



# 中华人民共和国劳动和劳动安全行业标准

LD/T 30.3—2009

---

## 人力资源和社会保障电子认证体系 第3部分:证书及证书撤销列表格式规范

Human resources and social security electronic authentication system—  
Part 3: Format specifications of digital certificate and CRL

2009-12-14 发布

2010-03-01 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 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 2

5 证书分类 ..... 2

6 数字证书通用格式 ..... 3

    6.1 基本结构 ..... 3

    6.2 基本证书域 ..... 3

    6.3 签名算法域 ..... 7

    6.4 签名值域 ..... 7

    6.5 命名规范 ..... 7

7 数字证书格式模板 ..... 7

    7.1 根 CA 证书格式模板 ..... 7

    7.2 二级 CA 证书格式模板 ..... 8

    7.3 机构证书格式模板 ..... 10

    7.4 工作人员证书格式模板 ..... 11

    7.5 设备证书格式模板 ..... 12

    7.6 单位证书格式模板 ..... 14

    7.7 个人证书格式模板 ..... 16

8 CRL 格式 ..... 17

    8.1 CRL 基本结构 ..... 17

    8.2 CRL 格式模板 ..... 18

附录 A (资料性附录) 主体命名规范 ..... 20

附录 B (资料性附录) 数字证书编码示例 ..... 22

附录 C (资料性附录) 算法举例 ..... 25

## 前 言

为适应人力资源和社会保障信息化发展要求,满足人力资源和社会保障网络信任体系建设和管理的需要,人力资源和社会保障部组织并制定了 LD/T 30—2009《人力资源和社会保障电子认证体系》。

网络信任体系包括电子认证体系、授权管理体系和责任认定体系,本标准主要描述了人力资源和社会保障电子认证体系相关内容,包括以下五个部分:

- 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:证书及证书撤销列表格式规范;
- 第 4 部分:证书应用管理规范;
- 第 5 部分:证书载体规范。

本部分为 LD/T 30—2009 的第 3 部分。

本部分描述了人力资源和社会保障电子认证系统签发的数字证书及证书撤销列表的基本结构和相关要求。

本部分重点引用了 GB/T 20518—2006《信息安全技术 公钥基础设施 数字证书格式》,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。

本部分由中华人民共和国人力资源和社会保障部信息中心提出并归口。

本部分主要起草单位:中华人民共和国人力资源和社会保障部信息中心、上海市人力资源和社会保障局信息中心、北京数字证书认证中心、维豪信息技术有限公司。

本部分主要起草人:赵锡铭、戴瑞敏、贾怀斌、翟燕立、李丽虹、吴问滨、黄勇、吕丽娟、许华光、罗震、张加会、靳朝晖、陆春生、李永亮、宋京燕、杜守国、欧阳晋、林雪焰、李述胜、顾青、宋成。

本部分凡涉及密码相关内容,均按国家有关法规实施。

## 人力资源和社会保障电子认证体系

### 第3部分：证书及证书撤销列表格式规范

#### 1 范围

LD/T 30 的本部分对人力资源和社会保障数字证书进行了分类,定义了数字证书及证书撤销列表的基本结构,描述了数字证书中的各数据项内容,制定了证书及证书撤销列表格式模板。

本部分适用于指导人力资源和社会保障系统按照统一的证书及证书撤销列表格式进行定制和签发,以保证人力资源和社会保障各应用系统之间的互信互认。

#### 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 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)

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)

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)

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)

GB/T 20518—2006 信息安全技术 公钥基础设施 数字证书格式  
信息技术 安全技术 密码术语(国家密码管理局)

#### 3 术语和定义

以下术语和定义适用于本部分。

##### 3.1

**证书认证机构** certification authority

CA

负责创建和分配证书,受用户信任的权威机构。用户可以选择该机构为其创建密钥。

##### 3.2

**数字证书** digital certificate

由权威认证机构进行数字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

**CA 证书** CA certificate

由一个证书认证机构给另一个证书认证机构签发的数字证书,一个证书认证机构也可以为自己签发数字证书,这是一种自签名的数字证书。



3.4

电子认证系统 electronic authentication system

证书认证系统 certificate authentication system

对生命周期内的数字证书进行全过程管理的安全系统。

3.5

证书撤销列表 certificate revocation list

CRL

标记一系列不再被证书发布者认为有效的证书的签名列表。

3.6

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证书使用者。

3.7

证书序列号 certificate serial number

在一个证书认证机构所签发的证书中用于唯一标识数字证书的一个整数。

3.8

信任 trust

通常,当一个实体(第一个实体)假设另一个实体(第二个实体)完全按照第一个实体的期望行动时,则称第一个实体“信任”第二个实体。这种“信任”可能只适用于某些特定功能。本框架中“信任”的关键作用是描述鉴别实体和认证机构之间的关系;鉴别实体应确信它能够“信任”认证机构仅创建有效且可靠的证书。

4 缩略语

下列缩略语适用于本部分:

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	甄别名称(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

人力资源和社会保障电子认证系统主要为两类用户提供电子认证服务,一是全国人力资源和社会保障系统业务专网用户(以下简称内部用户),二是人力资源和社会保障业务办理中涉及的社会用户(个人、用人单位等,以下称外部用户)。针对这两类用户,电子认证系统主要签发和管理以下五类用户证书:

a) 面向内部用户的证书有三类,分别是:

- 1) 机构证书——面向人力资源和社会保障系统内部机构(包括各级人力资源和社会保障部门、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)和服务于人力资源和社会保障业务的系统外机构(包括医疗机构、定点零售药店、人力资源社会保障事务代理机构等)发放。
- 2) 工作人员证书——面向人力资源和社会保障业务专网计算机终端用户(包括各级人力资源和社会保障部门工作人员、经办人员等)发放。
- 3) 设备证书——面向人力资源和社会保障信息系统的服务器、终端设备等发放。
- b) 面向外部用户的证书有两类,分别是:
  - 1) 单位证书——面向人力资源和社会保障业务所管理服务的用人单位发放。
  - 2) 个人证书——面向人力资源和社会保障业务所管理服务的个人发放。

6 数字证书通用格式

6.1 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。

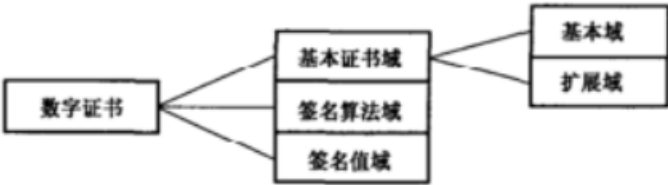


图 1 数字证书基本结构示意图

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 Signature
- 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 Version

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 SerialNumber

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。序列号可以是长整数,证书用户必须能够处理最长达 20 个 8 位字节的序列号值。证书签发管理系统必须确保不使用大于 20 个 8 位字节的序列号。

证书更新时序列号须改变。

本规范规定证书序列号的长度为 16 个 8 位字节,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 编号和 RA 编号应遵循《CA 和 RA 命名规则》,顺序号可从 1 开始依次累加。

例如:某一证书序列号是: 3434020012345678。前 2 位“34”代表安徽省,第 3 位到 8 位“340200”代表芜湖市,最后 8 位“12345678”代表证书的顺序号。

6.2.1.3 签名算法 Signature

本项包含 CA 签发该证书所使用的密码算法的标识符,这个算法标识符必须与证书中 Signature-Algorithm 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。

6.2.1.4 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。该项被定义为 X.500 的 Name 类型。

颁发者甄别名称的 C(Country)属性的编码使用 PrintableString。Email 属性的编码使用 IA5String。其他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,例如北京	UTF8String
L	城市	证书签发管理系统所在城市,例如北京	UTF8String
O	颁发机构名称	人力资源和社会保障部信息中心	UTF8String
CN	颁发机构别名	人力资源和社会保障部信息中心	UTF8String

6.2.1.5 有效期 Validity

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)。



```

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 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 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 AuthorityKeyIdentifier

本项提供了一种方式,以识别与证书签名私钥相应的公钥。当颁发者由于有多个密钥共存或由于发生变化而具有多个签名密钥时使用该扩展。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。CA 以“自签”(self-signed)证书形式发放其公钥时,可以省略认证机构密钥标识符。此时,主体和认证机构密钥标识符是完全相同的。

本项既可作为证书扩展亦可用作 CRI 扩展。本项标识用来验证在证书或 CRI 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 CertificatePolicies

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 SubjectUniqueID

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”的编码规则为:

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	组织机构代码	ZZ
工作人员证书	2	身份证	SF
设备证书	3	MAC地址	SB
单位证书	4	组织机构代码	ZZ
个人证书	5	身份证	SF

6.3 签名算法域

签名算法域(SignatureAlgorithm)包含数字证书的密码算法,如散列函数 SHA-1、签名算法 RSA,详细内容参见附录 C。在人力资源和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相关算法。

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,Email 属性的编码使用 IA5String,其他属性的编码一律使用 UTF8String。

数字证书中的主体 DN 命名规范为:

- a) C,表示国家。
- b) S,表示省、自治区、直辖市。
- c) L,表示地市。
- d) O,表示单位或机构名称。
- e) OU,表示部门名称。
- f) CN,表示单位或机构别名。

主体命名示例参见附录 A。

7 数字证书格式模板

7.1 根 CA 证书格式模板

人力资源和社会保障部采用统一的根证书格式,各级部门直接使用部里的根证书。

根 CA 证书模板如表 3 所示。

表 3 根 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		如:01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01
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
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	人力资源和社会保障部
		CN	单位或机构别名	人力资源和社会保障部
Validity	有效期限	最长 30 年		30 年
notBefore	有效期起始日期	签发日期		2008 年 8 月 7 日 13:01:52
notAfter	有效期终止日期	起始日期+有效期		2038 年 8 月 7 日 13:01:52
Subject	主体	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	人力资源和社会保障部
		CN	单位或机构别名	人力资源和社会保障部
Subject Public Key Info	公钥	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 2048
Extensions	扩展域			
KeyUsage	密钥用法	非关键扩展项		Certificate Signing, Off-line CRL Signing, CRL Signing (06)
SubjectKeyIdentifier	主体密钥标识符	非关键扩展项		根证书公钥的哈希值
BasicConstraints	基本限制	非关键扩展项		CA=True pathLenConstraint=1
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法		
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 二级 CA 证书格式模板

二级 CA 证书模板如表 4 所示。

表 4 二级 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		sha1RSA
Issuer	颁发者	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	人力资源和社会保障部
		CN	单位或机构别名	人力资源和社会保障部
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		2008 年 9 月 17 日 16:19:35
notAfter	有效期终止日期	起始日期+有效期		2028 年 9 月 17 日 16:19:35
Subject	主体	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××人力资源和社会保障厅(局)信息中心
		CN	单位或机构别名	××人力资源和社会保障厅(局)信息中心
Subject Public Key Info	公钥	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 2 048
Extensions	扩展域			
KeyUsage	密钥用法	非关键扩展项		Certificate Signing, Off-line CRL Signing, CRL Signing (06)
SubjectKeyIdentifier	主体密钥标识符	非关键扩展项		二级 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	非关键扩展项		CA=True pathLenConstraint=0
SignatureAlgorithm	签名算法	对证书基本信息的数字签名的签名算法		
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 机构证书格式模板

机构证书模板如表 5 所示。

表 5 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 6.2.1.2		按照序列号规范定义
Signature	签名算法	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 1 024
Issuer	颁发者	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××人力资源和社会保障厅(局)信息中心
		CN	单位或机构别名	××人力资源和社会保障厅(局)信息中心
Validity	有效期限	最长 5 年,根据应用需求定义,但必须在二级 CA 证书有效期限范围内		5 年
notBefore	有效期起始日期	签发日期		2009 年 9 月 17 日 16:19:35
notAfter	有效期终止日期	起始日期+有效期限		2014 年 9 月 17 日 16:19:35
Subject	主体	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	
		OU	部门名称	
		CN	单位或机构别名	
		Email	电子邮件	user@263.com
Subject Public Key Info	公钥	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 1 024
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		Digital Signature, keyEncipherment 根据证书用途,分签名或加密证书
SubjectUniqueID	实体唯一标识	关键扩展项		OID 为:1.2.156.2316; 值如:2@1ZZ123456789
SubjectKeyIdentifier	主体密钥标识符	关键扩展项		证书中公钥的哈希值
AuthorityKeyIdentifier	颁发机构密钥标识符	关键扩展项		颁发机构公钥的哈希值

表 5 机构证书模板 (续)

证书域名	含义	说明	字段内容(示例)
CRLDistribution-Points	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	
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 工作人员证书格式模板

工作人员证书模板如表 6 所示。

表 6 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	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 1 024
Issuer	颁发者	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××人力资源和社会保障厅(局)信息中心
		CN	用户名	××人力资源和社会保障厅(局)信息中心
Validity	有效期限	最长 5 年,根据应用需求定义,但必须在二级 CA 证书有效期范围内		5 年
notBefore	有效期起始日期	签发日期		2009 年 9 月 17 日 16:19:35
notAfter	有效期终止日期	起始日期+有效期限		2014 年 9 月 17 日 16:19:35

表 6 工作人员证书模板 (续)

证书域名	含义	说明		字段内容(示例)
Subject	主体	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××人力资源和社会保障厅(局)
		OU	部门名称	××人力资源和社会保障厅(局)信息中心
		CN	用户名	张三
		Email	电子邮件	(可选字段)
Subject Public Key Info	公钥	包括加密算法及公钥值		采用 RSA 算法,密钥长度大于或等于 1 024
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		Digital Signature, keyEncipherment; 根据证书用途,分签名或加密证书
SubjectUniqueID	实体唯一标识	关键扩展项		OID: 1.2.156.2316 值如: 1@2SF342222197805053618
Address	地址	非关键扩展项		用户地址
SubjectKeyIdentifier	主体密钥标识符	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	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		
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 设备证书格式模板

设备证书模板如表 7 所示。

表 7 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	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 1 024
Issuer	颁发者	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××人力资源和社会保障厅(局)信息中心
		CN	单位或机构别名	××人力资源和社会保障厅(局)信息中心
Validity	有效期限	最长 10 年,根据应用需求定义,但必须在二级 CA 证书有效期范围内		10 年
notBefore	有效期起始日期	签发日期		2009 年 9 月 17 日 16:19:35
notAfter	有效期终止日期	起始日期+有效期		2019 年 9 月 17 日 16:19:35
Subject	主体	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××人力资源和社会保障厅(局)
		OU	部门名称	××人力资源和社会保障厅(局)信息中心
		CN	单位或机构别名	可为 IP 地址、设备名称、域名等
Subject Public Key Info	公钥	包括加密算法及公钥值		采用 RSA 算法,密钥长度大于或等于 1 024
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		Digital Signature, keyEncipherment; 根据证书用途,分签名或加密证书
SubjectUniqueID	实体唯一标识	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@3SH192.168.2.23
Address	用户地址	非关键扩展项		××人力资源和社会保障厅(局)信息中心
SubjectKeyIdentifier	主体密钥标识符	关键扩展项		本证书公钥的哈希值

表 7 设备证书模板 (续)

证书域名	含义	说明	字段内容(示例)
AuthorityKeyIdentifier	颁发机构密钥标识符	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	
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

7.6 单位证书格式模板

单位证书模板如表 8 所示。

表 8 单位证书模板

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		按序列号规范定义
Signature	签名算法	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 1 024
Issuer	颁发者	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××人力资源和社会保障厅(局)信息中心
		CN	单位或机构别名	××人力资源和社会保障厅(局)信息中心
Validity	有效期限	最长 5 年,根据应用需求定义,但必须在二级 CA 证书有效期范围内		5 年
notBefore	有效期起始日期	签发日期		2009 年 9 月 17 日 16:19:35

表 8 单位证书模板 (续)

证书域名	含义	说明		字段内容(示例)
notAfter	有效期终止日期	起始日期+有效期限		2014 年 9 月 17 日 16:19:35
Subject	主体	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	
		OU	部门名称	
		CN	单位或机构别名	
		Email	电子邮件	
Subject Public Key Info	公钥	包括加密算法及公钥值		采用 RSA 算法, 密钥长度不少于 1 024
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		Digital Signature, keyEncipherment; 根据证书用途, 分签名或加密证书
SubjectUniqueID	实体唯一标识	关键扩展项, 标识一个单位的唯一编码的值		<b>OID:</b> 1.2.156.2316 值如: 2@4ZZ123456789
Address	单位地址	非关键扩展项		
SubjectKeyIdentifier	主体密钥标识符	关键扩展项		本证书公钥的哈希值
AuthorityKeyIdentifier	颁发机构密钥标识符	关键扩展项		颁发机构公钥的哈希值
CRLDistribution-Points	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.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		
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

7.7 个人证书格式模板

个人证书模板如表 9 所示。

表 9 个人证书模板

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	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 1 024
Issuer	颁发者	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××人力资源和社会保障厅(局)信息中心
		CN	用户名	××人力资源和社会保障厅(局)信息中心
Validity	有效期限	最长 5 年根据应用需求定义,但必须在二级 CA 证书有效期限范围内		5 年
notBefore	有效期起始日期	签发日期		2009 年 9 月 17 日 16:19:35
notAfter	有效期终止日期	起始日期+有效期限		2014 年 9 月 17 日 16:19:35
Subject	主体	C	国家	CN
		S	省份	××省
		L	城市	××市
		O	单位或机构名称	××单位
		OU	部门名称	部门
		CN	用户名	
		Email	电子邮件	(可选字段)
Subject Public Key Info	公钥	包括加密算法及公钥值		采用 RSA 算法,密钥长度不少于 1 024
Extensions	扩展域			
KeyUsage	密钥用法	关键扩展项		Digital Signature, keyEncipherment; 根据证书用途,分签名或加密证书
SubjectUniqueID	实体唯一标识	关键扩展项,标识一个个人的唯一编码的值		OID: 1. 2. 156. 2316 值如: 1@2SF342222197805053618
Address	单位地址	非关键扩展项		
SubjectKeyIdentifier	主体密钥标识符	关键扩展项		本证书公钥的哈希值

表 9 个人证书模板 (续)

证书域名	含义	说明	字段内容(示例)
AuthorityKeyIdentifier	颁发机构密钥标识符	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.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	
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 颁发者

颁发者的 X.500 目录示例如下:



CN=人力资源和社会保障部信息中心 //通用名  
OU=人力资源和社会保障部信息中心 //部门  
O=人力资源和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

8.1.3 生效日期

颁发 CRL 之日起生效。

8.1.4 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。

8.1.5 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 Signature-Algorithm 项的算法标识符相同。

应使用国家密码管理主管部门审核批准的相关算法,如 SHA1WithRSAEncryption 算法。

8.1.6 撤销日期

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。

8.1.7 扩展项

颁发机构密钥标识符(AuthorityKeyIdentifier)。

8.1.8 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。

8.2 CRL 格式模板

CRL 格式模板如表 10 所示。

表 10 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

表 10 CRL 格式模板表 (续)

证书域名	含义	说明
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
Revocationdate	时间	撤销时间
extnValue	扩展项	撤销原因代码
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  
(资料性附录)  
主体命名规范

以下所列示例仅供参考。

A.1 机构证书

人力资源和社会保障部的某一单位,其机构证书的主体 DN 为:

C=CN  
S=北京市  
L=北京市  
O=人力资源和社会保障部  
OU=人力资源和社会保障部某某单位  
CN=单位名称

A.2 工作人员证书

人力资源和社会保障部的某一单位的工作人员用户,其证书的主体 DN 为:

C=CN  
S=北京市  
L=北京市  
O=人力资源和社会保障部  
OU=人力资源和社会保障部某某单位  
CN=用户姓名

A.3 设备证书

人力资源和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=人力资源和社会保障部  
OU=人力资源和社会保障部某某单位  
CN=设备名称(MAC 地址或域名)

A.4 单位证书

单位证书的主体 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=北京某某单位

#### A.5 个人证书

个人证书的主体 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

附 录 B  
(资料性附录)  
数字证书编码示例

- a) 以工作人员证书为例,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: sha1RSA
  - 颁发者 DN: C=CN; S=北京; L=北京; O=人力资源和社会保障部信息中心; CN=人力资源和社会保障部信息中心
  - 主体 DN: C=CN; S=××省; L=××市; O=××人力资源和社会保障局; OU=××部门; CN=张三
  - 有效期: 从 2010 年 3 月 18 日 9:18:44 到 2015 年 3 月 18 日 9:18:44
  - 主体公钥信息中包含 1 024 比特的 RSA 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) 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	9	OBJECT IDENTIFIER: sha1withRSAEncryption [1.2.840.113549.1.1.5]
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 : '人力资源和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 : '人力资源和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 : '××省'
230| 15| SET ;
232| 13| SEQUENCE ;
234| 3| OBJECT IDENTIFIER : localityName [2.5.4.7]
239| 6| UTF8String : '××市'
247| 29| SET ;
249| 27| SEQUENCE ;
251| 3| OBJECT IDENTIFIER : organizationName [2.5.4.10]
256| 20| UTF8String : '××人力资源和社会保障局'
306| 29| SET ;
308| 27| SEQUENCE ;
310| 3| OBJECT IDENTIFIER : organizationalUnitName[2.5.4.11]
315| 20| UTF8String : '××部门'
337| 29| SET ;
339| 27| SEQUENCE ;
341| 3| OBJECT IDENTIFIER : commonName [2.5.4.3]
346| 20| UTF8String : '张三'
368| 159| SEQUENCE ;
371| 13| SEQUENCE ;
373| 9| OBJECT IDENTIFIER : rsaEncryption[1.2.840.113549.1.1.1]
384| 0| NULL ;
386| 141| BIT STRING UnusedBits:0 ;
390| 137| SEQUENCE ;
393| 129| INTEGER ;

```

0E8C3CE9E6CA1C75A71E3C6B4A908A6A8951AE224E5F3D15  
 067A6E35A1A00D9DC2755B3309B3794C03E80766E29CEC38D  
 B8B5AB2A8AAE1E095586E9645C100A16B8820345F0F84742C  
 F3878CBFD94FE6DCA7A305F47A112C91E3F95B0901CC1B7A2  
 17680836F4A244599046C66F691034E142BB1C7860BF78698  
 01B2B4D6A0191

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 : 'Co'
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 :
		3140325346373837363837363836383637383637383637
651	13	SEQUENCE :
653	9	OBJECT IDENTIFIER : sha1withRSAEncryption[1.2.840.113549.1.1.5]
664	0	NULL :
666	129	BIT STRING UnusedBits:0 :

0FE66EAF169EBA59353215E18DC0A12AF6531DD6F246CD054E85FA9B4F7C  
 1165187B5B8597D03F163C0F315B11DF8E2E28C42525A1698765A0A23CFF  
 55559005E4279C9FAE181110A33A337DC274E8DEB282B93A28EB8BA82A00  
 75192324E0E22F637E5E15411280096FEBB405BF1D047B4500A85D94463B  
 6853E10BE7449EC6

附 录 C  
(资料性附录)  
算 法 举 例

a) 散列函数

SHA-1 散列函数由一个任意长度的字符串产生一个 160 bit 的哈希值。

b) 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,签名算法与散列函数一起被使用。

本项包含建立在 RSA 非对称加密算法基础上的签名算法。签名算法把 RSA 与 SHA 1 散列函数结合起来。

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

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {
    iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
    pkcs-1(1) 5 }
```

c) 公开密钥算法

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

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

OID rsaEncryption 标识了 RSA 公开密钥。

```
pkcs-1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
    rsadsi(113549) pkcs(1) 1 }
rsaEncryption OBJECT IDENTIFIER ::= { pkcs-1 1 }
```

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

RSA 公开密钥的编码采用 ASN.1 的 RSAPublicKey 类型。

```
RSAPublicKey ::= SEQUENCE {
    modulus          INTEGER, -- n
    publicExponent    INTEGER -- e }
```

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

该 OID 是用于 RSA 签名密钥和 RSA 加密密钥的公钥证书。密钥的应用目的在密钥用法 (key usage) 项中指明。



中华人民共和国劳动和劳动安全  
行 业 标 准  
人力资源和社会保障电子认证体系  
第 3 部分:证书及证书撤销列表格式规范

LD/T 30.3—2009

\*

中国标准出版社出版发行  
北京复兴门外三里河北街 16 号  
邮政编码:100045

网址 [www.spc.net.cn](http://www.spc.net.cn)

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷

各地新华书店经销

\*

开本 880×1230 1/16 印张 2 字数 50 千字

2010 年 2 月第一版 2010 年 2 月第一次印刷

\*

书号:155066·2-20298

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68533533



LD/T 30.3-2009

# www.bzxz.net

免费标准下载网