET

0126 30 1D 29: . . . . SEQUENCE

0128 06 09 9: . . . . . OID 1.2.840.113549.1.9.1 emailAddress

: 2A 86 48 86 F7 0D 01 09 01

0139 16 10 16: . . . . . IA5String 'name@mail.com.cn'

: 6E 61 6D 65 40 6D 61 69 6C 2E 63 6F 6D 2E 63 6E

0157 31 0B 11: . . . SET

0159 30 09 9: . . . . SEQUENCE

0161 06 03 3: . . . . . OID 2.5.4.6: C

: 55 04 06

0166 13 02 2: . . . . . PrintableString 'CN'

: 43 4E

0170 31 11 17: . . . SET

0172 30 0F 15: . . . . SEQUENCE

0174 06 03 3: . . . . . OID 2.5.4.8: 'S'

: 55 04 08

0179 1E 08 8: . . . . . BMPString '省份名称'

: 77 01 4E FD 54 0D 79 F0

0189 31 11 17: . . . SET

0191 30 0F 15: . . . . SEQUENCE

0193 06 03 3: . . . . . OID 2.5.4.10 'O'

: 55 04 0A

0198 1E 08 8: . . . . . BMPString '组织名称'

: 7E C4 7E C7 54 0D 79 F0

0208 31 11 17: . . . SET

0210 30 0F 15: . . . . SEQUENCE

0212 06 03 3: . . . . . OID 2.5.4.11 'OU'

: 55 04 0B

0217 1E 08 8: . . . . . BMPString '部门名称'

: 90 E8 95 E8 54 0D 79 F0

0227 31 11 17: . . . SET

0229 30 0F 15: . . . . SEQUENCE

0231 06 03 3: . . . . . OID 2.5.4.3 'CN'

:55 04 03

0236 1E 08 8: . . . . . BMPString '用户名字'

:75 28 62 37 54 0D 5B 57

0246 30 81 9F 159: . . SEQUENCE

0249 30 0D 13: . . . SEQUENCE

0251 06 09 9: . . . . . OID 1.2.840.113549.1.1.1 rsaEncryption

: 2A 86 48 86 F7 0D 01 01 01

0262 05 00 0: . . . . . NULL

0264 03 81 8D 141: . . . BIT STRING

: 00 （0 unused bits）

30 81 89 02 81 81 00 E0 57 4A 86 B6 52 91 85 14

6B 44 DB 9E E9 58 2B 9F 20 86 B0 C1 E5 A9 3B C8

75 08 9C 59 C2 A9 DD 8A 42 6B F8 FC 5F 8C 2E 53

C6 B5 FD A3 EE 55 3D 12 01 05 3B E2 76 CB 59 CE

AE 2C 7A 3D 4C 6B 83 58 39 0F 74 09 0D 61 0C 25

2D 4F 98 3A F2 C7 84 B2 73 0F 61 34 24 CF 29 B8

FA 5C 7E 5F 2A 42 B2 72 E6 BE CA DE LD ED 3B D0

0E 25 C3 87 C7 36 EF 0E 4C 84 FA A7 00 44 8F 71

FE 46 62 A3 B0 C0 7D 02 03 01 00 01

0408 A3 82 01 6A 362: . . [3]

0412 30 82 01 66 358: . . . SEQUENCE

0416 30 1F 31: . . . . SEQUENCE

0418 06 03 3: . . . . . OID 2.5.29.35 authorityKeyIdentifier

: 55 1D 23

0423 04 18 24: . . . . . OCTET STRING

: 30 16 80 14 E7 9F 11 9C EA 2D 20 54 05 34 24 D1

B2 53 23 67 D5 A7 E5 EB

0449 30 1D 29: . . . . SEQUENCE

0451 06 03 3: . . . . . OID 2.5.29.14 subjectKeyIdentifier

: 55 1D 0E

0456 04 16 22: . . . . . OCTET STRING

: 04 14 5C F5 D9 F7 EC 3E A2 BE B1 3B 7E 63 5E C1

8B 2A 15 A3 BF 72

0480 30 0B 11: . . . . SEQUENCE

0482 06 03 3: . . . . . OID 2.5.29.15 keyUsage

: 55 1D 0F

0487 04 04 4: . . . . . OCTET STRING

: 03 02 03 F8

0493 30 1B 27: . . . . SEQUENCE

0495 06 03 3: . . . . . OID 2.5.29.17 subjectAltName

: 55 1D 11

0500 04 14 20: . . . . . OCTET STRING

: 30 12 81 10 73 69 6E 61 40 6D 61 69 6C 2E 63 6F

6D 2E 63 6E

0522 30 0C 12: . . . . SEQUENCE

0524 06 03 3: . . . . . OID 2.5.29.19 basicConstraints

: 55 1D 13

0529 04 05 5: . . . . . OCTET STRING

: 30 03 01 01 00

0536 30 3B 59: . . . . SEQUENCE

0538 06 03 3: . . . . . OID 2.5.29.37 extKeyUsage

: 55 1D 25

0543 04 34 52: . . . . . OCTET STRING

: 30 32 06 08 2B 06 01 05 05 07 03 01 06 08 2B 06

01 05 05 07 03 02 06 08 2B 06 01 05 05 07 03 03

06 08 2B 06 01 05 05 07 03 04 06 08 2B 06 01 05

05 07 03 08

0597 30 81 AE 174: . . . . SEQUENCE

0600 06 03 3: . . . . . OID 2.5.29.31 cRLDistributionPoints

:55 1D 1F

0605 04 81 A6 166: . . . . . OCTET STRING

: 30 81 A3 30 7C A0 7A A0 78 A4 76 30 74 31 0D 30

0B 06 03 55 04 03 13 04 63 72 6C 30 31 0C 30 0A

06 03 55 04 0B 13 03 63 72 6C 31 0C 30 0A 06 03

55 04 0B 13 03 31 30 32 31 0A 30 08 06 03 55 04

0B 13 01 31 31 0D 30 0B 06 03 55 04 0A 13 04 4A

44 5A 59 31 0B 30 09 06 03 55 04 07 13 02 63 43

31 12 30 10 06 03 55 04 08 13 09 4A 69 6C 69 6E

39 39 34 38 31 0B 30 09 06 03 55 04 06 13 02 63

6E 30 23 A0 21 A0 1F 86 1D 68 74 74 70 3A 2F 2F

63 72 6C 2E 63 6F 6D 2E 63 6E 2F 63 72 6C 2F 63

72 6C 2E 63 72 6C

0774 30 0D 13: . SEQUENCE

0776 06 09 9: . .OID 1.2.840.113549.1.1.5 sha1withRSAEncryption

: 2A 86 48 86 F7 0D 01 01 05

0787 05 00 0: . .NULL

0789 03 82 01 01 257: . BIT STRING

: 00 57 DF 8D D5 2A 06 56 84 3A FF 1F 2A FD 96 F6

2C 36 D0 24 9C 74 32 C3 C5 BA BB B7 24 29 EB EC

60 E3 EC 90 D6 51 9E 54 42 4D 1E 8C A0 79 4C 14

C8 E8 DC 20 A7 B9 0D 09 2A E8 9B 6C 19 44 B4 30

E7 BD F5 40 03 FB 14 89 5C E6 C5 47 E0 00 FA 17

45 61 0A C3 7C A3 7E B5 1D D6 A9 20 7E 70 89 91

4F F4 18 0E E6 C6 2A 7C 39 F4 8D 84 94 57 5B C3

B9 D5 12 C2 1B 54 6D F4 5D 88 6D AF 6C F7 28 DF

F9 23 58 BE 0B 1C 7A C9 83 82 80 98 98 F2 68 BF

BA 85 91 62 83 C4 E5 98 C2 A6 6B C2 B3 97 10 50

3B 0E 9C 08 00 A4 34 FB 1B 41 AD 87 5E 2D EB EC

46 45 EA 9A FB 82 B4 B9 A5 AF 4A 61 88 5F A8 49

97 44 08 C2 3B 32 00 64 07 87 0B 2D 9D 7A 62 8F

44 56 F9 71 B9 89 10 B0 13 94 3A BD 33 6B 19 89

14 9F 58 E6 7D 0F 94 64 32 EA 8E CE C8 77 65 C0

C5 D6 17 EA 71 A8 B8 D3 6B 50 D1 B3 86 28 C9 78

FE

C.2 SM2数字证书编码

以下内容将以X.509版本3证书为例，证书包含下列信息：

1. the serial number is 64 57 00 b7 00 00 02 f6 (dec is 7230248512745636598)；
2. the certificate is signed with SM2 and the SM3 hash algorithm；
3. the issuer’s distinguished name is CN=OSCCA SM2 CA, C=CN；
4. 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；
5. the certificate was issued on March 22, 2011 and expired on March 29,2014；
6. the certificate contains a 256 bit SM2 EC public key；
7. the certificate is an end entity certificate （not a CA certificate）；
8. the certificate include an authority key identifier ,subject KeyIdentifier and basic constraints extensions；
9. the certificate includes a critical key usage extension specifying the public is intended for generation of digital signatures；
10. 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: PrintableString '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 '?ㄦ.峰..绉?

: }

: }

0084 31 15: SET {

0086 30 13: SEQUENCE {

0088 06 3: OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)

008D 0C C: UTF8String '?ㄩ.ㄥ..绉?

: }

: }

009B 31 15: SET {

009D 30 13: SEQUENCE {

009F 06 3: OBJECT IDENTIFIER organizationName (2 5 4 10)

00A4 0C C: UTF8String '缁.缁.?.绉?

: }

: }

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:

: }

01BB 03 47: BIT STRING 0 unused bits

: 30 44 02 20 50 37 93 B4 0E 0F 1C 9D 3E EE 7F 7E

: 02 BE BD 3E DE 01 27 27 20 82 EE 8F 0F 6F E4 8A

: 36 3F 26 B9 02 20 B5 70 08 46 76 7B 6F 27 43 6C

: BE D7 45 98 C4 5B 98 5C CB C8 1A 14 0E 2A 3B 03

: 55 CA BE F1 72 F2

:

（规范性附录）  
证书撤销列表内容表

表D.1 证书撤销列表内容表

|  |  |  |  |
| --- | --- | --- | --- |
| 域 | 关键项标识 | 值 | 描述 |
| CertificateList |  |  |  |
| signature |  |  |  |
| AlgorithmIdentifier |  |  | 必须与signatureAlgorithm域匹配. |
| algorithm |  | 选择下列算法 | |
| 1.2.840.113549.1.1.5 | sha-1WithRSAEncryption |
| 1.2.840.113549.1.1.11 | sha256WithRSAEncryption |
| 1.2.156.10197.1.501 | SM3WithSM2Encryption |
| parameters |  | NULL |  |
| tbsCertList |  |  | 待签名内容 |
| version |  | 2 | 版本2(整数1) |
| issuer |  |  |  |
| Name |  |  | 必须与发行者主题DN一致 |
| RDNSequence |  |  |  |
| RelativeDistinguishedName |  |  |  |
| AttributeTypeAndValue |  |  |  |
| AttributeType |  | OID |  |
| AttributeValue |  |  | 参考5.2.3.4 |
| 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 |  | 如果需要提供废除原因，请使用该扩展 |
| 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，则此扩展项不要增加。removeFromCRL只能用于增量CRL中，关于证书冻结certificateHold建议不要使用。 |
| invalidtyDate | 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SHA-1哈希算法摘要 |
| 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 |
| CRLNumber | FALSE | INTEGER | 单调递增序列，所有的CRL都应该包含这一项。 |
| issuingDistributionPoint | TRUE | OCTET字符串 | 本项出现在分块CRL中，如果CRL覆盖所有发行者签发的证书，则不需要包含此项。规范不建议使用间接CRL或不能覆盖所有原因码的CRL。 |
| distributionPoint |  |  |  |
| DistributionPointName |  |  | 使用在分块CRL中，必须与证书中的发布点扩展值一致。 |
| fullName |  |  |  |
| GeneralNames |  |  |  |
| GeneralName |  |  |  |
| 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 | 本标准不推荐使用间接CRL，如果本CRL包含了非本CRL发行者所颁发的证书，这一项必须设置为真。 |
| 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 |

（资料性附录）  
算法技术支持

E.1 散列函数

单向哈希函数（Hash Functions）也称为信息摘要算法。由于在Internet PKI中单向哈希函数MD5和SHA-1存在安全性问题，所以不提倡使用，建议使用SHA-256算法和中国的商用密码管理部门公布的SM3算法。

E.1.1 SHA-256单向哈希函数

安全哈希算法（SHA-256）作为安全哈希标准而出名，它是由NIST和NSA开发的，并在美国政府中使用。它由一个任意长度的字符串产生一个256比特的哈希值。SHA 256在FIPS PUB180-2被完整描绘。

E.1.2 SM3单向哈希函数

SM3单向杂凑算法是中国国家密码管理局2010年公布的中国商用密码杂凑算法标准。该算法消息分组512比特，输出杂凑值256比特，采用Merkle-Damgard结构。SM3密码杂凑函数在压缩函数中设计更为复杂，每一轮都是用2个消息字。

E.2 签名算法

E.2.1 概述

签名算法在证书或者CertificateList中的signatureAlgorithm字段内使用。证书通过一个出现在证书或CertificateList中的signatureAlgorithm字段内的算法标识符来表明算法。

国际上，RSA是在Internet应用中应用最广签名算法，在国内，SM2是国家密码局公布的签名算法，签名算法与D.1描述的单向哈希函数一起被使用。

E.2.2 RSA签名算法

RSA签名算法把RSA与SHA 256、SM3单向哈希函数结合起来。

SHA 256和RSA加密算法的签名算法的应用要采用填充和PKCS#1[RFC 2313]中描述的编码惯例。信息摘要使用SHA 256哈希算法进行计算。用于标识该签名算法的ASN.1对象标识符是：

sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {

iso（1） member-body（2） us（840） rsadsi（113549） pkcs（1）

pkcs-1（1） 5 }

SM3和RSA加密算法的签名算法是中国国内定义的。用于标识该签名算法的ASN.1对象标识符是：

sm3WithRSAEncryption OBJECT IDENTIFIER ::= {

iso（1） member-body（2） cn（156） ccstc（10197）1.503 }

E.2.3 SM2签名算法

SM2签名算法把SM2与SHA 256、SM3单向哈希函数结合起来。

SHA 256和SM2加密算法的签名算法的应用要采用填充和PKCS#1[RFC 2313]中描述的编码惯例。信息摘要使用SHA 256哈希算法进行计算。用于标识该签名算法的ASN.1对象标识符是：

sha-256WithSM2Encryption OBJECT IDENTIFIER ::= {

iso（1） member-body（2） cn（156） ccstc（10197）1.503 }

SM3和SM2加密算法的签名算法是中国国内定义的。用于标识该签名算法的ASN.1对象标识符是：

sm3WithSM2Encryption OBJECT IDENTIFIER ::= {

iso（1） member-body（2） cn（156） ccstc（10197） 1.501 }

E.3 公开密钥算法

E.3.1 概述

本标准描述的证书可以为任何公开密钥算法传送一个公开密钥。证书通过一个算法标识符指示算法。该算法标识符是一个OID和可选参数的结合。

当签发证书含有这些算法的公钥时，相应CA应使用确定的OID。支持这些算法的相应应用应至少能识别出本节确认的OID标识符。

E.3.2 RSA密钥

OID rsaEncryption 标识了RSA公开密钥。

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

rsadsi（113549） pkcs（1） 1 }

rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1}

rsaEncryption OID用于AlgorithmIdentifier类型值的算法字段中。对于该算法标识符，参数字段为ASN.1的NULL类型。

RSA公开密钥的编码采用ASN.1的RSAPublicKey类型：

RSAPublicKey ::= SEQUENCE {

modulus INTEGER, -- n

publicExponent INTEGER -- e -- }

modulus是模数 n，publicExponent是公开指数e。DER编码的RSAPublicKey是BIT STRING subjectPublicKey的值。

该OID用于RSA签名密钥和RSA加密密钥的公钥证书。密钥的应用目的在密钥用法（key usage）项中指明。本标准不推荐使用（同一个）单密钥进行签名和加密，但也不禁止特定条件下的应用。

如果keyUsage扩展出现于一张传送RSA公开密钥的终端实体证书中，则可以出现有下列值的组合：digitalSignature，nonRepudiation，keyEncipherment和dataEncipherment。如果keyUsage扩展出现于一张传送RSA公开密钥的CA证书中，则可以出现有下列值的组合：digitalSignature，nonRepudiation，keyEncipherment，dataEncipherment，keyCertSign和cRLSign。但是，本标准建议如果出现keyCertSign或者cRLSign，则keyEncipherment和dataEncipherment都不应该出现。

E.3.3 SM2密钥

E.3.3.1 椭圆曲线参数语法

椭圆曲线参数的表达采用与X962相同的ASN.1定义，其定义如下：

Parameters ::= CHOICE {

ecParameters ECParameters,

namedCurve ObjectIdentifier,

implicitlyCA NULL }

在用于SM2密码算法表达时，只使用namedCurve这一种表达方法。

E.3.3.2 公钥语法

椭圆曲线公钥的表达采用与X962相同的ASN.1定义，其定义如下：

SubjectPublicKeyInfo ::= SEQUENCE {

algorithm AlgorithmIdentifier {{ECPKAlgorithms}},

subjectPublicKey SM2PublicKey

}

其中

algorithm 定义了公钥的类型

subjectPublicKey定义了公钥的实际值

AlgorithmIdentifier是对象标识与参数的绑定，其定义如下：

AlgorithmIdentifier ::= SEQUENCE {

algorithm OBJECT IDENTIFIER,

parameters ANY DEFINED BY algorithm OPTIONAL

}

E.3.3.3 私钥语法

椭圆曲线私钥的表达采用与X962相同的ASN.1定义，其定义如下：

ECPrivateKey{CURVES:IOSet} ::= SEQUENCE {

version INTEGER { ecPrivkeyVer1(1) } (ecPrivkeyVer1),

privateKey SM2PrivateKey,

parameters [0] Parameters{{IOSet}} OPTIONAL,

publicKey [1] SM2PublicKey

}

其中：

version指定了私钥的版本号，这里使用整数１来表示SM2私钥的版本号。

密钥的应用目的在密钥用法（key usage）项中指明。本标准不推荐使用（同一个）单密钥进行签名和加密，但也不禁止特定条件下的应用。

如果keyUsage扩展出现于一张传送SM2公开密钥的终端实体证书中，则可以出现有下列值的组合：digitalSignature，nonRepudiation，keyEncipherment和dataEncipherment。如果keyUsage扩展出现于一张传送SM2公开密钥的CA证书中，则可以出现有下列值的组合：digitalSignature，nonRepudiation，keyEncipherment，dataEncipherment，keyCertSign和cRLSign。但是，本标准建议如果出现keyCertSign或者cRLSign，则keyEncipherment和dataEncipherment都不应该出现