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 02.1—2022
代替 LD/T 30.1—2009

人力资源社会保障电子认证体系规范 第1部分：框架规范

Specifications for human resources and social security electronic authentication system—Part 1: Architecture specification

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1部分。

本文件代替LD/T 30.1—2009《人力资源社会保障电子认证体系 第1部分： 框架规范》，与LD/T 30.1—2009相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 更改了第1章中标准规范的适用范围要求（见第1章，2009版第1章）；
b) 更新了部分规范性引用文件，删除了部分不再被引用的文件（见第2章，2009版第2章）；
c) 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）；
d) 更改了电子认证体系应用范围（见第5章，2009版第5章）；
e) 更改了电子认证体系总体结构，按照人力资源社会保障电子认证业务发展规划，优化电子认证体系总体结构（见第6章，2009版第6章）；
f) 增加了关于国家电子认证根CA的表述，并完善各级电子认证系统建设内容（见7.2，2009版7.2）；
g) 更改了部级电子认证系统建设要求（见7.3，2009版7.3）；
h) 更改了省级电子认证系统建设要求（见7.4，2009版7.4）；
i) 更改了市级电子认证系统建设要求（见7.5，2009版7.5）；
j) 更改了电子认证管理层内容描述和功能要求（见第8章，2009版第8章）；
k) 更改了电子认证应用安全支撑层内容描述和功能要求（见第 9 章，2009 版第 9 章）。

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 30.1—2009《人力资源社会保障电子认证体系 第 1 部分： 框架规范》；

----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。

本部分重点补充和完善了人力资源社会保障电子认证体系的建设总体框架，重新规定了电子认证体系建设和应用范围，界定了框架内各层次建设内容以及各层之间的相互关系。

本文件指导建设全国统一、布局合理、运行有序、安全可靠的人力资源社会保障电子认证体系；指导各级人力资源社会保障部门建设合理的电子认证系统，为人力资源社会保障业务系统提供规范的电子认证服务；指导各级人力资源社会保障部门为应用系统建立电子认证应用技术支撑体系，提供安全、规范、易于集成的电子认证服务接口，为人力资源社会保障业务系统提供有效的身份认证、数字签名、数据加解密等安全机制。

人力资源社会保障电子认证体系规范
第1部分：框架规范

1 范围

本文件给出了人力资源社会保障电子认证体系的应用范围、总体结构，规定了电子认证体系应用范围、电子认证体系总体结构以及电子认证系统基础层、电子认证管理层、电子认证应用安全支撑层之间的关系和基本要求。

本文件适用于各级人力资源社会保障电子认证体系建设。

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 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 32918（所有部分） 信息安全技术 SM2椭圆曲线公钥密码算法

GB/T 36322-2018 信息安全技术 密码设备应用接口规范

GB/T 38540-2020 信息安全技术 安全电子签章密码技术规范

GB/T 38629-2020 信息安全技术 签名验签服务器技术规范

GM/T 0025-2014 SSL VPN 网关产品规范

GM/T 0026-2014 安全认证网关产品规范

GM/T 0030-2014 服务器密码机技术规范

GM/T 0033-2014 时间戳接口规范

LD/T 01-2022（所有部分） 人力资源社会保障电子印章体系规范

LD/T 33 社会保障卡读写终端规范

3 术语和定义

GB/T 25056 界定的以及下列术语和定义适用于本文件。

3.1

证书认证机构 Certificate Authority;CA

对数字证书进行全生命周期管理的实体，也称为电子认证服务机构。

［来源：GB/T 25056-2018，3.5］

3.2

数字证书 digital certificate

由证书认证机构（CA）签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。按类别可分为个人证书、机构证书和设备证书，按用途可分为签名证书和加密证书。

［来源：GB/T 25056-2018，3.9］

3.3

CA 证书 CA certificate

由一个 CA 给另一个 CA 签发的数字证书，一个 CA 也可以为自己签发证书，这是一种自签名的证书。

［来源：GB/T 25056-2018，3.1］

3.4

证书认证系统 certificate authentication system

电子认证系统

对数字证书的签发、发布、更新、撤销等数字证书全生命周期进行管理的系统。

［来源：GB/T 25056-2018，3.2］

3.5

证书撤销列表 Certificate Revocation List;CRL

由证书认证机构（CA）签发并发布的被撤销证书的列表。

［来源：GB/T 25056-2018，3.4］

3.6

SM2 算法 SM2 algorithm

由 GB/T 32918（所有部分）定义的算法。

[来源：GB/T 25056-2018，3.14]

3.7

公开密钥 public key

公钥

非对称密码算法可以公开的密钥。

［来源：GB/T 25056-2018，3.11］

3.8

信任 trust

通常说一个实体信任另一个实体表示后一个实体将完全按照第一个实体的规定进行相关的活动。在本标准中，信任用来描述一个认证实体与证书认证机构之间的关系。

［来源：GB/T 25056-2018，3.16］

4 缩略语

下列缩略语适用于本文件。

CA：证书认证机构（Certification Authority）

RA：证书注册机构（Registration Authority）

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

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

5 电子认证体系应用范围

人力资源社会保障电子认证体系所支撑的应用包括全国性、区域性的各类应用系统，按照业务类别划分为以下四类：

a) 就业创业类：就业创业、失业监测等业务系统；
b) 社会保障类：养老、工伤等社会保险业务系统、社会保障卡持卡库等业务系统、社会保险公共服务平台；
c) 人才人事类：事业单位人事管理、专业技术人员管理、人力资源市场、职业资格管理、职业技能培训等业务系统；
d) 劳动关系类：劳动用工备案、调解仲裁、劳动监察等业务系统。

6 电子认证体系总体结构

人力资源社会保障网络信任体系是以密码技术为支撑，以电子认证系统为基础设施，基于数字证书的应用开发接口，面向人力资源社会保障各类业务系统，实现以身份认证、授权管理和责任认定为主要内容的安全应用。电子认证体系是网络信任体系的基础，是基于密码技术，实现证书生命周期管理，以及安全认证、加密保护、签名验证等证书应用功能的技术体系和管理体系。

人力资源社会保障电子认证体系总体结构见图 1。

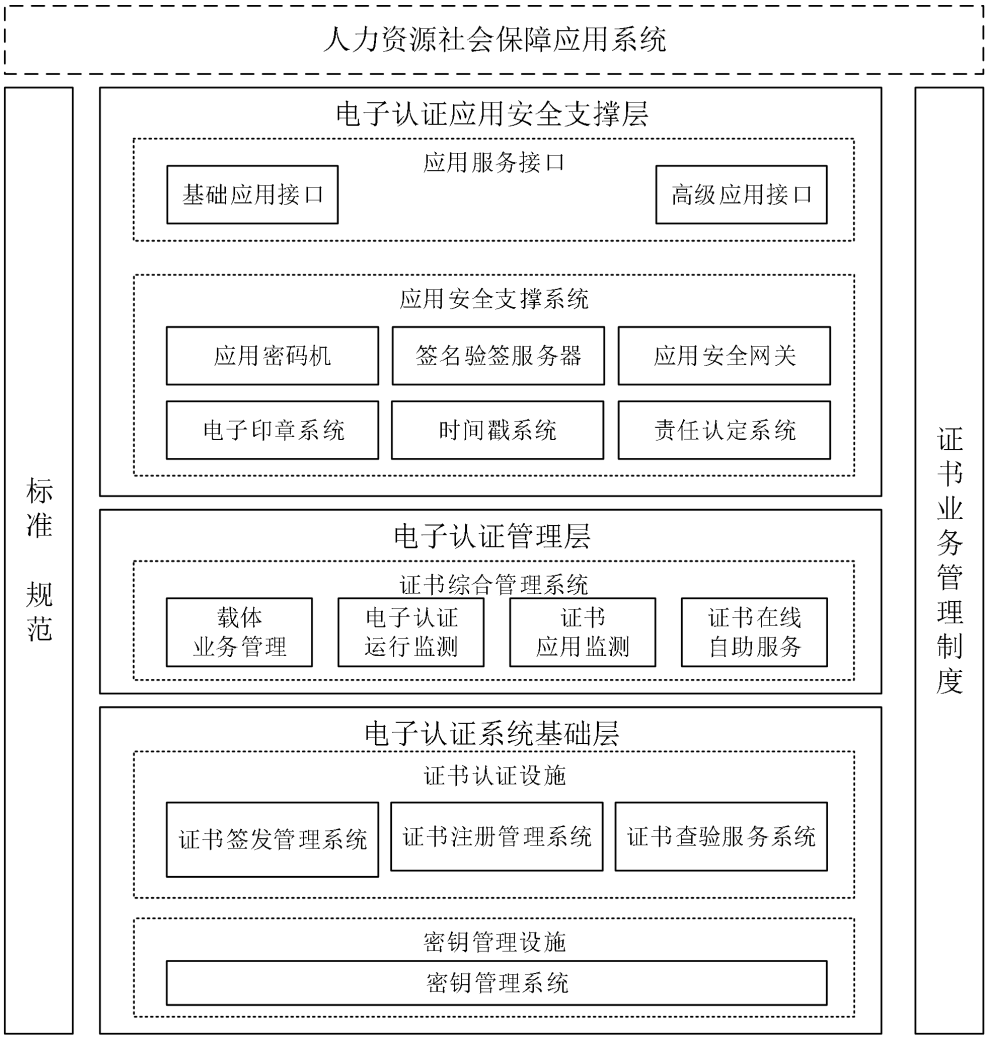

图 1　人力资源社会保障电子认证体系总体结构图

人力资源社会保障电子认证体系包含电子认证系统基础层、电子认证管理层、电子认证应用安全支撑层以及相关标准规范和证书业务管理制度。电子认证系统基础层包括密钥管理系统、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。电子认证管理层由证书综合管理系统组成，证书综合管理系统包括载体业务管理、电子认证系统运行监测、证书应用监测和证书在线自助服务等系统。电子认证应用安全支撑层由应用安全支撑系统和应用服务接口组成，其中，应用安全支撑系统主要包括应用密码机、签名验签服务器、应用安全网关、电子印章系统、时间戳系统、责任认定系统等；应用服务接口包括基础应用接口和高级应用接口，依赖于应用安全支撑系统进行密码运算。

7　电子认证系统基础层

7.1　概述

电子认证系统基础层是人力资源社会保障电子认证体系的基础设施，包括密钥管理设施和证书认证设施。密钥管理设施主要指密钥管理系统，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。

电子认证系统基础层各系统的具体技术规范应符合 LD/T 02.2 规定的要求，电子认证系统所签发的数字证书和 CRL 的格式应符合 LD/T 02.3 规定的要求，电子认证系统所采用的数字证书载体应符合

LD/T 02.5 规定的要求。

7.2 电子认证系统整体建设规划

人力资源社会保障电子认证系统建设应遵循以下总体策略：

a) 人力资源社会保障部：接入国家电子认证体系，以金保工程业务专网为依托建设人力资源社会保障行业 CA 和部级电子认证系统（业务 CA），为部本级和全国性应用系统提供电子认证服务；

b) 省级人力资源社会保障部门：以人力资源社会保障行业 CA 为依托，建设省级电子认证系统（业务 CA 或 RA），为省本级和省内应用系统提供电子认证服务；

c) 地市级人力资源社会保障部门：以省级电子认证系统为依托建设市级电子认证系统（RA 或证书注册点），作为省级电子认证系统的延伸，为本地市应用系统提供电子认证服务。

根据上述策略，人力资源社会保障电子认证系统总体建设规划如图 2 所示。

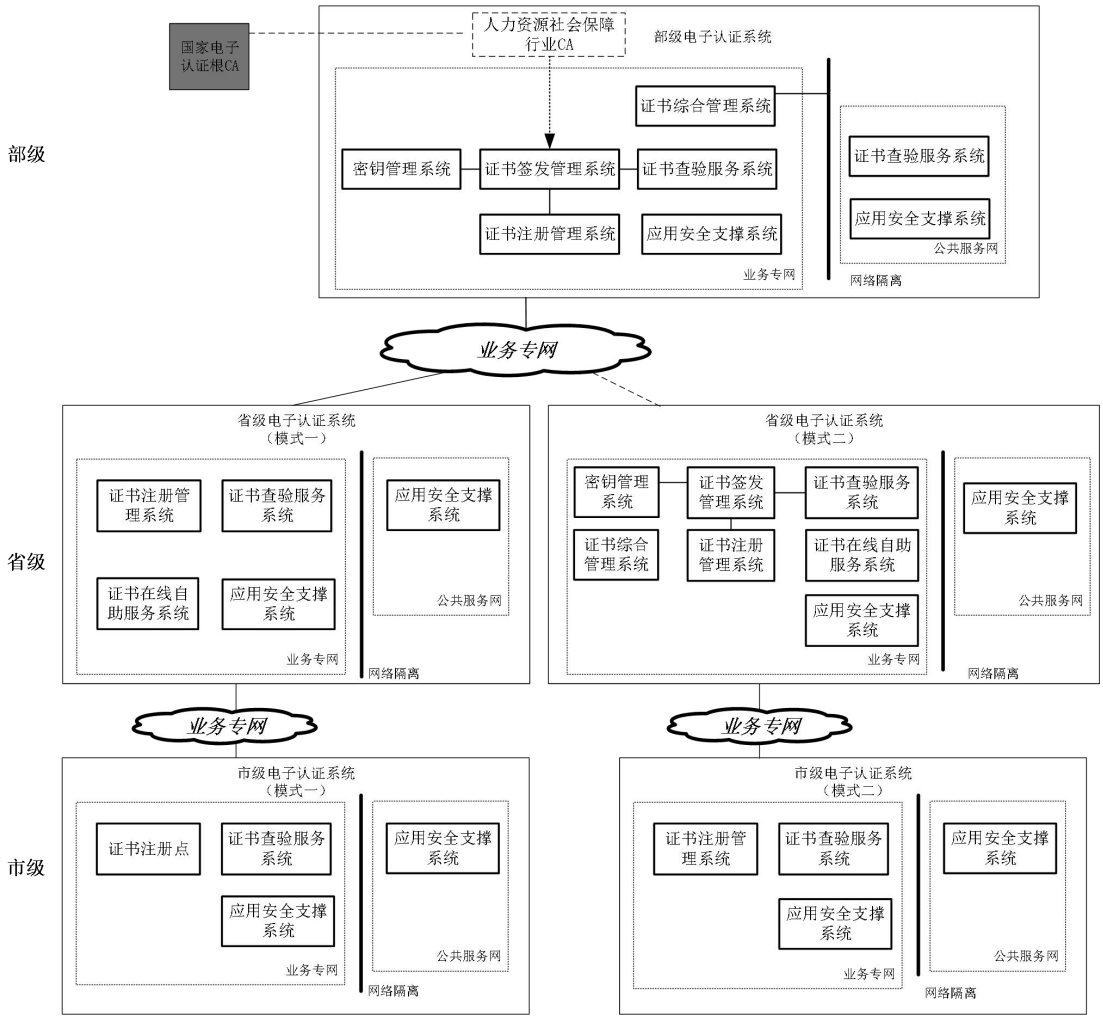

图 2 人力资源社会保障电子认证系统总体建设规划

7.3 部级电子认证系统

7.3.1 结构

部级电子认证系统的结构见图 3。

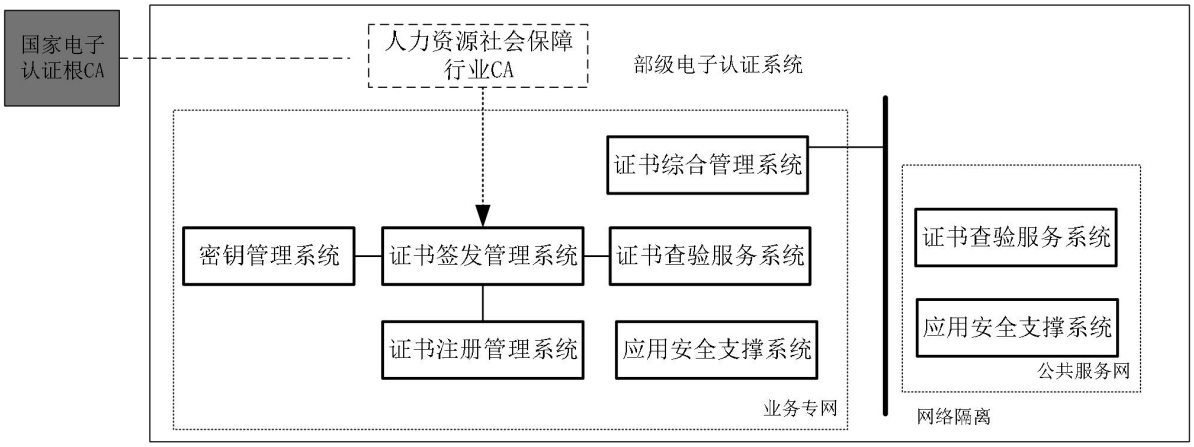

图 3　部级电子认证系统结构图

人力资源社会保障电子认证系统接入国家电子认证体系。在部级业务专网中，导入国家电子认证根CA为人力资源社会保障部签发的CA证书，并以此为基础建设部级电子认证系统（业务CA），主要包括：密钥管理系统、证书签发管理系统、证书注册管理系统、证书查验服务系统、证书综合管理系统以及应用安全支撑系统等。

在部级公共服务网中，建设证书查验服务系统和应用安全支撑系统。业务专网和公共服务网进行网络隔离，在安全控制的前提下，证书查验服务系统应实现主从系统的数据同步。

7.3.2　功能

人力资源社会保障行业 CA 主要功能包括：导入国家电子认证根 CA 证书、国家电子认证根 CA 为人力资源社会保障部签发的 CA 证书，签发业务 CA 证书，产生证书信任列表。

密钥管理系统对生命周期内的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、密钥恢复以及安全管理等。

证书签发管理系统提供对生命周期内的数字证书进行全过程管理的功能，主要功能包括：证书注册管理系统的管理，证书/证书撤销列表的生成、签发、存储、更新，并将证书/证书撤销列表发布到证书查验服务系统等。

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，主要功能包括：用户信息录入、修改、查询、审核以及用户证书下载等。

证书查验服务系统包括目录服务系统和证书状态查询系统，为用户和应用系统提供证书状态查询服务。目录服务系统应采用下推方式由主目录服务系统向从目录服务系统进行自动映射，实现数据同步，主要功能包括：证书/证书撤销列表的存储和发布。证书状态查询系统主要功能包括：证书状态查询服务，支持 CRL 查询和在线证书状态查询两种方式。

证书综合管理系统要求见 8.2。

应用安全支撑系统要求见 9.2。

7.3.3　性能

部级电子认证系统的基准性能要求：

a)　证书发放和管理能力（含第三代社会保障卡数字证书）不低于 1000 万张；

b)　可同时响应不低于 50 个 RA 系统的业务请求；

c)　证书签发速度不低于 50000 次/小时；证书注册申请不低于 30000 次/小时；SM2 密钥产生不低于 450 对/秒；

d)　密钥的保存期应大于 10 年；

e) 系统采用冗余设计，能够提供 7*24 小时不间断服务。

7.4 省级电子认证系统

7.4.1 结构

按照分步实施的建设原则，结合本地实际情况，省级电子认证系统可以选择以下两种建设模式：

a) 模式一：建设证书注册管理系统

在部级电子认证系统的基础上，在省级业务专网中建设省级证书注册管理系统。

省级证书注册管理系统作为部级电子认证系统的延伸，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。

省级电子认证系统（模式一）的结构见图 4。

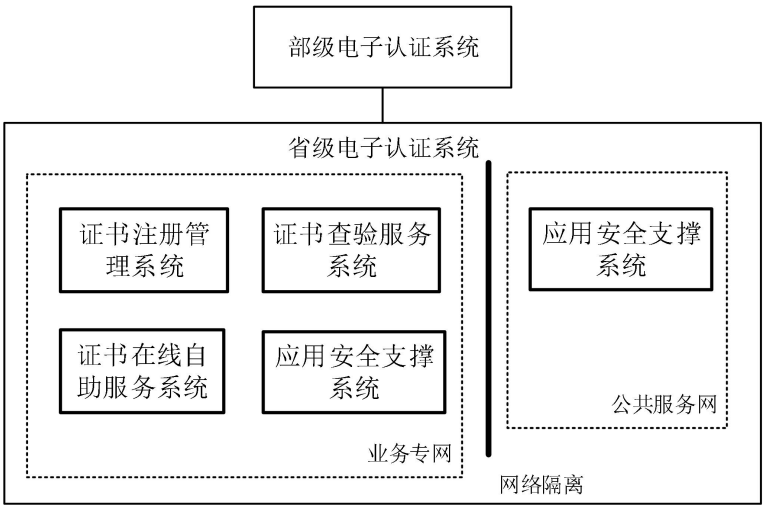

图 4 省级电子认证系统（模式一）结构图

省级电子认证系统（模式一）主要包括：证书注册管理系统、证书查验服务系统、证书在线自助服务系统。有第三代社会保障卡发放需求的省份，需建设证书注册管理前置机。

在业务专网和公共服务网中，按需建设应用安全支撑系统。

b) 模式二：建设省级电子认证系统

以部级电子认证系统为基础，在省级业务专网中建设省级电子认证系统。

省级电子认证系统向人力资源社会保障部提出申请，由部 CA 为其签发业务 CA 证书。省级电子认证系统为一个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，但需按照相关要求及时向部级电子认证系统提供数据。该模式须征得当地密码管理部门同意。

省级电子认证系统（模式二）的结构见图 5。

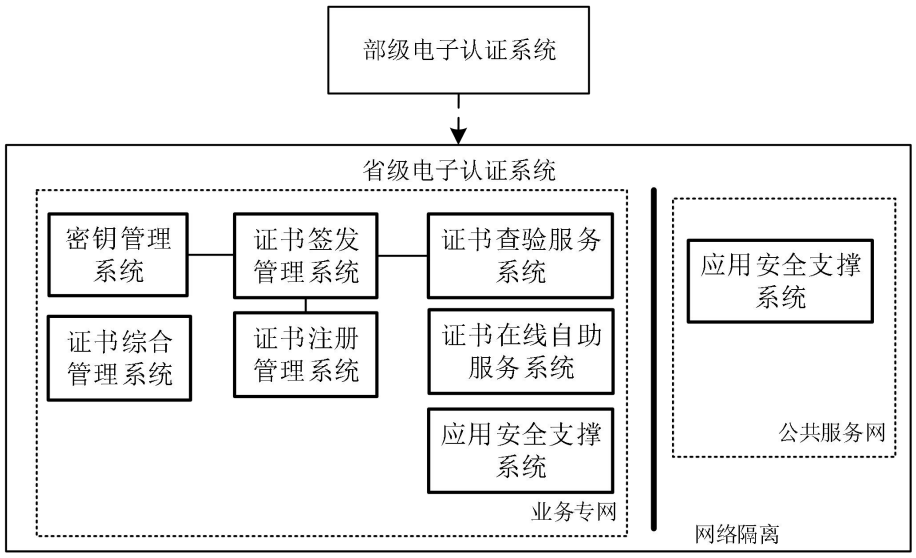

图 5　省级电子认证系统（模式二）结构图

省级电子认证系统（模式二）主要包括：密钥管理系统、证书签发管理系统、证书注册管理系统、证书综合管理系统、证书查验服务系统、证书在线自助服务系统等。有第三代社会保障卡发放需求的省份，需建设证书注册管理前置机。

在业务专网和公共服务网中，按需建设应用安全支撑系统。

7.4.2　功能

a)　省级电子认证系统（模式一）

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，主要功能包括：用户信息录入、修改、查询、审核以及用户证书下载等。

证书查验服务系统主要功能包括：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。

证书在线自助服务系统提供证书在线下载、在线更新、在线解锁等用户自助服务。

应用安全支撑系统要求见 9.2。

b)　省级电子认证系统（模式二）

密钥管理系统对生命周期内的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、密钥恢复以及安全管理等。

证书签发管理系统提供对生命周期内的数字证书进行全过程管理的功能，主要功能包括：证书注册管理系统的管理，证书/证书撤销列表的生成、签发、存储、更新，并将证书/证书撤销列表发布到证书查验服务系统等。

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，主要功能包括：用户信息录入、修改、查询、审核以及用户证书下载等。

证书查验服务系统主要功能包括：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。

证书在线自助服务系统提供证书在线下载、在线更新、在线解锁等用户自助服务。

证书综合管理系统要求见 8.2。

应用安全支撑系统要求见 9.2。

7.4.3 性能

省级电子认证系统（模式一）的基准性能要求：

a) 证书注册管理能力（含第三代社会保障卡数字证书）不低于 500 万张；
b) 证书注册申请不低于 30000 次/小时；
c) 系统采用冗余设计，能够提供 7*24 小时不间断服务。

省级电子认证系统（模式二）的基准性能要求：

a) 证书发放和管理能力（含第三代社会保障卡数字证书）不低于 1000 万张；
b) 可同时响应不低于 10 个 RA 系统的业务请求；
c) 证书签发速度不低于 50000 次/小时；证书注册申请不低于 30000 次/小时；SM2 密钥产生不低于 450 对/秒；
d) 密钥的保存期应大于 10 年；
e) 系统采用冗余设计，能够提供 7*24 小时不间断服务。

7.5 市级电子认证系统

7.5.1 结构

市级电子认证系统的结构见图 6。

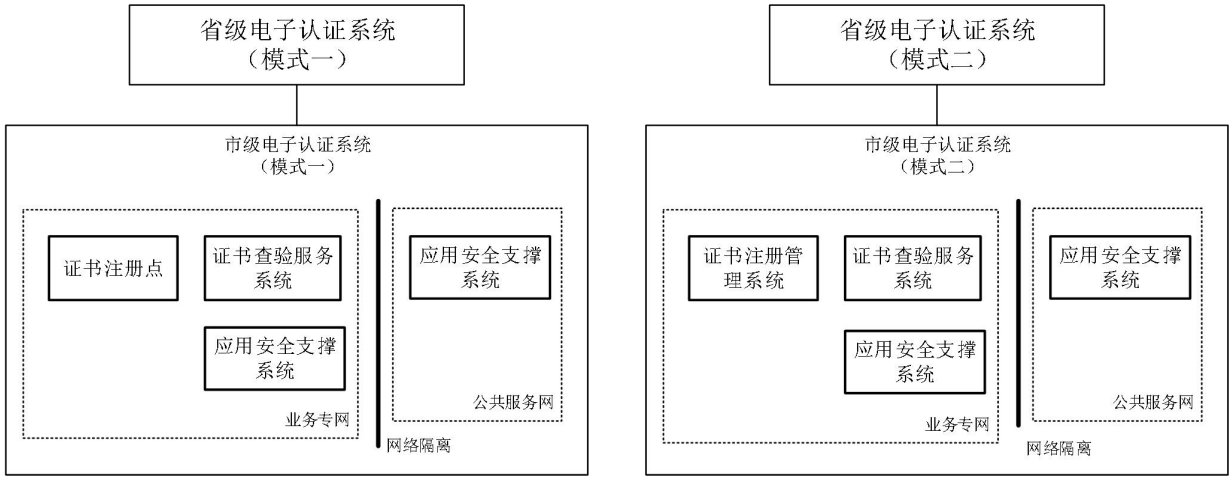

图 6 市级电子认证系统结构图

在省级电子认证系统的基础上，在市级业务专网中可选择以下两种模式建设。

a) 模式一：对应于省级模式一，在省级建设证书注册管理系统的基础上，按需建设证书注册点、证书查验服务系统以及应用安全支撑系统。
b) 模式二：对应于省级模式二，在省级建设业务 CA 系统的基础上，建设证书注册管理系统，按需建设证书查验服务系统和应用安全支撑系统。

7.5.2 功能

a) 市级电子认证系统（模式一）

证书注册点是证书注册管理系统的操作终端，是面向最终证书用户的服务窗口。主要功能包括：用户信息录入、审核、证书下载等。

证书查验服务系统主要功能包括：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和验证服务。

应用安全支撑系统要求见 9.2。

b) 市级电子认证系统（模式二）

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，主要功能包括：用户信息录入、修改、查询、审核以及用户证书下载等。

证书查验服务系统主要功能包括：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和验证服务。

应用安全支撑系统要求见 9.2。

7.5.3 性能

市级电子认证系统的基准性能要求：

a) 证书管理能力不低于 200 万张；

b) 系统采用冗余设计，能够提供 7*24 小时不间断服务。

8 电子认证管理层

8.1 概述

电子认证管理层由证书综合管理系统组成。证书综合管理系统包括载体业务管理、电子认证系统运行监测、证书应用监测和证书在线自助服务等系统。

8.2 证书综合管理系统

8.2.1 结构

证书综合管理系统的结构见图 7。

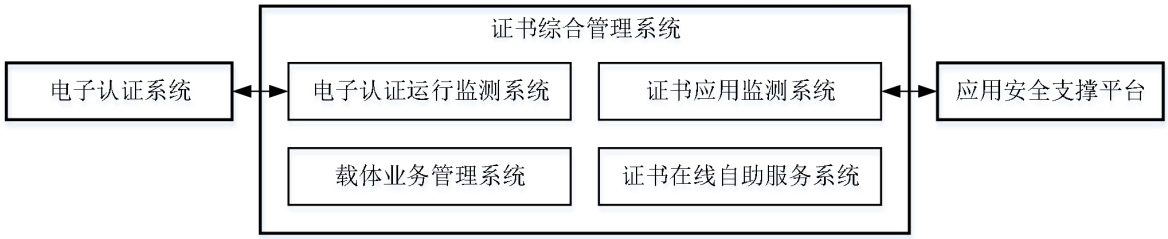

图 7 证书综合管理系统结构图

证书综合管理系统主要包括：载体业务管理系统、电子认证运行监测系统、证书应用监测系统和证书在线自助服务系统。

8.2.2 功能

载体业务管理系统负责数字证书载体从检测、入库、出库、使用、销毁全过程的管理，主要功能包括：证书载体出入库管理、载体检测、查询统计等。

电子认证运行监测系统负责监测电子认证系统和电子认证应用安全支撑平台运行状态，主要功能包括：电子认证系统运行状态采集、证书业务服务信息采集、电子认证应用支撑平台（主要指密码认证产品）设备运行状态采集和服务运行状态采集、故障报警和事件管理、系统管理等。

证书应用监测系统提供证书应用情况的分析，为证书应用提供决策支持，主要功能包括：证书应用情况管理接口服务、基础数据管理、证书应用情况统计分析、系统管理等。

证书在线自助服务系统主要面向证书用户提供证书在线下载、在线更新、在线解锁等自助服务。

9 电子认证应用安全支撑层

9.1 概述

电子认证应用安全支撑层是人力资源社会保障电子认证体系的重要组成部分，包括应用密码机、签名验签服务器、应用安全网关、电子印章系统、时间戳系统、责任认定系统等密码服务系统，通过应用服务接口面向人力资源社会保障应用系统提供身份认证、数字签名、数据加解密、时间戳、电子印章、责任认定等安全保障服务。其中，应用服务接口包括基础应用接口和高级应用接口。基础应用接口依赖于密码设备，为高级应用接口提供基础的、全面的密码服务。高级应用接口基于基础应用接口，以控件、COM 组件、Java 开发包、HTTPS restful 接口等形式为应用系统所调用，实现身份认证、数字签名、数据加解密为主要内容的安全应用。

9.2 密码服务系统

应用密码机应符合 GM/T 0030-2014、GB/T 36322-2018 规定的要求。

签名验签服务器应符合 GB/T 38629-2020 规定的要求。

应用安全网关应符合 GM/T 0026-2014、GM_T 0025-2014 规定的要求。

电子印章系统应符合 GB/T 38540-2020 和 LD/T 01-2022 规定的要求。

时间戳系统应符合 GM/T 0033-2014 规定的要求。

9.3 基础应用接口

基础应用接口是基于密码设备，直接对密码设备进行管理和操作的接口层，向高级应用接口提供标准化的密码服务。基础应用接口分为服务器端密码设备接口和证书载体接口两类，其中，数字证书载体接口包括智能密码钥匙接口和第三代社会保障卡读写终端接口。

9.4 高级应用接口

高级应用接口是基于基础应用接口，供应用系统直接调用的数字证书应用接口。高级应用接口应由 CA 系统承建商提供。

高级应用接口包括客户端应用接口和服务器端应用接口。

a） 客户端应用接口

根据数字证书载体类型，客户端应用接口分为两类。

数字证书载体为智能密码钥匙时，客户端应提供跨浏览器支持组件、ActiveX 控件、动态链接库、JAR 等开发包，客户端应用接口符合 LD/T 02.4 规定的要求。

数字证书载体为第三代社会保障卡时，客户端应提供 ActiveX 控件或 DLL 动态连接库，客户端应用接口符合 LD/T 33 规定的要求。

b） 服务器端应用接口

根据功能及接口形态不同，服务器端应用接口分为 COM 组件、Java 组件和应用安全支撑服务接口。

COM 组件、Java 组件主要提供身份认证、数字签名、数据加解密等功能，应用系统服务器端直接调用密码设备时，集成该接口。

应用安全支撑服务接口主要提供身份认证、数字签名、数据加解密、时间戳、电子印章、责任认定等功能，应用安全支撑服务接口形态为 HTTP restful，应用系统服务器端调用应用安全支撑平台时，集成该接口。其中，身份认证服务接口、数字签名服务接口、数据加解密服务接口，符合 LD/T 02.4 规定的要求；电子印章服务接口，符合 LD/T 01.4-2022 要求。