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 03—2022

人力资源社会保障
电子认证服务管理规范

Specification for human resources and social security electronic certification service management

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。

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。

本文件主要起草人：马丹蕾、张嵩、王岩、耿建军、唐淑静、韩晓颖、张博、李笑男、于斌、魏丽丽、郭丽芳、高五星。

人力资源社会保障电子认证服务管理规范

1 范围

本文件规定了电子认证服务的人员管理、证书业务管理、数字证书应用服务、系统运行管理、业务保障等方面的要求。

本文件适用于人力资源社会保障电子认证服务的提供与管理。

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 2887 计算机场地通用规范

GB/T 9361 计算机场地安全要求

GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式

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 50174 数据中心设计规范

BMB 3-1999 处理涉密信息的电磁屏蔽室的技术要求和测试方法

LD/T 01.4-2022 人力资源社会保障电子印章体系 第4部分：系统接口规范

LD/T 33 社会保障卡读写终端规范

LD/T 02-2022（所有部分） 人力资源社会保障电子认证体系规范

3 术语和定义

GB/T 25056、GB/T 35289 界定的以及下列术语和定义适用于本文件。

3.1

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］

3.2

电子认证 electronic authentication

采用电子技术检验用户真实性的操作。

[来源：GB/T 35289-2017，3.2]

3.3

电子认证服务 electronic certification service

为电子签名相关各方提供真实性、可靠性验证的活动。

［来源：GB/T 35289-2017，3.6］

3.4

证书申请人 certificate applicant

从电子认证服务机构接收证书的实体。

[来源：GB/T 35289-2017，3.9]

4 总则

人力资源社会保障数字证书使用和管理应遵循“统一规划、统一标准、集中管理、分级受理、一证多用和互信互认”原则，并符合 LD/T 02-2022 规定的要求。

5 人员管理

5.1 概述

数字证书管理机构应配备专人负责数字证书业务管理，数字证书业务人员应经过身份、背景、专业资格等背景审查过程，同时应签订保密协议。

5.2 资格与经历

所有担任认证系统管理的人员应签订保密承诺书，要求充当可信角色的人员政治素质高、思想上进、对工作敬业、做事认真负责、处理问题公正严明、业务技术合格、无同行业重大错误记录、无违法记录等。

5.3 背景调查

可信人员应接受并通过背景情况调查，调查程序包括：

a) 调查员工的个人资料，包括：履历、家庭背景、最高学历毕业证书、学位证书、资格证及身份证等相关有效证明；
b) 工作部门对使用员工进行考核观察；
c) 审查通过后，可正式上岗工作。

5.4 配置与职责

电子认证系统应设置下列管理和操作人员。

a) 超级管理员：

负责电子认证系统的策略设置，设置各子系统的业务管理员并对其管理的业务范围进行授权。

b) 审计管理员：

负责对审计员进行管理和监督。

c) 审计员：

负责对涉及系统安全的事件和各类管理和操作人员的行为进行审计和监督。

d) 业务管理员：

负责电子认证系统的某个子系统的业务管理，设置本子系统的业务操作员并对其操作的权限进行授权。

e) 业务操作员：

按其权限进行具体的业务操作。

f) 安全管理员：

全面负责系统的安全工作，包括：

1) 制定电子认证系统的安全策略；
2) 指导电子认证系统的安全管理；
3) 设计和指导电子认证系统的安全策略实施；
4) 对电子认证系统的安全管理进行定期的检查和评估；
5) 对安全策略和执行程序的日常维持；
6) 定期对相关人员开展安全教育。

5.5 轮岗

对于可替换角色，应根据业务的安排进行工作轮换。轮换的周期和顺序，应依据实际工作需求确定。

5.6 培训

对数字证书管理机构工作人员，按照其岗位和角色安排不同的培训。培训内容主要包括认证系统操作过程、软硬件配置、安全管理规范以及安全意识和他们未来工作中将使用到的软件。

对数字证书管理机构工作人员，其认证系统的相关知识与技能，每年应总结一次并由数字证书管理机构组织培训。技术的进步、系统功能更新或新系统的加入，都应对相关人员进行培训。

认证策略调整、系统更新时，应对全体人员进行再培训，以适应新的变化。

5.7 对未授权行为的处罚

当员工被怀疑，或者已进行了未授权的操作，例如滥用权利或超出权限使用认证系统或进行越权操作，得知情况属实后应立即对该员工进行工作隔离，随后对该员工的未授权行为进行评估，并根据评估结果对该员工进行相应处罚和采取相应的防范处理措施。

6 证书业务管理

6.1 证书分类

人力资源社会保障数字证书主要包括机构证书、人员证书、设备证书和持卡人证书等类型。

a) 机构证书——面向人力资源社会保障系统内部机构（包括各级人力资源社会保障部门、各类经办机构、公共服务机构、街道社区人力资源社会保障服务站、所等）、服务于人力资源社会保障业务的系统外机构（包括人力资源社会保障事务代理机构等），以及人力资源社会保障业务所管理服务的企事业单位发放。
b) 人员证书——面向人力资源社会保障业务专网计算机终端用户（包括各级人力资源社会保障部门工作人员、经办人员等）发放。
c) 设备证书——面向人力资源社会保障信息系统的服务器、终端设备等发放。
d) 持卡人证书——面向第三代社会保障卡持卡人发放。

6.2 业务规则

电子认证业务规则应当包括责任范围、作业操作规范、信息安全保障措施等事项。

6.3 服务事项

数字证书管理机构应制定证书服务规范，建立证书服务流程，按照人力资源社会保障电子认证服务机构认证业务规则办理相关业务。

数字证书管理机构应当提供如下服务：

a) 数字证书的申请、签发、更新、撤销等证书生命周期管理服务，用户加密密钥的生成、备份和恢复等服务；
b) 数字证书信息查询及状态信息查询服务；
c) 数字证书统计、查询、下载等支持服务，以及数字证书应用集成支持服务；
d) 为数字证书用户提供使用支持；
e) 提供数字证书相关培训服务。

6.4 业务流程

6.4.1 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，填写《数字证书申请表》（见附录A），提交数字证书信息资料。其中，设备证书申请时，应通过密码设备产生PKCS#10证书请求文件，并随《数字证书申请表》一并提交。

证书申请信息应当真实、完整和准确，证书申请人对其申请信息实质内容的真实性负责。

数字证书用户所在单位或部门负责证书信息真实性、准确性的审核，提交当地数字证书管理机构办理数字证书登记。

审核通过后，本地数字证书管理机构依据业务规则受理证书申请，进行证书签发。

数字证书签发完成后，数字证书管理机构通过机要邮寄、专人派送或现场领取的方式，将密封好的数字证书存储介质及清单交付给证书申请人。证书申请人履行签字等义务后，即完成证书交付。

证书申请服务流程如图 1所示。

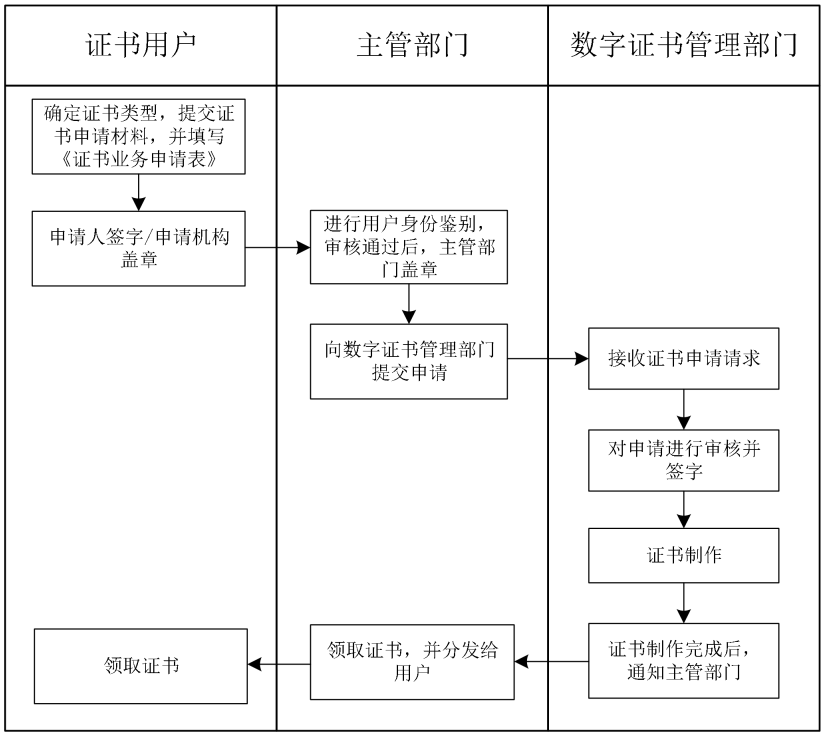

图 1 数字证书申请服务流程图

证书申请流程如下：

a) 申请人/申请单位/申请机构根据所要申请的证书类型，填写相应的证书申请表；用户在申请证书时，应如实填写《证书业务申请表》（见附录A.1~A.3），并按照申请表要求提交相关材料；个人用户应提供身份证等身份证明材料，单位用户应提供统一社会信用代码证书等证明材料；
b) 申请人在《证书业务申请表》上签字或申请单位/申请机构在《证书业务申请表》上盖章；
c) 在办理证书时，应严格鉴别用户真实身份，确保用户的申请材料真实、准确、齐全，并同时具有业务系统的相关权限；在完成身份鉴别后，由申请人/申请单位/申请机构所在主管部门盖章；
d) 主管部门盖章后，将证书申请提交给数字证书管理部门进行审核；
e) 数字证书管理部门接收证书申请要求；
f) 数字证书管理部门对证书申请审核并签字；
g) 全部审核通过后，开始制证。工作人员办理数字证书时，应按《证书业务申请表》上的信息如实录入电子认证系统，为用户分配证书载体并下载数字证书。数字证书下载成功后，工作人员应安全保管好用户申请表和相关资料的复印件；
h) 证书制作好之后，通知主管部门领取；
i) 主管部门领取数字证书并分发给证书用户；
j) 完成证书交付后，证书用户应妥善保管证书载体，并按照规定的操作流程进行使用。

用户领取数字证书后，应及时更改保护口令；在使用过程中，应定期更改保护口令；如忘记口令，或连续输入错误口令导致数字证书被锁死，用户应及时向部省市数字证书管理机构报告，由部省市数字证书管理机构负责处理。

6.4.2 证书更新

人员证书、机构证书和设备证书的证书有效期一般为5年，持卡人证书的证书有效期一般为10年。数字证书持有人应在证书有效期满之前通过本地数字证书管理机构办理更新业务。

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。

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。

在线自助更新流程如图 2 所示。

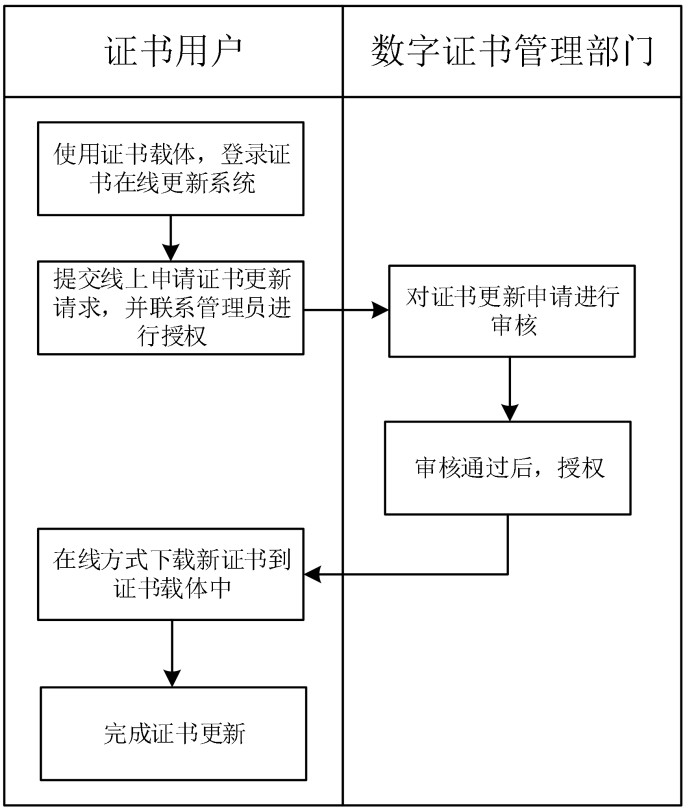

图 2　证书在线自助更新流程图

在线自助更新流程如下：

1) 证书用户使用证书载体登录证书在线更新系统；
2) 在线提交证书更新申请，并联系管理员进行授权；
3) 管理员对证书更新申请进行审核；
4) 审核通过后，管理员进行授权；
5) 授权成功后，证书用户以在线方式下载新证书到证书载体内；
6) 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。

人工更新流程如图 3所示。

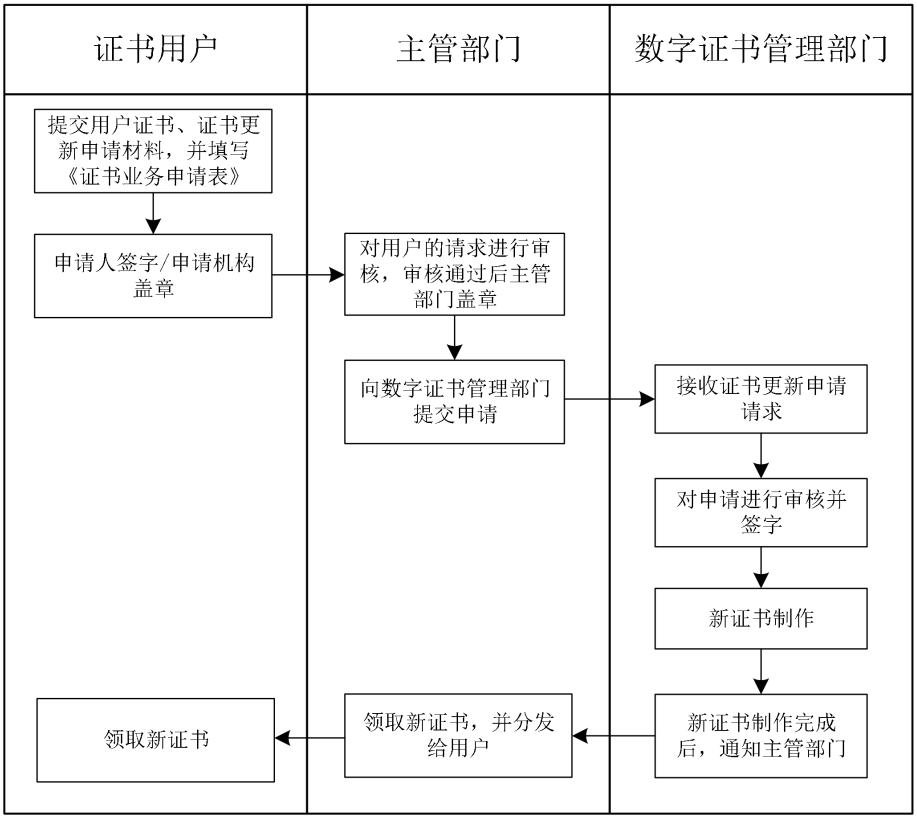

图 3　证书更新人工更新流程图

人工更新流程如下：

1) 申请人/申请单位/申请机构提交用户证书及证书更新申请相关材料，并按照要求填写《证书业务申请表》（见附录 A.1~A.3）；
2) 申请人在《证书业务申请表》上签字或申请单位/申请机构在《证书业务申请表》上盖章；
3) 申请人/申请单位/申请机构所在主管部门对证书更新申请进行审核，审核通过后在证书更新申请表上盖章；
4) 向数字证书管理部门提交证书申请；
5) 数字证书管理部门接收主管部门提交上来的证书更新申请；
6) 数字证书管理部门对证书更新申请审核并签字；
7) 全部审核通过后，开始制作新证书；
8) 新证书制作完成后，通知主管部门领取证书；
9) 由主管部门领取新证书，并分发给证书用户；
10) 证书用户在领取新证书后，应妥善保管证书载体，并按照规定的操作流程进行使用。

6.4.3　证书变更

当证书用户信息发生变更时，用户应到证书注册点申请变更证书信息。

证书变更按照证书更新流程执行，见6.4.2。

当用户证书载体丢失或损坏时，应重新申请数字证书，此时应按照首次证书申请流程执行，见6.4.1。

6.4.4　证书撤销

发生下列情形之一的，数字证书持有人应申请撤销或者变更数字证书：

a) 数字证书私钥泄露；

b) 数字证书中的信息发生重大变更；
c) 认为本人不能实际履行本行业电子认证有关规定的义务；
d) 辞职或调动工作岗位。

发生下列情形之一的，部省市数字证书管理机构应撤销其签发的数字证书：

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

证书撤销的办理流程如图 4所示。

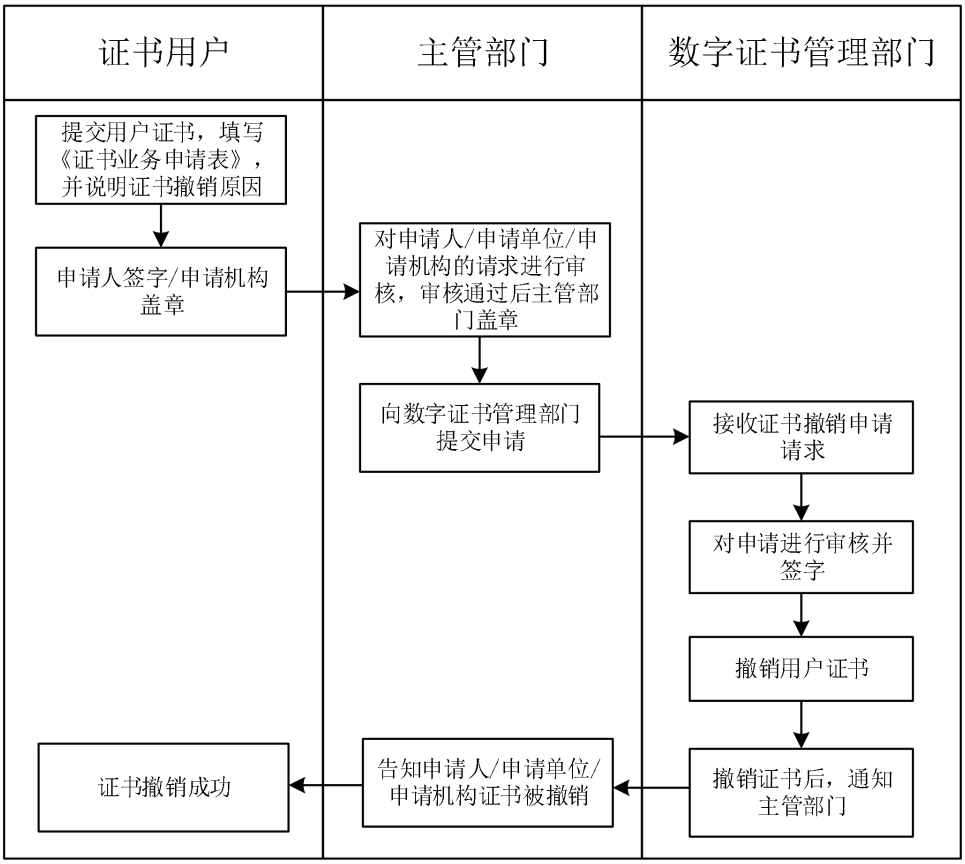

图 4 数字证书撤销服务流程图

证书撤销的办理流程如下：

a) 证书用户到证书注册点提交用户证书，填写《证书业务申请表》（见附录 A.1~A.3），并说明证书撤销原因；
b) 申请人在《证书业务申请表》上签字或申请单位/申请机构在《证书业务申请表》上盖章；
c) 主管部门对申请人/申请单位/申请机构提交的请求进行审核，确保其身份是真实有效的；审核通过后，申请人/申请单位/申请机构所在主管部门盖章；
d) 将证书撤销申请提交到数字证书管理部门；
e) 数字证书管理部门接收证书撤销申请；
f) 数字证书管理部门对收到的证书撤销申请进行审核并签字；

g) 全部审核通过后，撤销申请人/申请单位/申请机构证书；24 小时内将申请人/申请单位/申请机构证书签发到 CRL，并发布到证书查验服务系统；
h) 撤销证书后，通知主管部门；
i) 主管部门应及时通知申请人/申请单位/申请机构证书被撤销；
j) 证书撤销成功。

当证书用户违反法律法规或因其他原因无法承担数字证书相关责任时，证书注册机构可对用户证书进行强制撤销，撤销后及时告知该用户。

6.4.5 密钥恢复

6.4.5.1 服务要求

证书持有人的签名密钥对由用户的密码设备（如智能密码钥匙）生成，加密密钥对由密钥管理中心（KMC）生成。证书持有人的签名私钥由自己妥善保管，不做备份。加密密钥在KMC备份并能够恢复。

密钥恢复是指加密密钥的恢复，KMC不负责签名密钥的恢复。密钥恢复分为证书持有人密钥恢复和司法密钥恢复两类。

a) 证书持有人密钥恢复：当证书持有人的密钥损坏或丢失后，某些密文数据将无法还原，此时证书持有人可申请密钥恢复。证书持有人向部信息中心申请密钥恢复，经审核后，通过认证系统向KMC请求；密钥恢复模块接受证书持有人的恢复请求，恢复证书持有人的密钥并下载到持有者的证书存储介质中。
b) 司法密钥恢复：司法取证人员向部信息中心申请，经审核后，由密钥恢复模块恢复所需的密钥并记录于特定存储介质中。

6.4.5.2 证书持有人密钥恢复

证书载体丢失或损坏，应通过密钥恢复解密曾经加密的数据。

密钥恢复时，证书用户应提交真实、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 5所示。

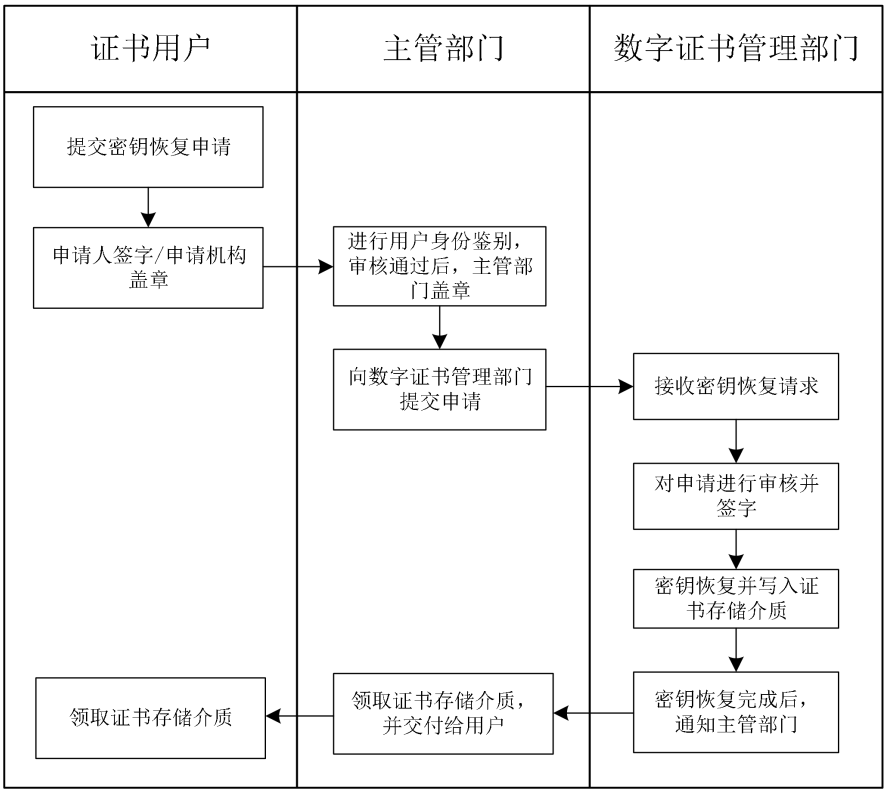

图 5　密钥恢复服务流程图

密钥恢复流程如下：

a) 申请人/申请单位/申请机构填写密钥恢复申请，用户应如实填写《证书载体解锁申请表》（见附录A.4）；

b) 申请人在《证书载体解锁申请表》上签字或申请单位/申请机构在《证书载体解锁申请表》上盖章；

c) 在办理密钥恢复时，主管部门应严格鉴别用户真实身份，确保用户的申请材料真实、准确、齐全。在完成身份鉴别后，由申请人/申请单位/申请机构所在主管部门盖章；

d) 主管部门将密钥恢复申请提交给数字证书管理部门进行审核；

e) 数字证书管理部门接收密钥恢复申请；

f) 数字证书管理部门对密钥恢复申请信息审核，并签字；

g) 全部审核通过后，开始密钥恢复申请；工作人员办理密钥恢复业务时，应按照密钥恢复申请材料上的信息如实录入电子认证系统，恢复证书用户的密钥并下载到证书存储介质中；密钥恢复完成后，数字证书管理机构应安全保管好用户申请表和身份证明材料等；

h) 密钥恢复完成之后，通知主管部门；

i) 由主管部门领取证书存储介质，并交付给证书用户；

j) 证书用户在领取证书存储介质后，应妥善保管并按照规定的操作流程进行使用。

6.4.5.3　司法密钥恢复

司法密钥恢复应有以下两方人员同时在场参与：

a) 有司法恢复权限的密钥管理中心业务操作员 ；

b) 司法取证人员。司法取证人员应持有能证明其身份的数字证书和能进行数字签名的密码硬件(如智能密码钥匙)。

司法密钥恢复流程如图 6 所示。

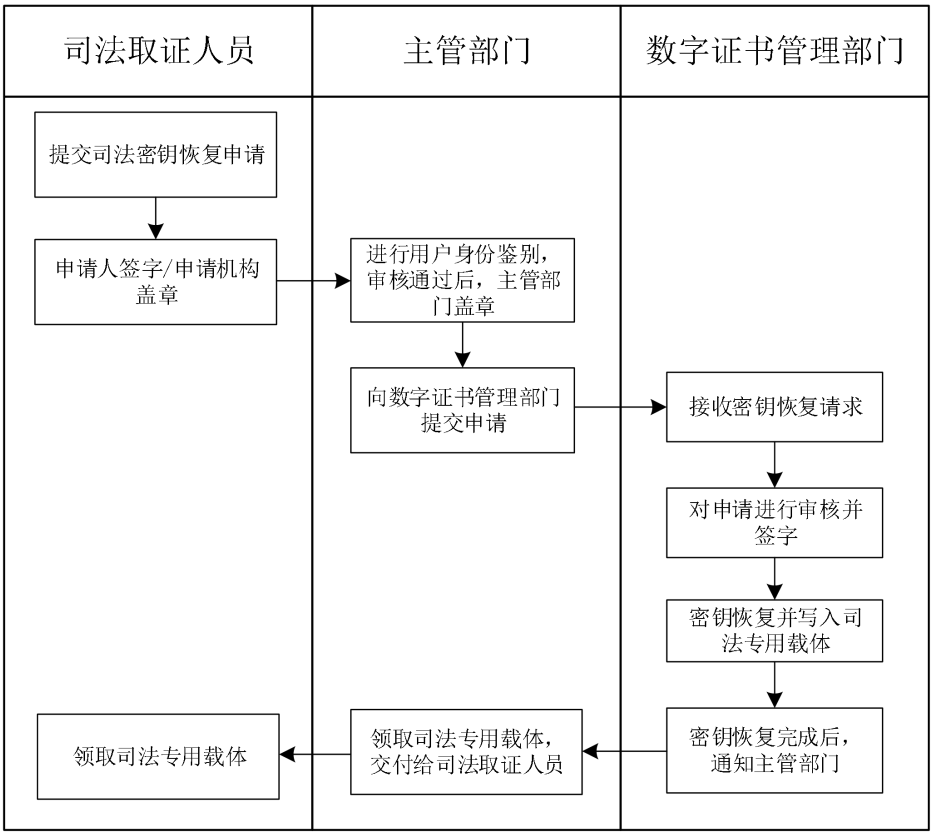

图 6　司法密钥恢复服务流程图

司法密钥恢复流程如下：

a) 司法取证人员填写司法密钥恢复申请，应如实填写《证书载体解锁申请表》（见附录A.4）；
b) 司法取证人员在《证书载体解锁申请表》上签字或申请单位/申请机构在《证书载体解锁申请表》上盖章；
c) 在办理密钥恢复时，主管部门应严格鉴别司法取证人员真实身份，确保司法取证人员的申请材料真实、准确、齐全；在完成身份鉴别后，由申请人/申请单位/申请机构所在主管部门盖章；
d) 主管部门将司法密钥恢复申请提交给数字证书管理部门进行审核；
e) 数字证书管理部门接收司法密钥恢复申请；
f) 数字证书管理部门对司法密钥恢复申请信息审核，并签字；
g) 全部审核通过后，开始司法密钥恢复申请；工作人员办理司法密钥恢复业务时，应按照司法密钥恢复申请材料上的信息如实录入电子认证系统，恢复加密密钥对并下载到司法专用载体中；司法密钥恢复完成后，数字证书管理机构应安全保管好司法密钥恢复申请表和身份证明材料等；
h) 司法密钥恢复完成之后，通知主管部门；
i) 由主管部门领取司法专用载体，并交付给司法取证人员。

6.4.6　信息发布

电子认证系统在签发证书、更新证书后，应及时将证书发布到数据库和目录服务系统中。在证书撤销后，应将 CRL 及时发布到目录服务系统中，用户或应用系统可通过证书查验系统查询证书的撤销情况。

6.4.7 持卡人证书业务流程

6.4.7.1 模式分类

第三代社保卡加载数字证书，是将持卡人证书写入第三代社保卡非对称认证系统环境个人化的过程。

第三代社保卡非对称认证系统环境个人化包括：卡商批量写入数字证书、个人化中心批量写入数字证书、快速发卡系统写入数字证书、服务窗口或持卡人自助写入证书和服务窗口申请并写入数字证书五种可选模式，由发卡地区根据现有条件自行选择其中一种模式或多种模式。不同的个人化模式，其持卡人证书业务流程不同。

6.4.7.2 模式一：卡商批量写入数字证书

模式一适用于批量制卡并由卡商进行个人化的情况，其具体流程如图7所示。

a) 完成卡体印制后，卡商首次个人化时，触发社保卡生成签名公私钥，并按照《第三代社会保障卡非对称认证应用制卡数据流转流程（试行）》有关格式要求整理并提交申请数据（含签名公钥及其他信息）。
b) 发卡地区人力资源社会保障部门将接收到的申请数据与发卡数据进行比对，比对无误后，将申请数据发送给省市级RA。
c) 省市级RA将申请数据上传给上一级CA，由上一级CA统一签发数字证书并下发至省市级RA。
d) 省市级RA获取数字证书后，经由发卡地区人力资源社会保障部门回传给卡商。
e) 卡商在获取数据后进行二次个人化，匹配签名密钥与数字证书后，将含数字证书的所有个人化数据写入社保卡，修改非对称认证系统环境主控密钥和管理员PIN，即完成卡片的个人化。

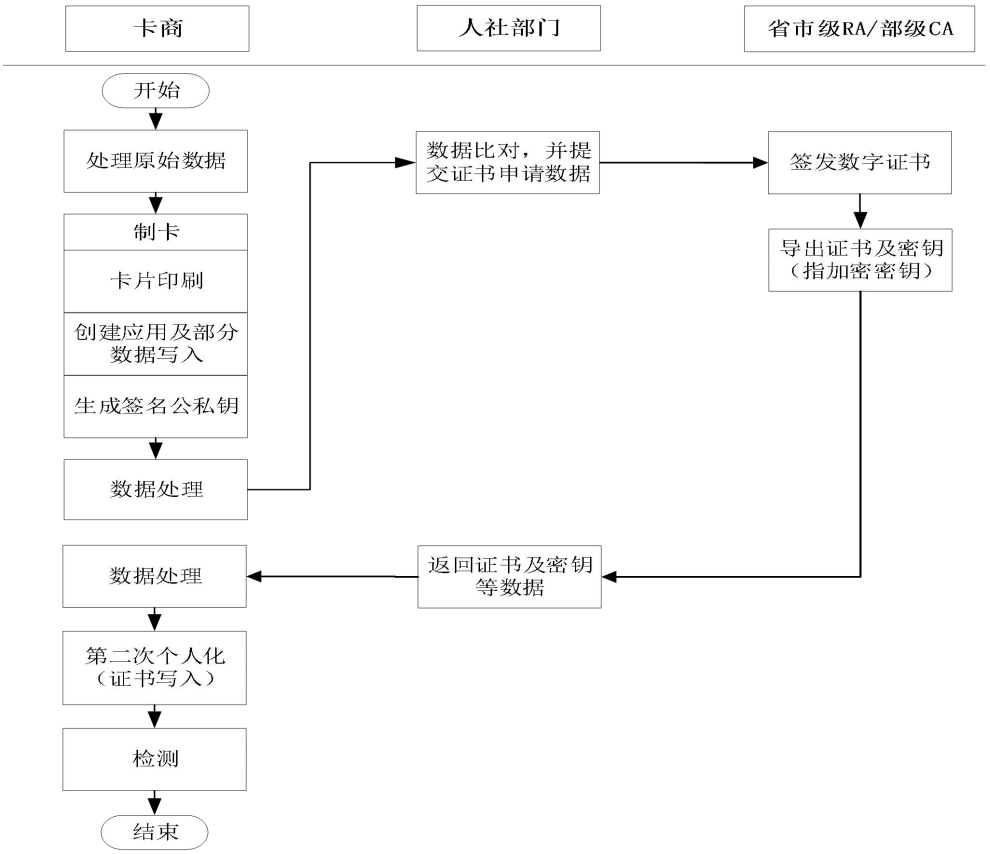

图 7 模式一：卡商批量写入数字证书的流程

6.4.7.3 模式二：个人化中心批量写入数字证书

模式二适用于批量制卡并由个人化中心进行个人化的情况，其具体流程如图8所示。

a) 第1步同模式一，卡商将半成品卡片和申请数据移交到发卡地区人力资源社会保障部门。
b) 发卡地区人力资源社会保障部门将接收到的申请数据与发卡数据进行比对，比对无误后，将申请数据发送给省市级RA。
c) 省市级RA将申请数据上传给上一级CA，由上一级CA统一签发数字证书并下发至省市级RA。
d) 省市级RA获取数字证书后，经由发卡地区人力资源社会保障部门回传给个人化中心。
e) 个人化中心进行签名密钥与数字证书的匹配，将含数字证书的所有个人化数据写入社保卡，修改非对称认证系统环境主控密钥和管理员PIN，以及进行社会保障系统环境主控密钥和应用密钥替换，即完成卡片的个人化。

说明：如果个人化中心没有数据准备系统，应在个人化中心现有系统中新增该功能模块。

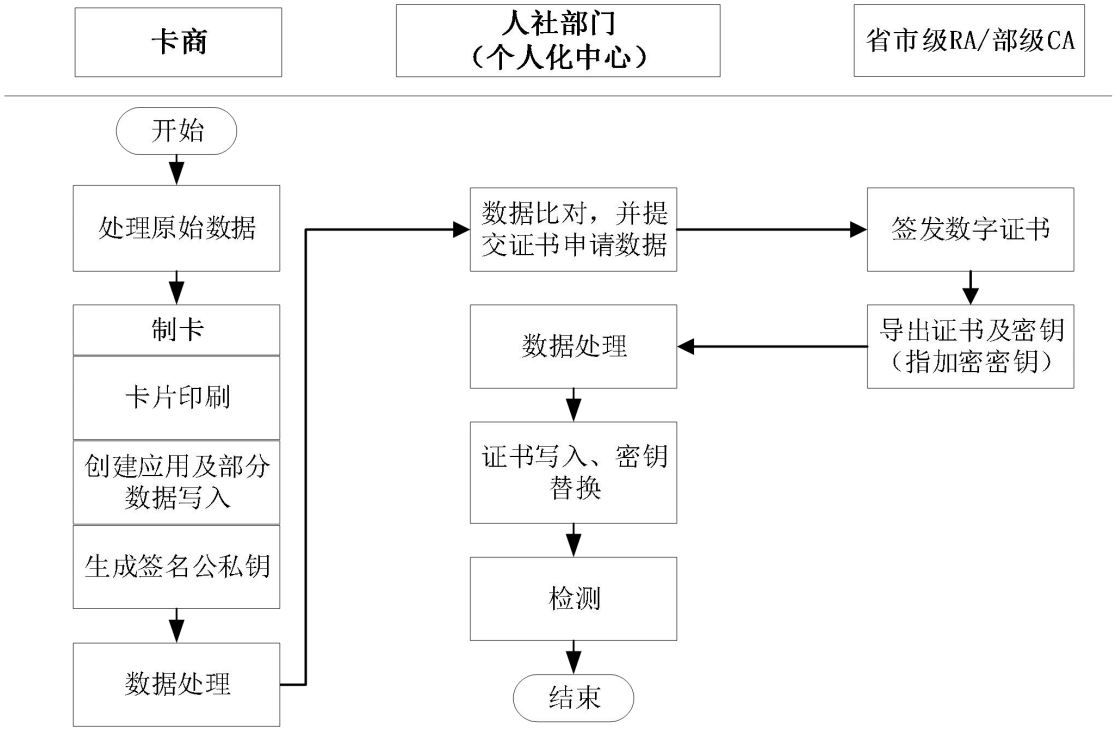

图 8 模式二：个人化中心批量写入数字证书的流程

6.4.7.4 模式三：快速发卡系统写入数字证书

模式三适用于零星制卡、补/换发卡并由快速发卡系统进行个人化的情况，其具体流程如图9所示。

a) 卡商完成卡体印制和部分应用个人化后，形成预制卡。
b) 前台受理发卡请求，快速发卡系统触发社保卡生成签名公私钥，并将申请数据上传给省市级RA。
c) 省市级RA受理申请后，将申请数据上传给上一级CA，由上一级CA统一签发数字证书并下发至省市级RA。基于快速发卡系统的时效性，数字证书的申请、签发和下发等工作应实时处理。
d) 省市级RA将签发好的数字证书返回给快速发卡系统。
e) 快速发卡系统进行签名密钥与数字证书的匹配，将含数字证书的所有个人化数据写入社保卡，修改非对称认证系统环境主控密钥和管理员PIN，即完成卡片的个人化。

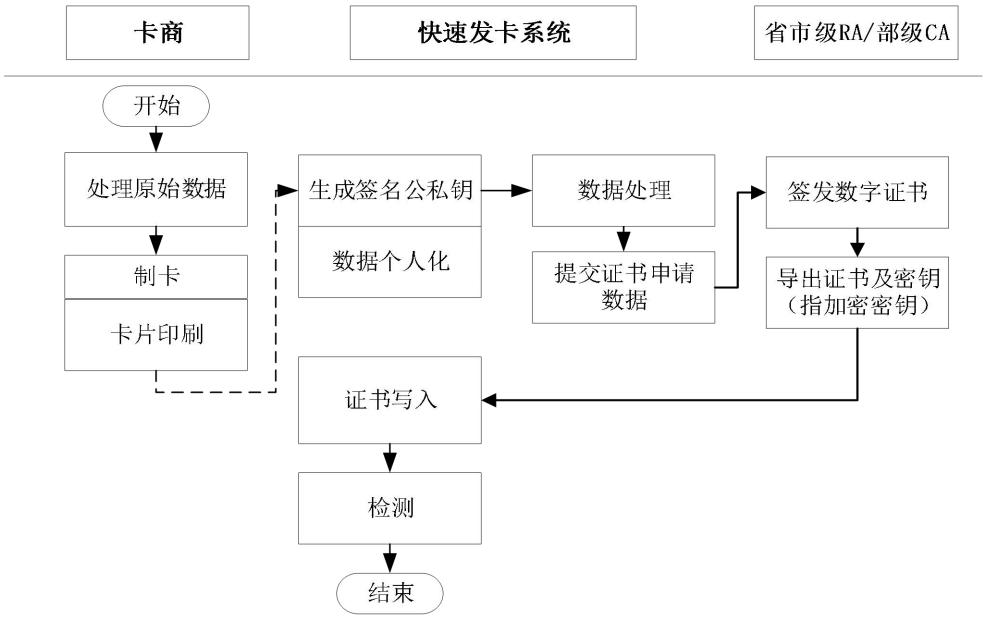

图 9　模式三：快速发卡系统写入数字证书的流程

6.4.7.5　模式四：服务窗口或持卡人自助写入数字证书

模式四适用于先行在发卡期间完成卡片个人化、后台证书生成，后续在应用期间完成数字证书个人化的情况，其具体流程如图10所示。

a）　第1步同模式一。

b）　第2步同模式一。

c）　第3步同模式一。

d）　第4步同模式一或二（选择模式一或二取决于卡商还是个人化中心进行个人化）。

e）　持卡人可通过服务窗口工作人员、经办大厅的自助终端、PC端自助设备等途径下载写入数字证书，也可直接访问证书在线自助服务系统完成数字证书的下载写入。

说明：在该模式下，需配置社保卡读写终端，并只能通过CA中间件方式写入数字证书。

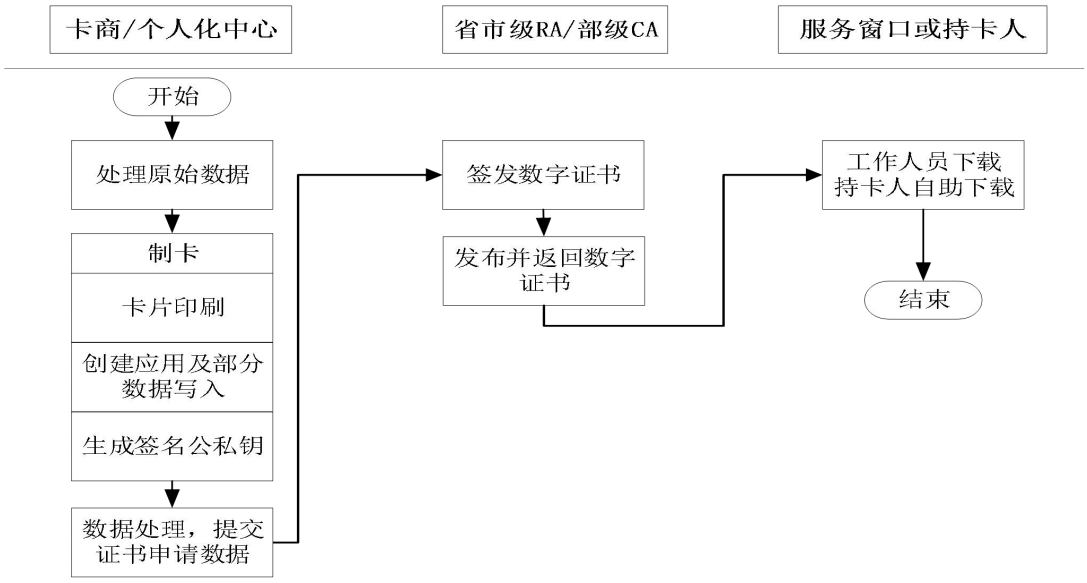

图 10　模式四：服务窗口或持卡人自助写入数字证书的流程

6.4.7.6 模式五：服务窗口申请并写入数字证书

模式五适用于地市发卡未做非对称认证应用数据加载，由服务窗口申请并写入数字证书的情况，其具体流程如图11所示。

该模式是应急方案，卡商在创建应用时，仅完成非对称认证系统环境的初始化，数字证书的申请及写入全部由服务窗口完成。

a) 卡商完成卡体印制和部分应用个人化，对于非对称认证系统环境，只建立文件结构，而不产生签名公私钥。服务窗口触发社保卡生成签名公私钥，并将申请数据上传给省市级RA。

b) 省市级RA受理申请后，将申请数据上传给上一级CA，由上一级CA统一签发数字证书，并将证书下发至省市级RA。

c) 省市级RA将签发好的数字证书返回给服务窗口。

d) 服务窗口将含数字证书的所有个人化数据写入社保卡，替换非对称认证系统环境主控密钥和管理员PIN，即完成卡片的个人化。

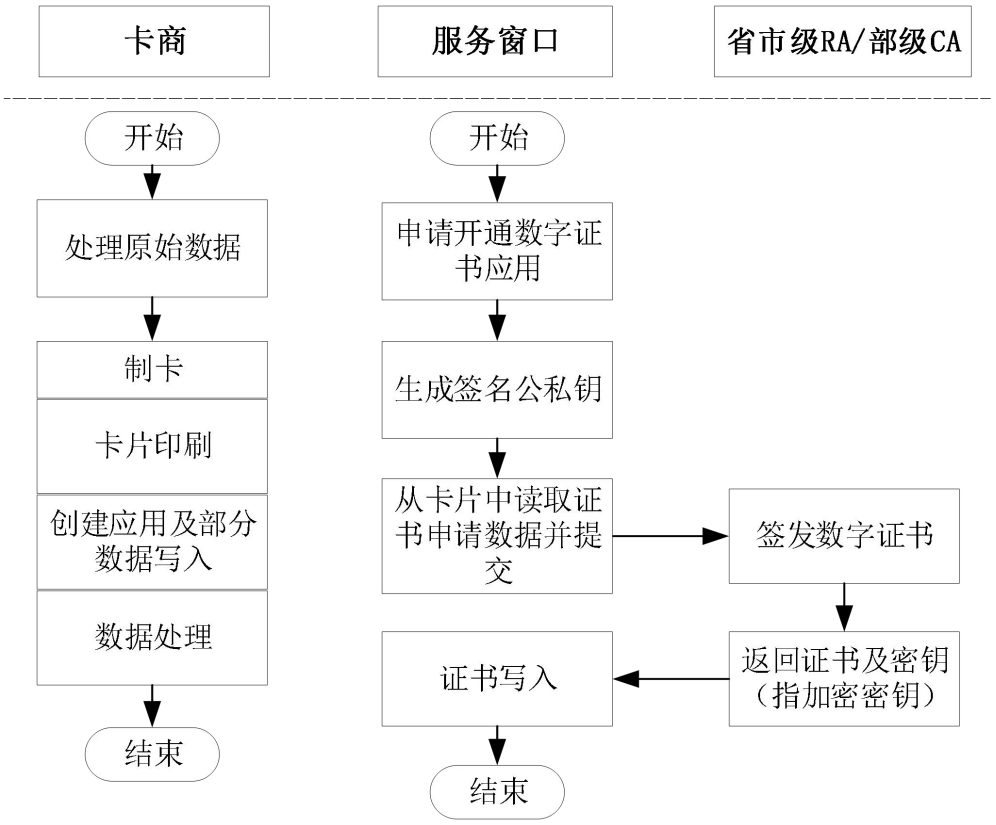

图 11 模式五：服务窗口申请并写入数字证书的流程

6.5 资料管理

6.5.1 证书资料管理

部省市数字证书管理机构应满足以下证书资料管理要求：

a) 数字证书原始资料、更新资料以及审核通过后的资料的管理；

b) 数字证书发放资料的管理；

c) 用户信息注册表和数字证书撤消列表的审核与备案资料的管理；

d) 只允许指定专人负责本机构数字证书资料的收集、更新与管理，并及时提交更新后的数字证书资料。

6.5.2 信息保存年限

部省市数字证书管理机构应当采用符合国家相关法律法规要求的载体，完整记录、妥善保存数字证书业务申请材料、与认证相关的信息，并承担保密责任，不得泄露或遗失，信息保存期至少为证书失效后5年。

6.5.3 信息保密要求

部省市数字证书管理机构应当按照《电子政务电子认证服务管理办法》等的规定，建立完善的保密制度，履行保密义务，并接受有关职能部门的监督指导。

除法律法规另有规定外，部省市数字证书管理机构及其工作人员不得泄露下列信息：

a) 数字证书持有人的身份信息；
b) 数字证书持有人委托认证机构保管的数字证书密钥。

6.6 数字证书管理

6.6.1 证书介质保管

数字证书使用单位应当加强证书管理，指导并要求证书持有人妥善保管数字证书介质及其密钥，未经明确授权，不得随意转借他人使用。

出现数字证书介质丢失或损坏等异常情况时，证书持有人应当立即联系数字证书管理机构进行妥善处理。

数字证书介质按照“专人专用”、“谁持有，谁负责”的原则进行管理，原则上不得转借他人使用。

6.6.2 PIN 码保护

数字证书持有人应保护好数字证书，及时更改数字证书初始保护密码。如果怀疑密码失密、数字证书信息有所改变、数字证书丢失等，应及时报告单位联系人，并通过单位联系人到数字证书管理机构办理变更等相关手续。

7 数字证书应用服务

7.1 证书应用安全功能

基于数字证书的应用安全功能包括身份认证、数据加密解密、数字签名验签等基本证书应用安全功能，以及统一身份认证、电子印章、时间戳和责任认定等增强证书应用安全功能。

7.2 证书应用安全要求

等级保护第三级以上（含三级）的人力资源社会保障重要信息系统须采用密码技术保障系统应用和数据安全，二级信息系统可根据自身安全防护需求采用密码技术保障系统应用和数据安全，具体包括：

a) 对于处于同一网络环境多个彼此独立、管理分散的应用系统，应建立统一身份认证管理机制；
b) 所有三级系统应提供基于数字证书的用户身份认证功能，实现对登录用户及通信实体的身份鉴别，确保用户及通信实体身份的真实性；
c) 所有三级系统应提供数据加密、解密的功能，实现对信息系统重要数据的数据加密存储，确保存储过程中的数据机密性；
d) 所有三级系统应提供数字签名与验签功能，实现对重要数据的数字签名，确保数据完整性；
e) 所有三级系统应提供基于数字证书的数据加密功能实现对重要业务操作的数据加密，或采用SSL、IPSec 等安全协议实现数据通道加密，确保其在传输过程中的数据机密性；

f) 所有三级系统应提供数字签名与验证功能实现对重要数据的数字签名保护，或采用 SSL、IPSec 等安全协议实现数据通道完整性保护，确保其在传输过程中的数据完整性；
g) 所有三级系统应提供数字签名与验签功能，实现对重要数据的数字签名，确保其在存储过程中的数据完整性；
h) 对交易时间有明确要求，需要可信、准确、标准时间的业务系统，宜提供时间戳功能，实现对业务时间敏感业务的可信时间服务，确保操作时间的不可否认性；
i) 对需要明确操作责任的业务系统，宜提供责任认定功能，实现对实体在网络中的操作行为进行证据保留；
j) 对业务表单和文档需要显性凭证的业务系统，宜提供电子签章功能，实现对业务表单和文档的电子印章显性凭证，确保签章行为的不可否认性。

7.3 证书应用服务支持

7.3.1 证书应用服务管理

数字证书管理机构参与用户的业务系统安全需求分析，并指导证书应用部分的开发和实施。

业务系统明确安全需求分析后，填写《电子认证应用登记表》，签字后提交给主管部门进行审核，审核通过后签字盖章，正式提交给数字证书管理部门。

数字证书管理部门对用户提交的资料进行复核，审核通过后进行应用集成的指导实施。

7.3.2 证书应用接口程序

数字证书管理机构提供统一的人力资源社会保障证书应用接口程序供应用系统调用和集成，包括客户端应用接口和服务端应用接口。

a) 客户端应用接口

数字证书载体为智能密码钥匙（USBKey）时，提供跨浏览器支持组件、ActiveX 控件、动态链接库、JAR 等开发包，供应用系统调用和集成。该接口应符合 LD/T 02.4-2022 规定的要求。

数字证书载体为第三代社会保障卡时，提供 ActiveX 控件或 DLL 动态连接库，供应用系统调用和集成。该接口应符合 LD/T 33 规定的要求。

b) 服务器端应用接口

提供 COM 组件、Java 组件和 HTTP restful 三种形态的接口，供应用系统调用和集成。

应用系统服务器端直接调用密码设备时，集成 COM 组件、Java 组件，实现身份认证、数字签名、数据加解密功能。COM 组件、Java 组件接口应符合 LD/T 02.4-2022 规定的要求。

应用系统服务器端调用应用安全支撑平台时，集成 HTTP restful 接口，实现身份认证、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应符合 LD/T 02.4-2022 以及 LD/T 01.4-2022 规定的要求。

7.3.3 技术支持服务

提供向用户解释电子认证应用架构方面的问题、接口实现问题、软件部署问题，以及关于集成标准规范问题。

8 系统运行管理

8.1 管理制度

电子认证系统相关管理制度包括电子认证系统运行场所进出管理制度、用户信息保密制度、电子认证服务工作人员管理制度、机房安全管理制度等。

各级数字证书管理机构在制定管理制度时，应按国家有关标准执行。

8.2 安全操作与维护规范

8.2.1 系统管理

系统管理的操作与维护规范应包括以下内容：

a) 对电子认证系统进行任何操作之前，应充分考虑并预计操作之后的结果，每次操作都应记录；
b) 改变系统的配置，应制订实施计划和相关文档说明，经上级领导批准后才能进行操作，操作时应有双人在场；
c) 系统出现故障时，应由系统管理人员检查处理，其它人员不经批准不得处理故障；
d) 不经批准不得在服务器上安装任何软件和硬件；
e) 不经批准不得删除服务器上的任何文件。

8.2.2 数据备份

数据备份的操作与维护规范应包括以下内容：

a) 系统升级后，应立即进行全备份；
b) 对数据变化量大的服务器，应每天做一次增量备份，每周做一次全备份；
c) 对数据变化量少的服务器，可每周做一次备份；
d) 对重要数据应准备两套备份，其中异地存放一套；
e) 对数据库的备份应单独进行；
f) 对重要的目录应单独进行备份；
g) 手工进行的备份，应在介质上标明备份的服务器及路径；
h) 自动进行的备份，应将备份介质有效区分；
i) 选择的备份介质应能保证数据的长期可靠，否则应定期更新。

8.2.3 口令管理

口令管理规范应包括以下内容：

a) 口令长度应为 8 个字符以上，应是字母、数字和特殊字符组成的混合体，口令不得采用有特殊意义的（如姓名、生日、电话号码等）数字和词组，以及连续或者相同的数字；
b) 规定口令的使用期限并定期更换；
c) 口令应妥善保管，防止泄漏；
d) 检查网络设备、主机和应用程序中是否设置有缺省口令或缺省用户名，找出并禁止。

8.2.4 应急处理

各级数字证书管理机构应制订应急处理预案，当出现重大故障或灾难性事故时，应启动预定的应急处理方案进行处理。

应急处理预案应根据事件的严重程度、紧急程度和事件类别，分别规范告警、报告、保护、处置、善后、总结等处理流程和处置措施。

系统恢复正常运行后，应对应急处理过程进行总结，总结中应详细记录事件起因、处理过程、经验教训、改进建议等。

应针对应急事件处理中暴露的问题，不断完善和修改应急处理预案。

8.3 安全管理要求

8.3.1 物理安全

a) 电子认证系统的建筑物及机房建设应按照国家密码管理相关政策要求，并按照下列标准实施：
   1) GB/T 9361；
   2) GB/T 2887；
   3) GB 50174；
   4) BMB3-1999。
b) 电子认证系统机房按功能分成不同区域，如：公共区、服务区、管理区和核心区，各区的功能和分区原则应符合 GB/T 20518-2018 等有关标准。所有进入电子认证系统机房的人员应使用身份识别卡，进入核心区和管理区还需同时使用人体特征鉴别方式。人员进出机房应有日志记录。核心区应为屏蔽机房，应加装高强度的钢制防盗门，所有进出屏蔽室的线路都应采取防电磁泄露措施，屏蔽效果达到 BMB3-1999 中 C 级要求。
c) 电子认证系统机房应设置安全监控室、系统监控室、配电室和消防器材室。安全监控室应对所有进出人员实行监控，只有安全管理人员同时使用身份识别卡和人体特征鉴别才可以进入，刷卡离开。系统监控室和配电室，只有相应的授权人员使用身份识别卡或人体特征鉴别才可以进入，刷卡离开。消防器材室建议使用身份识别卡进入。

8.3.2 制度安全

a) 应制定密码安全管理制度及操作规范、安全操作规范。密码安全管理制度应包括密码建设、运维、人员、设备、密钥等密码管理相关内容。
b) 应定期对密码安全管理制度的合理性和适用性进行审定，对存在不足或需要改进的安全管理制度进行修订。
c) 应明确相关管理制度发布流程。

8.3.3 人员安全

a) 应了解并遵守密码相关法律法规。
b) 应能够正确使用密码产品。
c) 根据相关密码管理政策、数据安全保密政策，结合组织实际情况，设置密钥管理人员、安全审计人员、密码操作人员等关键岗位；建立相应岗位责任制度，明确相关人员在安全系统中的职责和权限，对关键岗位建立多人共管机制；密钥管理、安全审计、密码操作人员职责，互相制约互相监督，相关设备与系统的管理和使用账号不得多人共用。
d) 建立可信人员及所有工作人员动态管理清单，包括岗位定义、背景调查内容和程序。
e) 在授权相关人员接触本单位重要资料前，证明其可信性，并签署保密协议。
f) 建立每个职位的工作范围及其责任，并确定每个重要职位的可信性要求。
g) 建立培训制度及培训档案，对于涉及密码的操作和管理以及密钥管理人员进行专门培训。
h) 建立人员异动管理制度，工作人员离职后应立即删除其相应的权限。

8.3.4 系统安全

应采取防火墙、病毒防治、漏洞扫描、入侵监测、数据备份、双机热备、灾难恢复等安全防护措施，保障网络、主机系统、应用系统及数据库运行的安全。

8.3.5 通信安全

应采取通信加密、安全通信协议等安全措施，保障电子认证系统各子系统之间、证书签发管理系统与密钥管理系统之间、证书签发管理系统与证书注册管理系统之间的通信安全。

8.3.6 密钥安全

应使用硬件密码设备采取密钥管理安全协议、密钥存取访问控制、密钥管理操作审计等多种安全措施，保障电子认证系统中所使用的密钥在其生成、存储、使用、更新、废除、归档、销毁、备份和恢复整个生命周期中的安全。

a) 密钥安全的基本要求是：
   1) 密钥的生成和使用应在硬件密码设备中完成；
   2) 密钥的生成和使用应有安全可靠的管理机制；
   3) 存在于硬件密码设备之外的所有密钥应加密；
   4) 密钥应有安全可靠的备份恢复机制；
   5) 对密码设备操作应由多个操作员实施。
b) 密码机的密钥安全除了满足基本要求外，还应满足下列要求：
   1) 密码机的密钥应采用（3，5）秘密共享机制将密钥份额分享给 5 个分管者保管，保存分割后的密钥的人员称为分管者；
   2) 密码机生成密钥时，应先选定分管者。选定的分管者应分别用自己输入的口令保护分管的密钥份额，分管的密钥份额应存放在硬件载体中。硬件载体也应备份，并安全存放；
   3) 恢复密码机的密钥时，由 5 个分管者中任意 3 个将各自保管的份额输入密码机，在密码机中恢复。
c) 证书载体的密钥安全除了满足基本要求外，还应满足下列要求：
   1) 证书载体密钥的产生和使用应在证书载体中完成；
   2) 密钥的生成和使用应有安全可靠的管理机制；
   3) 口令长度为 8 个字符以上；
   4) 管理员账号和普通用户账号要严格分类管理。
d) 密钥分管要求：

CA 和 KMC 的根密钥应用密钥分割或秘密共享机制分割备份出来，分别交予分管者保管。恢复时，到场的分管者的人数应满足恢复所需的人数。

分管者的选择条件如下：

a) 分管者应符合可信人员策略规定的条件；
b) 符合下列条件之一者，不能成为分管者：
   1) 本证书认证系统的超级管理员；
   2) 本证书认证系统的业务管理员；
   3) 本证书认证系统的业务操作员；
   4) 本证书认证系统的系统维护人员。

8.3.7 证书管理安全

证书的管理安全应满足下列要求：

a) 验证证书申请者的身份；
b) 防止非法签发和越权签发证书，通过审批的证书申请应提交给证书签发管理系统，由证书签发管理系统签发与申请者身份相符的证书；

c) 保证证书管理的可审计性，对于证书的任何处理都应作日志记录。通过对日志文件的分析，可以对证书事件进行审计和跟踪。

8.3.8 安全审计

电子认证系统在运行过程中涉及大量功能模块之间的相互调用，以及各种管理员的操作，对这些调用和操作应以日志的形式进行记载，以便用于系统错误分析、风险分析和安全审计等工作。

a) 功能模块调用日志

电子认证系统内的各功能模块在运行过程中会调用其他功能模块或被其他功能模块所调用，对于这些相互之间的功能调用，各模块应该记录如下数据：

1) 调用请求的接收时间；
2) 调用请求来自的网络地址；
3) 调用请求发起者的身份；
4) 调用请求的内容；
5) 调用请求的处理过程；
6) 处理结果等。

b) 业务管理员审计

业务管理员的下列操作应被记录：

1) CA 证书加载；
2) 证书撤销列表加载；
3) 证书撤销列表更新等；
4) 系统配置；
5) 权限分配。

c) 业务操作员审计

业务操作员的下列操作应被记录：

1) 证书请求批准；
2) 证书请求拒绝；
3) 证书请求分配；
4) 证书撤销；
5) 证书更新；
6) 密钥恢复。

8.3.9 应用安全

系统选用经国家密码管理部门核准的密码产品。

8.4 服务提供

各级数字证书管理机构应对用户提供全面、及时、有效的服务，保证用户在证书使用过程中出现的问题能及时得到响应和解决。

服务的过程应作详细记录。

9 业务保障

9.1 服务保障

数字证书管理机构应当建立电子认证系统信息安全保障机制，针对相关资产、人员、物理环境和软件系统等制订安全策略及管理制度，采取有效的安全保障措施，并对安全策略的执行情况进行有效的监督检查，确保运行服务安全可靠，满足电子认证系统信息系统业务连续性要求。

9.2 技术检测

部信息中心委托具有商用密码产品认证资质的专业机构进行密码机及相关设备、数字证书载体、认证应用接口等电子认证相关技术符合性检测。

各级数字证书管理机构应当严格遵守有关保密等法律法规规定，按要求采用密码技术，并定期开展密码应用安全性评估，确保信息系统运行安全和数据安全。

9.3 监督检查

部信息中心通过技术手段收集、汇总数字证书发放、应用和服务质量反馈等信息，综合掌握人社系统电子认证服务的整体应用情况。

附 录 A
（资料性）
证书业务申请表

表A.1~表A.4规定了人力资源社会保障数字证书业务申请表的样式。

表 A.1 人员证书业务申请表

请选择业务类型，在对应的栏目中打“√”
□ 证书申请 □证书更新 □ 证书撤销
申请人信息
姓名：---------- 性别：□ 男 □ 女 身份证号：□□□□□□□□□□□□□□□□□□ 所在省份/城市：---------- 通信地址：---------- 邮政编码：□□□□□□ 电子邮件：---------- 联系电话：---------- 所属单位及部门：---------- 职 务：----------
用户须知： 1. 人员证书的有效期为 5 年，自证书签发之日起计算，请在证书失效期前 20 日内提出证书更新申请。 2. 本人承诺此表所填写内容真实有效。 申请人（签字）: 日期：--------年----月----日
以下由审核单位填写
主管部门（盖章）: 日期：--------年----月----日
委托办理部门 审核人（签字）: 日期：--------年----月----日
数字证书管理部门 审核人（签字）: 日期：--------年----月----日

表 A.2 机构证书业务申请表

请选择业务类型，在对应的栏目中打“√”
□ 证书申请　　□证书更新　　□ 证书撤销
机构信息
机构名称：---------- 所在省份/城市：---------- 通信地址：----------　邮政编码：□□□□□□ 组织机构代码证：□□□□□□□□—□
联系人信息
姓名：----------　　职　　务：---------- 电子邮件：----------　联系电话：----------
用户须知： 1. 机构证书的有效期为 5 年，自证书签发之日起计算，请在证书失效期前 20 日内提出证书更新申请。 2. 本机构承诺此表所填写内容真实有效。 申请机构（盖章）: 日期：--------年----月----日
以下由审核单位填写
委托办理部门 审核人（签字）:　　日期：--------年----月----日
数字证书管理部门 审核人（签字）:　　日期：--------年----月----日

表 A.3 设备证书业务申请表

请选择业务类型，并在对应的栏目中打“√”
☐ 证书申请　　☐证书更新　　☐ 证书撤销
设备信息
设备名称：----------　　放置地址：---------- 设备用途：---------- 所在省份/城市：----------所属单位/部门：---------- MAC 地址：----------　　IP 地址：----------
联系人信息
姓名：----------　　职　　务：---------- 电子邮件：----------　　联系电话：---------- 通信地址：----------　　邮政编码：☐☐☐☐☐☐
用户须知： 1. 设备证书的有效期为 5 年，自证书签发之日起计算，请在证书失效期前 20 日内提出证书更新申请。 2. 本单位承诺此表所填写内容真实有效。 申请单位（盖章）: 日期：--------年----月----日
以下由审核单位填写
委托办理部门 审核人（签字）:　　日期：--------年----月----日
数字证书管理部门 审核人（签字）:　　日期：--------年----月----日

表 A.4 证书载体解锁申请表

申请人信息
姓名：----------　　性别：□ 男　　□ 女 身份证号：□□□□□□□□□□□□□□□□□□ 所在省份/城市：---------- 通信地址：----------　　邮政编码：□□□□□□ 电子邮件：----------　　联系电话：---------- 所属单位及部门：----------　　职　　务：---------- 证书载体编号：□□□□□□□□□□□□
用户须知： 1. “证书载体编号”是证书载体 USBKEY 背面印制的 16 位数字。 2. 本人承诺此表所填写内容真实有效。 申请人（签字）：　　日期：--------年----月----日
以下由审核单位填写
主管部门（盖章）： 日期：--------年----月----日
委托办理部门 审核人（签字）：　　日期：--------年----月----日
数字证书管理部门 审核人（签字）：　　日期：--------年----月----日

参考文献

[1] GB/T 35289-2017　信息安全技术 电子认证服务机构服务质量规范
[2] 电子政务电子认证服务业务规则规范
[3] 电子政务电子认证服务管理办法