ICS 35.040
L 80
备案号：27110—2010

LD

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：证书及证书撤消列表格式规范

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

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：证书及证书撤消列表格式规范；

——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消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消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:证书及证书撤消列表格式规范

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消列表的基本结构,描述了数字证书中的各数据项内容,制定了证书及证书撤消列表格式模板。

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消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。