ICS 35.040
L 71

MH

中华人民共和国民用航空行业标准

MH/T 0045.2—2013

民航电子政务数字证书服务及技术规范 第2部分：数字证书模板

Specifications for CAAC e-government digital certificate service and technique
Part 2：Digital certificate template

2013－11－11 发布　　2014－03－01 实施

中国民用航空局　发布

前　言

MH/T 0045《民航电子政务数字证书服务及技术规范》分为四个部分：

——第1部分：服务；

——第2部分：数字证书模板；

——第3部分：USB Key介质；

——第4部分：证书应用集成。

本部分为第2部分。

本部分按照GB/T 1.1-2009给出的规则起草。

本部分由中国民用航空局综合司提出。

本部分由中国民用航空局航空器适航审定司批准立项。

本部分由中国民航科学技术研究院归口。

本部分起草单位：中国民用航空局信息中心、北京数字认证股份有限公司。

本部分主要起草人：胡东宏、张威、宋晨、于飞、于清洋。

民航电子政务数字证书服务及技术规范
第2部分：数字证书模板

1 范围

MH/T 0045的本部分规定了民航各级行政机关在开展经济运行、安全监管等政务活动中所使用的数字证书的基本格式要求，并给出了数字证书的模板。民航电子政务内网数字证书有关要求不在本部分内涉及。

本部分适用于民航电子政务数字证书的管理方和服务提供方。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20518 信息安全技术 公钥基础设施 数字证书格式

GM/Z 0001 密码术语

GM/T 0015 基于SM2密码算法的数字证书格式规范

MH/T 0045.1 民航电子政务数字证书服务及技术规范 第1部分 服务

3 术语和定义

GB/T 20518、GM/Z 0001、GM/T 0015和MH/T 0045.1界定的的术语定义适用于本文件。

4 缩略语

下列缩略语适用于MH/T 0045 的本部分。

CA 认证机构(Certification Authority)

CRL 证书撤销列表(Certificate Revocation List)

ASN 抽象语法表示法（Abstract Syntax Notation）

DN 甄别名（Distinguished Name）

OID 对象标识符（Object Identifier）

5 数字证书基本格式

5.1 基本结构

数字证书的基本结构由三部分组成：基本证书域(TBSCertificate)、签名算法域(SignatureAlgorithm)、签名值域(SignatureValue)。其中，基本证书域由基本域和扩展域组成，如图1所示：

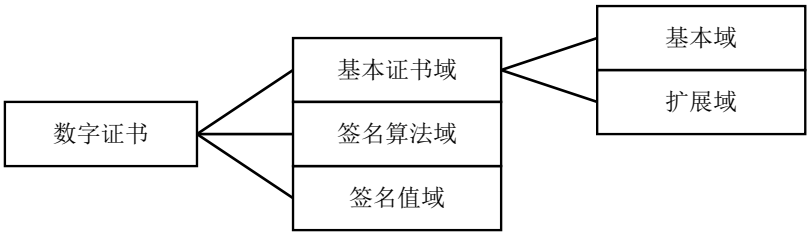

图1　数字证书基本结构

5.2　基本证书域 (TBSCertificate)

5.2.1　基本域

5.2.1.1　组成

基本域由如下部分组成：

a)　版本（Version）；
b)　序列号（SerialNumber）；
c)　签名算法（SignatureAlgorithm）；
d)　颁发者（Issuer）；
e)　有效期（Validity)；
f)　主题（Subject)；
g)　主题公钥信息（SubjectPublicKeyInfo)；

5.2.1.2　版本

描述了数字证书的版本号。MH/T 0045 的本部分本部分中数字证书应使用V3。

5.2.1.3　序列号

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应是唯一的。序列号最长可为20个8位字节的序列号值。

5.2.1.4　签名算法

包含CA签发该证书所使用的密码算法的标识符。算法标识符应与证书中SignatureAlgorithm项的算法标识符相同。

签名算法应符合国家密码主管部门对密码算法的规定，并根据国家密码主管部门批准的最新算法及时调整，以适应国家最新技术标准要求。

5.2.1.5　颁发者

标识了证书签名和证书颁发的实体。应包含一个非空的可甄别名。应被定义为X.500的Name类型。

颁发者甄别名称（Distinguished Name，简称DN）的 C（Country）属性的编码应使用PrintableString。Email属性的编码应使用IA5String。其他属性的编码应一律使用UTF8String。

证书颁发者DN编码规范如表1所示：

表1　证书颁发者 DN 编码规范表

Name 类型	说明	示例	编码格式
C	国家	CN	PrintableString
O	颁发机构名称	xxCA	UTF8String
OU	机构名称，可以是信任体系的名称	xxCA-1	UTF8String
CN	颁发机构通用名	xxCA	UTF8String

5.2.1.6　有效期

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）。

数字证书有效期的NotBefore和 NotAfter这两个时间应采用GeneralizedTime类型进行编码。GeneralizedTime字段包含一个本地和格林威治标准时间之间的时间差。GeneralizedTime值应用格林威治标准时间表示，且包含秒（即时间格式为YYYYMMDDHHMMSSZ）。

5.2.1.7　主题

与主题公钥项中的公钥相对应的实体。主题名称可以出现在主题项或主题替换名称扩展项中（SubjectAltName）。如果主题是一个CA，那么主题项应与其签发的所有证书的颁发者相同，一个CA认证的每个证书持有者的甄别名称应是唯一的。一个CA可以为同一个证书持有者以相同的甄别名称签发多个证书。

该项不应为空。

5.2.1.8　主题公钥信息

用于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。

5.2.2　扩展域

5.2.2.1　概述

MH/T 0045的本部分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，它们分别是扩展类型、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，应拒绝接受该证书，如果不能识别非关键的扩展，则可以忽略该扩展项的信息。

5.2.2.2　扩展域结构

证书扩展域可有多个扩展项，每个扩展项包括扩展类型、扩展关键和扩展项值三部分，结构如图2所示：

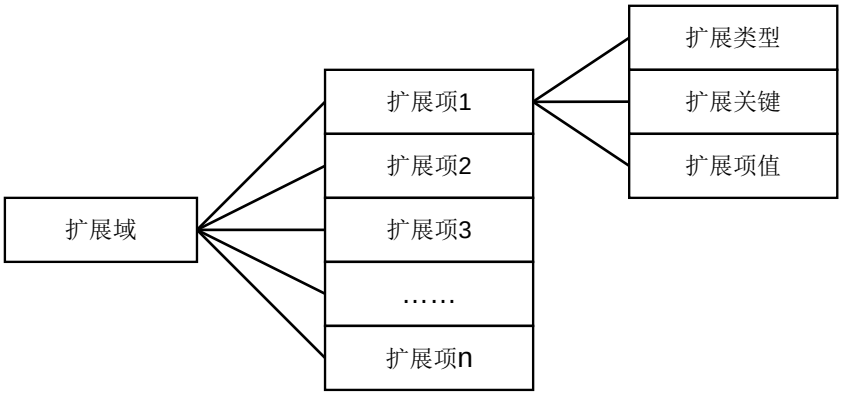

图2　扩展域构成

本部分定义了一些标准的扩展项，遵循本规范的程序应能识别以下扩展项：

a)　密钥用法（KeyUsage）；

b)　主题密钥标识符（SubjectKeyIdentifier）；

c)　颁发机构密钥标识符（AuthorityKeyIdentifier）；

d)　证书策略（CertificatePolicies）；

e)　唯一标识符（用户证书应签发证书唯一标识扩展项）。

5.2.2.3　密钥用法

本项说明已认证的公开密钥用于何种用途。

所有证书应具有密钥用法扩展项。

密钥用法定义：

```
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)}
```

所有的CA证书应包括本扩展，而且应包含keyCertSign这一密钥用途。用户证书则根据证书用途，分“签名”证书和“加密”证书，选择对应的密钥用途进行签发。

此扩展可定义为关键的或非关键的。

5.2.2.4　主题密钥标识符

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。

对于使用密钥标识符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。CA签发证书时应把CA证书中本扩展的值赋给终端实体证书AuthorityKeyIdentifier扩展中的KeyIdentifier项。 CA

证书的主题密钥标识符应从公钥中或者生成唯一值的方法中导出。终端实体证书的主题密钥标识符应从公钥中导出。

所有的CA证书应包括本扩展，此扩展项为非关键项。

5.2.2.5 颁发机构密钥标识符

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）。

5.2.2.6 证书策略

本项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。

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。

数字证书是否包括本扩展为可选的，是否为关键项也是可选的。

5.2.2.7 唯一标识符

单位证书中应具有实体唯一标识符，用于区分辨别名相同的数字证书，实体唯一标识的OID由证书认证机构自行申请和定义。

本部分中对单位数字证书的唯一标识符的编码规范如下：

实体唯一标识符 = 证书实体编号（变长）+ “@” + 证件类型代码（2位）+ 证件号码（变长）

其中，证书实体编号是一个证书实体的证书序号，同一个实体申请多个证书时，证书实体编号应不同，以便于区分不同的证书。证书类型和号码类型的代码如表2所示。

表2 证书类型与证件类型代码对应

证书类型	办理证书时可使用的证件名称	证件类型代码
单位证书	组织机构代码、工商营业执照、税务登记证、其他	JJ、GS、SW、QT
个人证书	身份证、军官证、护照、回乡证、其他	SF、JR、HZ、HX、QT
设备证书	组织机构代码、工商营业执照、税务登记证、其他	JJ、GS、SW、QT
其他证书	组织机构代码、工商营业执照、税务登记证、其他	JJ、GS、SW、QT

用户根据不同的证书类型，应提供不同的证件办理数字证书。

实体唯一标识项数据的总长度不应超过128字节，唯一标识属性的编码应使用UTF8String。

对于终端实体证书，该扩展项应签发，该项应为非关键扩展项。

5.3 签名算法域 (SignatureAlgorithm)

证书中的签名算法应使用国家密码管理主管部门审核批准的相关算法。

5.4 签名值域 (SignatureValue)

本项包含对基本证书域进行数字签名的结果。经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。

5.5 命名规范

数字证书中的主题DN命名规范为：

a) C（Country）应为证书持有者所在国家；
b) S（State）应为证书持有者所在省份；
c) L（Location）应为证书持有者所在地市州；
d) O（Organization）应为证书持有者所属单位的上一级单位的名称全称；
e) OU（OrganizationUnit）应为证书持有者或者证书持有者所属单位的名称全称；
f) CN（CommonName）中的内容分为四种：
   1) 个人证书中应为证书持有者的姓名；
   2) 机构证书中应为证书持有者单位的名称；
   3) 设备证书中应为证书持有者设备的设备编码、服务器地址、IP 或通用名；
   4) 代码签名证书中应为负责人的姓名，或者是所属单位的名称。

证书主题DN命名示例参见附录A。

6 数字证书模板

6.1 个人数字证书模板

个人数字证书模板见表3：

表3 个人数字证书模板

证书域名	含义	说明		字段内容（示例）
Version	版本号	证书版本号		V3
Serial Number	序列号	由颁发机构指定		证书序列号
Signature	签名算法	遵循国家密码主管部门的要求		sha1RSA
Issuer	颁发者	C	国家	CN
		O	单位	BJCA
		OU	部门	Public Trust CA
		CN	二级 CA 通用名	Public Trust CA-1
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	C	国家	CN
		S	省份	持证人所在省份，如：北京
		L	城市	持证人所在城市，如：北京

表 3（续）

证书域名		含义	说明		字段内容（示例）
Subject		主题	O	用户单位/机构	可选字段
			OU	部门名称，可多级	可选字段
			CN	用户姓名	张三
			Email	电子邮件	（可选字段）
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		遵循国家密码主管部门的要求
	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）		遵循国家密码主管部门的要求
	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		遵循国家密码主管部门的要求
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值		遵循国家密码主管部门的要求
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值		遵循国家密码主管部门的要求
	1.2.86.11.7.1	个人用户身份标识	自定义扩展项		用户证件类型和证件号码
	1.2.86.11.7.8	政务个人证书实体唯一标识符	自定义扩展项		
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

6.2 机构证书模板

机构数字证书模板如表4所示：

表4 机构数字证书模板

证书域名		含义	说明		字段内容（示例）
Version		版本号	证书版本号		V3
Serial Number		序列号	由颁发机构指定		证书序列号
Signature		签名算法	符合国家标准		sha1RSA
Issuer		颁发者	C	国家	CN
			O	单位	BJCA
			OU	部门	Public Trust CA
			CN	二级 CA 通用名	Public Trust CA-1
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	C	国家	CN
			S	省份	持证人所在省份，如：北京
			L	城市	持证人所在城市，如：北京
			O	用户单位或机构	可选字段
			OU	部门名称，可多级	可选字段
			CN	单位名称全称	具体根据实际机构名称填写
			Email	电子邮件	（可选字段）
Subject Public Key Information		公钥	包括加密算法及公钥值		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		遵循国家密码主管部门的要求
	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）（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

表 4（续）

证书域名		含义	说明	字段内容（示例）
扩展域	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）	遵循国家密码主管部门的要求
	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	遵循国家密码主管部门的要求
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值	遵循国家密码主管部门的要求
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值	遵循国家密码主管部门的要求
	1.2.86.11.7.3	机构身份标识	自定义扩展项	用户证件类型和证件号码
	1.2.86.11.7.9	政务机构证书实体唯一标识符	自定义扩展项	
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

6.3 设备证书模板

设备数字证书模板如表5所示：

表5 设备数字证书模板

证书域名	含义	说明		字段内容（示例）
Version	版本号	证书版本号		V3
Serial Number	序列号	由颁发机构指定		证书序列号
Signature	签名算法	符合国家标准		sha1RSA
Issuer	颁发者	C	国家	CN
		O	单位	BJCA
		OU	部门	Public Trust CA

表 5（续）

证书域名		含义	说明		字段内容（示例）
Validity		有效期限	CN	二级 CA 通用名	Public Trust CA-1
			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	C	国家	CN
			S	省份	持证人所在省份，如：北京
			L	城市	持证人所在城市，如：北京
Subject		主题	O	用户单位/机构	可选字段
			OU	部门名称，可多级	可选字段
			CN	服务器 MAC 地址/IP/名称或域名	例如：ca.caac.gov.cn 根据实际的名称填写
Subject Public Key Information		公钥	包括加密算法及公钥值		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		遵循国家密码主管部门的要求
	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）		遵循国家密码主管部门的要求
	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		遵循国家密码主管部门的要求
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值		遵循国家密码主管部门的要求
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值		遵循国家密码主管部门的要求
	1.2.86.11.7.3	机构身份标识	自定义扩展项		用户证件类型和证件号码
	1.2.86.11.7.9	政务机构证书实体唯一标识符	自定义扩展项		

表 5（续）

证书域名	含义	说明	字段内容（示例）
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

6.4 代码签名证书模板

代码签名证书的模板如表6所示：

表6 代码签名证书

证书域名	含义	说明		字段内容（示例）
Version	版本号	证书版本号		V3
Serial Number	序列号	由颁发机构指定		证书序列号
Signature	签名算法	符合国家标准		符合国家标准
Issuer	颁发者	C	国家	CN
		O	单位	BJCA
		OU	部门	Public Trust CA
		CN	二级CA通用名	Public Trust CA-1
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	C	国家	CN
		S	省份	持证人所在省份，如：北京
		L	城市	持证人所在城市，如：北京
		O	用户单位/机构	可选字段
		OU	部门名称，可多级	可选字段
		CN	代码所属单位或个人	例如：CN=运行保障处 具体可根据实际情况填写
Subject Public Key Information	公钥	包括加密算法及公钥值		遵循国家密码主管部门的要求

表 6（续）

证书域名		含义	说明	字段内容（示例）
扩展域	BasicConstraints	基本限制	该证书持有者是否是认证结点	遵循国家密码主管部门的要求
	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）	遵循国家密码主管部门的要求
	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	遵循国家密码主管部门的要求
	AuthorityInfoAccess	颁发机构信息访问	颁发机构的信息 URL，可以为多个值	遵循国家密码主管部门的要求
	SubjectKeyIdentifier	主题密钥标识符	本证书公钥的 hash 值	遵循国家密码主管部门的要求
	1.2.86.11.7.3	机构身份标识	自定义扩展项	用户证件类型和证件号码
	1.2.86.11.7.9	政务机构证书实体唯一标识符	自定义扩展项	
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

6.5 其他证书

MH/T 0045 的本部分没有涉及到的特殊需求的证书类型，在不违背本规范中定义的证书基本要求的前提下，根据业务的实际要求进行扩展定义。

附 录 A
（资料性附录）
证书主题 DN 命名示例

A.1 个人证书主题DN示例

个人证书主题DN命名示例适用于内部工作人员证书和外部个人证书，DN命名示例如下：

C=CN
S=北京市（省/直辖市，可选项）
L=北京市（市/地区，可选项）
O=民航局信息中心（单位名称，可选项）
OU=某某部门（部门名称，可选项）
CN=张三（个人姓名，必填项）
E=zhangsan@caac.gov.cn（电子邮件，可选）

A.2 单位证书主题DN示例

单位证书主题DN命名示例适用于民航各级单位，DN命名示例如下：

C=CN
S=四川省（省/直辖市，可选项）
L=成都市（市/地区，可选项）
O=西南地区管理局（单位名称，可选项）
OU=运行保障部（部门名称，可选项）
CN=西南地区管理局运行保障部（单位名称，必填项）

A.3 设备证书主题DN示例

设备证书主题DN命名示例适用于内部设备证书和外部设备证书，DN命名示例如下：

C=CN
S=新疆维吾尔族自治区（省/直辖市，可选项）
L=乌鲁木齐市（市/地区，可选项）
O=新疆管理局（单位名称，可选项）
OU=某某部门（部门名称，可选项）
CN=设备名称/MAC地址/IP地址/域名（设备名称，必填项）

A.4 代码签名证书主题DN示例

代码签名证书主题DN命名示例适用于机构或者个人，DN命名示例如下：

C=CN
S=北京市（省/直辖市，可选项）

L=北京市（市/地区，可选项）

O=某某单位（单位名称，可选项）

OU=某某部门（部门名称，可选项）

CN=代码发布机构名称/个人姓名（代码签名主题，必填项）