ICS 35.040
L 80
备案号：27109—2010

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 30.2—2009

人力资源和社会保障电子认证体系 第2部分：电子认证系统技术规范

Human resources and social security electronic authentication system—Part 2：Technology specification of electronic authentication system

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 2 部分。

本部分描述了人力资源和社会保障电子认证系统的体系架构、系统构成和系统功能等，是指导人力资源和社会保障部门建设电子认证系统的技术性规范和基本要求。

本部分重点引用了《证书认证系统密码及其相关安全技术规范》，并在此基础上，扩展了证书管理流程、省级系统建设拓扑图等相关内容，从满足人力资源社会保障业务需求的角度，对建设本行业的电子认证系统提出规范和要求。

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2部分:电子认证系统技术规范

1 范围

LD/T 30的本部分描述了人力资源和社会保障电子认证系统体系架构、系统构成,定义了电子认证系统各单元的结构和基本功能,规定了电子认证系统的基础安全防护措施,规范了电子认证业务流程及相关协议。

本部分适用于指导人力资源和社会保障部门建设基于PKI技术的电子认证系统,有助于各级人力资源和社会保障部门建立适用于人力资源和社会保障业务系统发展的电子认证体系。

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 19771—2005 信息技术 安全技术 公钥基础设施PKI组件最小互操作规范

GM 0001—2005 证书认证系统密码及其相关安全技术规范

信息技术 安全技术 密码术语(国家密码管理局)

数字证书认证系统密码协议规范(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。