ICS 35.040
L 80
备案号：27111—2010

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 30.4—2009

人力资源和社会保障电子认证体系 第4部分：证书应用管理规范

Human resources and social security electronic authentication system—Part 4：Management specification of digital certificate application

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 4 部分。

本部分描述了证书应用领域和证书应用技术体系，规范了证书应用接口规范和证书应用接口技术要求，给出了典型证书应用流程和应用场景。

本部分重点引用了国家密码局《公钥密码基础设施应用技术体系》相关规范，并在此基础上，扩展了典型证书应用流程等相关内容，给出了几类常见的人力资源社会保障业务系统的证书应用场景，从满足人力资源社会保障业务需求的角度，对本行业应用系统使用数字证书的接口和流程提出规范和要求。

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4部分:证书应用管理规范

1 范围

LD/T 30的本部分规定了数字证书的应用领域,制定了人力资源和社会保障数字证书应用的总体技术框架,规范了人力资源和社会保障应用系统在实现身份认证、数字签名及验签、加密与解密等安全功能时,所采取的应用接口和证书应用处理流程,给出了可供参考的典型应用场景。

本部分适用于指导人力资源和社会保障应用系统实现基于数字证书的安全功能,有助于各级人力资源和社会保障部门采用统一的基于数字证书应用的开发接口。

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 20518—2006 信息安全技术 公钥基础设施 数字证书格式

LD/T 30.5 人力资源和社会保障电子认证体系 第5部分:证书载体规范

公钥密码基础设施应用技术体系 密码设备应用接口规范(国家密码管理局)

公钥密码基础设施应用技术体系 通用密码服务接口规范(国家密码管理局)

公钥密码基础设施应用技术体系 密码设备管理规范(国家密码管理局)

智能IC卡及智能密码钥匙密码应用接口规范(国家密码管理局)

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

非对称密码算法 asymmetric cryptographic algorithm

使用两种相关变换和非对称密钥对的密码技术,一种是由公开密钥定义的公开变换,另一种是由私有密钥定义的私有变换。两种变换具有以下特性:即使给定公开变换,也不可能通过计算得出私有变换。