电子政务数字证书格式规范

Digital Certificate Format Specification for E-Government

国家密码管理局

2010 年 8 月

目　　次

前　言

本标准主要规范各级政务部门在开展社会管理、公共服务等活动中所使用的数字证书格式。电子政务内网有关要求不在本规范中涉及。

本规范针对我国电子政务业务活动的特定需求，对数字证书的格式进行了规范，保障在电子政务业务活动中，不同认证机构签发的数字证书格式的统一性和互认性。

本规范附录A为资料性附录。

本规范由国家密码管理局提出并归口。

本规范主要起草单位：国家信息中心、山东省数字证书认证管理有限公司、长春吉大正元信息技术股份有限公司、上海格尔软件股份有限公司。

本规范主要起草人：吴亚非、任金强、彭建新、周国良、罗红斌、孟凡利、高建峰、闫仲森、罗清彩、解楠。

责任专家：邹烈。

引　言

信息与网络技术在极大促进社会经济、科技、文化、教育和管理等各个方面发展的同时，也带来了巨大的信息安全风险。随着我国电子政务业务的快速发展和应用的日益增多，迫切需要在电子政务网络环境中建立真实、有效的身份信任体制，确认电子政务业务参与方的有效身份，建立彼此间的信任关系以及保证信息的真实性、完整性、机密性和关键操作的不可否认性。

国家密码管理局已制定并颁布了相关的标准和规范，以促进和管理数字证书的应用。为了进一步促进和规范数字证书在电子政务中的应用，国家密码管理局同期开展电子认证服务数字证书系列标准规范的编制工作。

本规范为国家密码管理局编制的电子认证服务系列标准规范之一，以保障在电子政务业务活动中，不同认证机构签发的数字证书格式的统一性和互认性。

本规范根据电子政务业务的特点进行了细化，规定了电子政务个人证书、电子政务机构证书、电子政务设备证书、电子政务代码签名证书的格式，制定了相应的数字证书格式的模板。

本规范规定的电子政务数字证书格式支持双证书体系。

在本规范实施过程中，应遵守国家有关法律、法规的规定。

电子政务数字证书格式规范

1 范围

本规范定义了电子政务数字证书的基本结构，描述了数字证书中的各项数据内容，规范了证书扩展域，增加了满足国内电子政务应用需求的部分扩展项，并以电子政务数字证书基本结构为基础，定义了电子政务活动中个人、机构、设备、代码签名等不同类型数字证书的详细格式。

本规范适用于电子政务电子认证服务机构、数字证书认证系统的研制单位以及基于数字证书的安全应用开发单位。

2 规范性引用文件

下列文件中的条款通过本规范的引用而成为本规范的条款。凡是注明日期的引用文件，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规范，凡是未注明日期的引用文件，其最新版本适用于本规范。

GB/T 20518-2006 信息安全技术 公钥基础设施数字证书格式

GB/T 16262.1-2006 抽象语法记法一(ASN.1) 第 1 部分:基本记法规范(ISO/IEC 8824-1:2002,IDT)

GB/T 16262.2-2006 抽象语法记法一(ASN.1) 第 2 部分:客体信息规范(ISO/IEC 8824-2:2002,IDT)

GB/T 16262.3-2006 抽象语法记法一(ASN.1) 第 3 部分:约束规范(ISO/IEC 8824-3:2002,IDT)

GB/T 16262.4-2006 抽象语法记法一(ASN.1) 第 4 部分:ASN.1 规范的参数化(ISO/IEC 8824-4:2002,IDT)

GB/T 16264.8-2005 信息技术 开放系统互联 目录 第 8 部分:公钥和属性证书框架(ISO/IEC 9594-8:2001,IDT)

ISO/IEC 9594-2:2001 信息技术 开放系统互联 目录 第 2 部分:模型

GB/T 17969.1-2000 信息技术 开放系统互联 OSI 登记机构的操作规程 第 1 部分:一般规程(eqv ISO/IEC 9834-1:1993)

GB/T 11714-1997 全国组织机构代码编码规则

GB/T 16284.4-1996 信息技术 文本通信 面向信报的文本交换系统 第 4 部分:抽象服务定义和规程(IDT ISO/IET 10021-4:1990)

GB 12403-1990 干部职务名称代码

GB 8561-1988 专业技术职务代码

3 术语和定义

以下术语和定义适用于本规范。

3.1

公钥基础设施 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。

3.2

数字证书 digital certificate

由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.3

证书撤销列表 certificate revocation list

一个已标识的列表，它指定了一套证书发布者认为无效的证书。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CRL。

3.4

证书序列号 certificate serial number

为每个证书分配的唯一整数值，在CA颁发的证书范围内，此整数值与该CA所颁发的证书相关联并一一对应。

3.5

电子认证服务机构 electronic certification service provider

负责创建和分配证书，被用户信任的权威机构。用户可以选择该机构为其创建密钥。

3.6

证书撤销列表分布点 CRL distribution point

一个CRL目录项或其他CRL分发源，由CRL分布点分发的CRL可以包括仅对某CA所发证书全集某个子集的撤销条目，或者可以包括有多个CA的撤销条目。

4 符号和缩略语

下列缩略语适用于本规范：

ASN	抽象语法表示法	（Abstract Syntax Notation）
BER	基本编码规则	（Basic Encoding Rules）
C	国家	（Country）
CA	认证机构	（Certificate Authority）
CN	通用名	（Common Name）
CRL	证书撤销列表	（Certificate Revocation List）
DER	可区分编码规则	（Distinguished Encoding Rules）
DIT	目录信息树	（Directory Information Tree）
DN	可辨别名	（Distinguished Name）
O	机构	（Organization）
OID	对象标识符	（OBJECT IDENTIFIER）
OU	机构单位	（Organization Unit）
PKI	公钥基础设施	（Public Key Infrastructure）

5 电子政务数字证书格式

5.1 电子政务数字证书基本格式

5.1.1 数据结构

电子政务数字证书由基本证书域（TBSCertificate）、签名算法域（SignatureAlgorithm）和签名值域（SignatureValue）三部分组成。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v3
subjectUniqueID [2] IMPLICIT Unique Identifier OPTIONAL,
                    -- 如果出现，version必须是v3
extensions [3] EXPLICIT Extensions OPTIONAL 扩展项
                    -- 如果出现，version 必须是v3
}

Version ::= INTEGER { 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 }

上述证书数据结构中的tbsCertificate，signatureAlgorithm和signatureValue域的含义如下：

— tbsCertificate域包含了主题名称和签发者名称、主题的公钥、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标识符。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tbsCertificate中的signature标识的签名算法项相同。

—signatureValue域保存对tbsCertificate域进行数字签名的结果。以经过ASN.1 DER编码的tbsCertificate值作为数字签名的输入，签名的结果按照ASN.1编码的方式，生成BIT STRING，保存在证书签名值域内。

5.1.2 基本证书域（TBSCertificate）

基本证书域包含基本域和扩展域两部分。

5.1.2.1 基本域

基本域包含了证书结构中前十个项的信息，这些信息主要有主题和签发者的名称、主题公钥、有效期、版本号和序列号等。

5.1.2.1.1 版本 Version

本项描述了数字证书的版本号。

5.1.2.1.2 序列号 Serial number

本项是CA系统分配给每个证书的一个正整数，一个CA系统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 系统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。

5.1.2.1.3 签名算法 Signature

本项包含CA系统签发该证书所使用的密码算法标识符，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。

5.1.2.1.4 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、省、市名称等。其中AttributeValue部分的类型是由AttributeType确定的，通常它是一个DirectoryString类型。

签发的证书必须使用UTF8String格式对DirectoryString项进行编码。

5.1.2.1.5 有效期 Validity

本项是一个时间段，在这个时间段内，CA系统担保它将维护关于证书状态的信息。该项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。

遵循本规范的CA系统在2049年之前必须将该时间编码为UTCTime类型，在2050年之后，编码为GeneralizedTime类型。

a) 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。

在本项中，UTCTime值必须用格林威治标准时间（Zulu）表示，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）必须作如下解释：

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

b) 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。

本项中，GeneralizedTime值必须用格林威治标准时间表示，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）。

5.1.2.1.6 主题 Subject

本项用于描述与主题公钥项中的公钥相对应的实体的情况。主题名称可以出现在主题项或主题可选替换名称扩展项中（subjectAltName）。如果主题是一个CA系统，那么主题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）。如果主题的命名信息只出现在主题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），那么主题名称必须是一个空序列，主题可选替换名称扩展项必须被标识成关键的。

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

主题名称扩展项被定义成X.501的名字类型。

5.1.2.1.7 主题公钥信息 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。

5.1.2.1.8 颁发者唯一标识符 IssuerUniqueID

本项主要用来处理主题或者颁发者名称的重用问题。本规范建议不同的实体名称不要重用。遵循本规范的证书签发机构不应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。

5.1.2.1.9 主题唯一标识符 SubjectUniqueID

本项主要用来处理主题名称的重用问题，本规范建议对不同的实体名称不要重用，并且不建议使用此项，遵循本规范的证书签发机构不应生成带有主题唯一标识符的证书，但是在应用过程中应该能够解析唯一标识符并进行对比。

5.1.2.1.10 扩展项 Extensions

本项是一个或多个证书扩展的序列（SEQUENCE），其内容和数据结构在5.1.2.2中定义。

5.1.2.2 扩展域

本规范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。一个扩展项含有三部分，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。

本条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值。

遵循本规范的CA系统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系统签发的证书中的主题项为空序列，该CA系统就必须支持主题可替换名称扩展。其它的扩展是可选的。CA系统还可以支持本规范定义之外的其它扩展。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。

遵循本规范的应用必须至少能够识别密钥用法、主题替换名称、基本限制、名称限制、策略限制和扩展的密钥用法。另外，本规范建议还能支持认证机构（authority）和主题密钥标识符（subject key identifier）。

5.1.2.2.1 机构密钥标识符 authorityKeyIdentifier

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对应的公钥。当发起方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。识别可基于发起方证书中的主题密钥标识符或基于发起方的名称和序列号。

相应CA产生的所有证书应包括authorityKeyIdentifier扩展的keyIdentifier项，以便于证书信任链的建立。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，主题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：

a） keyIdentifier 由 BIT STRING subjectPublicKey 值的 160-bit SHA-1 散列值组成（去掉标签、长度和不使用的字节数目）。

b） keyIdentifier 由 0100 加上 subjectPublicKey 值的 SHA -1 散列值中最低位的 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。

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，如果证书颁发者的证书没有SubjectKeyIdetifier扩展，则可以使用以上介绍的两种方法之一来产生。

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

5.1.2.2.2 主题密钥标识符 subjectKeyIdentifier

本项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。它能够区分同一主题使用的不同密钥（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题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。

5.1.2.2.3 密钥用法 keyUsage

本项说明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：加密密钥或其它安全信息，例如用于密钥传输。
d) dataEncipherment：加密用户数据，但不包括上面 c）中的密钥或其它安全信息。
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）。
i) 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系统证书。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系统还可使用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，主题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，主题公钥可只用于脱密数据，同时执行密钥协议。

所有的CA系统证书必须包括本扩展，而且必须包含keycertSign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用途或其它多种用途，并可用于查找具有多密钥/证书实体的正确密钥/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。

5.1.2.2.4 扩展密钥用法 extKeyUsage

本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其它用途，并可用于查找多密钥/证书实体的正确密钥/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。

本规范定义下列密钥用途：

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

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

－TLS Web server 鉴别

－Key usage 比特可以与digitalSignature， keyEncipherment或keyAgreement一致

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

－TLS Web client鉴别

－Key usage 比特可以与digitalSignature和/或keyAgreement一致

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

－可下载执行代码的签名

－Key usage 比特可以与digitalSignature一致

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

－E-mail 保护

－Key usage比特可以与digitalSignature， nonRepudiation和/或（keyEncipherment或keyAgreement）一致

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

－将对象的散列值与同一时间源提供的时间绑定

－Key usage 比特可以与digitalSignature，nonRepudiation一致

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

－OCSP 应答签名

－Key usage 比特可以与digitalSignature，nonRepudiation一致

5.1.2.2.5 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，就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，就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。

注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。

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，例如，由于密钥泄露，那么，在验证时，必须有包含公开密钥的有效证书。在公开密钥的证书期满之后，签名验证者不能依赖CRL验证机制来验证密钥是否有效。

5.1.2.2.6 主题可选替换名称 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。

主题可选替换名扩展允许把附加身份加到证书的主题上。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，必须使用主题选择名称或颁发者选择名称扩展。由于主题可替换名被认为是与公钥绑在一起的，主题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/T 17969.1-2000对注册的客体分配的标识符。

CA系统不得签发带有subjectAltNames却包含空GeneralName项的证书。如果证书中的唯一主题身份是一个选择格式（如一个电子邮件地址），则主题的甄别名必须是空的（一个空序列），且subjectAltName扩展必须存在。如果主题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，证书的主题项包含无二义的标识主体的目录名称，推荐将此项标记为非关键的。

TYPE-IDENTIFIER类别的使用在GB/T 16262.2-2006的附录A和C中描述。

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，主题只能用此扩展中的名称或一些扩展名称来标识。

5.1.2.2.7 颁发者可选替换名称 issuerAltName

本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

此项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，允许证书使用系统忽略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5.1.2.2.6的说明进行编码。

5.1.2.2.8 主题目录属性 subjectDirectoryAttributes

本项为证书主题传送其期望的任何目录属性值。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。

5.1.2.2.9 基本限制 basicConstraints

本项用来标识证书的主题是否是一个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字段标识此数字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证书中必须包括本扩展，而且必须是关键的，否则，未被授权为CA的实体便可以签发证书，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。

注1：如果此扩展不存在或标记为非关键项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。

注2：为限制一证书主题只是一个端实体，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。

5.1.2.2.10 名称限制 nameConstraints

本项仅在一张CA证书使用，它指示了一个名称空间，在此空间设置的认证路径可以在后续证书主题名称中被找到。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，在主题CA和认证路径中后续CA颁发的所有证书中，只有那些在子树中具有与permittedSubtrees字段规定主题名称相同的证书才是可接受的。如果excludedSubtrees存在，由主题CA或认证路径中后续CA颁发的所有证书中，同excludedSubtrees规定主题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，并且证书在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。当证书主题具有同一名称形式的多个名称时（在directory Name名称形式情况下，包括证书主题项中的名称，如果非“0”），对于同一名称形式的名称限制应检验所有这些名称一致性。

可以对主题名称或主题选择名称进行限制。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题名称时，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。

本规范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。

本规范中，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。

5.1.2.2.11 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。它可用于认证政务机构证书，终端实体数字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，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）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CACompromise，或二者之一。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）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：

——能从 CA 获得一份完整 CRL 并检查该证书（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 分发者与签发 CA 的协调是 CA 策略的一个方面。

注2：证书撤销列表 CRL 的应用，请参照 RFC2459 中的第 5 章。

5.1.2.2.12 最新证书撤销列表 freshestCRL

最新CRL扩展一般作为证书扩展使用，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策略来决定是否需要检查最新的CRL。

5.1.2.2.13 个人身份标识码 IdentifyCode

个人身份证号码扩展项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}

```
IdentifyCode ::=SET {
        residenterCardNumber          [0] PRINTABLESTRING OPTIONAL,
        militaryOfficerCardNumber     [1] UTF8String OPTIONAL,
        passportNumber                [2] PRINTABLESTRING OPTIONAL,
        ...
}
```

residenterCardNumber　　－身份证号码

militaryOfficerCardNumber　　－军官证号码

passportNumber　　－护照号码

此扩展项标记为非关键的。

5.1.2.2.14 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。

5.1.2.2.15 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 ::={ 1.2.156.10260.4.1.3 }

ICRegistrationNumber::= PRINTABLESTRING

此扩展项标记为非关键的。

5.1.2.2.16 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。

5.1.2.2.17 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 ::={ 1.2.156. 10260.4.1.5 }

TaxationNumeber::= PRINTABLESTRING

此扩展项标记为非关键的。

5.1.2.2.18 增强型密钥用法 extendedKeyUsage

增强型密钥用法用于说明证书用于何种扩展性的用途，其定义如下：

```
extendedKeyUsage EXTENSION ::= {
        SYNTAX SEQUENCE SIZE （1..MAX） OF KeyPurposeId
        IDENTIFIED BY id-ce-extKeyUsage }

KeyPurposeId ::= OBJECT IDENTIFIER
-- PKIX-defined extended key purpose OIDs
id-kp-serverAuth          OBJECT IDENTIFIER ::= { id-kp 1 }
id-kp-clientAuth          OBJECT IDENTIFIER ::= { id-kp 2 }
id-kp-codeSigning         OBJECT IDENTIFIER ::= { id-kp 3 }
id-kp-emailProtection OBJECT IDENTIFIER ::= { id-kp 4 }
id-kp-ipsecEndSystem    OBJECT IDENTIFIER ::= { id-kp 5 }
id-kp-ipsecTunnel         OBJECT IDENTIFIER ::= { id-kp 6 }
id-kp-ipsecUser           OBJECT IDENTIFIER ::= { id-kp 7 }
id-kp-timeStamping        OBJECT IDENTIFIER ::= { id-kp 8 }
```

5.1.2.2.19 颁发机构信息访问 AuthorityInfoAccess

本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。

当id-ad-caIssuers以accessInfoType出现时，acessLocaion字段描述了获得访问协议的形式。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。

5.1.2.2.20 主体信息访问 SubjectInformationAccess

本项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，如果主体是用户，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协议的说明中定义。这个扩展项必须定义为非关键的。

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

SubjectInfoAccessSyntax ::=
SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription ::= SEQUENCE {
accessMethod OBJECT IDENTIFIER,
accessLocation GeneralName }

5.1.3 签名算法域（SignatureAlgorithm）

该域包含CA系统颁发该证书所使用的密码算法标识符，应与基本证书域中的签名算法所标识的签名算法相同，可选参数的内容完全依赖所标识的具体算法。

5.1.4 签名值域（SignatureValue）

该域保存对基本证书域进行数字签名的结果，经过ASN.1 DER编码的基本证书域作为数字签名算法的输入，签名的结果按照ASN.1编码成BIT STRING类型并保存在签名值域。

5.2 电子政务个人数字证书格式

5.2.1 概述

电子政务个人数字证书指面向政务业务所涉及到的计算机终端用户（如各级政府部门工作人员、经办人员、公众等）发放的证书。

5.2.2 电子政务个人数字证书基本证书域

电子政务个人数字证书基本证书域由基本域和扩展域组成。

5.2.2.1 电子政务个人证书基本域

见5.1.2.1章节。

5.2.2.2 电子政务个人证书扩展域

电子政务个人证书扩展域可包含如下扩展项：

a) 机构密钥标识符AuthorityKeyIdentifier
b) 主题密钥标识符 SubjectKeyIdentifier
c) 密钥用法 KeyUsage
d) 增强型密钥用法 ExtendedKeyUsage
e) 主题可选替换名称 SubjectAlternativeName
f) 颁发者可选替换名称 IssuerAlternativeName

g) 主题目录属性 SubjectDirectoryAttributes
h) 基本限制 BasicConstraints
i) 证书撤销列表分发点 CRLDistributionPoints
j) 最新证书撤销列表 FreshestCRL
k) 颁发机构信息访问 AuthorityInfoAccess
l) 主题信息访问 SubjectInformationAccess
m) 个人身份证标识码 IdentifyCardNumber
n) 个人社会保险号 InsuranceNumber

5.2.3 电子政务个人证书模板定义

电子政务个人证书包含如下扩展项：
a) 基本限制BasicConstraints
b) 密钥用法 KeyUsage
c) 增强型密钥用法 ExtendedKeyUsage
d) 颁发机构密钥标识符 AuthorityKeyIdentifier
e) 证书撤销列表分发点 CRLDistributionPoints
f) 颁发机构信息访问 AuthorityInfoAccess
g) 主题密钥标识符 SubjectKeyIdentifier

电子政务个人签名证书密钥用法（KeyUsage）扩展域子项可为：
a) 数字签名（digitalSignature）
b) 不可否认（nonRepudiation）

电子政务个人加密证书密钥用法（KeyUsage）扩展域子项可为：
a) 密钥加密（keyEncipherment）
b) 数据加密（dataEncipherment）

电子政务个人证书增强型密钥用法（ExtendKeyUsage）扩展域子项可为：
a) 客户端认证（ClientAuth）

5.2.4 电子政务个人数字证书格式

电子政务个人数字证书的发放对象包括政务部门工作人员和参与电子政务活动的社会公众人员等。

5.2.4.1 电子政务部门工作人员数字证书

数字证书的大小一般不应超过4K字节，请在设定数字证书各项取值的时候予以注意。

证书域名	含义	说明	字段内容（示例）
Version	版本号	表示 X.509 证书版本	V3
Serial Number	序列号	由证书颁发机构指定，参见 5.1.2.1.2 章节	
Signature	签名算法	遵循国家密码主管部门的要求	

Issuer	颁发者	CN	名称(CN)	证书颁发 CA 的名称
		O	(O)	例如：电子政务电子认证基础设施
		C	国家(C)	CN
Validity	有效期限	notBefore	有效期起始日期	签发日期,年月日+时分秒
		notAfter	有效期终止日期	起始日期+有效期,年月日+时分秒
Subject	主题	名称(CN)	个人姓名	例如：吴永胜
		E	邮件地址	
		OU	10 级组织机构名称	从 1 级组织机构名称到 10 级组织机构名称均为可选，具体按照政务部门实际组织层级结构进行定义。例如：ou=内蒙古自治区公安厅，ou=呼和浩特市公安局，ou=交警支队，ou=事故科
		OU	……	
		OU	1 级组织机构名称	
		O	省部级名称	必填
		C	C	CN
Subject Public Key Information	公钥	主题公钥信息		遵循国家密码主管部门的要求
BasicConstraints	基本限制	表示证书持有者是否是认证结点		详细定义见基本限制 basicConstraints

扩展域	KeyUsage	密钥用法	个人签名证书密钥用法（KeyUsage）扩展域子项为： 数字签名（digitalSignature） 不可否认（nonRepudiation） 个人加密证书密钥用法（KeyUsage）扩展域子项为： 密钥加密（keyEncipherment） 数据加密（dataEncipherment）	详细定义见密钥用法 keyUsage
	ExtendedKeyUsage	增强型密钥用法	增强型密钥用法，包括扩展域： 客户端认证（clientAuth）	详细定义见增强型密钥用法 extendedKeyUsage
	AuthorityKeyIdentifier	颁发机构密钥标识符	颁发机构公钥的 hash 值	详细定义见机构密钥标识符 authorityKeyIdentifier
	CRLDistributionPoints	证书撤销列表分发点	CRL 发布点，可以为多个值	详细定义见证书撤销列表分发点 CRLDistributionPoints
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值	详细定义见颁发机构信息访问 AuthorityInfoAccess
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值	详细定义见主题密钥标识符 subjectKeyIdentifier
SignatureAlgorithm		该域包含 CA 系统颁发该证书所使用的密码算法标识符	遵循国家密码主管部门的要求	
Issuer’s Signature		签名值	颁发机构对证书基本信息的数字签名	数字签名值

5.2.4.2 社会公众数字证书

数字证书的大小一般不应超过4K字节，请在设定数字证书各项取值的时候予以注意。

证书域名		含义	说明		字段内容（示例）
Version		版本号	表示 X.509 证书版本		V3
Serial Number		序列号	由证书颁发机构指定，参见 5.1.2.1.2 章节		
Signature		签名算法	遵循国家密码主管部门的要求		
Issuer		颁发者	CN	名称(CN)	证书颁发 CA 的名称
			O	(O)	证书颁发 CA 的组织机构名称
			C	国家(C)	CN
Validity		有效期限	notBefore	有效期起始日期	签发日期,年月日+时分秒
			notAfter	有效期终止日期	起始日期+有效期,年月日+时分秒
Subject		主题	名称(CN)	个人姓名	例如：李军
			E	邮件地址	例如：lj@@kejifz.com
			OU	10 级地域名称	从 1 级地域名称到 10 级地域名称均为可选，按照实际的证书持有人所属地域名称进行定义。例如：ou=海淀区，ou=知春路 10008 号，ou=知春里小区，ou=501 号楼 3 单元 307
			OU	……	
			OU	1 级地域名称	
			O	省、自治区、直辖市	必填
			C	C	CN
Subject Public Key Information		公钥	主题公钥信息		遵循国家密码主管部门的要求
	BasicConstraints	基本限制	表示证书持有者是否是认证结点		详细定义见基本限制 basicConstraints
	KeyUsage	密钥用法	个人签名证书密钥用法（KeyUsage）扩展域子项为：		详细定义见密钥用法 keyUsage

扩展域			数字签名（digitalSignature） 不可否认（nonRepudiation） 加密证书密钥用法（KeyUsage）扩展域子项为： 密钥加密（keyEncipherment） 数据加密（dataEncipherment）	
	ExtendedKeyUsage	增强型密钥用法	增强型密钥用法，包括扩展域： 客户端认证（clientAuth）	详细定义见增强型密钥用法 extendedKeyUsage
	AuthorityKeyIdentifier	颁发机构密钥标识符	颁发机构公钥的 hash 值	详细定义见机构密钥标识符 authorityKeyIdentifier
	CRLDistributionPoints	证书撤销列表分发点	CRL 发布点，可以为多个值	详细定义见证书撤销列表分发点 CRLDistributionPoints
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值	详细定义见颁发机构信息访问 AuthorityInfoAccess
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值	详细定义见主题密钥标识符 subjectKeyIdentifier
SignatureAlgorithm		该域包含 CA 系统颁发该证书所使用的密码算法标识符	遵循国家密码主管部门的要求	
Issuer’s Signature		签名值	颁发机构对证书基本信息的数字签名	数字签名值

5.3 电子政务机构数字证书格式

5.3.1 概述

电子政务机构数字证书指面向政务业务所涉及到的机构（如各级政务部门、企事业单位等）发放的证书。

5.3.2 电子政务机构证书基本证书域

基本证书域由基本域和扩展域组成。

5.3.2.1 电子政务机构证书基本域

见5.1.2.1章节。

5.3.2.2 电子政务机构证书扩展域

电子政务机构证书扩展域可包含如下扩展项：

a) 机构密钥标识符 AuthorityKeyIdentifier
b) 主题密钥标识符 SubjectKeyIdentifier
c) 密钥用法 KeyUsage
d) 增强型密钥用法 ExtendedKeyUsage
e) 主题可选替换名称 SubjectAlternativeName
f) 颁发者可选替换名称 IssuerAlternativeName
g) 主题目录属性 SubjectDirectoryAttributes
h) 基本限制 BasicConstraints
i) 证书撤销列表分发点 CRLDistributionPoints
j) 最新证书撤销列表 FreshestCRL
k) 颁发机构信息访问 AuthorityInfoAccess
l) 主题信息访问 SubjectInformationAccess
m) 企业工商注册号 ICRegistrationNumber
n) 企业组织机构代码 OrganizationCode
o) 企业税号 TaxationNumber

5.3.3 电子政务机构证书模板定义

电子政务机构证书包含如下扩展项：

a) 基本限制 BasicConstraints
b) 密钥用法 KeyUsage
c) 增强型密钥用法 ExtendedKeyUsage
d) 颁发机构密钥标识符 AuthorityKeyIdentifier
e) 证书撤销列表分发点 CRLDistributionPoints
f) 颁发机构信息访问 AuthorityInfoAccess
g) 主题密钥标识符 SubjectKeyIdentifier

电子政务机构签名证书密钥用法（KeyUsage）扩展域子项可为：

a) 数字签名（digitalSignature）
b) 不可否认（nonRepudiation）
c) 密钥协商（key agreement）
d) 密钥加密（keyEncipherment）

电子政务机构加密证书密钥用法（KeyUsage）扩展域子项可为：

a) 密钥加密（keyEncipherment）
b) 数据加密（dataEncipherment）

电子政务机构证书增强型密钥用法（ExtendKeyUsage）扩展域子项可为：

a) 客户端认证（ClientAuth）

5.3.4 电子政务机构证书格式

电子政务机构数字证书的发放对象包括政务部门、企事业单位等。

5.3.4.1 政务部门机构证书

数字证书的大小一般不应超过4K字节，请在设定数字证书各项取值的时候予以注意。

证书域名	含义	说明		字段内容（示例）
Version	版本号	表示 X.509 证书版本		V3
Serial Number	序列号	由证书颁发机构指定，参见 5.1.2.1.2 章节		
Signature	签名算法	遵循国家密码主管部门的要求		
Issuer	颁发者	CN	名称(CN)	证书颁发 CA 的名称
		O	(O)	证书颁发 CA 的组织机构名称
		C	国家(C)	CN
Validity	有效期限	notBefore	有效期起始日期	签发日期,年月日+时分秒
		notAfter	有效期终止日期	起始日期+有效期,年月日+时分秒
Subject	主题	名称(CN)	机构名称	例如：事故科
		E	邮件地址	
		OU	10 级组织机构名称	从 1 级组织机构名称到 10 级组织机构名称均为可选，具体按照政务部门实际组织层级结构进行定义。例如：ou=内蒙古自治区公安厅，ou=呼和浩特市公安局，ou=交警支队
		OU	……	
		OU	1级组织机构名称	
		O	省部级名称	必填
		C	C	CN
Subject Public Key Information	公钥	主题公钥信息		按照国家密码管理局的要求来执行

扩展域	BasicConstraints	基本限制	表示证书持有者是否是认证结点	详细定义见基本限制 basicConstraints
	KeyUsage	密钥用法	机构签名证书密钥用法（KeyUsage）扩展域子项为： 数字签名（digitalSignature） 不可否认（nonRepudiation） 密钥协商（key agreement） 密钥加密（keyEncipherment） 机构加密证书密钥用法（KeyUsage）扩展域子项为： 密钥加密（keyEncipherment） 数据加密（dataEncipherment）	详细定义见密钥用法 keyUsage
	ExtendedKeyUsage	增强型密钥用法	增强型密钥用法，包括扩展域：客户端认证（clientAuth）	详细定义见增强型密钥用法 extendedKeyUsage
	AuthorityKeyIdentifier	颁发机构密钥标识符	颁发机构公钥的 hash 值	详细定义见机构密钥标识符 authorityKeyIdentifier
	CRLDistributionPoints	证书撤销列表分发点	CRL 发布点，可以为多个值	详细定义见证书撤销列表分发点 CRLDistributionPoints
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值	详细定义见颁发机构信息访问 AuthorityInfoAccess
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值	详细定义见主题密钥标识符 subjectKeyIdentifier

SignatureAlgorithm	该域包含CA 系统颁发该证书所使用的密码算法标识符	遵循国家密码主管部门的要求	
Issuer’s Signature	签名值	颁发机构对证书基本信息的数字签名	数字签名值

5.3.4.2 企业机构证书

数字证书的大小一般不应超过4K字节，请在设定数字证书各项取值的时候予以注意。

证书域名	含义	说明		字段内容（示例）
Version	版本号	表示 X.509 证书版本		V3
Serial Number	序列号	由证书颁发机构指定，参见 5.1.2.1.2 章节		
Signature	签名算法	遵循国家密码主管部门的要求		
Issuer	颁发者	CN	名称(CN)	证书颁发 CA 的名称
		O	(O)	证书颁发 CA 的组织机构
		C	国家(C)	CN
Validity	有效期限	notBefore	有效期起始日期	签发日期,年月日+时分秒
		notAfter	有效期终止日期	起始日期+有效期,年月日+时分秒
Subject	主题	名称(CN)	机构注册名称	例如：科技发展公司
		E	邮件地址	例如：kjfz@kejifz.com
		OU	10 级地域名称	从 1 级地域名称到 10 级地域名称均为可选，按照实际的证书持有机构所属地域名称进行定义。例如：ou=海淀区，ou=知春路 118 号，ou=银网中心，ou=B 座 12 层
		OU	……	
		OU	1 级地域名称	
		O	省、自治区、直辖市	必填
		C	C	CN

Subject Public Key Information		公钥	主题公钥信息	遵循国家密码主管部门的要求
扩展域	BasicConstraints	基本限制	表示证书持有者是否是认证结点	详细定义见基本限制 basicConstraints
	KeyUsage	密钥用法	机构签名证书密钥用法（KeyUsage）扩展域子项为： 数字签名（digitalSignature） 不可否认（nonRepudiation） 密钥协商（key agreement） 密钥加密（keyEncipherment） 机构加密证书密钥用法（KeyUsage）扩展域子项为： 密钥加密（keyEncipherment） 数据加密（dataEncipherment）	详细定义见密钥用法 keyUsage
	ExtendedKeyUsage	增强型密钥用法	增强型密钥用法，包括扩展域：客户端认证（clientAuth）	详细定义见增强型密钥用法 extendedKeyUsage
	AuthorityKeyIdentifier	颁发机构密钥标识符	颁发机构公钥的 hash 值	详细定义见机构密钥标识符 authorityKeyIdentifier
	CRLDistributionPoints	证书撤销列表分发点	CRL 发布点，可以为多个值	详细定义见证书撤销列表分发点 CRLDistributionPoints
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值	详细定义见颁发机构信息访问 AuthorityInfoAccess
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值	详细定义见主题密钥标识符 subjectKeyIdentifier
SignatureAlgorithm		该域包含 CA 系统颁发该证书所使用的密码算法标识符	遵循国家密码主管部门的要求	
Issuer’s Signature		签名值	颁发机构对证书基本信息的数字签名	数字签名值

5.4 电子政务设备数字证书格式

5.4.1 概述

电子政务设备数字证书指面向政务业务所涉及到的设备（如网络设备、服务器、终端设备等）发放的证书。

5.4.2 电子政务设备证书基本证书域

基本证书域由基本域和扩展域组成。

5.4.2.1 电子政务设备证书基本域

见5.1.2.1章节。

5.4.2.2 电子政务设备证书扩展域

电子政务设备证书扩展域可包含如下扩展项：

a) 机构密钥标识符 AuthorityKeyIdentifier
b) 主题密钥标识符 SubjectKeyIdentifier
c) 密钥用法 KeyUsage
d) 增强型密钥用法 ExtendedKeyUsage
e) 主题可选替换名称 SubjectAlternativeName
f) 颁发者可选替换名称 IssuerAlternativeName
g) 主题目录属性 SubjectDirectoryAttributes
h) 基本限制 BasicConstraints
i) 证书撤销列表分发点 CRLDistributionPoints
j) 最新证书撤销列表 FreshestCRL
k) 颁发机构信息访问 AuthorityInfoAccess

5.4.3 电子政务设备证书模板定义

电子政务设备证书包含如下扩展项：

a) 基本限制 BasicConstraints
b) 密钥用法 KeyUsage
c) 增强型密钥用法 ExtendedKeyUsage
d) 颁发机构密钥标识符 AuthorityKeyIdentifier
e) 证书撤销列表分发点 CRLDistributionPoints
f) 颁发机构信息访问 AuthorityInformationAccess
g) 主题密钥标识符 SubjectKeyIdentifier

电子政务设备证书密钥用法（KeyUsage）扩展域子项可为：

a) 数字签名（digitalSignature）
b) 不可否认（nonRepudiation）
c) 密钥协商（key agreement）
d) 密钥加密（keyEncipherment）
e) 数据加密（dataEncipherment）

电子政务设备证书增强型密钥用法（ExtendKeyUsage）扩展域子项可为：

a） 服务端认证（ServerAuth）

5.4.4 电子政务设备证书格式

数字证书的大小一般不应超过4K字节，请在设定数字证书各项取值的时候予以注意。

证书域名		含义	说明		字段内容（示例）
Version		版本号	表示 X.509 证书版本		V3
Serial Number		序列号	由证书颁发机构指定，参见 5.1.2.1.2 章节		
Signature		签名算法	遵循国家密码主管部门的要求		
Issuer		颁发者	CN	名称(CN)	证书颁发 CA 的名称
			O	(O)	证书颁发 CA 的组织机构名称
			C	国家(C)	CN
Validity		有效期限	notBefore	有效期起始日期	签发日期,年月日+时分秒
			notAfter	有效期终止日期	起始日期+有效期,年月日+时分秒
Subject		主题	名称(CN)	证书持有者的域名、IP 地址或者其他可以标识身份的内容	www.audit.gov 或 192.168.87.7
			OU	10 级组织机构名称	从 1 级组织机构名称到 10 级组织机构名称均为可选，具体按照政务部门实际组织层级结构进行定义。例如：ou=内蒙古自治区公安厅，ou=呼和浩特市公安局，ou=交警支队，ou=事故科
			OU	……	
			OU	1 级组织机构名称	
			O	省部级名称	必填
			C	C	CN
Subject Public Key Information		公钥	主题公钥信息		遵循国家密码主管部门的要求
	BasicConstraints	基本限制	该证书持有者是否是认证结点		详细定义见基本限制 basicConstraints

扩展域	KeyUsage	密钥用法	密钥用法（KeyUsage）扩展域子项为： 数字签名（digitalSignature） 不可否认（nonRepudiation） 密钥协商（key agreement） 密钥加密（keyEncipherment） 数据加密（dataEncipherment）	详细定义见密钥用法 keyUsage
	ExtendedKeyUsage	增强型密钥用法	增强型密钥用法，包括扩展域： 服务端认证（serverAuth）	详细定义见增强型密钥用法 extendedKeyUsage
	AuthorityKeyIdentifier	颁发机构密钥标识符	颁发机构公钥的 hash 值	详细定义见机构密钥标识符 authorityKeyIdentifier
	CRLDistributionPoints	证书撤销列表分发点	CRL 发布点，可以为多个值	详细定义见证书撤销列表分发点 CRLDistributionPoints
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值	详细定义见颁发机构信息访问 AuthorityInfoAccess
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值	详细定义见主题密钥标识符 subjectKeyIdentifier
SignatureAlgorithm		该域包含 CA 系统颁发该证书所使用的密码算法标识符	遵循国家密码主管部门的要求	
Issuer’s Signature		签名值	颁发机构对证书基本信息的数字签名	数字签名值

5.5 电子政务代码签名数字证书格式

5.5.1 概述

电子政务代码签名数字证书是指向电子政务系统代码进行数字签名发放的数字证书。

5.5.2 电子政务代码签名证书基本证书域

基本证书域由基本域和扩展域组成。

5.5.2.1 电子政务代码签名证书基本域

见5.1.2.1章节。

5.5.2.2 电子政务代码签名证书扩展域

电子政务代码签名证书扩展域可包含如下扩展项：

a) 机构密钥标识符 AuthorityKeyIdentifier
b) 主题密钥标识符 SubjectKeyIdentifier
c) 密钥用法 KeyUsage
d) 增强型密钥用法 ExtendedKeyUsage
e) 主题可选替换名称 SubjectAlternativeName
f) 颁发者可选替换名称 IssuerAlternativeName
g) 主题目录属性 SubjectDirectoryAttributes
h) 基本限制 BasicConstraints
i) 证书撤销列表分发点 CRLDistributionPoints
j) 最新证书撤销列表 FreshestCRL
k) 颁发机构信息访问 AuthorityInfoAccess
l) 主题信息访问 SubjectInformationAccess

5.5.3 电子政务代码签名证书模板定义

电子政务个人证书包含如下扩展项：

a) 基本限制 BasicConstraints
b) 密钥用法 KeyUsage
c) 颁发机构密钥标识符 AuthorityKeyIdentifier
d) 证书撤销列表分发点 CRLDistributionPoints
e) 颁发机构信息访问 AuthorityInfoAccess
f) 主题密钥标识符 SubjectKeyIdentifier
g) 增强型密钥用法 ExtendedKeyUsage

证书密钥用法（KeyUsage）扩展域子项为：

a) 数字签名（digitalSignature）
b) 不可否认（nonRepudiation）

电子政务代码签名证书增强型密钥用法（ExtendKeyUsage）扩展域子项为：

a) 代码签名（codeSign）

5.5.4 电子政务代码签名证书格式

一般数字证书的大小不应该超过4K字节，请在设定数字证书各项取值的时候予以注意。

证书域名	含义	说明	字段内容（示例）
Version	版本号	表示 X.509 证书版本	V3
Serial Number	序列号	由证书颁发机构指定，参见 5.1.2.1.2 章节	
Signature	签名算法	遵循国家密码主管部门的要求	

Issuer		颁发者	CN	名称(CN)	证书颁发 CA 的名称
			O	(O)	证书颁发 CA 的组织机构名称
			C	国家(C)	CN
Validity		有效期限	notBefore	有效期起始日期	签发日期,年月日+时分秒
			notAfter	有效期终止日期	起始日期+有效期,年月日+时分秒
Subject		主题	名称(CN)	机构名称	例如：科技发展公司
			E	邮件地址	
			OU	10 级地域名称	从 1 级地域名称到 10 级地域名称均为可选，按照实际的证书持有机构所属地域名称进行定义。例如：ou=海淀区，ou=知春路 118 号，ou=银网中心，ou=B 座 12 层
			OU	……	
			OU	1 级地域名称	
			O	省、自治区、直辖市	必填
			C	C	CN
Subject Public Key Information		公钥	主题公钥信息		遵循国家密码主管部门的要求
扩展域	BasicConstraints	基本限制	该证书持有者是否是认证结点		详细定义见基本限制 basicConstraints
	KeyUsage	密钥用法	密钥用法（KeyUsage）扩展域子项为： 数字签名（digitalSignature） 不可否认（nonRepudiation）		详细定义见密钥用法 keyUsage
	ExtendedKeyUsage	增强型密钥用法	增强型密钥用法，包括扩展域： 代码签名（codeSign）		详细定义见增强型密钥用法 extendedKeyUsage
	AuthorityKeyIdentifier	颁发机构密钥标识符	颁发机构公钥的 hash 值		详细定义见机构密钥标识符 authorityKeyIdentifier

	CRLDistributionPoints	证书撤销列表分发点	CRL 发布点，可以为多个值	详细定义见证书撤销列表分发点 CRLDistributionPoints
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值	详细定义见颁发机构信息访问 AuthorityInfoAccess
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值	详细定义见主题密钥标识符 subjectKeyIdentifier
SignatureAlgorithm		该域包含 CA 系统颁发该证书所使用的密码算法标识符	遵循国家密码主管部门的要求	
Issuer’s Signature		签名值	颁发机构对证书基本信息的数字签名	数字签名值

5.6 其他

本规范没有涉及到的特殊需求的证书格式，在不违背本规范中定义的证书基本格式的前提下，根据业务的实际要求进行扩展定义。

6 密码算法技术的支持

密码算法使用国家密码管理主管部门审核批准的相关算法。

附 录 A
（资料性附录）
数字证书编码举例

A.1 电子政务部门工作人员数字证书编码举例

以下内容以电子政务部门工作人员数字证书中的签名证书为例，证书包含下列信息：

a) the serial number is 32 1B B3 63 E6 43 B1 7A AE A4 1E 73;
b) the certificate is signed with RSA and the sha1 hash algorithm;
c) the issuer's distinguished name is CN=SubCA;O=test;C=CN;
d) the subject's distinguished name is CN=测试证书; E=test@mail.com;OU=东城区;OU=北京市; O=测试证书; C=CN;
e) the certificate was issued on 20100809 and expired on 20100809
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 include an authority key identifier ,subject KeyIdentifier and basic constraints extensions;
i) the certificate includes a critical key usage extension: Digital Signatures, Non-Repudiation;
j) the certificate include an extend key usage extensions:Client Auth,Email Protection ;
k) the certificate include a CRL distribution points extensions;
l) the certificate include a authority info access extensions;

```
0000 30   419: SEQUENCE {
0004 30   382:   SEQUENCE {
0008 A0     3:     [0] {
000A 02     1:       INTEGER 2
             :       }
000D 02     C:     INTEGER
             :       32 1B B3 63 E6 43 B1 7A       2..c.C.z
             :       AE A4 1E 73                     ...s
001B 30     D:     SEQUENCE {
001D 06     9:       OBJECT IDENTIFIER
             :         sha1withRSAEncryption (1 2 840 113549 1 1 5)
             :         (PKCS #1)
0028 05     0:       NULL
             :       }
002A 30    2C:     SEQUENCE {
002C 31     B:       SET {
002E 30     9:         SEQUENCE {
0030 06     3:           OBJECT IDENTIFIER countryName (2 5 4 6)
```

```
                :                 (X.520 id-at (2 5 4))
0035 13      2:               PrintableString 'CN'
                :               }
                :             }
0039 31      D:           SET {
003B 30      B:             SEQUENCE {
003D 06      3:               OBJECT IDENTIFIER organizationName (2 5 4 10)
                :                 (X.520 id-at (2 5 4))
0042 0C      4:               UTF8String 'test'
                :               }
                :             }
0048 31      E:           SET {
004A 30      C:             SEQUENCE {
004C 06      3:               OBJECT IDENTIFIER commonName (2 5 4 3)
                :                 (X.520 id-at (2 5 4))
0051 0C      5:               UTF8String 'SubCA'
                :               }
                :             }
                :           }
0058 30     1E:         SEQUENCE {
005A 17      D:           UTCTime '100809073950Z'
0069 17      D:           UTCTime '110809073950Z'
                :           }
0078 30     81:         SEQUENCE {
007B 31      B:           SET {
007D 30      9:             SEQUENCE {
007F 06      3:               OBJECT IDENTIFIER countryName (2 5 4 6)
                :                 (X.520 id-at (2 5 4))
0084 0C      2:               UTF8String 'CN'
                :               }
                :             }
0088 31     15:           SET {
008A 30     13:             SEQUENCE {
008C 06      3:               OBJECT IDENTIFIER organizationName (2 5 4 10)
                :                 (X.520 id-at (2 5 4))
0091 0C      C:               UTF8String ‘测试证书’
                :               }
                :             }
009F 31     12:           SET {
00A1 30     10:             SEQUENCE {
00A3 06      3:               OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
                :                 (X.520 id-at (2 5 4))
00A8 0C      9:               UTF8String '北京市'
                :               }
```

```
                :             }
00B3 31    12:           SET {
00B5 30    10:             SEQUENCE {
00B7 06     3:               OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
                :                 (X.520 id-at (2 5 4))
00BC 0C     9:               UTF8String '东城区'
                :             }
                :           }
00C7 31    1C:           SET {
00C9 30    1A:             SEQUENCE {
00CB 06     9:               OBJECT IDENTIFIER emailAddress (1 2 840 113549 1 9 1)
                :                 (PKCS #9 (1 2 840 113549 1 9).  Deprecated, use an altName
extension instead)
00D6 16     D:               IA5String 'test@mail.com'
                :             }
                :           }
00E5 31    15:           SET {
00E7 30    13:             SEQUENCE {
00E9 06     3:               OBJECT IDENTIFIER commonName (2 5 4 3)
                :                 (X.520 id-at (2 5 4))
00EE 0C     C:               UTF8String '测试证书'
                :             }
                :           }
                :         }
00FC 30    9F:         SEQUENCE {
00FF 30     D:           SEQUENCE {
0101 06     9:             OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
                :                 (PKCS #1)
010C 05     0:             NULL
                :           }
010E 03    8D:           BIT STRING 0 unused bits
                :             30 81 89 02 81 81 00 C8       0.......
                :             75 D2 11 E2 5C F7 E1 C6       u...\...
                :             53 16 97 31 9D 60 0D 11       S..1.`..
                :             00 55 48 93 9B 9C 09 F6       .UH.....
                :             46 87 04 B5 AC A5 ED 42       F......B
                :             CC 5C 91 85 D1 33 F8 C4       .\...3..
                :             8F 5D 90 45 BD BA A6 6E       .].E...n
                :             43 AC 3F 28 F3 EC 88 36       C.?(...6
                :             C3 6A FF 09 A4 34 2E 5F       .j...4._
                :             56 49 61 1F C8 3E D6 A6       VIa..>..
                :             F6 8D 15 E6 F1 21 74 FA       .....!t.
                :             66 14 95 45 E9 E4 A4 18       f..E....
                :             E3 31 B7 BC 15 DF 50 A6       .1....P.
```

```
                :              B3 AB 13 DE DD 04 CB 81        ........
                :              76 A0 3F 73 6C F1 67 48        v.?sl.gH
                :              DC 96 00 D3 3C 90 98 BC        ....<...
                :              48 62 B5 CA 3B 47 A9 02        Hb..;G..
                :              03 01 00 01                    ....
                :            }
019E A3   1E8:       [3] {
01A2 30   1E4:         SEQUENCE {
01A6 30     F:           SEQUENCE {
01A8 06     3:             OBJECT IDENTIFIER basicConstraints (2 5 29 19)
                :               (X.509 id-ce (2 5 29))
01AD 01     1:             BOOLEAN FALSE
01B0 04     5:             OCTET STRING
                :               30 03 01 01 00                 0....
                :             }
01B7 30    20:           SEQUENCE {
01B9 06     3:             OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
                :               (X.509 id-ce (2 5 29))
01BE 01     1:             BOOLEAN FALSE
01C1 04    16:             OCTET STRING
                :               30 14 06 08 2B 06 01 05        0...+...
                :               05 07 03 02 06 08 2B 06        ......+.
                :               01 05 05 07 03 04              ......
                :             }
01D9 30     E:           SEQUENCE {
01DB 06     3:             OBJECT IDENTIFIER keyUsage (2 5 29 15)
                :               (X.509 id-ce (2 5 29))
01E0 01     1:             BOOLEAN FALSE
01E3 04     4:             OCTET STRING
                :               03 02 00 C0                    ....
                :             }
01E9 30    14:           SEQUENCE {
01EB 06     9:             OBJECT IDENTIFIER
                :               netscape-cert-type (2 16 840 1 113730 1 1)
                :               (Netscape certificate extension)
01F6 01     1:             BOOLEAN FALSE
01F9 04     4:             OCTET STRING
                :               03 02 00 80                    ....
                :             }
01FF 30    22:           SEQUENCE {
0201 06     3:             OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
                :               (X.509 id-ce (2 5 29))
0206 01     1:             BOOLEAN FALSE
0209 04    18:             OCTET STRING
```

```
                :                 30 16 80 14 40 66 36 6A       0...@f6j
                :                 89 0E 55 88 CB DB 4B AC       ..U...K.
                :                 32 83 06 23 95 02 D7 8E
                :               }
0223 30     9C:             SEQUENCE {
0226 06      8:               OBJECT IDENTIFIER
                :                 authorityInfoAccess (1 3 6 1 5 5 7 1 1)
                :                 (PKIX private extension)
0230 01      1:               BOOLEAN FALSE
0233 04     8C:               OCTET STRING
                :                 30 81 89 30 81 86 06 08      0..0....
                :                 2B 06 01 05 05 07 30 02      +.....0.
                :                 86 7A 6C 64 61 70 3A 2F      .zldap:/
                :                 2F 31 39 32 2E 31 36 38      /192.168
                :                 2E 32 31 30 2E 34 3A 33      .210.4:3
                :                 38 39 2F 43 4E 3D 53 75      89/CN=Su
                :                 62 43 41 2C 43 4E 3D 53      bCA,CN=S
                :                 75 62 43 41 2C 4F 55 3D      ubCA,OU=
                :                 63 41 43 65 72 74 69 66      cACertif
                :                 69 63 61 74 65 73 2C 6F      icates,o
                :                 3D 73 69 63 63 61 3F 63      =sicca?c
                :                 41 43 65 72 74 69 66 69      ACertifi
                :                 63 61 74 65 3F 62 61 73      cate?bas
                :                 65 3F 6F 62 6A 65 63 74      e?object
                :                 43 6C 61 73 73 3D 63 65      Class=ce
                :                 72 74 69 66 69 63 61 74      rtificat
                :                 69 6F 6E 41 75 74 68 6F      ionAutho
                :                 72 69 74 79                  rity
                :               }
02C2 30     A3:             SEQUENCE {
02C5 06      3:               OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
                :                 (X.509 id-ce (2 5 29))
02CA 01      1:               BOOLEAN FALSE
02CD 04     98:               OCTET STRING
                :                 30 81 95 30 81 92 A0 81      0..0....
                :                 8F A0 81 8C 86 81 89 6C      .......l
                :                 64 61 70 3A 2F 2F 31 39      dap://19
                :                 32 2E 31 36 38 2E 32 31      2.168.21
                :                 30 2E 34 3A 33 38 39 2F      0.4:389/
                :                 43 4E 3D 53 75 62 43 41      CN=SubCA
                :                 2C 43 4E 3D 53 75 62 43      ,CN=SubC
                :                 41 2C 6F 75 3D 43 52 4C      A,ou=CRL
                :                 44 69 73 74 72 69 62 75      Distribu
                :                 74 65 50 6F 69 6E 74 73      tePoints
```

```
                :                 2C 6F 3D 73 69 63 63 61       ,o=sicca
                :                 3F 63 65 72 74 69 66 69       ?certifi
                :                 63 61 74 65 52 65 76 6F       cateRevo
                :                 63 61 74 69 6F 6E 4C 69       cationLi
                :                 73 74 3F 62 61 73 65 3F       st?base?
                :                 6F 62 6A 65 63 74 63 6C       objectcl
                :                 61 73 73 3D 63 52 4C 44       ass=cRLD
                :                 69 73 74 72 69 62 75 74       istribut
                :                 69 6F 6E 50 6F 69 6E 74
                :               }
0368 30     20:             SEQUENCE {
036A 06      3:               OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
                :                 (X.509 id-ce (2 5 29))
036F 01      1:               BOOLEAN FALSE
0372 04     16:               OCTET STRING
                :                 04 14 27 C2 AC BD 28 79       ..'...(y
                :                 BC FB 11 D7 AA 35 F9 6A       .....5.j
                :                 D7 29 D4 94 C1 6B             .)...k
                :               }
                :             }
                :           }
                :         }
038A 30      D:       SEQUENCE {
038C 06      9:         OBJECT IDENTIFIER
                :           sha1withRSAEncryption (1 2 840 113549 1 1 5)
                :           (PKCS #1)
0397 05      0:         NULL
                :         }
0399 03     81:       BIT STRING 0 unused bits
                :         96 BD 40 04 B2 85 D6 FC       ..@.....
                :         76 F1 B8 6D 03 09 C1 89       v..m....
                :         5A 87 03 57 F4 60 1D F5       Z..W.`..
                :         33 6C 69 68 EC F5 C1 08       3lih....
                :         A9 7E AB C7 1F AB 32 A7       .~....2.
                :         E1 CF D9 2E 34 D5 F7 5A       ....4..Z
                :         CE 0A 3B CD EE 0D 35 B3       ..;...5.
                :         21 80 8A EB 1E 12 60 BD       !.....`.
                :         01 AA 03 C2 56 FA A5 57       ....V..W
                :         4A 7D 77 95 A5 67 EB 60       J}w..g.`
                :         5F 72 FC A0 8C AD 50 0E       _r....P.
                :         91 BF 0C 56 78 3B 13 3C       ...Vx;.<
                :         0C 59 8D EA B7 D0 5C 7C       .Y....\|
                :         9D 92 74 93 1D C1 96 7A       ..t....z
                :         67 35 01 E8 3E 62 4F F4       g5..>bO.
```

```
:         9C 2A 97 87 43 60 16 0C
:     }
```

A.2　政务部门机构证书编码举例

以下内容以政府机构证书中的签名证书为例，证书包含下列信息：

a) the serial number is 6E 66 3F 0E A2 E4 E0 B7 3F D5 48 72;
b) the certificate is signed with RSA and the sha1 hash algorithm;
c) the issuer's distinguished name is CN=SubCA;O=test;C=CN;;
d) the subject's distinguished name is CN =测试机构证书,OU = 测试组织,O =测试证书,C = CN
e) the certificate was issued on 20100809 and expired on 20110809
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 include an authority key identifier ,subject KeyIdentifier and basic constraints extensions;
i) the certificate includes a critical key usage extension: Digital Signatures, Non-Repudiation, Key Encipherment, Key Agreement;
j) the certificate include an extend key usage extensions:Client Auth;
k) the certificate include a CRL distribution points extensions;
l) the certificate include a authority info access extensions;

```
0000 30   3EF: SEQUENCE {
0004 30   358:    SEQUENCE {
0008 A0     3:      [0] {
000A 02     1:        INTEGER 2
            :        }
000D 02     C:      INTEGER
            :        6E 66 3F 0E A2 E4 E0 B7      nf?.....
            :        3F D5 48 72                   ?.Hr
001B 30     D:      SEQUENCE {
001D 06     9:        OBJECT IDENTIFIER
            :          sha1withRSAEncryption (1 2 840 113549 1 1 5)
            :          (PKCS #1)
0028 05     0:        NULL
            :        }
002A 30    2C:      SEQUENCE {
002C 31     B:        SET {
002E 30     9:          SEQUENCE {
0030 06     3:            OBJECT IDENTIFIER countryName (2 5 4 6)
            :              (X.520 id-at (2 5 4))
0035 13     2:            PrintableString 'CN'
            :            }
            :          }
```

```
0039 31    D:          SET {
003B 30    B:            SEQUENCE {
003D 06    3:              OBJECT IDENTIFIER organizationName (2 5 4 10)
           :                (X.520 id-at (2 5 4))
0042 0C    4:              UTF8String 'test'
           :              }
           :            }
0048 31    E:          SET {
004A 30    C:            SEQUENCE {
004C 06    3:              OBJECT IDENTIFIER commonName (2 5 4 3)
           :                (X.520 id-at (2 5 4))
0051 0C    5:              UTF8String 'SubCA'
           :              }
           :            }
           :          }
0058 30   1E:        SEQUENCE {
005A 17    D:          UTCTime '100809074447Z'
0069 17    D:          UTCTime '110809074447Z'
           :          }
0078 30   58:        SEQUENCE {
007A 31    B:          SET {
007C 30    9:            SEQUENCE {
007E 06    3:              OBJECT IDENTIFIER countryName (2 5 4 6)
           :                (X.520 id-at (2 5 4))
0083 0C    2:              UTF8String 'CN'
           :              }
           :            }
0087 31   15:          SET {
0089 30   13:            SEQUENCE {
008B 06    3:              OBJECT IDENTIFIER organizationName (2 5 4 10)
           :                (X.520 id-at (2 5 4))
0090 0C    C:              UTF8String '测试证书'
           :              }
           :            }
009E 31   15:          SET {
00A0 30   13:            SEQUENCE {
00A2 06    3:              OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
           :                (X.520 id-at (2 5 4))
00A7 0C    C:              UTF8String '测试组织'
           :              }
           :            }
00B5 31   1B:          SET {
00B7 30   19:            SEQUENCE {
00B9 06    3:              OBJECT IDENTIFIER commonName (2 5 4 3)
```

```
                :                 (X.520 id-at (2 5 4))
00BE 0C    12:                  UTF8String '测试机构证书'
                :                }
                :              }
                :            }
00D2 30    9F:          SEQUENCE {
00D5 30     D:            SEQUENCE {
00D7 06     9:              OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
                :                (PKCS #1)
00E2 05     0:              NULL
                :              }
00E4 03    8D:            BIT STRING 0 unused bits
                :              30 81 89 02 81 81 00 AF       0.......
                :              FA 0E 69 00 4E 9D 1E 0C       ..i.N...
                :              C3 95 04 EB C9 B6 71 11       ......q.
                :              65 18 E1 6A F1 C6 66 76       e..j..fv
                :              45 0F 38 9B 32 04 A8 D3       E.8.2...
                :              A3 0A 6E 9D C4 85 6D D3       ..n...m.
                :              97 2B 05 7C C6 D0 01 F3       .+.|....
                :              03 F1 50 07 8B A4 DA D7       ..P.....
                :              CA 23 D8 9C 1D F6 FE 26       .#.....&
                :              60 A4 9E 9D 63 D4 0C 8A       `...c...
                :              79 8F 5F CC AB 51 C5 39       y._..Q.9
                :              09 17 BC 2C D3 0F 00 A6       ...,....
                :              E0 F5 01 59 A7 F0 B7 CE       ...Y....
                :              2A F5 F8 CE F9 1F F9 CC       *.......
                :              A2 81 D3 55 88 9D 1A 3E       ...U...>
                :              03 E5 8D D4 D0 08 48 A5       ......H.
                :              37 58 60 63 00 16 AB 02       7X`c....
                :              03 01 00 01                    ....
                :            }
0174 A3   1E8:          [3] {
0178 30   1E4:            SEQUENCE {
017C 30     F:              SEQUENCE {
017E 06     3:                OBJECT IDENTIFIER basicConstraints (2 5 29 19)
                :                  (X.509 id-ce (2 5 29))
0183 01     1:                BOOLEAN FALSE
0186 04     5:                OCTET STRING
                :                  30 03 01 01 00                0....
                :                }
018D 30    20:              SEQUENCE {
018F 06     3:                OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
                :                  (X.509 id-ce (2 5 29))
0194 01     1:                BOOLEAN FALSE
```

```
0197 04   16:             OCTET STRING
          :               30 14 06 08 2B 06 01 05       0...+...
          :               05 07 03 02 06 08 2B 06       ......+.
          :               01 05 05 07 03 04              ......
          :             }
01AF 30    E:           SEQUENCE {
01B1 06    3:             OBJECT IDENTIFIER keyUsage (2 5 29 15)
          :               (X.509 id-ce (2 5 29))
01B6 01    1:             BOOLEAN FALSE
01B9 04    4:             OCTET STRING
          :               03 02 00 C0                    ....
          :             }
01BF 30    14:          SEQUENCE {
01C1 06    9:             OBJECT IDENTIFIER
          :               netscape-cert-type (2 16 840 1 113730 1 1)
          :               (Netscape certificate extension)
01CC 01    1:             BOOLEAN FALSE
01CF 04    4:             OCTET STRING
          :               03 02 00 80                    ....
          :             }
01D5 30    22:          SEQUENCE {
01D7 06    3:             OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
          :               (X.509 id-ce (2 5 29))
01DC 01    1:             BOOLEAN FALSE
01DF 04    18:            OCTET STRING
          :               30 16 80 14 40 66 36 6A       0...@f6j
          :               89 0E 55 88 CB DB 4B AC       ..U...K.
          :               32 83 06 23 95 02 D7 8E
          :             }
01F9 30    9C:          SEQUENCE {
01FC 06    8:             OBJECT IDENTIFIER
          :               authorityInfoAccess (1 3 6 1 5 5 7 1 1)
          :               (PKIX private extension)
0206 01    1:           BOOLEAN FALSE
0209 04    8C:            OCTET STRING
          :               30 81 89 30 81 86 06 08       0..0....
          :               2B 06 01 05 05 07 30 02       +.....0.
          :               86 7A 6C 64 61 70 3A 2F       .zldap:/
          :               2F 31 39 32 2E 31 36 38       /192.168
          :               2E 32 31 30 2E 34 3A 33       .210.4:3
          :               38 39 2F 43 4E 3D 53 75       89/CN=Su
          :               62 43 41 2C 43 4E 3D 53       bCA,CN=S
          :               75 62 43 41 2C 4F 55 3D       ubCA,OU=
          :               63 41 43 65 72 74 69 66       cACertif
```

```
                :                 69 63 61 74 65 73 2C 6F       icates,o
                :                 3D 73 69 63 63 61 3F 63       =sicca?c
                :                 41 43 65 72 74 69 66 69       ACertifi
                :                 63 61 74 65 3F 62 61 73       cate?bas
                :                 65 3F 6F 62 6A 65 63 74       e?object
                :                 43 6C 61 73 73 3D 63 65       Class=ce
                :                 72 74 69 66 69 63 61 74       rtificat
                :                 69 6F 6E 41 75 74 68 6F       ionAutho
                :                 72 69 74 79                     rity
                :               }
0298 30     A3:             SEQUENCE {
029B 06      3:               OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
                :                 (X.509 id-ce (2 5 29))
02A0 01      1:               BOOLEAN FALSE
02A3 04     98:               OCTET STRING
                :                 30 81 95 30 81 92 A0 81       0..0....
                :                 8F A0 81 8C 86 81 89 6C       .......l
                :                 64 61 70 3A 2F 2F 31 39       dap://19
                :                 32 2E 31 36 38 2E 32 31       2.168.21
                :                 30 2E 34 3A 33 38 39 2F       0.4:389/
                :                 43 4E 3D 53 75 62 43 41       CN=SubCA
                :                 2C 43 4E 3D 53 75 62 43       ,CN=SubC
                :                 41 2C 6F 75 3D 43 52 4C       A,ou=CRL
                :                 44 69 73 74 72 69 62 75       Distribu
                :                 74 65 50 6F 69 6E 74 73       tePoints
                :                 2C 6F 3D 73 69 63 63 61       ,o=sicca
                :                 3F 63 65 72 74 69 66 69       ?certifi
                :                 63 61 74 65 52 65 76 6F       cateRevo
                :                 63 61 74 69 6F 6E 4C 69       cationLi
                :                 73 74 3F 62 61 73 65 3F       st?base?
                :                 6F 62 6A 65 63 74 63 6C       objectcl
                :                 61 73 73 3D 63 52 4C 44       ass=cRLD
                :                 69 73 74 72 69 62 75 74       istribut
                :                 69 6F 6E 50 6F 69 6E 74
                :               }
033E 30     20:             SEQUENCE {
0340 06      3:               OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
                :                 (X.509 id-ce (2 5 29))
0345 01      1:               BOOLEAN FALSE
0348 04     16:               OCTET STRING
                :                 04 14 F8 FE 5D 6C A5 D8        ....]l..
                :                 4F 73 81 8E B3 1E 63 F6       Os....c.
                :                 EB B3 CC 9D 68 DD                ....h.
                :               }
```

```
                :             }
                :           }
                :         }
0360 30       D:      SEQUENCE {
0362 06       9:        OBJECT IDENTIFIER
                :           sha1withRSAEncryption (1 2 840 113549 1 1 5)
                :           (PKCS #1)
036D 05       0:        NULL
                :         }
036F 03     81:       BIT STRING 0 unused bits
                :         15 25 24 63 CD E2 60 98        .%$c..`.
                :         80 BC FC FA F2 01 44 A5        ......D.
                :         B7 5D 08 68 6D 5A 16 A9        .].hmZ..
                :         3C 16 B5 76 18 51 B6 94        <..v.Q..
                :         CB 3C F8 E2 20 24 6B B6        .<.. $k.
                :         72 84 92 8A 2E 96 6F 05        r.....o.
                :         B7 43 B0 A7 4B 60 DE 4B        .C..K`.K
                :         7D 2E 43 FA D3 6B 98 00        }.C..k..
                :         46 EA 37 C5 21 04 07 5D        F.7.!..]
                :         84 A2 5F 19 C0 82 A8 BE        .._.....
                :         8B 70 64 AC 20 03 8D 98        .pd. ...
                :         E3 5B D2 D1 4C E6 97 89        .[..L...
                :         73 BC FB B5 82 3E 13 A0        s....>..
                :         37 FA 70 C8 DB F3 D1 74        7.p....t
                :         C0 96 80 27 E9 BB DA C5        ...'....
                :         C7 B6 64 AF 8A B5 EE 99
                :       }
```

A.3　电子政务设备证书编码举例

以下内容以设备证书为例，证书包含下列信息：

a) the serial number is 3B 33 48 78 3F 3C 36 7D A7 74 30 28;
b) the certificate is signed with RSA and the sha1 hash algorithm;
c) the issuer's distinguished name is CN=GXSUBCA2，C = CN
d) and the subject's distinguished name is CN=192.168.1.56,OU=机构 1,OU=机构 2,
e) OU=机构 3,OU=机构 4,O=组织,C=CN
f) the certificate was issued on　20100310 and expired on 20150310
g) the certificate contains a 1024 bit RSA public key;
h) the certificate is an end entity certificate （not a CA certificate）;
i) the certificate include an authority key identifier ,subject KeyIdentifier and basic constraints extensions;
j) the certificate includes a critical key usage extension :Digital Signature, Non-Repudiation.
k) the certificate include an extend key usage extensions: Server Auth;

```
0000 30   2C0: SEQUENCE {
0004 30   229:    SEQUENCE {
0008 A0     3:      [0] {
000A 02     1:        INTEGER 2
             :        }
000D 02     C:      INTEGER
             :        3B 33 48 78 3F 3C 36 7D       ;3Hx?<6}
             :        A7 74 30 28                    .t0(
001B 30     D:      SEQUENCE {
001D 06     9:        OBJECT IDENTIFIER
             :          sha1withRSAEncryption (1 2 840 113549 1 1 5)
             :          (PKCS #1)
0028 05     0:        NULL
             :        }
002A 30    2A:      SEQUENCE {
002C 31     D:        SET {
002E 30     B:          SEQUENCE {
0030 06     3:            OBJECT IDENTIFIER countryName (2 5 4 6)
             :              (X.520 id-at (2 5 4))
0035 1E     4:            BMPString 'CN'
             :            }
             :          }
003B 31    19:        SET {
003D 30    17:          SEQUENCE {
003F 06     3:            OBJECT IDENTIFIER commonName (2 5 4 3)
             :              (X.520 id-at (2 5 4))
0044 1E    10:            BMPString ' GXSUBCA2'
             :            }
             :          }
             :        }
0056 30    1E:      SEQUENCE {
0058 17     D:        UTCTime '100310065402Z'
0067 17     D:        UTCTime '150305065402Z'
             :        }
0076 30    7C:      SEQUENCE {
0078 31     B:        SET {
007A 30     9:          SEQUENCE {
007C 06     3:            OBJECT IDENTIFIER countryName (2 5 4 6)
             :              (X.520 id-at (2 5 4))
0081 13     2:            PrintableString 'CN'
             :            }
             :          }
0085 31     E:        SET {
```

```
0087 30    C:           SEQUENCE {
0089 06    3:             OBJECT IDENTIFIER organizationName (2 5 4 10)
           :               (X.520 id-at (2 5 4))
008E 0C    5:             UTF8String '组织'
           :             }
           :           }
0095 31   10:         SET {
0097 30    E:           SEQUENCE {
0099 06    3:             OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
           :               (X.520 id-at (2 5 4))
009E 0C    7:             UTF8String '机构 1'
           :             }
           :           }
00A7 31   10:         SET {
00A9 30    E:           SEQUENCE {
00AB 06    3:             OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
           :               (X.520 id-at (2 5 4))
00B0 0C    7:             UTF8String '机构 2'
           :             }
           :           }
00B9 31   10:         SET {
00BB 30    E:           SEQUENCE {
00BD 06    3:             OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
           :               (X.520 id-at (2 5 4))
00C2 0C    7:             UTF8String '机构 3'
           :             }
           :           }
00CB 31   10:         SET {
00CD 30    E:           SEQUENCE {
00CF 06    3:             OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
           :               (X.520 id-at (2 5 4))
00D4 0C    7:             UTF8String '机构 4'
           :             }
           :           }
00DD 31   15:         SET {
00DF 30   13:           SEQUENCE {
00E1 06    3:             OBJECT IDENTIFIER commonName (2 5 4 3)
           :               (X.520 id-at (2 5 4))
00E6 0C    C:             UTF8String '192.168.1.56'
           :             }
           :           }
           :         }
00F4 30   9F:       SEQUENCE {
00F7 30    D:         SEQUENCE {
```

```
00F9 06   9:           OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
          :             (PKCS #1)
0104 05   0:           NULL
          :           }
0106 03   8D:        BIT STRING 0 unused bits, encapsulates {
010A 30   89:          SEQUENCE {
010D 02   81:            INTEGER
          :              00 DE EA 10 8B 86 AA 6B       .......k
          :              28 9D C1 48 7D A1 9D 4A       (..H}..J
          :              43 6A D0 7C 52 8B EC 33       Cj.|R..3
          :              FE FB E5 45 43 71 2E 4C       ...ECq.L
          :              AE C7 2F 4E F6 E0 C6 28       ../N...(
          :              04 32 1E AA A9 F4 C0 06       .2......
          :              63 D8 DF B9 F4 9B 4A 38       c.....J8
          :              A0 5B F2 59 4F 24 DC 12       .[.YO$..
          :              D9 5E C4 55 22 3B C0 FF       .^.U";..
          :              0D 27 94 40 DB F2 DC E2       .'.@....
          :              D2 8F 3C 51 AE B1 98 75       ..<Q...u
          :              96 7F D7 8E 5B 48 79 22       ....[Hy"
          :              70 6F 55 D1 28 27 F8 92       poU.('..
          :              3F C0 EA 43 2E 4F 8F C8       ?..C.O..
          :              BE 2A A9 51 AB DD 28 16       .*.Q..(.
          :              03 34 93 5A 4C 71 30 83       .4.ZLq0.
          :              A3                            .
0191 02   3:            INTEGER 65537
          :           }
          :         }
          :       }
0196 A3   98:      [3] {
0199 30   95:        SEQUENCE {
019C 30   F:           SEQUENCE {
019E 06   3:             OBJECT IDENTIFIER basicConstraints (2 5 29 19)
          :               (X.509 id-ce (2 5 29))
01A3 01   1:             BOOLEAN FALSE
01A6 04   5:             OCTET STRING, encapsulates {
01A8 30   3:               SEQUENCE {
01AA 01   1:                 BOOLEAN FALSE
          :               }
          :             }
          :           }
01AD 30   16:          SEQUENCE {
01AF 06   3:             OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
          :               (X.509 id-ce (2 5 29))
01B4 01   1:             BOOLEAN FALSE
```

```
01B7 04    C:          OCTET STRING, encapsulates {
01B9 30    A:            SEQUENCE {
01BB 06    8:              OBJECT IDENTIFIER serverAuth (1 3 6 1 5 5 7 3 1)
           :                (PKIX key purpose)
           :              }
           :            }
           :          }
01C5 30    E:        SEQUENCE {
01C7 06    3:          OBJECT IDENTIFIER keyUsage (2 5 29 15)
           :            (X.509 id-ce (2 5 29))
01CC 01    1:          BOOLEAN FALSE
01CF 04    4:          OCTET STRING, encapsulates {
01D1 03    2:            BIT STRING 0 unused bits
           :              '00010111'B
           :            }
           :          }
01D5 30    14:       SEQUENCE {
01D7 06    9:          OBJECT IDENTIFIER
           :            netscape-cert-type (2 16 840 1 113730 1 1)
           :            (Netscape certificate extension)
01E2 01    1:          BOOLEAN FALSE
01E5 04    4:          OCTET STRING, encapsulates {
01E7 03    2:            BIT STRING 0 unused bits
           :              '00000010'B (bit 1)
           :            }
           :          }
01EB 30    22:       SEQUENCE {
01ED 06    3:          OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
           :            (X.509 id-ce (2 5 29))
01F2 01    1:          BOOLEAN FALSE
01F5 04    18:         OCTET STRING, encapsulates {
01F7 30    16:           SEQUENCE {
01F9 80    14:             [0]
           :                AF 33 81 8A 2D AD 7D A4        .3..-.}.
           :                5C 28 32 80 84 83 32 A2        \(2...2.
           :                E4 55 DF 45                    .U.E
           :             }
           :           }
           :         }
020F 30    20:       SEQUENCE {
0211 06    3:          OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
           :            (X.509 id-ce (2 5 29))
0216 01    1:          BOOLEAN FALSE
0219 04    16:         OCTET STRING, encapsulates {
```

```
021B 04    14:                    OCTET STRING
             :                      8C 53 86 9C A6 C5 EF 70        .S.....p
             :                      B4 88 EC 9C 08 F3 FE 2B        .......+
             :                      B8 3A CE 46                    .:.F
             :                    }
             :                  }
             :                }
             :              }
             :            }
0231 30      D:      SEQUENCE {
0233 06      9:        OBJECT IDENTIFIER
             :           sha1withRSAEncryption (1 2 840 113549 1 1 5)
             :           (PKCS #1)
023E 05      0:        NULL
             :        }
0240 03      81:     BIT STRING 0 unused bits
             :        2F 4B C3 B5 46 A2 DB DD        /K..F...
             :        C3 F9 30 7A 70 04 3A 85        ..0zp.:.
             :        47 36 B7 EF 3C 7B 90 BF        G6..<{..
             :        7C 15 F6 6B B8 A8 49 57        |..k..IW
             :        F8 8F 58 25 7A 1C 69 A7        ..X%z.i.
             :        22 24 4F 75 81 BD 28 C5        "$Ou..(.
             :        F0 4C 34 08 19 CC 3B 05        .L4...;.
             :        2C 1F 92 7F A4 1E 8A 35        ,.....5
             :        DC E3 53 DE EC 32 3F BB        ..S..2?.
             :        28 E9 DB 71 FB 29 22 01        (..q.)".
             :        88 A1 CE 25 29 ED 2F A3        ...%)./.
             :        43 6F 1A 47 FA 28 14 BA        Co.G.(..
             :        20 FD AD 6F 60 97 9D 59        ..o`..Y
             :        15 D6 90 DF 00 D5 99 77        .......w
             :        E3 7E 67 9F 41 34 54 28        .~g.A4T(
             :        ED 00 C1 04 6C C7 70 8A
             :      }
```

A.4 电子政务代码签名证书编码举例

以下内容以代码签名证书为例，证书包含下列信息：

a) the serial number is 2B 0B 93 E6 4B 35 F2 76 72 F1 11 47;
b) the certificate is signed with RSA and the sha1 hash algorithm;
c) the issuer's distinguished name is CN= CEGN CA,O=China E-Government Network,C=CN;
d) and the subject's distinguished name is CN = 代码签名,E = email@test.com,OU = 机构 1,O = 组织,C = CN;
e) the certificate was issued on 20100310 and expired on 20110310

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 include an authority key identifier ,subject KeyIdentifier and basic constraints extensions;
i) the certificate includes a critical key usage extension :Digital Signature, Non-Repudiation.
j) the certificate include an extend key usage extensions:CodeSign;
k) the certificate include a CRL distribution points extensions;
l) the certificate include a authority info access extensions;

```
0000 30   41B: SEQUENCE {
0004 30   384:    SEQUENCE {
0008 A0     3:      [0] {
000A 02     1:        INTEGER 2
             :        }
000D 02     C:      INTEGER
             :        2B 0B 93 E6 4B 35 F2 76       +...K5.v
             :        72 F1 11 47                    r..G
001B 30     D:      SEQUENCE {
001D 06     9:        OBJECT IDENTIFIER
             :          sha1withRSAEncryption (1 2 840 113549 1 1 5)
             :          (PKCS #1)
0028 05     0:        NULL
             :        }
002A 30    44:      SEQUENCE {
002C 31     B:        SET {
002E 30     9:          SEQUENCE {
0030 06     3:            OBJECT IDENTIFIER countryName (2 5 4 6)
             :              (X.520 id-at (2 5 4))
0035 13     2:            PrintableString 'CN'
             :            }
             :          }
0039 31    23:        SET {
003B 30    21:          SEQUENCE {
003D 06     3:            OBJECT IDENTIFIER organizationName (2 5 4 10)
             :              (X.520 id-at (2 5 4))
0042 0C    1A:            UTF8String 'China E-Government Network'
             :            }
             :          }
005E 31    10:        SET {
0060 30     E:          SEQUENCE {
0062 06     3:            OBJECT IDENTIFIER commonName (2 5 4 3)
             :              (X.520 id-at (2 5 4))
0067 0C     7:            UTF8String 'CEGN CA'
```

```
                :               }
                :             }
                :           }
    0070 30   1E:         SEQUENCE {
    0072 17    D:           UTCTime '100310054412Z'
    0081 17    D:           UTCTime '110310054412Z'
                :           }
    0090 30   7F:         SEQUENCE {
    0092 31    D:           SET {
    0094 30    B:             SEQUENCE {
    0096 06    3:               OBJECT IDENTIFIER countryName (2 5 4 6)
                :                 (X.520 id-at (2 5 4))
    009B 1E    4:               UTF8String 'CN'
                :               }
                :             }
    00A1 31   13:           SET {
    00A3 30   11:             SEQUENCE {
    00A5 06    3:               OBJECT IDENTIFIER organizationName (2 5 4 10)
                :                 (X.520 id-at (2 5 4))
    00AA 1E    A:               BMPString '组织'
                :               }
                :             }
    00B6 31   17:           SET {
    00B8 30   15:             SEQUENCE {
    00BA 06    3:               OBJECT IDENTIFIER organizationalUnitName (2 5 4 11)
                :                 (X.520 id-at (2 5 4))
    00BF 1E    E:               UTF8String '机构 1'
                :               }
                :             }
    00CF 31   1D:           SET {
    00D1 30   1B:             SEQUENCE {
    00D3 06    9:               OBJECT IDENTIFIER emailAddress (1 2 840 113549 1 9 1)
                :                 (PKCS #9 (1 2 840 113549 1 9). Deprecated, use an
altName extension instead)
    00DE 16    E:               IA5String 'email@test.com'
                :               }
                :             }
    00EE 31   21:           SET {
    00F0 30   1F:             SEQUENCE {
    00F2 06    3:               OBJECT IDENTIFIER commonName (2 5 4 3)
                :                 (X.520 id-at (2 5 4))
    00F7 1E   18:               UTF8String   '代码签名'
                :               }
                :             }
```

```
                :         }
0111 30     9F:       SEQUENCE {
0114 30      D:         SEQUENCE {
0116 06      9:           OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
                :             (PKCS #1)
0121 05      0:           NULL
                :           }
0123 03     8D:         BIT STRING 0 unused bits, encapsulates {
0127 30     89:           SEQUENCE {
012A 02     81:             INTEGER
                :               00 BA 6B 08 95 0F EE 0E       ..k.....
                :               A0 39 1B 82 6F D0 C7 EC       .9..o...
                :               5D 5F 51 88 CF CB 83 74       ]_Q....t
                :               3D 13 2C 28 1D CA 77 E5       =.,(..w.
                :               F3 8A 45 21 BC AB 10 58       ..E!...X
                :               9F 72 44 78 4D E8 23 E2       .rDxM.#.
                :               53 99 B4 7B 53 E1 8A 0C       S..{S...
                :               E7 D9 C1 6D 66 4C C3 68       ...mfL.h
                :               90 AA 2F D2 17 65 3D 7F       ../..e=.
                :               CF 29 9A 0A 41 AB 56 76       .)..A.Vv
                :               98 C4 03 AC E0 87 22 5E       ......"^
                :               CC 83 68 AF 11 11 B7 AB       ..h.....
                :               99 59 6E B9 13 FE B7 44       .Yn....D
                :               7C B6 B5 F7 9F 2D 5D 25       |....-]%
                :               AF 12 B9 48 1B A9 E7 6C       ...H...l
                :               1B 5D 57 E9 D5 F4 FD 1D       .]W.....
                :               35                             5
01AE 02      3:             INTEGER 65537
                :             }
                :           }
                :         }
01B3 A3    1D5:       [3] {
01B7 30    1D1:         SEQUENCE {
01BB 30      F:           SEQUENCE {
01BD 06      3:             OBJECT IDENTIFIER basicConstraints (2 5 29 19)
                :               (X.509 id-ce (2 5 29))
01C2 01      1:             BOOLEAN FALSE
01C5 04      5:             OCTET STRING, encapsulates {
01C7 30      3:               SEQUENCE {
01C9 01      1:                 BOOLEAN FALSE
                :                 }
                :               }
                :             }
01CC 30      E:           SEQUENCE {
```

```
01CE 06   3:             OBJECT IDENTIFIER keyUsage (2 5 29 15)
          :               (X.509 id-ce (2 5 29))
01D3 01   1:             BOOLEAN FALSE
01D6 04   4:             OCTET STRING, encapsulates {
01D8 03   2:                 BIT STRING 0 unused bits
          :                   '00000011'B
          :                 }
          :             }
01DC 30  16:           SEQUENCE {
01DE 06   3:             OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
          :               (X.509 id-ce (2 5 29))
01E3 01   1:             BOOLEAN FALSE
01E6 04   C:             OCTET STRING, encapsulates {
01E8 30   A:                 SEQUENCE {
01EA 06   8:                   OBJECT IDENTIFIER codeSigning (1 3 6 1 5 5 7 3 3)
          :                     (PKIX key purpose)
          :                   }
          :                 }
          :             }
01F4 30  22:           SEQUENCE {
01F6 06   3:             OBJECT IDENTIFIER authorityKeyIdentifier (2 5 29 35)
          :               (X.509 id-ce (2 5 29))
01FB 01   1:             BOOLEAN FALSE
01FE 04  18:             OCTET STRING, encapsulates {
0200 30  16:                 SEQUENCE {
0202 80  14:                   [0]
          :                     5A D4 9D 70 48 CD D4 EB        Z..pH...
          :                     AA 6B 25 14 93 70 EC C9        .k%..p..
          :                     9E 38 D7 BA                    .8..
          :                   }
          :                 }
          :             }
0218 30  9D:           SEQUENCE {
021B 06   8:             OBJECT IDENTIFIER
          :               authorityInfoAccess (1 3 6 1 5 5 7 1 1)
          :               (PKIX private extension)
0225 01   1:             BOOLEAN FALSE
0228 04  8D:             OCTET STRING, encapsulates {
022B 30  8A:                 SEQUENCE {
022E 30  87:                   SEQUENCE {
0231 06   8:                     OBJECT IDENTIFIER
          :                       caIssuers (1 3 6 1 5 5 7 48 2)
          :                       (PKIX authority info access descriptor)
023B 86  7B:                     [6]
```

```
                :                                   'ldap://59.255.128.13:389/CN=CEGN
CA,CN=CEGN CA,O'
                :                       'U=cACertificates,c=CN?cACertificate?base?objectC'
                :                       'lass=certificationAuthority'
                :                       }
                :                     }
                :                   }
                :                 }
    02B8 30     AF:             SEQUENCE {
    02BB 06      3:               OBJECT IDENTIFIER cRLDistributionPoints (2 5 29 31)
                 :                 (X.509 id-ce (2 5 29))
    02C0 01      1:               BOOLEAN FALSE
    02C3 04     A4:               OCTET STRING, encapsulates {
    02C6 30     A1:                 SEQUENCE {
    02C9 30     9E:                   SEQUENCE {
    02CC A0     9B:                     [0] {
    02CF A0     98:                       [0] {
    02D2 86     95:                         [6]
                 :                       'ldap://59.255.128.13:389/CN=entityid36groupid0,C'
                 :                                                       'N=CEGN
CA,ou=CRLDistributePoints,c=CN?certificat'
                 :                       'eRevocationList?base?objectclass=cRLDistribution'
                 :                       'Point'
                 :                           }
                 :                       }
                 :                     }
                 :                   }
                 :                 }
                 :               }
    036A 30     20:             SEQUENCE {
    036C 06      3:               OBJECT IDENTIFIER subjectKeyIdentifier (2 5 29 14)
                 :                 (X.509 id-ce (2 5 29))
    0371 01      1:               BOOLEAN FALSE
    0374 04     16:               OCTET STRING, encapsulates {
    0376 04     14:                 OCTET STRING
                 :                   04 87 BE A3 CC F5 E9 7D       .......}
                 :                   CE AA EF AD 22 28 8F 68       ...."(.h
                 :                   5F 33 8C B3                    _3..
                 :                 }
                 :               }
                 :             }
                 :           }
                 :         }
    038C 30      D:     SEQUENCE {
```

```
038E 06       9:       OBJECT IDENTIFIER
                :         sha1withRSAEncryption (1 2 840 113549 1 1 5)
                :         (PKCS #1)
0399 05       0:       NULL
                :       }
039B 03      81:     BIT STRING 0 unused bits
                :       27 BD 20 89 7F 4D 02 E5       '. ..M..
                :       57 D9 88 F7 D8 3F 2C B8       W....?,.
                :       96 EC F6 CE 48 8E 01 0E       ....H...
                :       AB E0 48 7C 88 DF 9E C0       ..H|....
                :       3F BB 3B 0F CF 9D 34 BE       ?.;...4.
                :       44 7E C4 43 35 09 ED EE       D~.C5...
                :       4D 09 20 F4 48 D8 EA 15       M. .H...
                :       E9 D7 CF 22 74 FF 2D 2A       ..."t.-*
                :       F7 8A D4 74 3B F8 79 00       ...t;.y.
                :       39 53 31 A1 32 F6 1E 2F       9S1.2../
                :       F8 BC 31 28 A2 D4 04 4D       ..1(...M
                :       B8 E0 7C 9F F4 D8 78 C5       ..|...x.
                :       FC 31 78 16 83 E1 62 7B       .1x...b{
                :       78 C4 87 23 DD CC C1 B3       x..#....
                :       E9 9E 1A 8E FC D9 70 8E       ......p.
                :       DE 7F E0 4D C0 96 AB 66
                :     }
```