ICS 35.040
CCS L 80

LD

中华人民共和国劳动和劳动安全行业标准

LD/T 02.2-2022
代替 LD/T 30.2—2009

人力资源社会保障电子认证体系规范 第2部分：电子认证系统技术规范

Specifications for human resources and social security electronic authentication system— Part 2:Technology specification for electronic authentication system

2022-06-22 发布　　2022-07-01 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

本文件按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

LD/T 02人力资源社会保障电子认证体系系列规范，已经发布了以下五个部分：

----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：数字证书格式规范

----第4部分：数字证书应用接口规范

----第5部分：数字证书载体规范

本文件为LD/T 02的第2部分。

本文件代替 LD/T 30.2—2009《人力资源社会保障电子认证体系 第 2 部分： 电子认证系统技术规范》，与 LD/T 30.2—2009 相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了部分规范性引用文件（见第2章，2009版第2章）；

b) 删除了部分不必要的术语定义，同时增加了关于国产密码算法的术语和定义（见第3章，2009版第3章）；

c) 删除了电子认证体系的总体布局以及电子认证体系建设内容（见第5章，2009版5.1）；

d) 更改了电子认证系统的构成，按照GB/T 25056-2018，修订密钥管理设施组成，将“密码服务系统”调整为密钥管理系统的密码服务模块。（见第5章，2009版5.2）；

e) 更改了证书认证设施系统描述，并明确其运行管理要求（见第6章，2009版第6章）；

f) 更改了密钥管理设施组成，并明确其运行管理要求（见第7章，2009版第7章）；

g) 增加了第8章，描述系统中密码算法、密码设备及接口要求（见第8章）；

h) 更改了证书业务管理流程（见10.1，2009版9.1）；

i) 更改了证书状态查询内容描述，在原有查询方式后，新增OCSP查询方式（见10.2.2，2009版9.2.2）；

j) 更改了省级电子认证系统网络结构示意图，并在示意图后增加对电子认证系统中与关键业务相关的服务器、密码设备等设备进行双机部署的说明（见附录A、附录B，2009版附录A、附录B）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由中华人民共和国人力资源社会保障部信息中心提出并归口。

本文件起草单位：中华人民共和国人力资源和社会保障部信息中心、普华诚信信息技术有限公司、北京数字认证股份有限公司。

本文件主要起草人：马丹蕾、张嵩、王岩、耿建军、唐淑静、韩晓颖、成勇、王祥宇、李娜、王智飞、郭丽芳、高五星、李述胜。

本文件所代替的历次版本发布情况为：

----LD/T 30.2—2009 人力资源社会保障电子认证体系 第 2 部分：电子认证系统技术规范；

----本次为第一次修订。

引　言

为适应人力资源社会保障信息化发展要求，满足人力资源社会保障网络信任体系建设和管理的需要，人力资源社会保障部组织并制定了人力资源社会保障电子认证体系系列规范。随着我国商用密码技术的发展、国产密码算法的标准发布，以及人力资源社会保障行业的业务发展，需要对行业标准LD/T 30—2009《人力资源社会保障电子认证体系规范》进行修改和完善。

本次修订，是在充分借鉴原标准的框架和结构的基础上，根据人力资源社会保障行业特点和电子认证业务发展需求，对电子认证体系总体结构和电子认证系统整体建设规划进行扩充完善，以符合国家及国家密码主管部门相关标准规范要求，满足人力资源社会保障业务和管理需求，推进SM2算法在人社信息系统中的应用，另一方面，也可有效配合《中华人民共和国密码法》、《中华人民共和国网络安全法》、密码管理及密码应用安全测评工作、等级保护工作的落实与实施。

LD/T 02描述了人力资源社会保障电子认证体系总体结构和电子认证系统整体建设规划，规定了各级人力资源社会保障部门电子认证系统建设和应用要求，由以下五个部分构成。

----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：数字证书格式规范

----第4部分：数字证书应用接口规范

----第5部分：数字证书载体规范

LD/T 02的第1部分，是人力资源社会保障电子认证体系系列规范的总纲，规定了电子认证体系规范的总体框架。LD/T 02的第2部分~第5部分分别从电子认证系统技术、数字证书格式、数字证书应用接口、数字证书载体四个方面提出具体规范要求。

本部分描述了人力资源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，重点引用了GB/T 25056-2018，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。

人力资源社会保障电子认证体系规范
第2部分：电子认证系统技术规范

1 范围

本文件给出了人力资源社会保障电子认证系统的系统构成，规定了电子认证系统各单元的结构和基本功能、密码算法、密码设备及接口、基础安全防护措施、业务流程及相关协议。

本文件适用于各级人力资源社会保障部门建设基于PKI技术的电子认证系统。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件仅该日期对应的版本适用于本文件；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

GB/T 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 37092-2018 信息安全技术 密码模块安全要求

GM/Z 0001-2013 密码术语

GM/T 0014-2012 数字证书认证系统密码协议规范

LD/T 03-2022 人力资源社会保障 电子认证服务管理规范

3 术语和定义

GB/T 25056、GB/T 19771、GM/Z 0001界定的以及下列术语和定义适用于本文件。

3.1

私有密钥 private key

私钥

非对称密码算法中只能由拥有者使用的不公开密钥。

［来源：GB/T 25056-2018，3.10］

3.2

证书认证路径 certification path

在目录信息树（DIT）中对象证书的有序序列。通过处理该有序序列及其起始对象的公钥可以获得该路径的末端对象的公钥。

［来源：GB/T 19771-2005，3.9］

3.3

SM1 算法 SM1 algorithm

一种分组加密算法，分组长度为 128 比特，密钥长度为 128 比特。

[来源：GM/Z 0001-2013，2.117]

3.4

SM3 算法 SM3 algorithm

由 GB/T 32905 定义的算法。

[来源：GB/T 25056-2018，3.15]

3.5

SM4 算法 SM4 algorithm

一种分组密码算法，分组长度为 128 比特，密钥长度为 128 比特。

[来源：GM/Z 0001-2013，2.120]

4 缩略语

下列缩略语适用于本文件：

CA：证书认证机构（Certification Authority）

CRL：证书撤销列表（Certificate Revocation List）

HTTP：超文本传输协议（Hypertext Transfer Protocol）

KMC：密钥管理中心（Key Management Center）

RA：证书注册机构（Registration Authority）

LDAP：轻量级目录访问协议（Lightweight Directory Access Protocol）

OCSP：在线证书状态查询协议（Online Certificate Status Protocol）

5 电子认证体系结构

人力资源社会保障电子认证系统主要包括证书认证设施和密钥管理设施，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；密钥管理设施主要指密钥管理系统；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 1 所示。

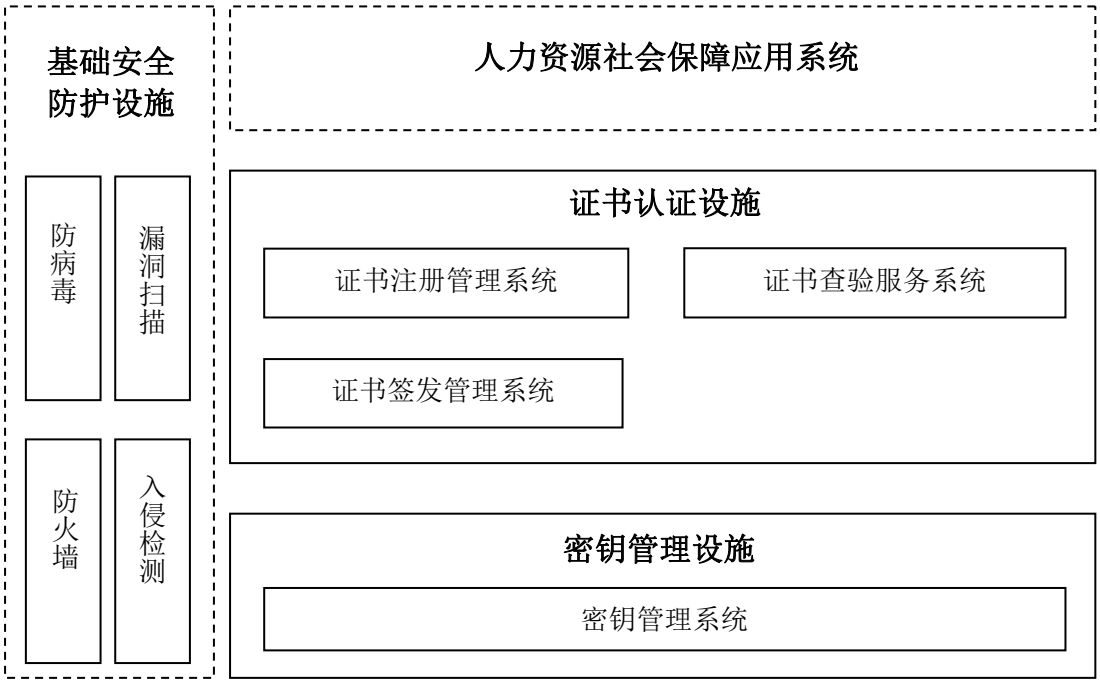


图1 电子认证系统构成

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，使用SM2算法签发各类数字证书。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 2 所示。

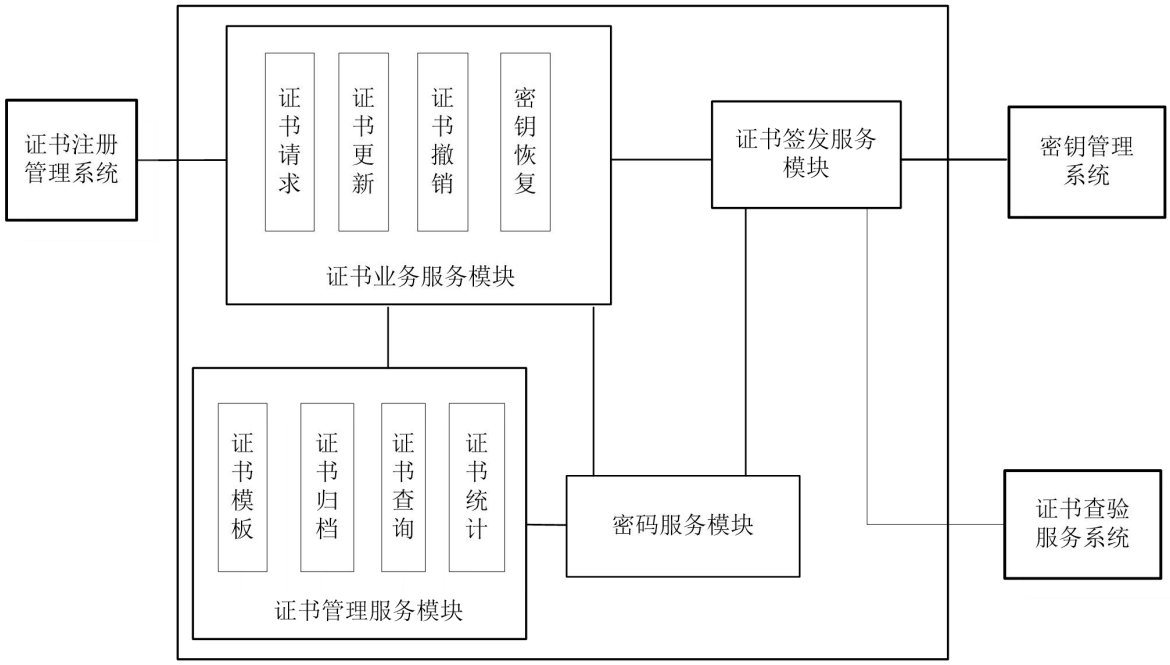


图 2 证书签发管理系统结构

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。

6.1.3 系统功能

证书签发管理系统是电子认证系统的核心，不仅为整个电子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、审计员，并为这些人员申请和下载数字证书；配置不同的证书模板，支持证书模板灵活定制；

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3所示。

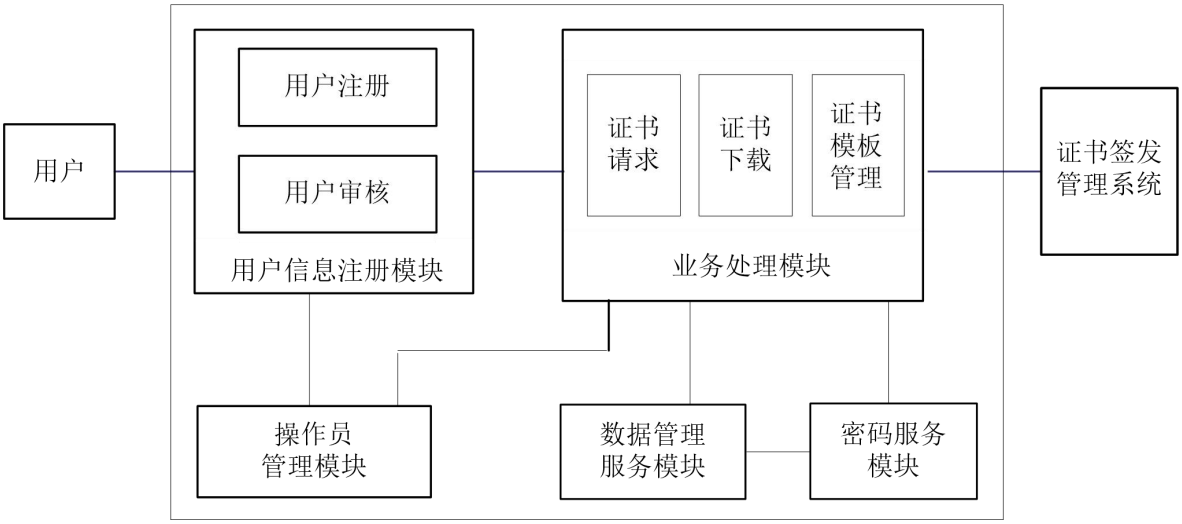


图3 证书注册管理系统结构

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由不同级别的管理员进行审核，能够根据需求支持多级审核模式；

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 目录服务系统

6.3.1.1 系统描述

目录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，从而检验证书的状态。

6.3.1.2 系统结构

目录服务系统包括主目录服务器和从目录服务器，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。

目录服务系统结构如图 4 所示。

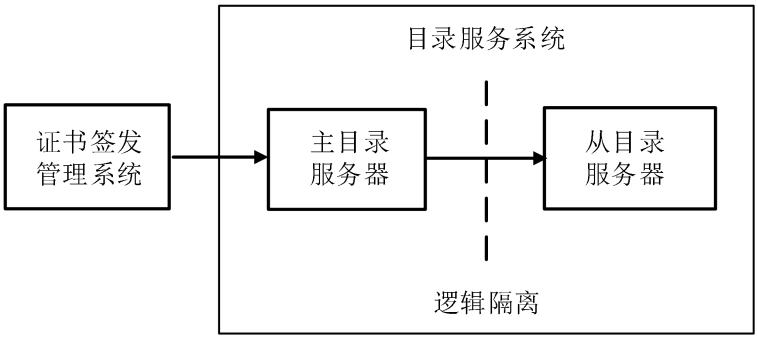


图4 目录服务系统结构

6.3.1.3 系统功能

目录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) CRL 下载：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：目录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。

6.3.2 证书状态查询系统

6.3.2.1 系统描述

证书状态查询系统主要负责为用户和应用系统提供证书状态查询服务，除提供基于 HTTP 协议的 CRL 查询、下载服务外，还提供基于 OCSP 协议的证书状态实时在线查询。

6.3.2.2 系统结构

证书状态查询系统由证书状态数据库/OCSP 服务器、安全管理模块、安全审计模块、数据管理模块以及密码设备组成。

证书状态查询系统结构如图 5 所示。

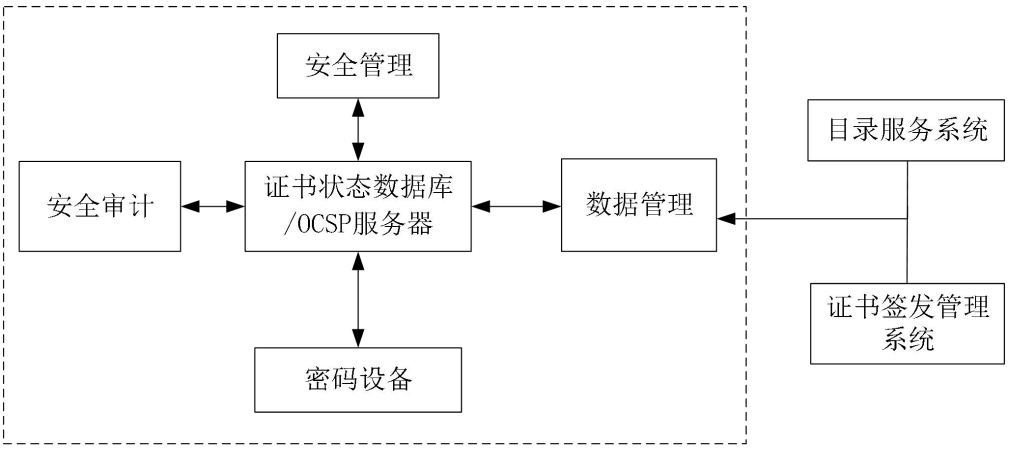


图 5 证书状态查询系统结构

a) 证书状态数据库/OCSP 服务器

接受用户及应用系统的证书状态查询请求，根据请求信息中的证书序列号，从证书状态数据库中查询证书的状态，查询结果返回给请求者。

b) 密码设备

验证请求信息中的签名，并对查询结果进行签名。

c) 安全管理

主要包括：

1) OCSP 服务器的配置，定义可接受的访问控制信息以及查询的证书状态数据库的地址；

2) 启动/停止查询服务配置，可接受的用户请求数量等。

d) 安全审计

查询证书状态查询系统中的安全审计日志，并进行统计与打印等。

e) 数据管理

对证书状态查询系统中的证书状态信息的数据同步、CRL 列表的同步的配置管理，支持自动数据同步和人工数据同步两种方式。

6.3.2.3 系统功能

证书状态查询系统为用户和应用系统提供证书状态查询服务，包括 CRL 查询、在线证书状态查询两种方式。

a) CRL 查询：提供基于 HTTP 协议查询 CRL 列表，用户或应用系统利用证书中标识的 CRL 地址，查询并下载 CRL 到本地，进行证书状态的检验。通过此方式，可以让证书认证中心提供通过 HTTP 协议下载 CRL 列表的服务；

b) 在线证书状态查询：用户或应用系统利用 OCSP 协议，在线实时查询证书的状态，查询结果经过签名后返回给请求者，进行证书状态的检验。

6.4 网络划分

证书认证系统的计算机网络需要合理分段，原则上要求整个网络应划分为四部分：

a) 公共部分：为电子认证用户所在的网络，所有用户将通过该网络访问电子认证系统；

b) 服务部分：为外部用户提供域名解析功能，并负责内部系统对外邮件的收发功能；包括系统的各种 WEB 服务器和从目录服务器，是外部用户访问内部功能的接口，为用户提供访问界面；

c) 管理部分：仅供电子认证系统的工作人员使用的网络；

d) 核心部分：包括各种核心应用、数据库和密码设备等在内的实现系统功能的安全网络。

6.5 数据备份

数据备份的目的是确保证书认证设施的关键业务数据在发生灾难性破坏时，系统能够及时和尽可能完整地恢复被破坏的数据。应选择适当的存储备份系统对重要数据进行备份。数据备份要求应符合 GB/T 25056-2018 中 8.3 的要求。

6.6 可靠性

证书认证设施应提供 7×24h 服务，对影响系统可靠性的主要因素如网络故障、主机故障、密码设备故障、数据库故障和电源故障等，宜采取软硬件冗余配置作为预防措施。证书认证设施的可靠性要求应符合 GB/T 25056-2018 中 8.4 的要求。

6.7 物理安全

证书认证设施建设应从物理环境安全、对 CA 的分层访问、门禁和物理侵入报警系统等方面采取安全措施。证书认证设施的物理安全应符合 GB/T 25056-2018 中 8.5 的要求。

6.8 运行管理要求

人员管理要求，应符合 LD/T 03-2022 中 5.2 的要求。

CA 业务运行管理要求包括制度管理、安全操作与运行规范、证书认证服务规范、系统安全管理等，应符合 LD/T 03-2022 中第 7 章的要求。

7 密钥管理设施

7.1 系统描述

密钥管理设施主要指密钥管理系统。

密钥管理系统基于公开密钥密码技术，负责为证书认证设施提供SM2算法加密证书密钥对等密钥服务，并对生命周期内的SM2算法加密证书密钥对进行全过程管理，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。

7.2 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。

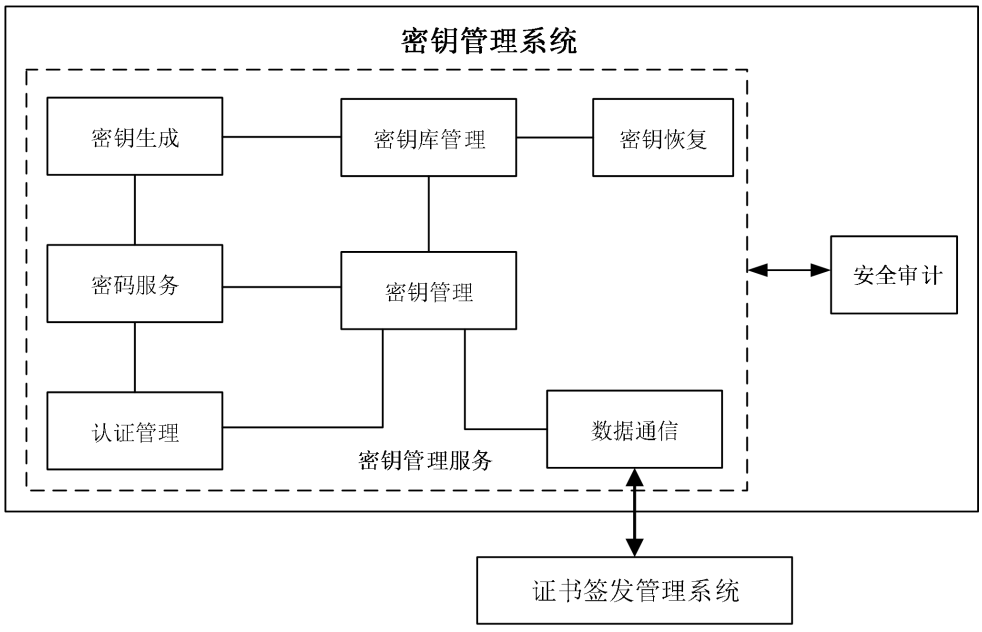


图6 密钥管理系统结构

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销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。

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） 数据通信

数据通信模块提供密钥管理系统与证书签发管理系统之间的通信功能，保证通信的数据安全，其主要包括身份认证、数据协议处理、数据加密解密、数据签名验签等功能。

h） 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。

7.3 系统功能

密钥管理系统提供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SM2算法非对称密钥对，该密钥对由密钥管理系统的硬件密码设备生成，加密保存在密钥管理系统的备用库中；
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) 密钥撤销：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销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销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，为司法取证提供密钥恢复服务。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。

7.4 数据备份

密钥管理设施的数据备份符合 6.5 要求。

7.5 可靠性

密钥管理设施的可靠性符合 6.6 要求。

7.6 物理安全

密钥管理设施的物理安全符合 6.7 要求。

7.7 运行管理要求

密钥管理设施的运行管理符合 6.8 要求。

8 密码算法、密码设备及接口

8.1 密码算法

电子认证系统使用对称密码算法、公钥密码算法和密码杂凑算法等三类算法实现有关密码服务各项功能，其中，对称密码算法实现数据加解密；公钥密码算法实现签名以及签名验证；密码杂凑算法实现待签名消息的摘要运算。这些功能的实现依赖于密码设备。

电子认证系统使用的密码算法要求如下：

a) 对称密码算法：采用国家密码主管部门批准使用的对称密码算法 SM1、SM4 算法；
b) 公钥密码算法：采用国家密码主管部门批准使用的公钥密码算法 SM2 算法；
c) 密码杂凑算法：采用国家密码主管部门批准使用的密码杂凑算法 SM3 算法。

8.2 密码设备

密码设备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数字签名及验证、数据加解密、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) 数字证书载体：用于存储密钥和数字证书并具有密码运算功能的载体，其安全性须符合 GB/T 37092-2018 中安全等级第二级及以上相关要求。目前，人力资源社会保障电子认证系统采用的数字证书载体包括两类：
   1）智能密码钥匙，应符合 LD/T 02.5 规定的要求。证书载体应支持 SM2 算法；
   2）社会保障卡持卡人证书载体，载体为第三代社会保障卡，符合 LD/T 32 的要求。

8.2.1 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) 公钥密码算法的加解密运算；
e) 对称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。

8.2.2 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。

8.3 密码服务接口

密码服务的接口符合LD/T 02.4规定的要求。

9 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。

9.1 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。

9.2 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。

9.3 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。

9.4 入侵检测

应配备入侵检测系统，监测电子认证系统的运行，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管理区、核心区上，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。

10 业务流程与协议

10.1 证书管理流程

证书管理流程包括证书申请、证书更新、证书撤销、用户加密密钥恢复等。

10.1.1 证书申请

使用数字证书的单位、个人、设备或应用系统，应按照数字证书申请流程及规范，提交数字证书信息资料，申请证书。

证书申请流程如图 7 所示。

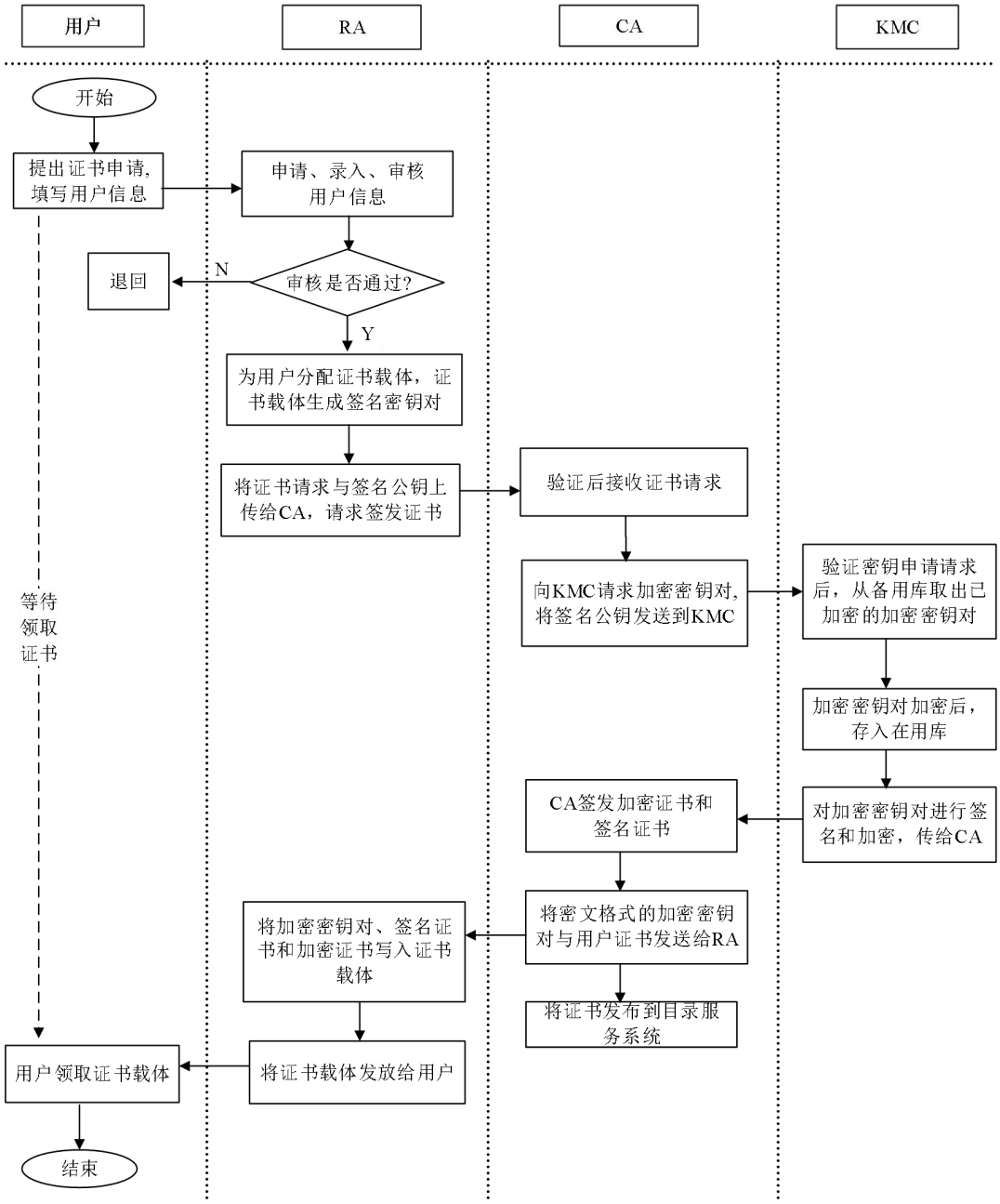


图7 证书申请流程示意图

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的提交申请，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。

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

证书签发管理系统得到用户签发证书请求后，向KMC申请一对加密密钥对，从备用库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密钥对加密保护后返回给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系统上，然后将数字证书以及加密证书密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按照GM/T 0014-2012。

d) 下载证书

操作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密钥对，下载到用户的证书载体中。

10.1.2 证书更新

证书过期前两个月内，系统应提示用户进行证书更新，证书用户按照提示及时申请更新证书，以确保信息的有效性和密钥的安全。

证书更新可采用以下两种方式：

a) 在线自助更新：对于证书信息无须改变的证书用户，在证书即将过期时，获得工作人员的授权后，证书用户自助进行在线证书更新操作，通过在线方式下载新证书到证书载体内，从而完成证书更新；

b) 人工更新方式：证书用户持证书载体到证书注册点现场办理证书更新，由证书注册点工作人员为用户办理证书更新。

证书更新流程如图 8 所示。

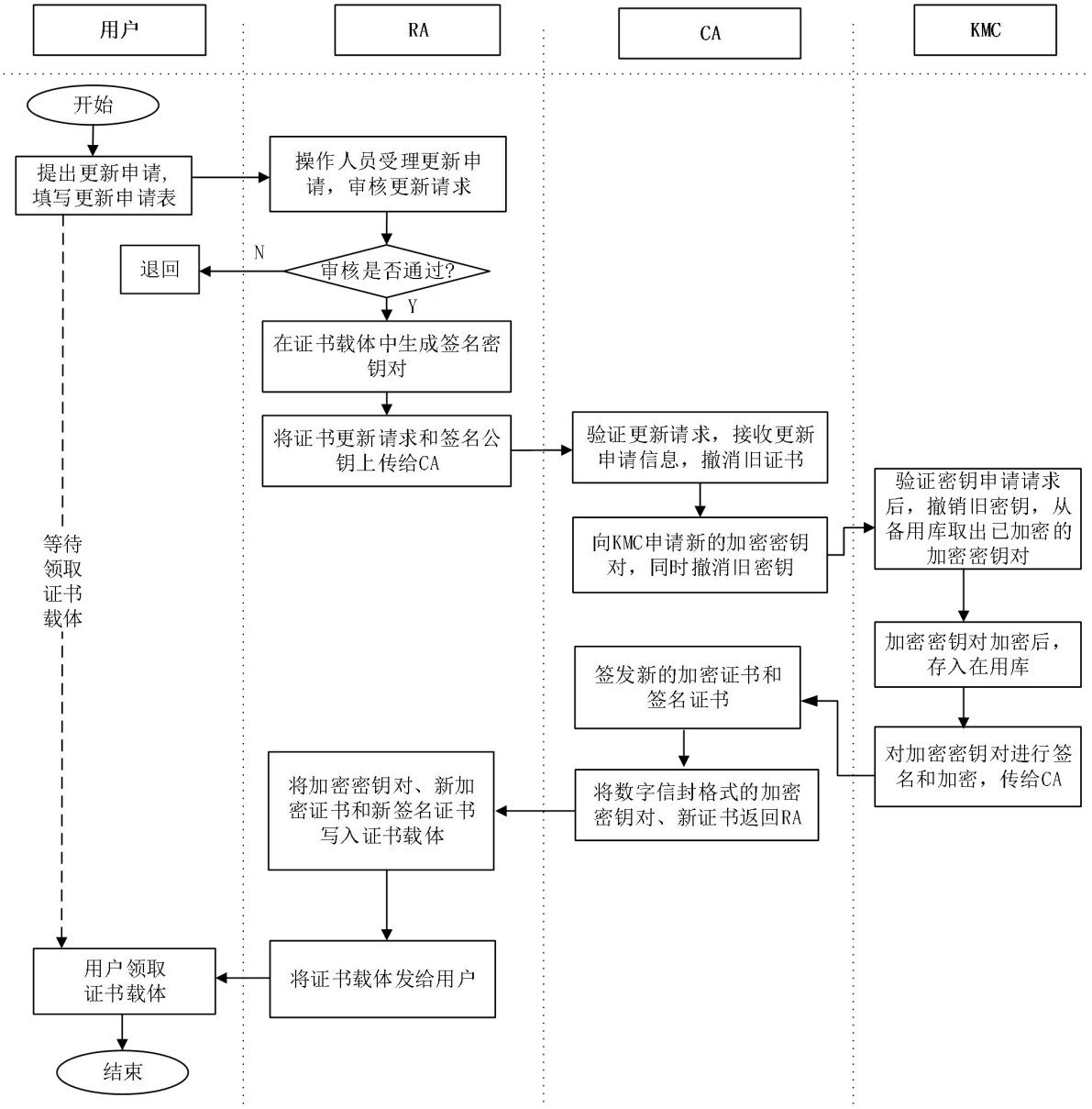


图8 证书更新流程示意图

证书更新流程可分成以下几个子流程：

a) 证书更新申请

用户首先向证书注册管理系统提交证书更新申请，将自己的身份信息提交给RA，即填写证书更新申请表。

b) 证书更新申请的审核

为用户签发新证书之前，必须对用户的真实身份进行确认，要求用户提交的证书更新申请信息与其真实身份信息相符。

在用户证书载体中生成新的签名密钥对，将证书更新请求和签名公钥通过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新的用户证书。

c) 签发新证书

证书签发管理系统得到用户更新证书请求后，向KMC申请撤销原加密密钥对，并签发CRL，发布到目录服务系统上。同时向KMC申请一对新的加密密钥对，从备用库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密钥对加密保护后返回给CA。CA再根据证书更新申请信息为用户签发新的签名证书和新的加密证书，并将两张数字证书发布到目录服务系统上，然后将新的数字证书以及加密密钥对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按照GM/T 0014-2012。

d) 下载更新后证书

操作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更新后的签名证书、加密证书和加密密钥对，下载到用户的证书载体中。

10.1.3 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：

1. 强制撤销：当发生下列情形之一时，电子认证系统管理员可以在策略规定的范围内强制撤销用户的证书；

1) 证书持有人提供的信息不真实；
2) 司法机构要求撤销证书持有人证书；
3) 证书持有人申请撤销数字证书；
4) 证书持有人丧失民事行为能力；
5) 证书持有人严重违反本行业电子认证有关规定的义务；
6) 数字证书的安全性不能得到保证；
7) 法律、行政法规规定的其他情形。

证书强制撤销流程如图9所示。

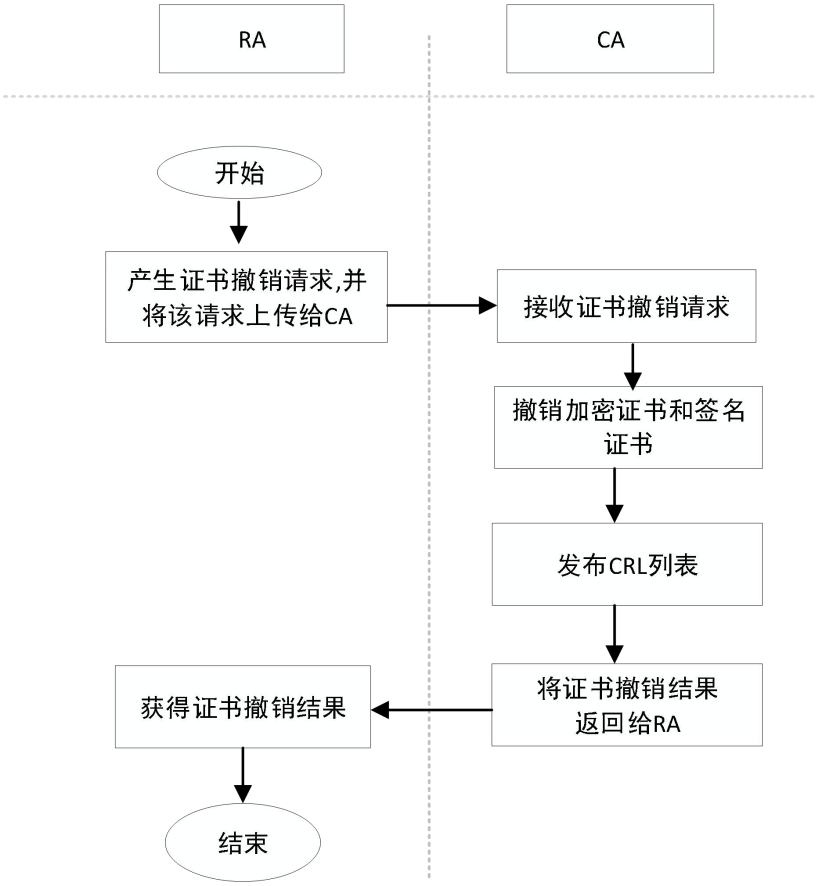


图9 证书强制撤销流程示意图

a） 证书撤销申请

电子认证系统管理员将证书撤销请求通过RA系统提交到证书签发管理系统，由证书签发管理系统撤销用户证书。

b） 撤销用户证书

证书签发管理系统接受证书撤销请求后，撤销用户签名证书和加密证书，签发CRL列表发布到目录服务系统上，并将证书撤销信息返回给RA证书注册管理系统。

2. 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10所示。

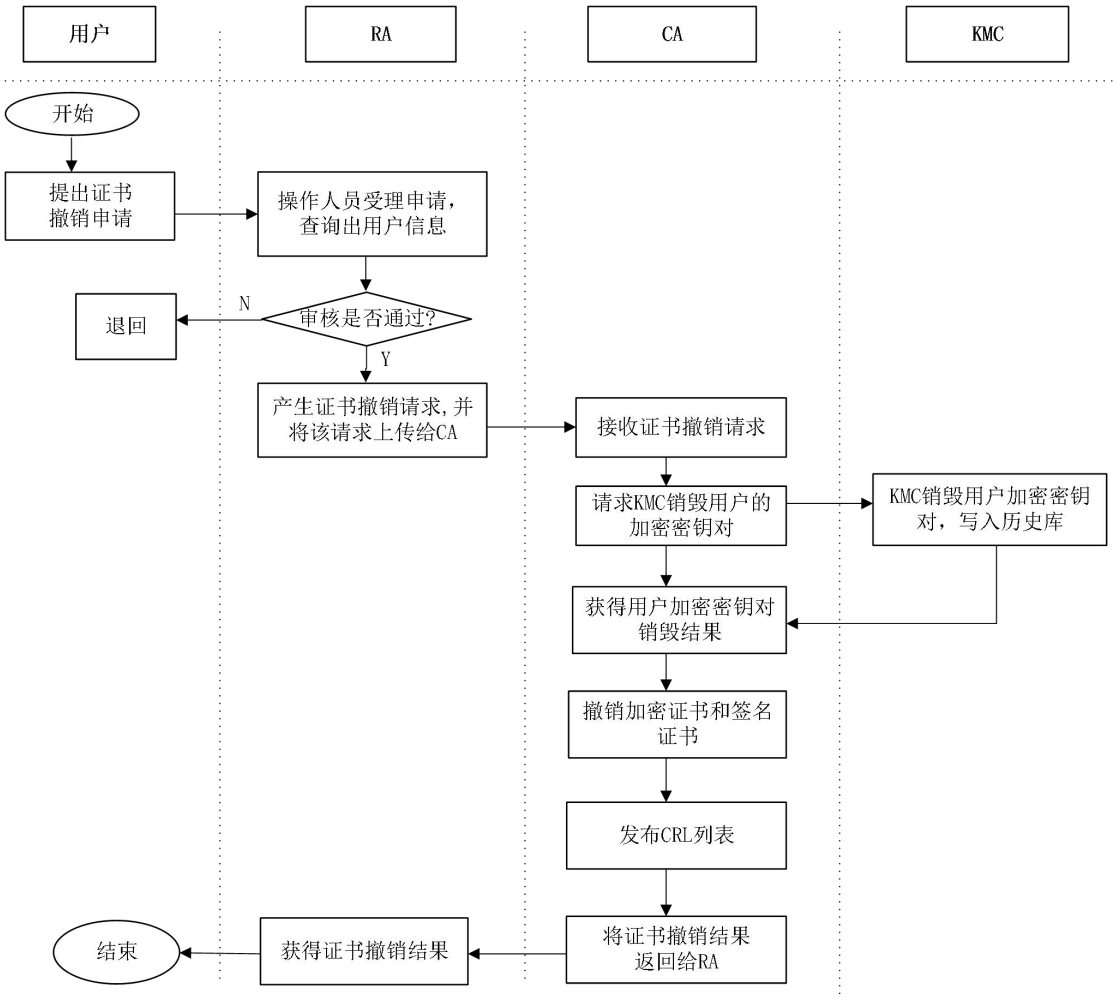


图10 证书撤销流程示意图

c） 证书撤销申请

用户首先向证书注册管理系统提交证书撤销申请，将自己的身份信息提交给RA，即填写证书撤销申请表。

d） 证书撤销申请的审核

操作人员受理申请，对用户的真实身份进行确认，要求用户提交的证书撤销申请信息与其真实身份信息相符。审核通过后，产生证书撤销请求，将证书撤销请求和签名公钥通过RA系统提交到证书签发管理系统，由证书签发管理系统撤销用户证书。

e） 撤销用户证书

证书签发管理系统接受用户证书撤销请求后，向KMC申请销毁用户的加密密钥对，由KMC销毁用户加密密钥对，并写入历史库。CA签发管理系统获得用户加密密钥对销毁结果后，撤销用户签名证书和加密证书，签发CRL列表发布到目录服务系统上，并将证书撤销信息返回给RA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按照GM/T 0014-2012。

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证书撤销列表；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证书撤销列表，而是按照系统的设定，在确定的时间里签发证书撤销列表；

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。

10.1.4 密钥恢复

用户加密证书密钥损坏，需要通过加密密钥对的恢复方可解密曾经加密的数据。

密钥恢复时，证书用户必须提交真实、完整的身份证明材料。数字证书管理机构应严格审核用户身份的真实性，由两名工作人员共同完成密钥恢复操作

密钥恢复流程如图 11 所示。

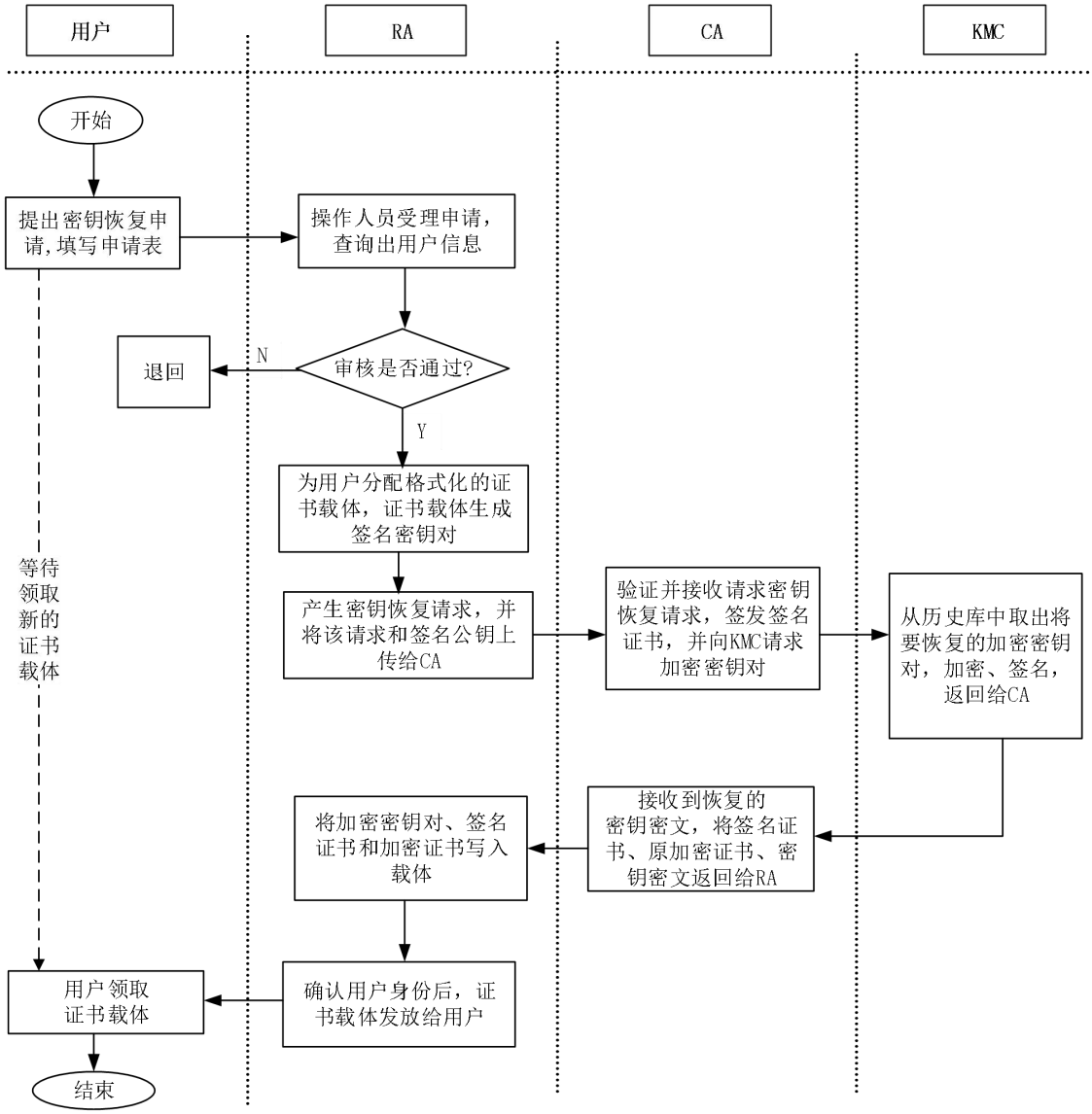


图 11 证书密钥恢复流程示意图

a） 密钥恢复申请

用户要进行密钥恢复，须向证书注册管理系统提交密钥恢复申请，将自己的身份信息提交给RA，即填写密钥恢复申请表。

b） 密钥恢复申请的审核

操作人员对用户的真实身份进行确认，要求用户提交的密钥恢复申请信息与其真实身份信息相符。

审核通过后，为用户分配格式化的证书载体，并在证书载体中生成签名密钥对，同时将密钥恢复请求、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的签名证书。

c） 密钥恢复

证书签发管理系统得到用户密钥恢复请求后，签发用户签名证书，并向KMC申请一对加密密钥对，从历史库中取出将要恢复的加密密钥对，使用用户证书载体中的签名公钥将用户的加密密

钥对加密保护后返回给CA。CA再根据申请信息为用户签发签名证书，并发布到目录服务系统上，然后将签名证书以及原加密证书、加密密钥对密文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按照GM/T 0014-2012。

d) 下载证书

操作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恢复的加密证书、加密密钥对，下载到用户的证书载体中。

10.2 证书验证

用户在使用数字证书进行加密和验签时，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（CA 证书）验证用户证书中的签名，确认此用户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。

10.2.1 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。

有关认证路径的具体处理过程，参见国家相关标准。

10.2.2 证书状态查询

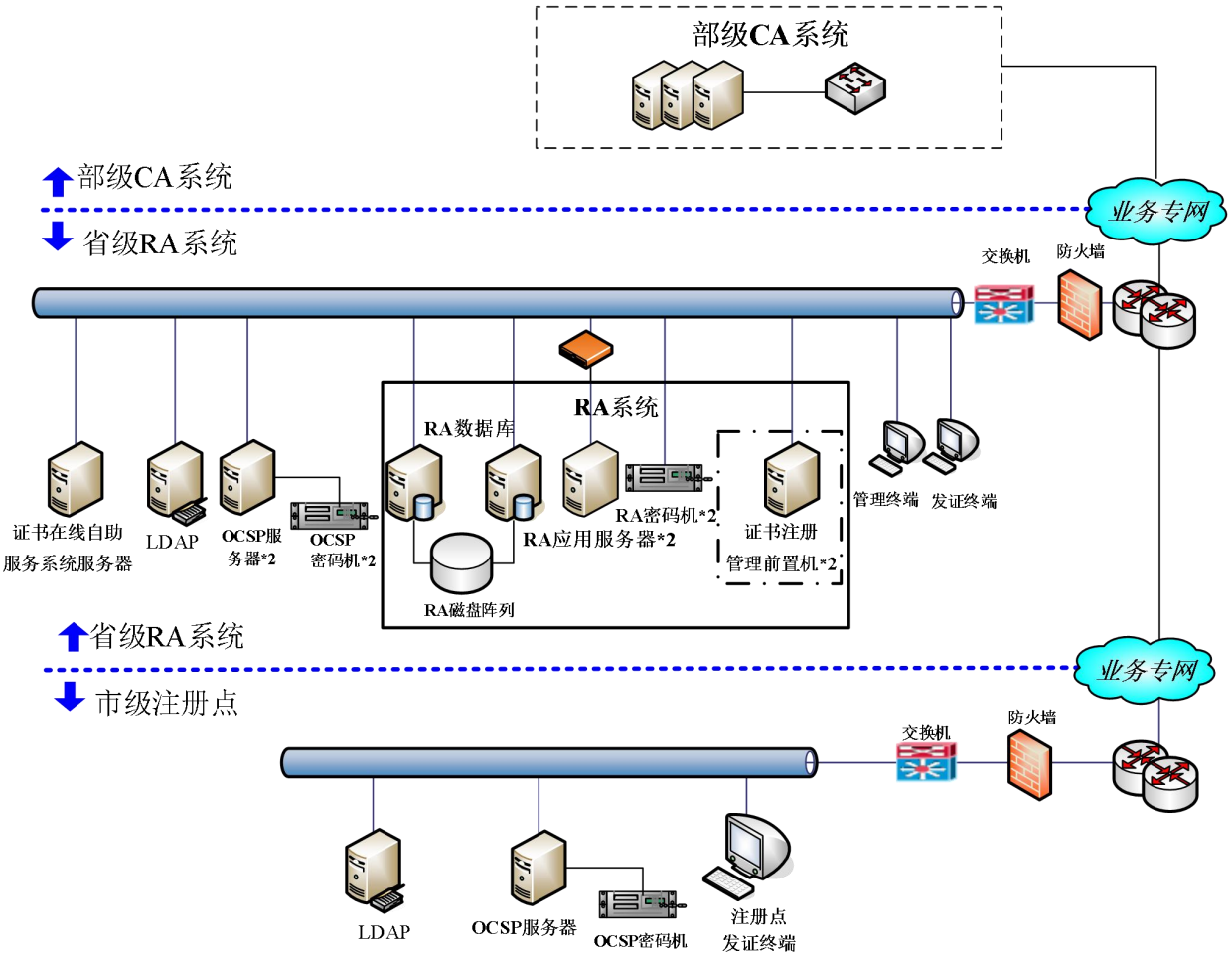
a) CRL 的获取：用户或应用系统可通过证书中的 CRL 地址标识下载；
b) CRL 验证：验证时，首先检查 CRL 文件是否在有效期间内，否则重新下载；然后验证 CRL 的签名以确认其正确性；最后检查 CRL 文件中是否包含所需要验证的证书的序列号，如果包含则说明该证书已经被撤销；
c) 在线证书状态查询：用户或应用系统可以按照 OCSP 协议，实时在线查询证书的状态。

10.2.3 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见GM/T 0014-2012第5章“相关协议”。

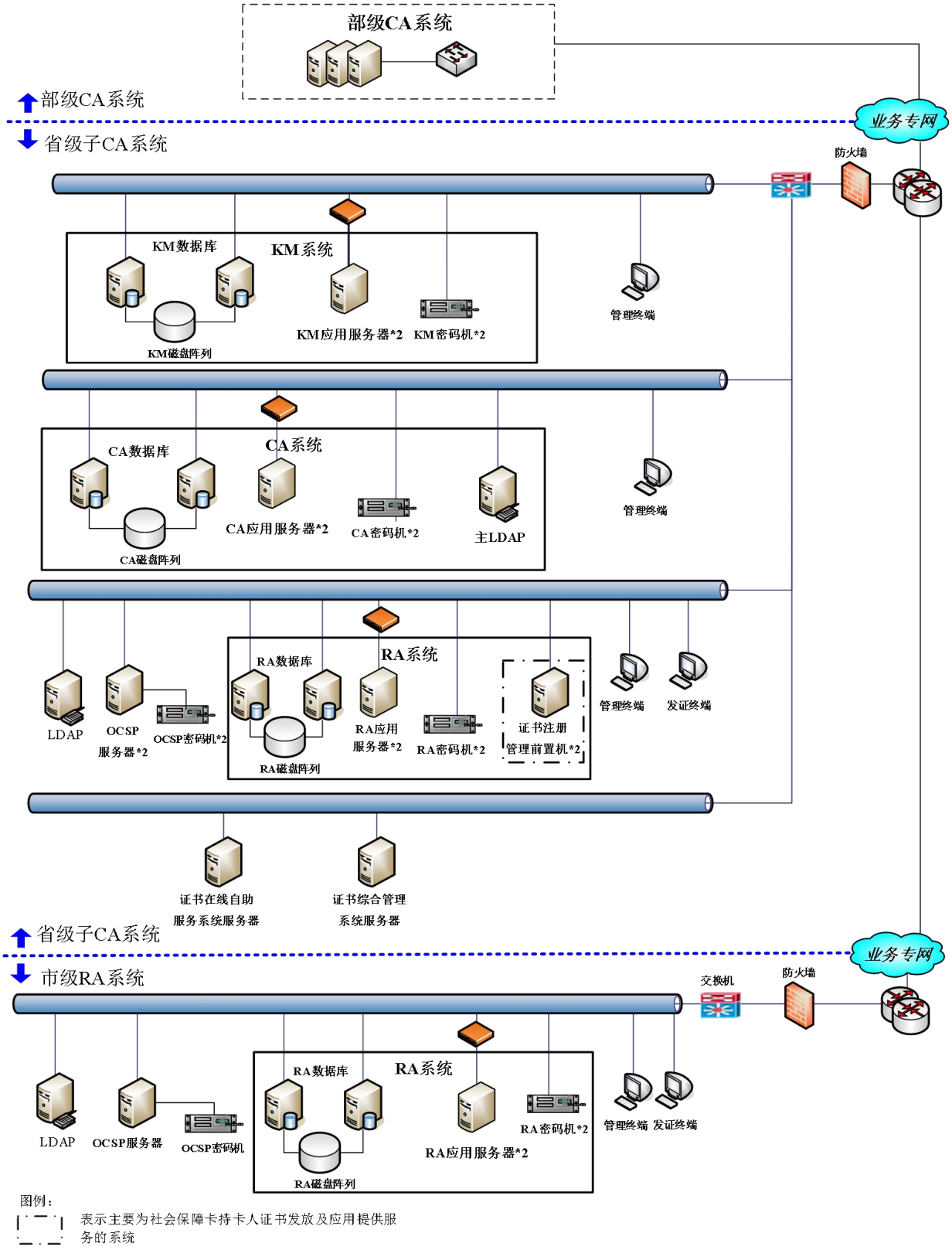
附 录 A
（资料性）
省级电子认证系统（模式一）网络结构示意图



图A.1 省级电子认证系统（模式一）网络结构示意图

根据GB/T 25056-2018中“8.4可靠性”要求，电子认证系统中与关键业务相关的主机、密码设备及在服务网段和核心网段中的服务器应采用双机热备份、双机备份、集群等措施。

附 录 B
（资料性）
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

根据GB/T 25056-2018中“8.4可靠性”要求，电子认证系统中与关键业务相关的主机、密码设备及在服务网段和核心网段中的服务器应采用双机热备份、双机备份、集群等措施。