ICS 35.040
L 80
备案号：27112—2010

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 30.5—2009

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

Human resources and social security electronic authentication system—Part 5：Specification of digital certificate storage medium

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 5 部分。

本部分主要描述了证书载体的技术指标，包括硬件规范和软件规范，并规定了证书载体的相关接口和外观规范。

本部分重点引用了《智能 IC 卡及智能密码钥匙密码应用接口规范》，并在此基础上，扩展了证书载体基本技术要求、证书载体管理要求、软件的安装卸载以及证书载体外观设计要求等相关内容，从满足人力资源社会保障业务需求的角度，对本行业发放的证书载体的软硬件和外观提出规范和要求。

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、李冰松、耿建军、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5部分:证书载体规范

1 范围

LD/T 30的本部分描述了在人力资源和社会保障系统中使用的证书载体的各项要求,包括硬件要求、软件要求、管理要求、安全机制以及相关接口标准等内容。

本部分适用于人力资源社会保障证书载体的设计、应用开发、使用和检测。

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。

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)

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)

3 术语和定义

以下术语和定义适用于本规范。

3.1

证书载体 certificate entity

用于存储密钥和数字证书并具有密码运算功能的载体,包括智能密码钥匙(USBKey)和IC卡等。

3.2

容器 container

特指密钥容器,是一个用于存放非对称密钥对和证书的逻辑对象。每个用户对应一个密钥容器,与用户相关的非对称密钥对和证书存放于该密钥容器,每个容器中最多可以存放一对加密密钥对和一对签名密钥对以及一张加密证书和一张签名证书。

3.3

证书撤消列表 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。

3.4

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。

3.5

加密 encrypt

通过密码算法对数据进行变换来产生密文,以便隐藏数据的信息内容。