



# 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 ..... I

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 电子认证体系的布局与结构 ..... 3

    5.1 总体布局 ..... 3

    5.2 电子认证系统的构成 ..... 4

6 证书认证设施 ..... 4

    6.1 证书签发管理系统 ..... 4

    6.2 证书注册管理系统 ..... 6

    6.3 证书查验服务系统 ..... 7

7 密码管理设施 ..... 8

    7.1 密钥管理系统 ..... 8

    7.2 密码服务系统 ..... 11

8 基础安全防护设施 ..... 12

    8.1 防病毒系统 ..... 12

    8.2 防火墙 ..... 12

    8.3 漏洞扫描 ..... 12

    8.4 入侵检测 ..... 12

9 业务流程与协议 ..... 12

    9.1 证书管理流程 ..... 12

    9.2 证书验证协议 ..... 16

附录 A (资料性附录) 省级电子认证系统(模式一)网络结构示意图 ..... 18

附录 B (资料性附录) 省级电子认证系统(模式二)网络结构示意图 ..... 19

## 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。

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

私有密钥 private key

私钥

在公钥密码体制中,用户密钥对中仅为该用户持有的密钥。

3.7

公开密钥 public key

公钥

在公钥密码体制中,用户密钥对中公布给其他用户的密钥。

3.8

证书验证 certificate validation

确定证书在指定的时间内是否有效的过程。证书验证包括有效期验证、签名验证以及证书状态的检验。

3.9

证书认证路径 certification path

在目录信息树中对象证书的一个有序的序列。路径的初始节点是最初待验证对象的公钥,可以通过路径获得最终的顶点的公钥。

3.10

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。

3.11

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。

3.12

公开密钥基础设施 public key infrastructure

PKI

用公钥密码技术建立的普遍适用的基础设施,为用户提供证书管理和密钥管理等安全服务。

## 4 缩略语

下列缩略语适用于本部分:

CA	证书认证机构(Certification Authority)
CRL	证书撤销列表(Certificate Revocation List)
dCRL	增量证书撤销列表(delta-CRL)
KMC	密钥管理中心(Key Management Center)
LDAP	轻量级目录访问协议(Lightweight Directory Access Protocol)
RA	证书注册机构(Registration Authority)

## 5 电子认证体系的布局与结构

### 5.1 总体布局

人力资源和社会保障电子认证体系由部、省、市三级电子认证系统组成,采用部、省两级电子认证模式(见图 1)。

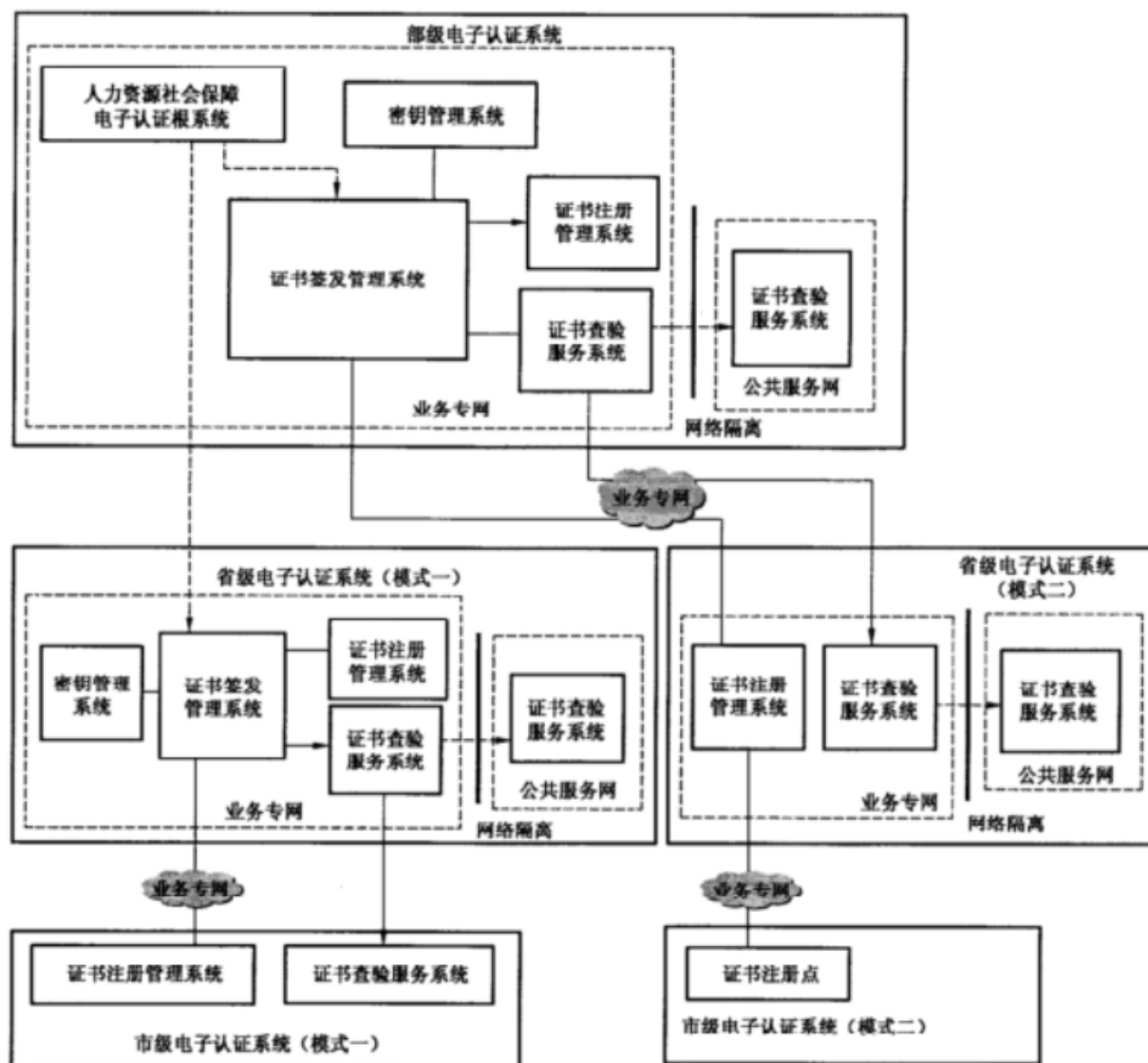


图 1 人力资源和社会保障电子认证体系总体布局

- a) 人力资源和社会保障部建立人力资源和社会保障电子认证根系统(一级 CA),作为人力资源和社会保障网络信任体系的信任源点;建立部级电子认证节点(二级 CA),包括:密钥管理系统、证书签发管理系统、证书注册管理系统和证书查验服务系统等,为部本级和全国性应用系统提供电子认证服务。
- b) 省级电子认证系统可选择以下两种建设模式:  
 模式一,省级电子认证系统作为省级电子认证节点(二级 CA),以人力资源和社会保障电子认证根系统为依托,直接建立密钥管理系统、证书签发管理系统、证书注册管理系统和证书查验服务系统。此模式为一个相对独立运行的电子认证系统,日常证书业务不与部级电子认证系

统实时通信,但需由部级电子认证系统为其签发二级 CA 证书。

模式二:省级电子认证系统作为部级电子认证节点的延伸,建立证书注册管理系统和证书查验服务系统,直接接入部级电子认证系统,所有数字证书由部级电子认证系统统一签发。

- c) 市级电子认证系统作为省级电子认证系统的延伸,根据省级所选建设模式,可选择以下两种建设模式:

模式一:在省级建设二级 CA 系统的基础上,建设证书注册管理系统、证书查验服务系统和证书注册点等。

模式二:在省级建设二级 CA 系统或 RA 系统的基础上,建设证书注册点。

人力资源和社会保障电子认证体系总体布局如图 1 所示。

5.2 电子认证系统的构成

人力资源和社会保障电子认证系统主要包括证书认证设施和密码管理设施,以及相配套的基础安全防护设施。其中,证书认证设施包括证书签发管理系统、证书注册管理系统和证书查验服务系统;密码管理设施包括密钥管理系统和密码服务系统;基础安全防护设施包括防病毒、漏洞扫描、防火墙、入侵检测等系统。

电子认证系统的构成如图 2 所示。

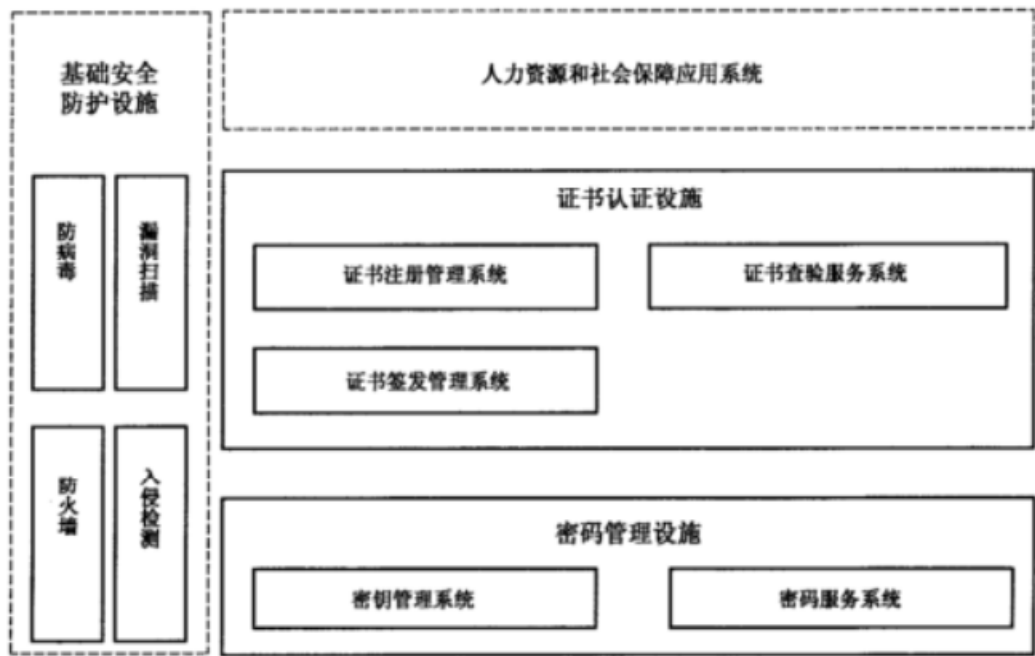


图 2 电子认证系统构成

6 证书认证设施

6.1 证书签发管理系统

6.1.1 系统描述

证书签发管理系统是对生命周期内的数字证书进行全过程管理的安全系统,采用双证书(签名证书和加密证书)机制。证书签发管理系统提供数字证书生成、发布、撤销和存档等服务,接收来自证书注册管理系统的证书请求,向密钥管理系统请求加密密钥对,为用户签发数字证书和证书撤销列表,并将证

书/证书撤销列表发布到证书查验服务系统。

### 6.1.2 系统结构

证书签发管理系统由证书业务服务、证书管理服务、证书签发服务、密码服务等模块组成。

证书签发管理系统结构如图 3 所示。

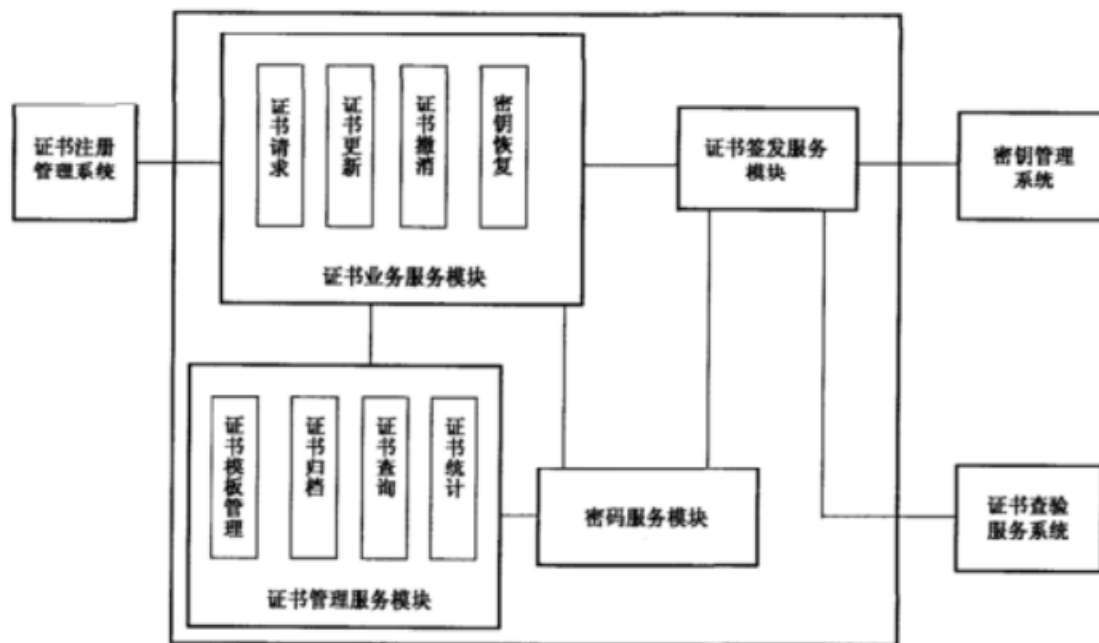


图 3 证书签发管理系统结构

#### a) 证书业务服务模块

证书业务服务模块提供处理证书请求、证书更新、证书撤销、密钥恢复等功能。在处理完相关请求后，证书业务服务模块将证书或 CRL 的签发工作转交给证书签发服务模块处理。

#### b) 证书签发服务模块

证书签发服务模块根据证书业务服务模块的签发请求，向密钥管理系统申请密钥，获取密钥后，调用密码服务模块签发数字证书。对于 CRL 签发请求，直接由签发服务模块调用密码服务模块签发 CRL。证书或 CRL 签发完成后，签发服务模块将证书和 CRL 发布到证书查验服务系统中。

#### c) 证书管理服务模块

证书管理服务模块提供证书模板管理、证书归档、证书查询、证书统计等功能。

#### d) 密码服务模块

密码服务模块负责为证书签发管理系统的各模块提供密码支持，以及负责与其他系统通信过程中的密码运算，主要完成签名和验证工作，签名密钥保存在密码设备中。在上述工作中，必须保证所使用的密钥不能以明文形式被读出密码设备。

### 6.1.3 系统功能

证书签发管理系统是电子认证系统的核心，不仅为整个证书认证系统提供签发证书/证书撤销列表的服务，还承担整个电子认证系统中主要的安全管理工作。

证书签发管理系统的主要功能如下：

#### a) 证书生成与签发：从数据库中读取用户信息，根据拟签发的证书类型向密钥管理系统申请加密



密钥对,生成用户的签名证书和加密证书,将签发完成的证书发布到证书查验服务系统和数据库中。根据系统的配置和管理策略,不同种类或用途的证书可以采用不同的签名密钥。

- b) 证书更新:系统应提供 CA 证书及用户证书的更新功能。
- c) 证书撤销列表生成与签发:接收撤销信息,签发证书撤销列表,将签发后的撤销列表发布到证书查验服务系统和数据库中。
- d) 安全审计:负责对证书签发管理系统的管理人员、操作人员的操作日志进行查询、统计以及报表生成等。
- e) 安全管理:对证书签发管理系统的登录进行安全访问控制,对数据库进行管理和备份;设置管理员、操作员,并为这些人员申请和下载数字证书;配置不同的密码设备;配置不同的证书模板。
- f) 证书/证书撤销列表的存储。
- g) 证书签发管理系统应具有并行处理的能力。

6.2 证书注册管理系统

6.2.1 系统描述

证书注册管理系统负责用户的证书申请、身份审核和证书下载。在数字证书申请过程中,证书注册管理系统的核心职责是将证书请求安全可信的提交到证书签发管理系统,等待其签发证书,签发完成后,将证书下载到证书载体中。

6.2.2 系统结构

证书注册管理由用户信息注册、业务处理、数据管理服务、操作员管理、密码服务等模块组成。证书注册管理系统结构如图 4 所示。

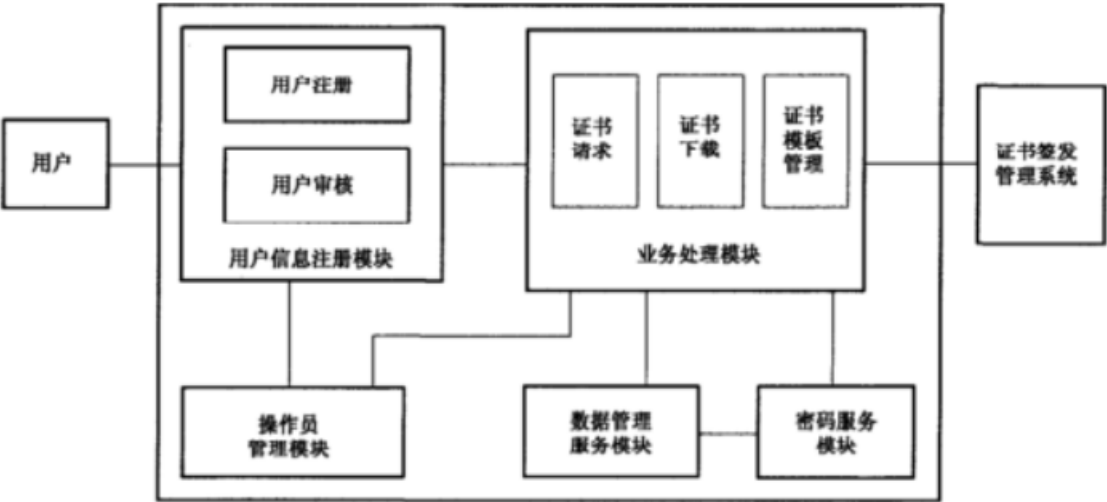


图 4 证书注册管理系统结构

- a) 用户信息注册模块  
用户信息注册模块提供用户注册和用户审核等功能。
- b) 业务处理模块  
业务处理模块是证书注册管理系统的核心服务模块,提供证书请求、证书下载和证书模板管

理等功能。证书请求是将经过身份审核的证书业务请求通过安全通道传输给证书签发管理系统。证书下载是将证书签发管理系统签发完成的证书通过安全通道下载到证书注册管理系统,并将证书下载到证书载体中;证书模板管理是定制证书类型和证书格式的管理工具。

c) 数据管理服务模块

数据管理服务模块提供完善的数据库管理服务,用于保存和管理用户信息、证书信息、操作员信息等。

d) 操作员管理模块

操作员管理模块负责证书注册管理系统的操作员注册及其权限设置等管理工作。

e) 密码服务模块

密码服务模块负责为证书注册管理系统的各模块提供密码支持,以及负责与其他系统通信过程中的密码运算,主要完成签名和验证工作,签名密钥保存在密码设备中。在进行上述工作中,必须保证所使用的密钥不能以明文形式被读出密码设备。

### 6.2.3 系统功能

证书注册管理系统负责用户证书/证书撤销列表的申请、审核以及证书的制作,其主要功能如下:

- a) 用户信息的录入:录入用户的申请信息,用户申请信息包括签发证书所需要的信息,还包括用于验证用户身份的信息,这些信息存放在证书注册管理系统的数据库中。证书注册管理系统应能够批量接收从外部系统生成的、以电子文档方式存储的用户信息。
- b) 用户信息的审核:提取用户的申请信息,审核用户的真实身份,当审核通过后,将证书签发所需要的信息提交给证书签发管理系统。
- c) 用户证书下载:证书注册管理系统提供证书下载功能,当证书签发管理系统为用户签发证书后,证书注册管理系统能够下载用户证书,并将用户证书写入指定的证书载体中,然后分发给用户。
- d) 安全审计:负责对证书注册管理系统的管理人员、操作人员的操作日志进行查询、统计以及报表生成等。
- e) 安全管理:对证书注册管理系统的登录进行安全访问控制,并对用户信息数据库进行管理和备份。
- f) 多级审核:证书注册管理系统可根据需要采用分级部署的模式,对不同类型的证书,可由不同级别的证书注册管理系统进行审核。证书注册管理系统应能够根据需求支持多级注册管理系统的建立和多级审核模式。
- g) 证书注册管理系统应具有并行处理的能力。

## 6.3 证书查验服务系统

### 6.3.1 系统描述

证书查验服务系统负责数字证书\证书撤销列表的存储和发布,为用户和应用系统提供证书状态查询服务,用户或应用系统利用数字证书中标识的 CRL 地址下载 CRL 文件,从而检验证书的有效性。

### 6.3.2 系统结构

证书查验服务系统应采用主从目录结构以保证证书查验服务系统的安全。证书签发管理系统签发完成的数据直接写入主目录服务器,然后由目录服务器的主从映射功能自动映射到从目录服务器中,从目录服务器可以采用分布式的方式进行设置,以提高系统的效率。主、从目录服务器通常配置在不同等

级的安全区域。用户只能访问从目录服务器。

证书查验服务系统结构如图 5 所示。

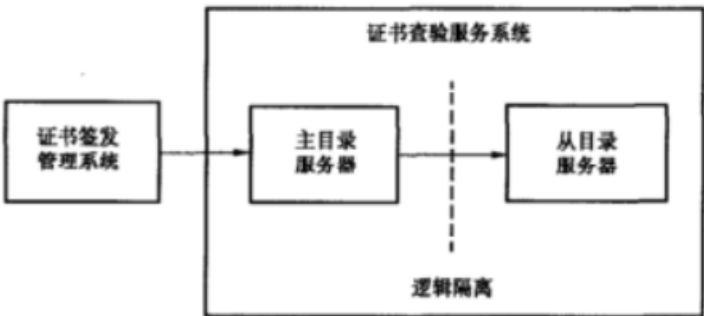


图 5 证书查验服务系统结构

6.3.3 系统功能

证书查验服务系统面向用户和应用系统提供证书下载及 CRL 下载功能。

- a) 证书存储。
- b) 证书撤销列表存储。
- c) 证书和 CRL 发布。
- d) 证书状态查询：用户或应用系统使用数字证书中签发的 CRL 地址，根据需要到目录服务器下载 CRL 列表，查询证书状态，验证证书有效性。
- e) 目录访问控制：证书查验服务系统需要对目录的访问进行控制，用户和应用系统可根据证书中签发的目录服务器地址及 DN 访问从目录服务器，可下载对应的数字证书和 CRL。

7 密码管理设施

7.1 密钥管理系统

7.1.1 系统描述

密钥管理系统基于公开密钥技术，负责为证书认证设施提供密钥服务，主要功能包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档和密钥恢复等。

7.1.2 系统结构

密钥管理系统由密钥生成、密钥管理、密钥库管理、认证管理、密码服务、密钥恢复和安全审计等模块组成。

密钥管理系统结构如图 6 所示。

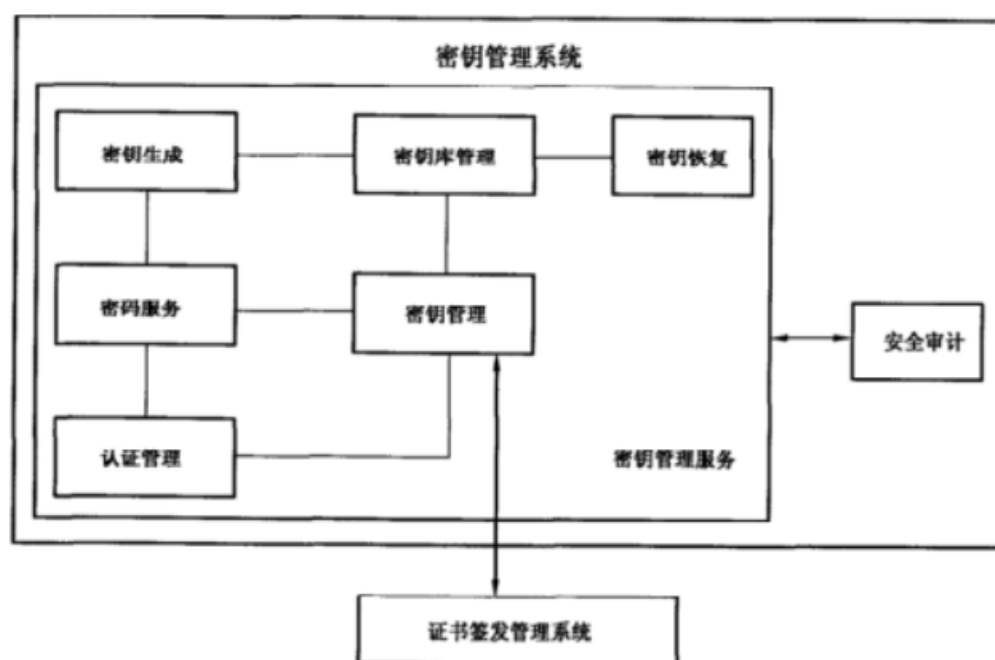


图6 密钥管理系统结构

## a) 密钥生成模块

密钥生成模块应提供以下主要功能：

- 1) 生成非对称密钥对,并将其保存在备用库中;当备用库中密钥数量不足时,自动补充备用密钥。
- 2) 生成对称密钥。
- 3) 生成随机数。

## b) 密钥管理模块

密钥管理模块应提供以下主要功能：

- 1) 接收、审核证书签发管理系统的密钥申请。
- 2) 调用备用密钥库中的密钥对。
- 3) 向证书签发管理系统发送密钥对。
- 4) 对调用的备用密钥库中的密钥对进行处理,并将其转移到在用密钥库。
- 5) 对在用密钥库中的密钥进行定期检查,将超过有效期的或被撤消的密钥转移到历史密钥库。
- 6) 对历史密钥库中的密钥进行处理,将超过规定保留期的密钥转移到规定载体。
- 7) 接收与审查关于恢复密钥的申请,依据安全策略进行处理。
- 8) 对进入本系统的有关操作及操作人员进行身份与权限的认证。

## c) 密钥库管理模块

密钥库管理模块负责密钥的存储管理,按照其存储的密钥的状态,密钥库分为备用库、在用库和历史库等三种类型,密钥库中的密钥数据必须加密存放。

## 1) 备用库

备用库存放待使用的密钥对。密钥生成模块预生成一批密钥对,存放于备用库中;证书签发管理系统需要时可及时调出,将其提供给证书签发管理系统后转入在用库。

备用密钥库应保持一定数量的待用密钥对,存放的密钥数量依系统的用户数量而定,若少

于设定的最低数量时应自动补足到规定数量。

2) 在用库

在用库存放当前使用的密钥对。在用库中的密钥记录包含用户证书的序列号、ID 号和有效时间等标志。

3) 历史库

历史库存放过期或已被撤销的密钥对。历史库中的密钥记录包含用户证书的序列号、ID 号、有效时间和作废时间等标志。

d) 认证管理模块

认证管理模块负责对进入本系统的有关操作及操作人员进行身份与权限的认证。

e) 密码服务模块

密码服务模块负责为密钥管理系统的各模块提供密码支持,以及负责与其他系统通信过程中的密码运算,主要完成密钥生成、签名和验证工作,签名密钥保存在密码设备中。在上述工作中,必须保证所使用的密钥不能以明文形式被读出密码设备。

f) 密钥恢复模块

密钥恢复模块负责为用户恢复加密私钥,被恢复的私钥必须安全地下载到证书载体。

g) 安全审计模块

密钥管理系统设置日志审计模块,包括全程审计和事件审计。审计员定时调出审计记录,制作统计分析表。审计员可以查询分析但不能修改日志审计数据。

审计员可以处理但不能修改日志审计数据。

日志记录的主要内容包括:

- 1) 操作员姓名;
- 2) 操作项目;
- 3) 操作起始时间;
- 4) 操作终止时间;
- 5) 证书序列号;
- 6) 操作结果。

日志管理的主要内容包括:

- 1) 日志参数设置,设置日志保存的最大规模和日志备份的目录;
- 2) 日志查询,日志查询主要是查询操作员、认证机构操作事件信息;
- 3) 日志备份,当日志保存到日志参数设置的最大规模时,将保存的日志备份;
- 4) 日志处理,对日志记录的正常业务流量和各类事件进行分类整理;
- 5) 证据管理,对证据数据进行审计、统计和记录。

### 7.1.3 系统功能

密钥管理系统提供了对生命周期内的加密证书密钥对进行全过程管理的功能,包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档、密钥恢复以及安全管理等。

- a) 密钥生成:根据证书签发管理系统的请求为用户生成非对称密钥对,该密钥对由密钥管理系统的硬件密码设备生成。
- b) 密钥存储:密钥管理系统生成的非对称密钥对,经硬件密码设备加密后存储在密钥数据库中。
- c) 密钥分发:密钥管理系统生成的非对称密钥对通过证书签发管理系统和证书注册管理系统分发到证书载体中。

- d) 密钥备份:密钥管理系统采用热备份、冷备份和异地备份等措施实现密钥备份。
- e) 密钥更新:当证书到期或用户需要时,密钥管理系统根据证书签发管理系统请求为用户生成新的非对称密钥对。
- f) 密钥撤消:当证书到期、用户需要或管理机构认为必要时,密钥管理系统根据证书签发管理系统请求撤消用户当前使用的密钥。
- g) 密钥归档:密钥管理系统为到期或撤消的密钥提供安全长期的存储。
- h) 密钥恢复:密钥管理系统可为用户提供密钥恢复服务。密钥恢复需按管理策略进行审批,一般用户只限于恢复自身密钥。

## 7.2 密码服务系统

电子认证系统使用对称密码算法、非对称密码算法和数据摘要算法三类算法实现有关密码服务各项功能,这些功能的实现依赖于密码服务系统。

### 7.2.1 密码设备

密码服务系统应采用国家密码主管部门批准使用的密码设备,包括:

- a) 应用类密码设备:在电子认证系统中提供签名/验证、数据加密/解密、数据摘要、数字信封、密钥生成和管理等密码服务。
- b) 通信类密码设备:用于密钥管理系统与证书签发管理系统之间、证书签发管理系统与证书注册管理系统间的传输加密。
- c) 证书载体:用于存储密钥和数字证书并具有密码运算功能的载体,如 USBKey。

### 7.2.2 密码算法

电子认证系统使用的密码算法要求如下:

- a) 对称密钥密码算法:采用国家密码主管部门批准使用的对称密码算法。
- b) 非对称密钥密码算法:采用国家密码主管部门批准使用的非对称密钥密码算法。
- c) 数据摘要算法:采用国家密码主管部门批准使用的数据摘要算法。

### 7.2.3 密码设备的功能

密码设备必须具备如下基本功能:

- a) 随机数生成。
- b) 非对称密钥的产生。
- c) 对称密钥的产生。
- d) 非对称密钥密码算法的加解密运算。
- e) 对称密钥密码算法的加解密运算。
- f) 数据摘要运算。
- g) 密钥的存储。
- h) 密钥的安全备份和安全导入导出。
- i) 多密码设备并行工作时,密钥的安全同步。

### 7.2.4 密码设备的安全要求

密码设备应满足下列要求:

- a) 接口安全,不执行规定命令以外的任何命令和操作。

- b) 协议安全,所有命令的任意组合,不能得到密钥的明文。
- c) 密钥安全,密钥不以明文的形式出现在密码设备之外。
- d) 物理安全,密码设备应具有物理防护措施,任何情况下的拆卸均应立即销毁设备内保存的密钥。

#### 7.2.5 密码服务接口

密码服务接口为调用密码服务提供统一的基本接口函数,密码设备的其他管理函数可自行定义。密码设备的基本接口函数主要包括:密钥对生成、非对称加解密函数、对称加解密函数、数据摘要函数等,有关函数定义以及功能说明可参见国家密码管理局相关标准。

### 8 基础安全防护设施

基础安全防护设施是保证电子认证系统安全可靠运行的必要条件,基础安全防护设施主要包括防病毒系统、防火墙、漏洞扫描、入侵检测等安全防护设备,具体部署方式参见附录。

#### 8.1 防病毒系统

应根据不同的操作系统类型,配备相应的防病毒系统,通过这些防病毒系统所具有的实时检测病毒和杀毒功能,达到防范病毒侵害的目的。

#### 8.2 防火墙

应配备防火墙进行网络安全域划分,实现对各安全域之间的访问控制和安全防护。工作模式设置为路由模式。关闭所有系统不需要的端口。

#### 8.3 漏洞扫描

应配备漏洞扫描工具定期对关键服务器、网络设备、操作系统、数据库和应用等进行不同层次的漏洞扫描,及时发现系统中的潜在漏洞、后门、风险,然后根据扫描工具的提示对这些安全问题进行处理。

#### 8.4 入侵检测

应配备入侵检测系统,监测计算机网络或计算机系统的运行,从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象,实时分析进出网络数据流,对网络违规事件进行跟踪、实时报警、阻断连接并记录日志,对入侵行为进行检测和控制,一旦发现攻击能够发出报警并采取相应的措施。入侵检测设备应部署在核心交换机上,以保证对外来所有信息包的检测。入侵检测管理控制台与入侵检测探测设备应采取直连的方式,保证其独立的管理及检测。入侵检测对信息包的检测与分析应设置为高警戒级别。

### 9 业务流程与协议

#### 9.1 证书管理流程

证书管理流程包括证书申请、证书更新、证书撤消、用户密钥恢复等。

##### 9.1.1 证书申请

证书申请流程如图7所示。

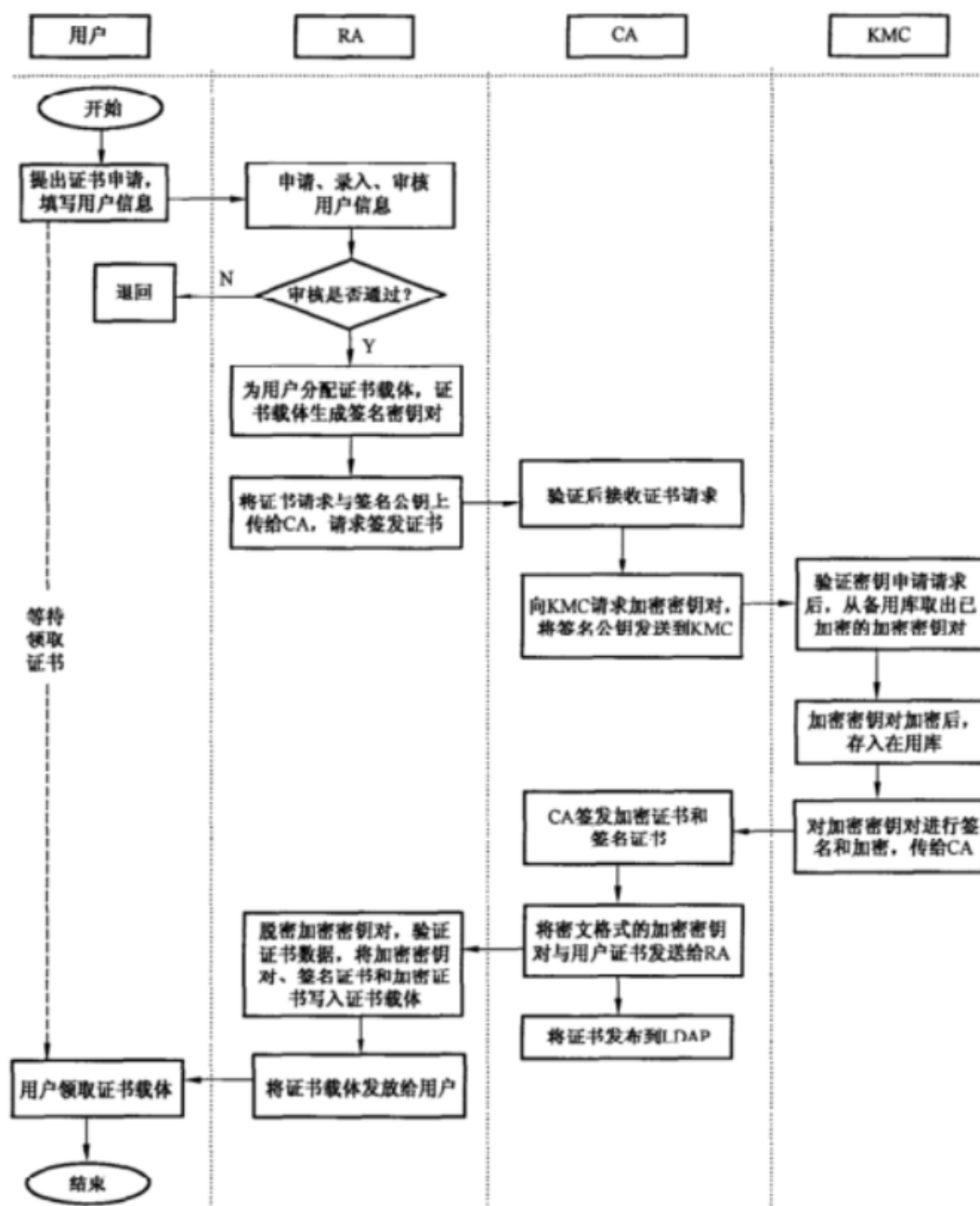


图7 证书申请流程示意图

证书申请流程可分成以下几个子流程：

a) 证书申请

用户要获得证书首先必须向证书注册管理系统提交申请,将自己的身份信息提交给 RA,即填写证书申请表。

b) 证书申请的审核

为用户签发证书之前,必须对用户的真实身份进行确认,要求用户提交的注册申请信息与其真实身份信息相符。身份确认可以采用面对面的方式,即要求用户或其代理者携带证明资料到证书注册管理系统进行验证。

审核通过后,在用户证书载体中生成签名密钥对,同时将签名公钥及用户信息通过 RA 系统提交到证书签发管理系统,由证书签发管理系统签发用户证书。



c) 签发证书

CA 签发管理系统得到用户签发证书请求后,向 KMC 申请一对加密密钥,从密钥池中随机取出一对加密密钥对,使用用户证书载体中的签名公钥将用户的加密私钥加密保护后返回给 CA。CA 再根据申请信息为用户签发签名证书和加密证书并将两张数字证书发布到目录服务器上,然后将数字证书以及加密证书对应的私钥发送给证书注册管理系统。

关于证书签发管理系统与密钥管理系统之间的消息格式参见《数字证书认证系统密码协议规范》。

d) 下载证书

管理员进行证书的下载时,首先向证书注册管理系统提供确认信息。通过确认后,证书注册管理系统将签发好的用户证书和加密证书的私钥,下载到用户的证书载体中。

9.1.2 证书更新

证书更新流程如图 8 所示。

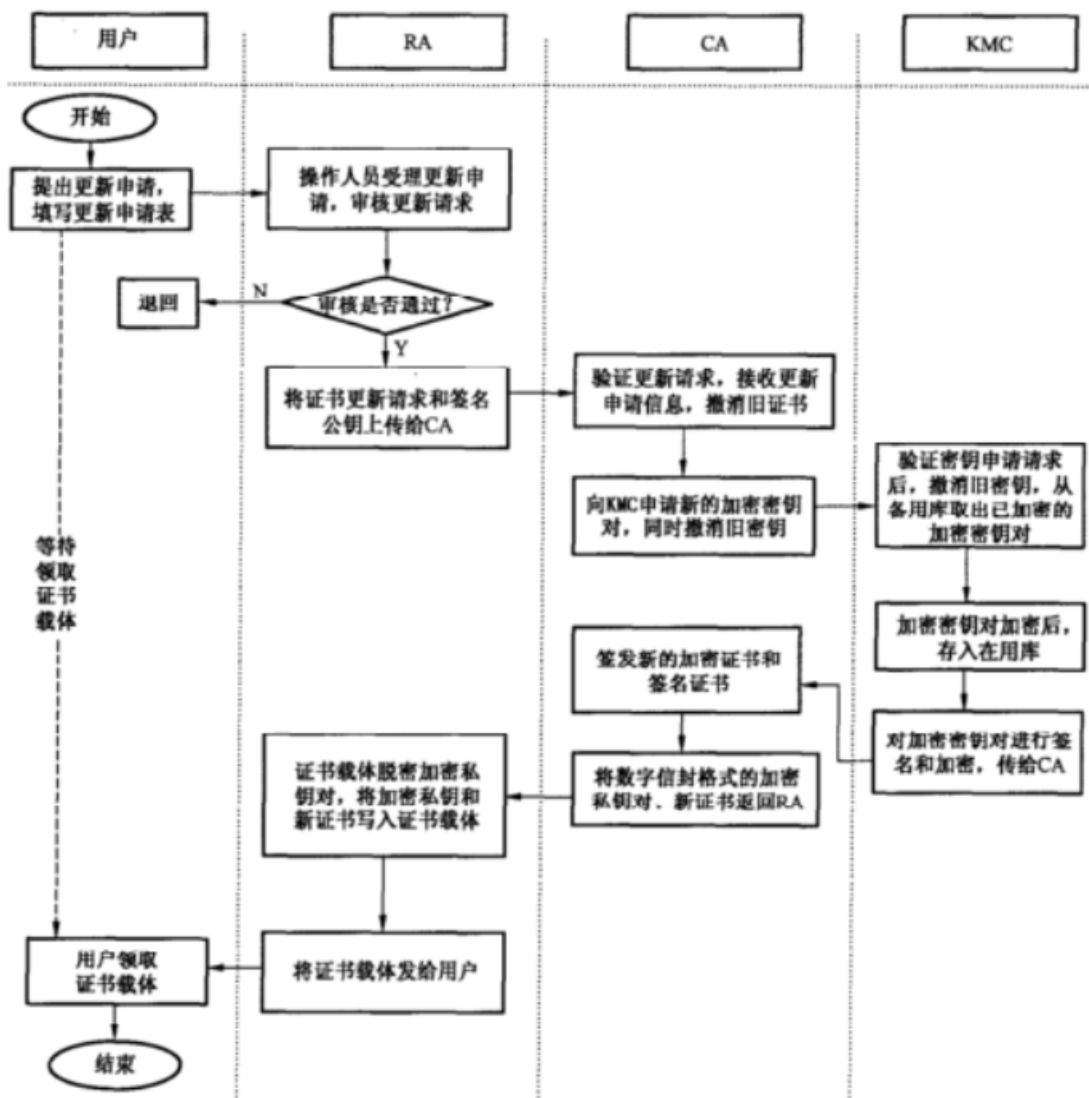


图 8 证书更新流程示意图

### 9.1.3 证书撤销

证书撤销分为强制撤销和用户申请撤销两种情况：

- a) 强制撤销：电子认证系统的管理人员可以在策略规定的范围内强制撤销用户的证书。
- b) 用户申请撤销：当用户因某种原因不再或不能使用证书时，可以通过证书注册管理系统申请撤销证书。

证书撤销流程如图 9 所示。

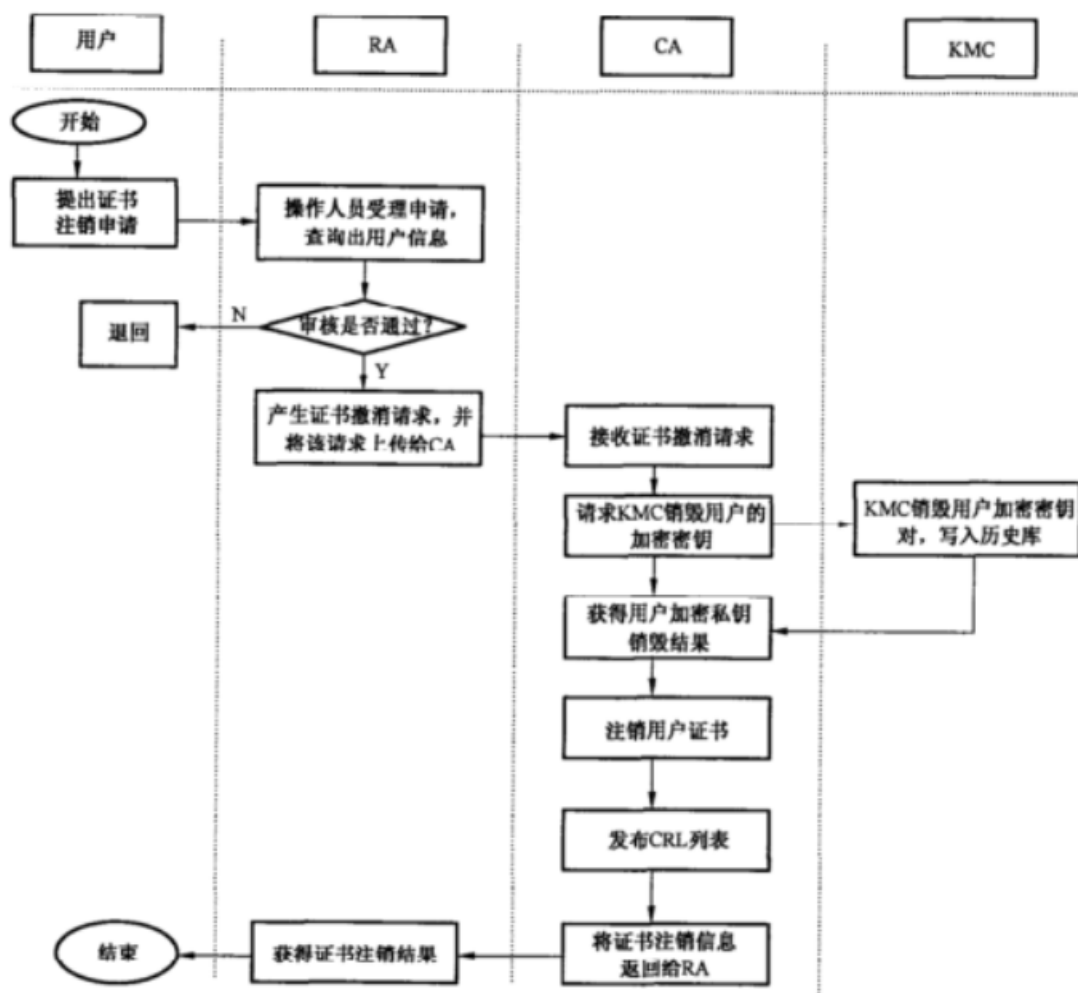


图 9 证书撤销流程示意图

证书撤销后，CRL 需要按照策略及时发布。

- a) CRL 发布的时间策略：可以采取实时发布和定时发布两种策略。实时发布是指证书签发管理系统接到撤销请求后，立刻根据请求信息签发撤销列表；定时发布是指证书签发管理系统接到撤销请求信息后不立刻签发撤销列表，而是按照系统的设定，在确定的时间里签发撤销列表。
- b) CRL 发布的形式：可以采用完全的撤销列表、增量证书撤销列表以及证书分布点技术发布证书撤销列表。

### 9.1.4 密钥恢复

用户证书密钥损坏或者过期，需要进行密钥恢复。密钥恢复流程如图 10 所示。

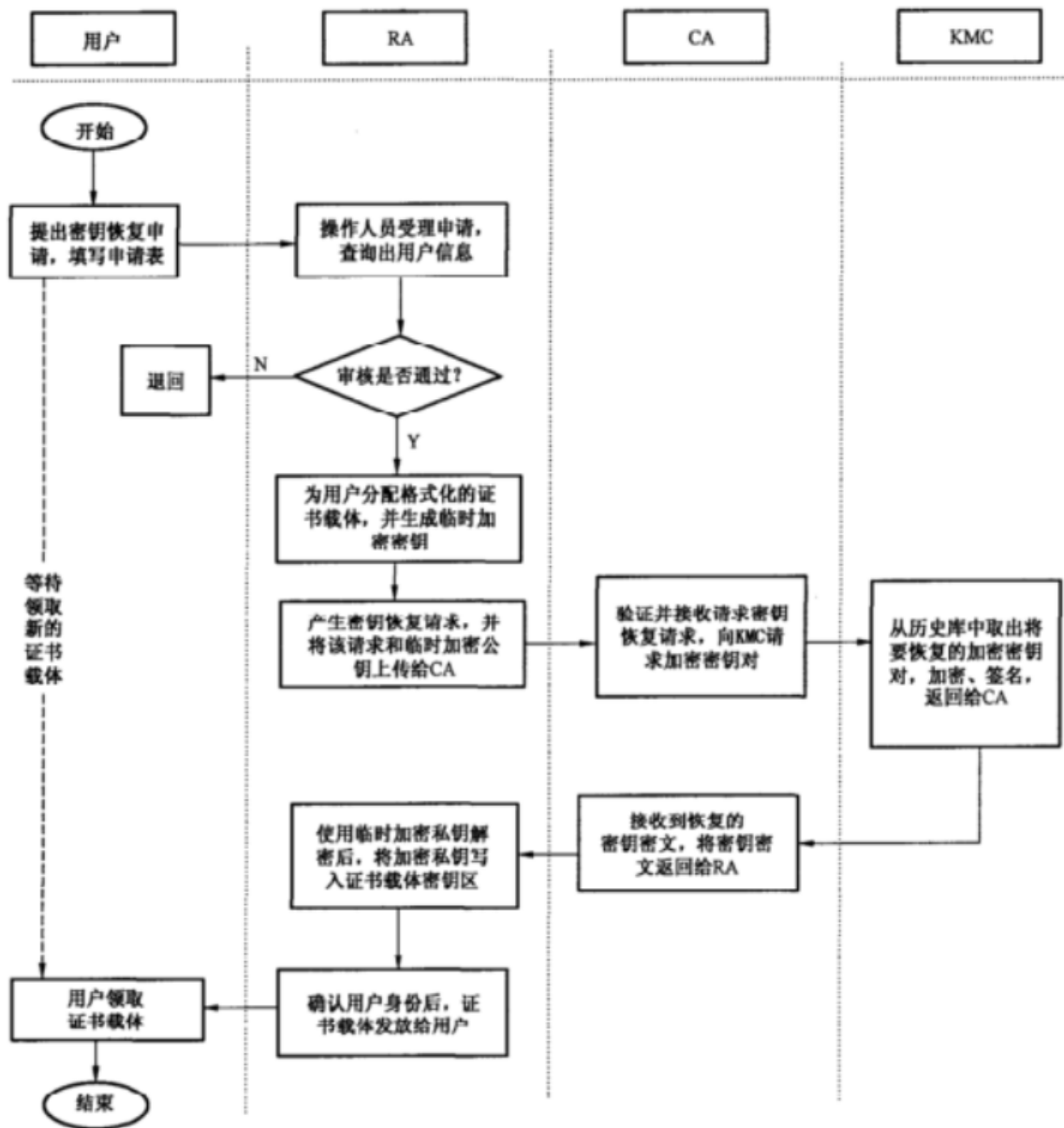


图 10 证书密钥恢复流程示意图

9.2 证书验证协议

用户在使用数字证书进行加密和验证数字签名时,必须验证证书的有效性,主要包括三个方面的内容:

- a) 用证书签发管理系统的证书验证用户证书中的签名,确认该证书是该证书签发管理系统签发的,并且证书的内容没有被篡改。
- b) 检验证书的有效期,确认该证书在有效期之内。
- c) 查验 CRL,确认该证书没有被撤销。

9.2.1 认证路径

在进行证书验证时,需要根据证书的签发者查询签发者证书并验证其有效性,直到找到一个预先确定的可信任的证书签发管理系统证书。在这个过程中,形成了一个包含多个证书签发管理系统证书的证书列表,这个列表就是证书的认证路径。

证书认证路径的获取可以在用户申请证书之前从证书签发管理系统下载,也可以在需要时实时分别从不同证书签发管理系统下载。

有关认证路径的具体处理过程,参见国家相关标准。

### 9.2.2 证书状态查询

- a) CRL 的获取:用户或应用系统可通过证书中的 CRL 地址标识下载。
- b) CRL 验证:验证时,首先检查 CRL 文件是否在有效期内,否则重新下载;然后验证 CRL 的签名以确认其正确性;最后检查 CRL 文件中是否包含所需要验证的证书的序列号,如果包含则说明该证书已经被撤销。

### 9.2.3 安全通信协议

电子认证系统各子系统之间需要采用安全通信协议以保证通信安全。

有关安全通信协议的详细内容可参见国家密码管理局相关标准。

附录 A  
(资料性附录)  
省级电子认证系统(模式一)网络结构示意图

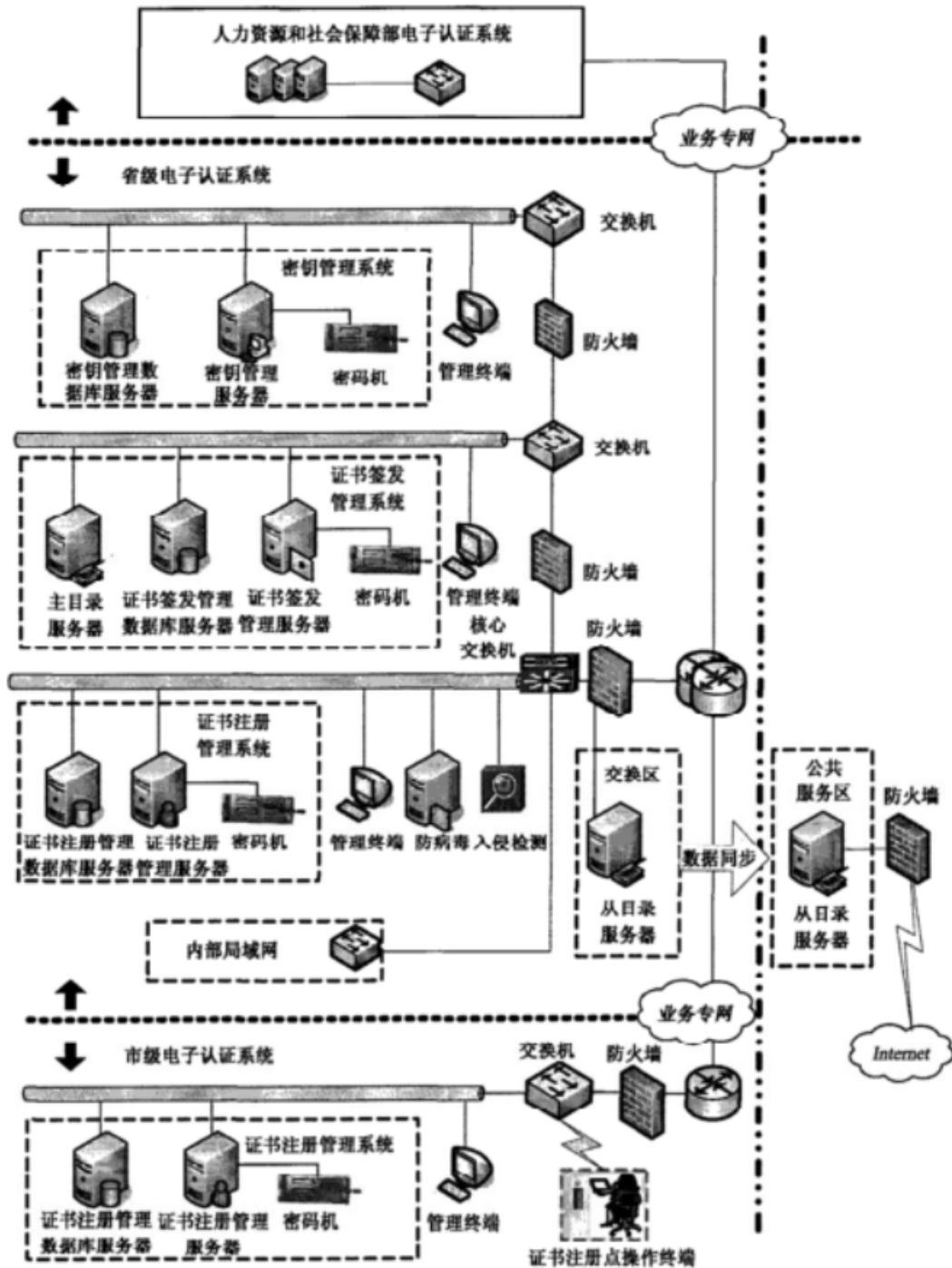


图 A.1 省级电子认证系统(模式一)网络结构示意图

附录 B  
(资料性附录)  
省级电子认证系统(模式二)网络结构示意图

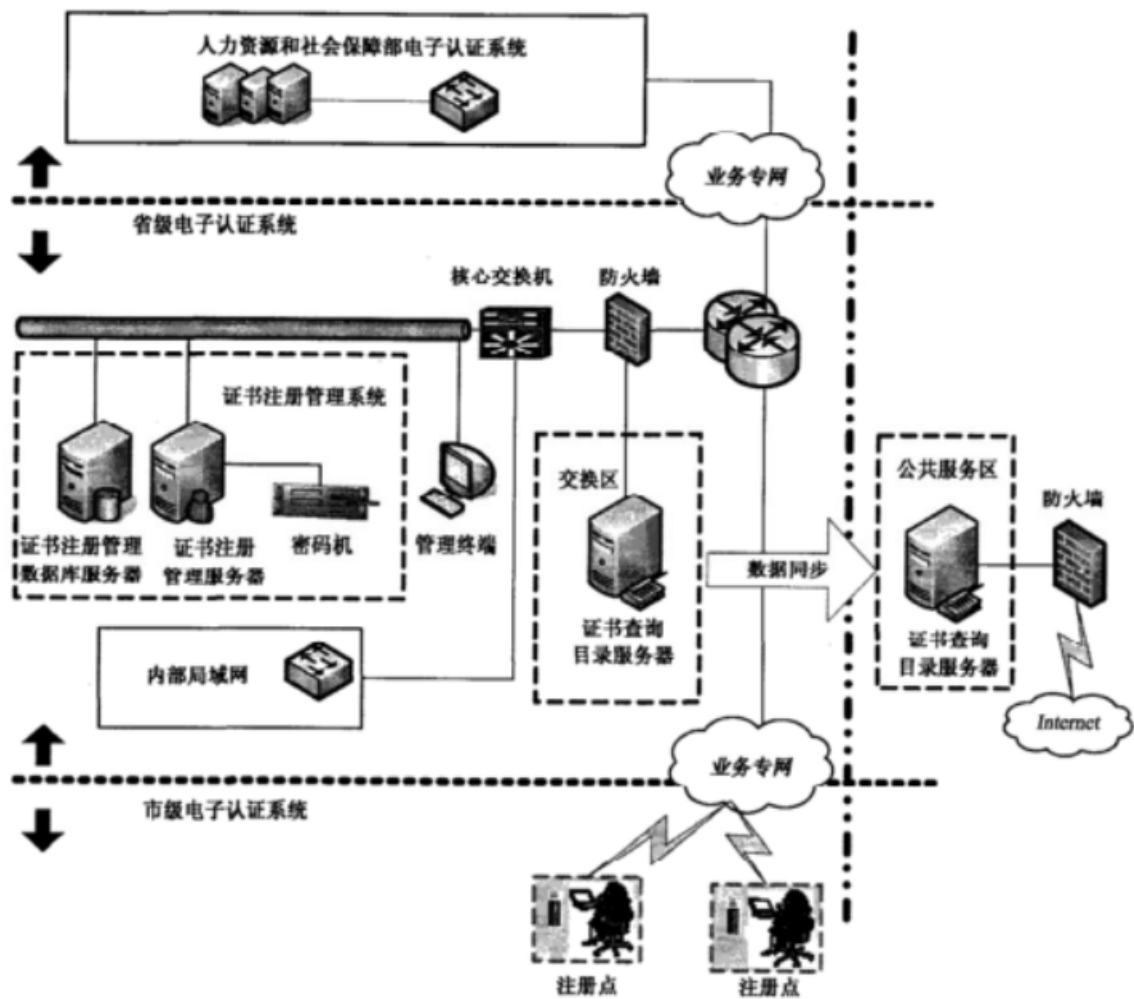


图 B.1 省级电子认证系统(模式二)网络结构示意图

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 2 部分:电子认证系统技术规范  
LD/T 30.2—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 1.5 字数 39 千字  
2010 年 2 月第一版 2010 年 2 月第一次印刷

\*

书号: 155066 · 2-20297



LD/T 30.2-2009

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