ICS 35.040
CCS L 80

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 02.3—2022
代替 LD/T 30.3—2009

人力资源社会保障电子认证体系规范 第3部分：数字证书格式规范

Specifications for human resources and social security electronic authentication system— Part 3: Format specifications for digital certificate

2022-06-22 发布　　2022-07-01 实施

中华人民共和国人力资源和社会保障部　发布

目　　次

前　言

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

LD/T 02人力资源社会保障电子认证体系系列规范，已经发布了以下五个部分：

----第1部分：框架规范

----第2部分：电子认证系统技术规范

----第3部分：数字证书格式规范

----第4部分：数字证书应用接口规范

----第5部分：数字证书载体规范

本文件为LD/T 02的第3部分。

本文件代替LD/T 30.3—2009《人力资源社会保障电子认证体系 第3部分：证书及证书撤消列表格式规范》，与LD/T 30.3—2009相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了本部分规范名称为《人力资源社会保障电子认证体系 第3部分：数字证书格式规范》；

b) 删除了部分不再被引用的文件（见第2章，2009版第2章）；

c) 删除了部分不必要的术语定义，同时增加了的术语和定义的来源（见第3章，2009版第3章）；

d) 更改了证书分类，根据人力资源社会保障数字证书业务需求，重新划分证书类别，增加持卡人证书（见第5章，2009版第5章）；

e) 更改了数字证书通用格式，对数字证书基本结构进行细化（见第6章，2009版第6章）；

f) 更改了数字证书格式模板，增加持卡人证书格式模板（见第7章，2009版第7章）；

g) 更改了签名算法（见8.1.5，2009版8.1.5）；

h) 更改主体命名规范，将名称修改为主体命名示例，根据证书分类，修订各类证书的主体DN描述（见附录A，2009版附录A）；

i) 更改了数字证书编码示例，所有涉及密码算法的描述均采用国家密码管理批准的密码算法（见附录B，2009版附录B）；

j) 更改了密码算法的描述，将章节名称修改为“算法说明”，涉及密码算法的描述均采用国家密码管理批准的密码算法（见附录C，2009版附录C）；

k) 增加了参考文献，为本文件提供标准文本的参考。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中华人民共和国人力资源社会保障部信息中心提出并归口。

本文件起草单位：中华人民共和国人力资源和社会保障部信息中心、普华诚信信息技术有限公司、北京数字认证股份有限公司。

本文件主要起草人：马丹蕾、张嵩、王岩、耿建军、唐淑静、韩晓颖、成勇、王祥宇、李娜、王智飞、郭丽芳、高五星、李述胜。

本文件所代替的历次版本发布情况为：

----LD/T 30.3—2009《人力资源社会保障电子认证体系 第3部分：证书及证书撤消列表格式规范》；

----本次为第一次修订。

引　言

为适应人力资源社会保障信息化发展要求，满足人力资源社会保障网络信任体系建设和管理的需要，人力资源社会保障部组织并制定了人力资源社会保障电子认证体系系列规范。随着我国商用密码技术的发展、国产密码算法的标准发布，以及人力资源社会保障行业的业务发展，需要对行业标准 LD/T 30—2009《人力资源社会保障电子认证体系规范》进行修改和完善。

本次修订，是在充分借鉴原标准的框架和结构的基础上，根据人力资源社会保障行业特点和电子认证业务发展需求，对电子认证体系总体结构和电子认证系统整体建设规划进行扩充完善，以符合国家及国家密码主管部门相关标准规范要求，满足人力资源社会保障业务和管理需求，推进 SM2 算法在人社信息系统中的应用，另一方面，也可有效配合《中华人民共和国密码法》、《中华人民共和国网络安全法》、密码管理及密码应用安全测评工作、等级保护工作的落实与实施。

LD/T 02描述了人力资源社会保障电子认证体系总体结构和电子认证系统整体建设规划，规定了各级人力资源社会保障部门电子认证系统建设和应用要求，由以下五个部分构成。

----第1部分：框架规范

----第2部分：电子认证系统技术规范

----第3部分：数字证书格式规范

----第4部分：数字证书应用接口规范

----第5部分：数字证书载体规范

LD/T 02的第1部分，是人力资源社会保障电子认证体系系列规范的总纲，规定了电子认证体系规范的总体框架。LD/T 02的第2部分~第5部分分别从电子认证系统技术、数字证书格式、数字证书应用接口、数字证书载体四个方面提出具体规范要求。

本部分重点引用了GB/T 20518-2018，并在此基础上，扩展了证书分类、各类证书模板、证书DN命名规范、CRL格式规范等相关内容，给出了数字证书编码格式示例，从满足人力资源社会保障业务需求的角度，对本行业内所发放的数字证书和证书撤销列表的类型和格式提出规范和要求。

人力资源社会保障电子认证体系规范
第3部分： 数字证书格式规范

1 范围

本文件给出了人力资源社会保障数字证书分类，规定了数字证书通用格式和格式模板，以及 CRL 格式的基本结构和格式模板。

本文件适用于人力资源社会保障电子认证系统数字证书格式的定制和签发。

2 规范性引用文件

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

GB/T 19714-2005 信息技术 安全技术 公钥基础设施 证书管理协议

GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

3 术语和定义

GB/T 25056、GB/T 20518、GB/T 19714 界定的和下列术语和定义适用于本文件。

3.1

证书序列号 certificate serial number

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

［来源：GB/T 20518-2018，3.4］

3.2

CRL 分发点 CRL distribution point

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

[来源：GB/T 20518-2018，3.6]

3.3

终端实体 end entity

不以签署证书为目的而使用其私钥的证书主体或者是依赖（证书）方。

［来源：GB/T 19714-2005，3.15］

3.4

抽象记法1 abstract syntax notation 1;ASN.1

用来组织复杂数据对象的表示法。

［来源：GB/T 19714-2005，3.1］

3.5

可辨别编码规则 distinguished encoding rules;DER

对ASN.1对象进行编码的规则。

注：本文件中使用DER对ASN.1对象进行编码。

［来源：GB/T 19714-2005，3.12］

3.6

可辨别名 distinguished name

数字证书实体特征名

用来识别公钥的实体名称，通常包括实体的通用名、单位、组织和国家信息。

4 缩略语

下列缩略语适用于本文件：

ASN：抽象语法表示法（Abstract Syntax Notation）

C：国家（Country）

CA：证书认证机构（Certification 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）

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）

RA：证书注册机构（Registration Authority）

5 证书分类

人力资源社会保障电子认证系统主要签发和管理以下四类用户证书：

a) 机构证书——面向人力资源社会保障系统内部机构（包括各级人力资源社会保障部门、各类经办机构、公共服务机构、街道社区人力资源社会保障服务站、所等）、服务于人力资源社会保障业务的系统外机构（包括人力资源社会保障事务代理机构等），以及人力资源社会保障业务所管理服务的企事业单位发放；

b) 人员证书——面向人力资源社会保障业务专网计算机终端用户（包括各级人力资源社会保障部门工作人员、经办人员等）发放；

c) 设备证书——面向人力资源社会保障信息系统的服务器、终端设备等发放；

d) 持卡人证书——面向第三代社会保障卡持卡人发放。

6 数字证书通用格式

6.1 基本结构

数字证书由三部分组成：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。

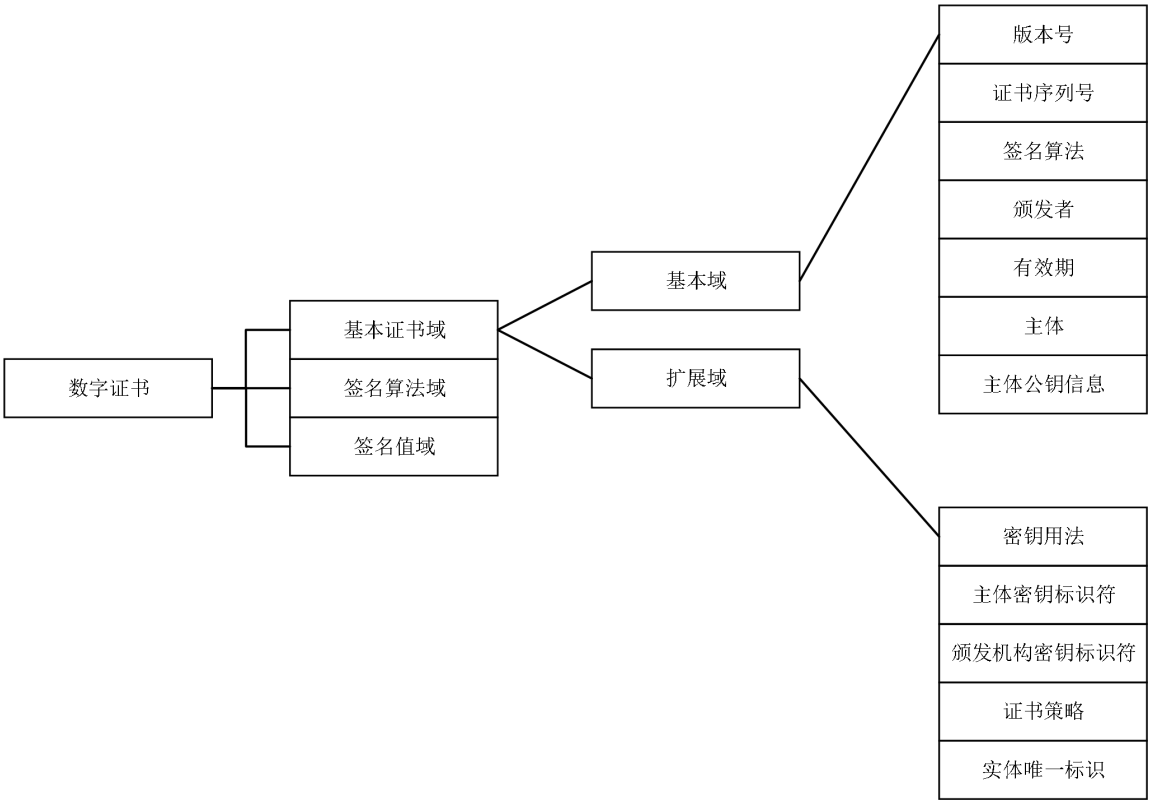

图 1 数字证书基本结构示意图

6.2 基本证书域

基本证书域（TBSCertificate）包括基本域和扩展域。

6.2.1 基本域

基本域由以下部分组成：

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） 主体 Subject
g） 主体公钥信息 SubjectPublicKeyInfo

6.2.1.1 版本

本项描述了数字证书的版本号。

数字证书应使用版本 3（对应的数值是整数“2”）。

6.2.1.2 序列号

本项是证书签发管理系统分配给每个证书的一个正整数，一个证书签发管理系统签发的每张证书的序列号必须是唯一的（通过颁发者的名字和序列号就可以唯一地确定一张证书），证书签发管理系统必须保证序列号是非负整数。

证书更新时序列号须改变。

a) 机构证书、人员证书、设备证书的序列号规则一致，证书序列号的长度为16个16进制数字，序列号编码规则如下：

证书序列号（16位）= CA编号（2）+RA编号（6）+ 顺序号（8）

其中，CA编号编码规则为 “CA+行政区划前4位”，RA编号编码规则为 “RA+行政区划（6位）”，顺序号可从1开始依次累加。

例如：某一证书序列号是: 1034000000316098。前2位“10”代表部CA系统，第3位到8位“340000”代表安徽省RA，最后8位“00316098”代表证书的顺序号。

b) 持卡人证书序列号的长度为32个16进制数字，序列号编码规则如下：

持卡人证书序列号（32位）= 证书类型编号（2）+发卡地行政区划代码（6）+CA编号（2）+ 随机数（22）

其中，发卡地行政区划代码遵循《社会保障卡发行地区行政区划代码》，CA编号CA编号编码规则为 “CA+行政区划前4位”。

例如：某一证书序列号是: 10341000347517737135237362193813。前2位“10”代表签名证书，第3位到8位“341000”代表安徽省黄山市，第9位到10位“34”代表安徽省，最后22位“7517737135237362193813”代表证书的随机号。

6.2.1.3 签名算法

本项包含CA签发该证书所使用的密码算法的标识符，这个算法标识符必须与证书中SignatureAlgorithm项的算法标识符相同，签名算法采用SM3withSM2。

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。

6.2.1.4 颁发者

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可辨别名（DN）。该项被定义为Name类型，其ASN.1的结构如下：

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

Name 描述了一些属性组成的层次结构的名称，如国家名、相应的值，如“C=CN”。颁发者可辨别名的 C（Country）属性的编码使用 PrintableString。其它属性的编码一律使用 UTF8String。

各项编码规范如表 1 所示。

表 1 颁发者 DN 编码规范

Name 类型	说明	示例	编码格式
C	国家	CN	PrintableString
S	省份	证书签发管理系统所在省份，例北京	UTF8String
L	城市	证书签发管理系统所在城市，例北京	UTF8String
O	颁发机构名称	人力资源社会保障部信息中心	UTF8String
CN	颁发机构别名	人力资源社会保障部信息中心	UTF8String

6.2.1.5 有效期

本项是指一个时间段，在这个时间段内，证书签发管理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）。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。

在本项中，UTCTime 值必须用格林威治标准时间表示，并且必须包含秒，即使秒的数值为零（即时间格式为 YYMMDDHHMMSSZ）。系统对年字段（YY）应解释为 20YY。

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

CA 证书的有效期最长为 20 年。

6.2.1.6 主体

本项描述了与主体公钥项中的公钥相对应的实体。主体名称可以出现在主体项和/或主体替换名称扩展项中（SubjectAltName）。如果主体是一个 CA，那么主体项必须是一个非空的与颁发者项的内容相匹配的甄别名称（Distinguished Name），一个 CA 认证的每个主体实体的甄别名称必须是唯一的。一个 CA 可以为同一个主体实体以相同的甄别名称签发多个证书。

该项不能为空。

6.2.1.7 主体公钥信息

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，公钥算法采用 SM2 椭圆曲线公钥密码算法。

6.2.2 扩展域

本文件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，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。

证书扩展域结构如图 2 所示。

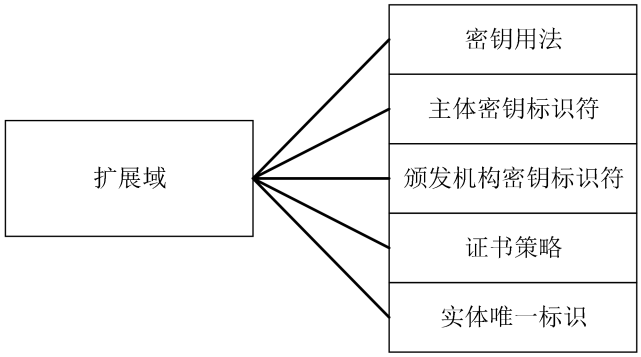

图 2 扩展域构成

本条定义了如下一些标准扩展项和专用扩展项：

a) 密钥用法 KeyUsage
b) 主体密钥标识符 SubjectKeyIdentifier
c) 颁发机构密钥标识符 AuthorityKeyIdentifier
d) 证书策略 CertificatePolicies
e) 实体唯一标识 SubjectUniqueID

注：对于 CA 证书，可以不签发实体唯一标识；对于终端实体证书，则必须签发实体唯一标识，以用于区分用户。

6.2.2.1 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。该项定义如下：

id-ce-keyUsage OBJECT IDENTIFIER ::= {id-ce 15}
KeyUsage::=BIT STRING{

digitalSignature (0)，--数字签名
nonRepudiation (1)，--防抵赖
keyEncipherment (2)，--密钥加密
dataEncipherment (3)，--数据加密
keyAgreement (4)，--密钥协议
keyCertSign (5)，--证书签发
cRLSign (6)，--证书撤销列表签发
encipherOnly (7)，--仅加密
decipherOnly (8) }--仅签名

所有的 CA 证书必须包括本扩展，而且必须包含 keyCertSign 这一用法。用户证书则根据证书用途，分为签名证书和加密证书，选择对应的密钥用途进行签发。此扩展可以定义为关键的或非关键的，由证书颁发者选择。

6.2.2.2 主体密钥标识符

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。它能够区分同一主体使用的不同密钥（例如，当密钥更新发生时）。

对于使用密钥标识符的主体的各个密钥标识符而言，每一个密钥标识符均应是唯一的。CA签发证书时必须把CA证书中本扩展的值赋给终端实体证书的AuthorityKeyIdentifier扩展中的KeyIdentifier项。CA证书的主体密钥标识符应从公钥中或者生成唯一值的方法中导出。终端实体证书的主体密钥标识符应从公钥中导出。

所有的CA证书必须包括本扩展，此扩展项总是非关键的。

6.2.2.3 颁发机构密钥标识符

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

相应CA产生的所有证书应包括AuthorityKeyIdentifier扩展的KeyIdentifier项，以便于链的建立。

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）。

6.2.2.4 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。这个可选的限定条件不能改变策略的定义。

在用户证书中，这些策略信息条目描述了证书发放所依据的策略以及证书的应用目的；在CA证书中，这些策略条目指定了包含这个证书的验证路径的策略集合。具有特定策略需求的应用系统应该拥有它们将接受的策略的列表，并把证书中的策略OID与该列表进行比较。如果该扩展是关键的，则路径有效性软件必须能够解释该扩展（包括选择性限定语），否则必须拒绝该证书。

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。

6.2.2.5 实体唯一标识

本项是代表证书持有者身份的唯一编码，在业务系统中，本标识可与系统内用户名一一关联，从而实现证书用户与系统用户的绑定。实体唯一标识可以用来处理主体名称的重用问题，例如一个用户申请多张证书，业务系统可通过解析实体唯一标识来区分用户。

“实体唯一标识”编码规则为：

用户编号（变长）+@+证书类型代码（1 位）+证件类型代码（2 位）+证件号码（变长）

“实体唯一标识”的数据总长度不限制，可根据证件号码长度灵活调整。其中，用户编号是同一用户所持证书的顺序号，一个证件号码允许申请多张证书，例如一个用户申请2张证书，则其用户编号为1和2。证件号码是指用户申请证书时使用的证件号码。证书类型代码和证件类型代码如表2所示。

表 2 证书类型与证件类型代码对应表

证书类型	证书类型代码	证件名称	证件类型代码
机构证书	1	统一社会信用代码	ZZ
人员证书	2	身份证	SF
设备证书	3	MAC 地址	SB

6.2.2.6 社会保障号码标识

本项是代表持卡人证书持有者身份的编码，采用社会保障号码经 SM3 算法运算后的哈希值作为社会保障号码标识。

6.2.2.7 卡号

本项是持卡人证书持有者所持有的社会保障卡卡号。

6.3 签名算法域

签名算法域（SignatureAlgorithm）包含数字证书的密码算法，如杂凑算法 SM3、签名算法 SM3WithSM2 等，详细内容参见附录 C。在人力资源社会保障系统应用时，应使用国家密码管理主管部门审核批准的 SM2、SM3 等密码算法。

6.4 签名值域

签名值域（SignatureValue）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。

6.5 命名规范

数字证书中的主体DN的编码规范是：DN_C（Country）属性的编码使用PrintableString，其它属性的编码一律使用UTF8String。最后一项必须是C=CN；CN项需要放在DN的最前面；其它项按照从小到大的顺序排列：OU在O前面，L在S前面。

数字证书中的主体DN命名规范为：

a） C，表示国家，例：CN；

b） S，表示省份，所在省份，例：北京；

c） L，表示城市，所在城市，例：北京；

d） O，表示单位或机构名称，例：人力资源社会保障部；

e） OU，表示部门名称，例：人力资源社会保障部信息中心；

f） CN，表示单位或机构别名，例：人力资源社会保障部。

主体命名示例见附录A。

另外，数字证书编码示例见附录B。

7 数字证书格式模板

7.1 CA 证书格式模板

CA 证书模板如表 3 所示。

表 3 CA 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		10 00 00 00 00 00 00 02 00 03
Signature	签名算法	符合国家标准		SM3WithSM2Encryption(1.2.156.10197.1.501)
Issuer	颁发者	C	国家	CN
		S	省份	北京
		L	城市	北京
		O	颁发机构名称	人力资源社会保障部
		CN	颁发机构别名	人力资源社会保障部

Validity	有效期限	最长20年，根据应用需求定义，但必须在根证书有效期范围内。		20年
notBefore	有效期起始日期	签发日期		2020年9月17日 16:19:35
notAfter	有效期终止日期	起始日期＋有效期		2040年9月17日 16:19:35
Subject	主体	C	国家	CN
		S	省份	xx省
		L	城市	xx市
		O	用户单位/机构	xx人力资源社会保障厅（局）信息中心
		CN	用户别名	xx人力资源社会保障厅（局）信息中心
Subject Public Key Information	公钥	包括加密算法及公钥值		采用SM2椭圆曲线密码算法
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		Certificate Signing, Off-line CRL Signing, CRL Signing
SubjectKeyIdentifier	主体密钥标识符	非关键扩展项		CA证书公钥的哈希值
AuthorityKeyIdentifier	颁发机构密钥标识符	非关键扩展项		根证书公钥的哈希值
BasicConstraints	基本限制	关键扩展项		CA＝True
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法		SM3WithSM2Encryption(1.2.156.10197.1.501)
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

7.2 机构证书格式模板

机构证书模板如表4所示。

表 4 机构证书模板

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	按照本文件6.2.1.2	按照序列号规范定义

Signature	签名算法	符合国家标准		SM3WithSM2Encryption(1.2.156.10197.1.501)
Issuer	颁发者	C	国家	CN
		S	省份	xx 省
		L	城市	xx 市
		O	颁发机构名称	xx 人力资源社会保障厅（局）信息中心
		CN	颁发机构别名	xx 人力资源社会保障厅（局）信息中心
Validity	有效期限	最长 5 年，根据应用需求定义，但必须在 CA 证书有效期范围内。		5 年
notBefore	有效期起始日期	签发日期		2020 年 9 月 17 日 16:19:35
notAfter	有效期终止日期	起始日期＋有效期限		2025 年 9 月 17 日 16:19:35
Subject	主体	C	国家	CN
		S	省份	持证机构所在省份
		L	城市	持证机构所在城市
		O	机构名称	
		OU	证书管理者	
		CN	机构别名	
Subject Public Key Information	公钥	包括加密算法及公钥值		采用 SM2 椭圆曲线密码算法
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		签名证书密钥用法包括：数字签名 digitalSignature 、防抵赖 nonRepudiation 加密证书密钥用法包括：密钥加密 keyEncipherment 、数据加密 dataEnciphermen 、密钥协议 keyAgreement
SubjectUniqueID	实体唯一标识	非关键扩展项		OID 为：1.2.156.2316； 值如：2@1ZZ123456789
SubjectKeyIdentifier	主体密钥标识符	非关键扩展项		证书中公钥的哈希值
AuthorityKeyIdentifier	颁发机构密钥标识符	非关键扩展项		颁发机构公钥的哈希值
CRLDistributionPoints	CRL 分发点	非关键扩展项		[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address:

			DN… [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ldap.xxca.gov.cn/crl/xx.crl
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法	SM3WithSM2Encryption(1.2.156.10197.1.501)
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

7.3 人员证书格式模板

工作人员证书模板如表5所示。

表 5 工作人员证书模板

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		按照序列号规范定义
Signature	签名算法	符合国家标准		SM3WithSM2Encryption(1.2.156.10197.1.501)
Issuer	颁发者	C	国家	CN
		S	省份	如:xx省
		L	城市	如:xx市
		O	颁发机构名称	如：xx人力资源社会保障厅（局）信息中心
		CN	颁发机构别名	如：xx人力资源社会保障厅（局）信息中心
Validity	有效期限	最长5年，根据应用需求定义，但必须在CA证书有效期范围内。		5年
notBefore	有效期起始日期	签发日期		2020年9月17日 16:19:35
notAfter	有效期终止日期	起始日期＋有效期限		2025年9月17日 16:19:35
Subject	主体	C	国家	CN
		S	省份	持证人所在省份，如：xx
		L	城市	持证人所在城市，如：xx
		O	用户单位/机构	xx省xx人力资源社会保障厅（局）
		OU	部门名称	xx省xx人力资源社会保障厅（局）信

				息中心
		CN	用户别名	张三
Subject Public Key Information	公钥	包括加密算法及公钥值		采用 SM2 椭圆曲线密码算法
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		签名证书密钥用法包括：数字签名 digitalSignature 、防抵赖 nonRepudiation 加密证书密钥用法包括：密钥加密 keyEncipherment 、数据加密 dataEnciphermen 、密钥协议 keyAgreement
SubjectUniqueID	实体唯一标识	非关键扩展项		OID：1.2.156.2316 值如：1@2SF342222197805053618
SubjectKeyIdentifier	主体密钥标识符	非关键扩展项		用户证书公钥的哈希值
AuthorityKeyIdentifier	颁发机构密钥标识符	非关键扩展项		颁发机构证书公钥的哈希值
CRLDistributionPoints	CRL 分发点	非关键扩展项		[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: DN… [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ldap.xxca.gov.cn/crl/xx.crl
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法		SM3WithSM2Encryption(1.2.156.10197.1.501)
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

7.4 设备证书格式模板

设备证书模板如表 6 所示。

表 6 设备证书模板

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		按照序列号规范定义
Signature	签名算法	符合国家标准		SM3WithSM2Encryption(1.2.156.10197.1.501)
Issuer	颁发者	C	国家	CN
		S	省份	如:xx 省
		L	城市	如:xx 市
		O	颁发机构名称	如:xx 人力资源社会保障厅（局）信息中心
		CN	颁发机构别名	如:xx 人力资源社会保障厅（局）信息中心
Validity	有效期限	最长 5 年，根据应用需求定义，但必须在 CA 证书有效期范围内。		5 年
notBefore	有效期起始日期	签发日期		2020 年 9 月 17 日 16:19:35
notAfter	有效期终止日期	起始日期＋有效期		2025 年 9 月 17 日 16:19:35
Subject	主体	C	国家	CN
		S	省份	设备所在省份，例 xx
		L	城市	设备所在城市，例 xx
		O	设备所属单位	例：xx 人力资源社会保障厅（局）
		OU	部门名称	例：xx 人力资源社会保障厅（局）信息中心
		CN	设备别名	可为 IP 地址、设备名称、域名等
Subject Public Key Information	公钥	包括加密算法及公钥值		采用 SM2 椭圆曲线密码算法
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		签名证书密钥用法包括：数字签名 digitalSignature 、防抵赖 nonRepudiation 加密证书密钥用法包括：密钥加密 keyEncipherment 、数据加密 dataEnciphermen 、密钥协议 keyAgreement
SubjectUniqueID	实体唯一标识	非关键扩展项； 标识一个设备的唯一编码的值		OID：1.2.156.2316; 值如：1@3SB192.168.2.23
SubjectKeyIdentifier	主体密钥标识符	非关键扩展项		本证书公钥的哈希值

AuthorityKeyIdentifier	颁发机构密钥标识符	非关键扩展项	颁发机构公钥的哈希值
CRLDistributionPoints	CRL分发点	非关键扩展项	[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: DN… [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ldap.xxca.gov.cn/crl/xx.crl
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法	SM3WithSM2Encryption(1.2.156.10197.1.501)
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

7.5 持卡人证书格式模板

持卡人证书模板如表7所示。

表 7 持卡人证书模板

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		按照序列号规范定义
Signature	签名算法	符合国家标准		SM3WithSM2Encryption(1.2.156.10197.1.501)
Issuer	颁发者	C	国家	CN
		S	省份	如:xx省
		L	城市	如:xx市
		O	颁发机构名称	如：xx人力资源社会保障厅（局）信息中心
		CN	颁发机构别名	如：xx人力资源社会保障厅（局）信息中心
Validity	有效期限			最长10年
notBefore	有效期起始日期	签发日期		2020年9月17日 16:19:35
notAfter	有效期终止日期	起始日期＋有效期限		2030年9月17日 16:19:35

Subject	主体	C	国家	CN
		S	省份	持证人所在省份，例山东
		L	城市	持证人所在城市，例淄博
		CN	用户别名	张三
Subject Public Key Information	公钥	SM2 椭圆曲线密码算法		SM2 公钥
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		签名证书密钥用法包括：数字签名 digitalSignature、防抵赖 nonRepudiation 加密证书密钥用法包括：密钥加密 keyEncipherment、数据加密 dataEnciphermen、密钥协议 keyAgreement
SsNo	社会保障号码标识	非关键扩展项，标识持卡人身份的编码的值		OID：1.2.156.2316.1.1 社会保障号码采用 SM3 算法进行哈希运算后的哈希值
cardNo	卡号	非关键扩展项		OID：1.2.156.2316.1.2 长度 9 位
SubjectKeyIdentifier	主体密钥标识符	非关键扩展项		本证书公钥的哈希值
AuthorityKeyIdentifier	颁发机构密钥标识符	非关键扩展项		颁发机构公钥的哈希值
CRLDistributionPoints	CRL 分发点	非关键扩展项		CRL 分发点
critical	扩展项类别			[1]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: DN… [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ldap.xxca.org.cn/crl/xx.crl
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法		SM3WithSM2Encryption(1.2.156.10197.1.501)

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

8 CRL 格式

8.1 CRL 基本结构

CRL 是 CA 对撤销的证书而签发的一个列表文件，该文件可用于业务系统鉴别用户证书的有效性。CRL 文件结构主要包括：

a) 版本号
b) 颁发者
c) 生效日期
d) 下次更新日期
e) 签名算法
f) 撤销日期
g) 扩展项
h) 被撤销的证书列表

8.1.1 版本号

CRL 版本号采用 v2。

8.1.2 签名算法

本项包含 CA 签发该 CRL 所使用的密码算法的标识符，这个算法标识符必须与证书中 SignatureAlgorithm 项的算法标识符相同。

人力资源社会保障电子认证系统应使用国家密码管理主管部门审核批准的 SM3withSM2 算法。

8.1.3 颁发者

颁发者的 X.500 目录示例如下：

CN＝人力资源社会保障部信息中心; //通用名
OU＝人力资源社会保障部信息中心 //部门
O＝人力资源社会保障部信息中心 //组织名称
L＝北京 //城市
S＝北京 //省份
C＝CN //国家名

8.1.4 生效日期

颁发 CRL 之日起生效。

8.1.5 下次更新日期

该域含有一个日期/时间值，用以表明下一次 CRL 将要发布的时间。

8.1.6 被撤销的证书列表

该域签发被撤销的证书序列号、撤销时间和撤销原因。

8.1.6.1 被撤销的证书序列号

被撤销的证书序列号（SerialNumber）。

8.1.6.2 撤销时间

该域含有已经撤销或者挂起的证书列表。本列表中含有证书的序列号和证书被撤销的日期和时间。

8.1.6.3 撤销原因

撤销原因（CRLReason），表明证书撤销的原因。

8.1.7 扩展项

该域主要包括颁发机构密钥标识符和证书撤销列表号。

8.1.7.1 颁发机构密钥标识符

颁发机构密钥标识符（AuthorityKeyIdentifier）扩展提供了一种方式，以识别与 CRL 签名私钥相应的公钥。当颁发者由于有多个密钥共存或由于发生变化而具有多个签名密钥时使用该扩展。颁发机构密钥标识符应符合 GB/T 20518-2018 中 5.3.4.3 规定的要求。

8.1.7.2 证书撤销列表号

证书撤销列表号（CRLNumber）是一个非关键的 CRL 扩展，表示在给定的 CRL 颁发者和 CRL 范围内一个单调递增序列。这个扩展可以让用户方便地确定一个特定的 CRL 何时取代另一个 CRL。证书撤销列表号也支持鉴别一个附件的完整 CRL 和增量 CRL。证书撤销列表号的编码规则应符合 GB/T 20518-2018 中 5.3.4.1 规定的要求。

8.2 CRL 格式模板

CRL 格式模板如表 8 所示。

表 8 CRL 格式模板表

证书域名	含义	说明	
Version	版本号	采用 V2 版本	
Signature	签名算法	符合国家标准	
Issuer	签发机构名	DN_C	国家代码
		DN_S	省份
		DN_L	城市
		DN_O	组织名称
		DN_OU	组织地址
		DN_CN	组织编号
Validity	有效期限		
ThisUpdata	本次更新日期	签发时确定	
NextUpdate	下次更新日期	根据签发 CRL 策略确定	
Revoke cert List	被撤销的证书列表		
Cert info	证书信息	被撤销的证书关键信息	
SerialNumber	序列号	被撤销的证书序列号	

证书域名	含义	说明
Revocationdate	时间	撤销时间
CRLReason	注销原因	撤销原因代码
extnValue	扩展项	
AuthorityKeyIdentifier	颁发机构密钥标识符	颁发机构公钥的哈希值
CRLNumber	CRL 撤销列表号	单调递增序列
SignatureAlgorithm	签名算法	对 CRL 基本信息的数字签名的签名算法
SignatureValue	签名值	对 CRL 基本信息的数字签名的签名值

附 录 A
（资料性）
主体命名示例

以下所列示例仅供参考。

A.1 机构证书

机构证书的主体DN为:

C=CN
S=北京市
L=北京市
O=北京某某单位
OU=某某部门
CN=单位名称

A.2 人员证书

人员证书的主体DN为：

C=CN
S=北京市
L=北京市
O=北京某某单位
OU=某某部门
CN=用户姓名

A.3 设备证书

人力资源社会保障部的某一单位，其设备证书的主体DN为:

C=CN
S=北京市
L=北京市
O=人力资源社会保障部
OU=人力资源社会保障部某某单位
CN=设备名称

A.4 持卡人证书

持卡人证书的主体DN为：

C=CN
S=北京市
L=北京市
CN=颁发机构别名

附 录 B
（资料性）
数字证书编码示例

B.1 以人员证书为例，证书内容主要包含下列信息：

- 序列号：11 11 00 01 00 00 05 85
- 签名算法:SM3WithSM2Encryption
- 颁发者DN：C=CN；S=北京；L=北京；O=人力资源社会保障部信息中心；CN=人力资源社会保障部信息中心
- 主体DN：C=CN；S=xx省；L=xx市；O=xx人力资源社会保障局；OU=xx部门；CN=张三
- 有效期：从2020年3月18日9:18:44到2025年3月8日9:18:44
- 主体公钥信息中包含256比特的 SM2 密钥
- 机构密钥标识符扩展项：KeyID=318fa094895bdf573b7f67a1da98cf8987bf80b9
- 主体密钥标识符扩展：fbafa55a41ac6fdd59a6618539389af582b92f2b
- 密钥用法扩展项：Digital Signature，Non-Repudiation（c0）
- 主体唯一标识：1@2SF110101197805053618

B.2 以某一测试证书为例，数字证书格式如下：

```
Offset|  Len |
 ==== +====+=============================================================
    0|  794|  SEQUENCE :
    4|  643|      SEQUENCE :
    8|    3|          CONTEXT SPECIFIC (0) :
   10|    1|              INTEGER : 2
   13|    8|          INTEGER : '1111000100000585'
   23|   13|          SEQUENCE :
   25|    8|              OBJECT IDENTIFIER :  SM3WithSM2Encryption [1. 2. 156. 10197. 1. 501]
   36|    0|              NULL :
   38|  123|          SEQUENCE :
   40|   13|              SET :
   42|   11|                  SEQUENCE :
   44|    3|                      OBJECT IDENTIFIER :  countryName [2.5.4.6]
   49|    4|                      PrintableString : 'CN'
   55|   13|              SET :
   57|   11|                  SEQUENCE :
   59|    3|                      OBJECT IDENTIFIER :  stateOrProvinceName [2.5.4.8]
   64|    4|                      UTF8String : '北京'
   70|   13|              SET :
   72|   11|                  SEQUENCE :
   74|    3|                      OBJECT IDENTIFIER :  localityName [2.5.4.7]
   79|    4|                      UTF8String : '北京'
   85|   37|              SET :
   87|   35|                  SEQUENCE :
```

```
  89|     3|                 OBJECT IDENTIFIER :  organizationName [2.5.4.10]
  94|    28|                 UTF8String : '人力资源社会保障部信息中心'
 124|    37|             SET :
 126|    35|                 SEQUENCE :
 128|     3|                     OBJECT IDENTIFIER :  commonName [2.5.4.3]
 133|    28|                     UTF8String : '人力资源社会保障部信息中心'
 163|    30|         SEQUENCE :
 165|    13|             UTC TIME : '100318091844Z'
 180|    13|             UTC TIME : '120318091844Z'
 195|   170|         SEQUENCE :
 198|    13|             SET :
 200|    11|                 SEQUENCE :
 202|     3|                     OBJECT IDENTIFIER :  countryName [2.5.4.6]
 207|     4|                     PrintableString : CN'
 213|    15|             SET :
 215|    13|                 SEQUENCE :
 217|     3|                     OBJECT IDENTIFIER :  stateOrProvinceName [2.5.4.8]
 222|     6|                     UTF8String : 'xx 省'
 230|    15|             SET :
 232|    13|                 SEQUENCE :
 234|     3|                     OBJECT IDENTIFIER :  localityName [2.5.4.7]
 239|     6|                     UTF8String : 'xx 市'
 247|    29|             SET :
 249|    27|                 SEQUENCE :
 251|     3|                     OBJECT IDENTIFIER :  organizationName [2.5.4.10]
 256|    20|                     UTF8String : 'xx 人力资源社会保障局'
 306|    29|             SET :
 308|    27|                 SEQUENCE :
 310|     3|                     OBJECT IDENTIFIER :  organizationalUnitName [2.5.4.11]
 315|    20|                     UTF8String : 'xx 部门'
 337|    29|             SET :
 339|    27|                 SEQUENCE :
 341|     3|                     OBJECT IDENTIFIER :  commonName [2.5.4.3]
 346|    20|                     UTF8String : '张三'
 368|    89|         SEQUENCE :
 371|    19|             SEQUENCE :
 373|     7|                 OBJECT IDENTIFIER :  [1.2.840.10045.2.1]
 384|     8|                 OBJECT IDENTIFIER :  [1.2.156.10197.1.301]
 386|    66|             BIT STRING UnusedBits:0 :
 390|    66|  00045D87C8ADC5FA247BB7DFFB7FFB35C6298DEB28E73315780098C8C428EE32
              531C09CF61B261E1004505297E75BCE9F9BDFD3E7160F2FEEB0F437E2A0A431C
C73F
 525|     3|                     INTEGER : 65537
 530|   119|         CONTEXT SPECIFIC (3) :
```

```
532|  117|          SEQUENCE :
534|   29|            SEQUENCE :
536|    3|              OBJECT IDENTIFIER :  subjectKeyIdentifier [2.5.29.14]
541|   22|              OCTET STRING :
543|   20|                OCTET STRING :
   |     |                  FBAFA55A41AC6FDD59A6618539389AF582B92F2B
565|   14|            SEQUENCE :
567|    3|              OBJECT IDENTIFIER :  keyUsage [2.5.29.15]
572|    1|              BOOLEAN : 'FF'
575|    4|              OCTET STRING :
577|    2|                BIT STRING UnusedBits:6 : 'C0'
581|   31|            SEQUENCE :
583|    3|              OBJECT IDENTIFIER :  authorityKeyIdentifier [2.5.29.35]
588|   24|              OCTET STRING :
590|   22|                SEQUENCE :
592|   20|                  CONTEXT SPECIFIC (0) :
   |     |                    318FA094895BDF573B7F67A1DA98CF8987BF80B9
614|   35|            SEQUENCE :
616|    5|              OBJECT IDENTIFIER :  [1.2.156.2316]
623|    1|              BOOLEAN : 'FF'
626|   23|              OCTET STRING :
   |     |                31403253463738373638373638363836373836373836373
651|   13|        SEQUENCE :
653|    9|          OBJECT IDENTIFIER :  SM3WithSM2Encryption [1. 2. 156. 10197. 1. 501]
664|    0|          NULL :
666|   77|        BIT STRING UnusedBits:0 :
                  003045022024B95A0198530D203ECB4DFFD8C4F4EE141E277E511D8290DF1F65
                  5B0160281C022100EC081108AE928DCDDEA637473A0DCF6C9F96167B7B57A177
                  17253E97939086D4
```

附 录 C
（资料性）
算法说明

C.1 杂凑算法

SM3 算法是国家密码管理主管部门公布的杂凑算法，也称为信息摘要算法。

C.2 签名算法

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

SM2 算法是国家密码管理局主管部门公布的签名算法，签名算法与杂凑算法一起被使用。

用于标识该签名算法的 ASN.1 对象的标识符是：

SM3WithSM2Encryption OBJECT IDENTIFIER ：：={

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

参考文献

[1] GB/T 16262.1-2006 信息技术 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）

[2] GB/T 16262.2-2006 信息技术 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）

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

[4] GB/T 16262.4-2006 信息技术 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）

[5] GB/T 35276-2017 信息安全技术 SM2密码算法使用规范

[6] GB/T 33560-2017 信息安全技术 密码应用标识规范