人力资源社会保障电子印章 总体技术架构（试行）

1 范围

本标准规定了人力资源社会保障电子印章体系的总体框架结构、系统组成和建设要求。
本标准适用于指导部省市人力资源社会保障电子印章系统的建设。

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 32905 信息安全技术 SM3 密码杂凑算法
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 35291 信息安全技术 智能密码钥匙应用接口规范
GB/T 36322 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
ZWFW C 0118-2019 国家政务服务平台统一电子印章 总体技术架构

3 术语和定义

下列术语和定义适用于本文件。

3.1 **电子印章基础设施** electronic seal infrastructure

包括硬件、软件、策略和规程的集合，能够实现电子印章的产生、管理、备案、分发和撤销，实现电子印章制作单位的注册管理，以及电子印章相关数据、系统的符合性检测等功能。

3.2 **电子印章制作监管单位** supervision organization of electronic seal making

能够对电子印章制作单位进行有效监督和管理的职能部门。

3.3 **电子印章制发单位** organization of electronic seal making and distributing

审批制作单位、指定制作单位和发放电子印章的职能部门。

3.4 **电子印章制作单位** organization of electronic seal making

经监管单位、制发单位批准并在电子印章基础设施中注册的，为电子印章使用单位制作电子印章的部门。

3.5 **电子印章制作终端** electronic seal making terminal

用于连接电子印章制作系统的计算机设备，提供上传电子印章制作信息和电子印章下载的功能。

3.6 **电子印章客户端软件** electronic seal client software

部署于用章用户计算机端的电子印章应用软件，为用户提供对电子文件的签章和验章功能。

3.7 **分散式用章** decentralized seal using

将电子印章密钥和信息存储于印章所有者的客户端设备中（例如智能密码钥匙等），管理方式近似实物印章。

3.8 **集中式用章** centralized seal using

将电子印章密钥和信息存储于印章所有者指定的密码设备（例如密码机、数字签名服务器等）以及系统中，通过网络连接方式进行使用，采用身份认证、授权管理等技术进行管控。

3.9 **智能密码钥匙** cryptographic smart token

实现密码运算、密钥管理功能，提供密码服务的终端密码设备。

3.10 **数字证书** digital certificate

数字证书是由人力资源社会保障电子认证系统（CA）进行数字签名的一个可信的数字化文件。数字证书包含有公开密钥拥有者的信息、公开密钥，签名算法和CA的数字签名。

3.11 **SM2 算法** SM2 cryptographic algorithm

由GB/T 32918（所有部分）定义的一种算法。

3.12 **SM3 算法** SM3 cryptographic algorithm

由GB/T 32905定义的一种算法。

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）

OCSP 在线证书状态协议（Online Certificate Status Protocol）

PIN 个人身份识别码（Personal Identification Number）

USB 通用串行总线（Universal Serial Bus）

5 电子印章体系总体结构

人力资源社会保障电子印章体系依托人力资源社会保障电子认证系统，以密码技术为支撑，面向人力资源社会保障各类业务系统，实现以电子印章为主要内容的安全应用。通过电子形式对电子文档进行ovt 数字签名及签章，以确保文档来源的真实性和文档的完整性，防止对文档未经授权的篡改，并确保签章行为的不可否认性。

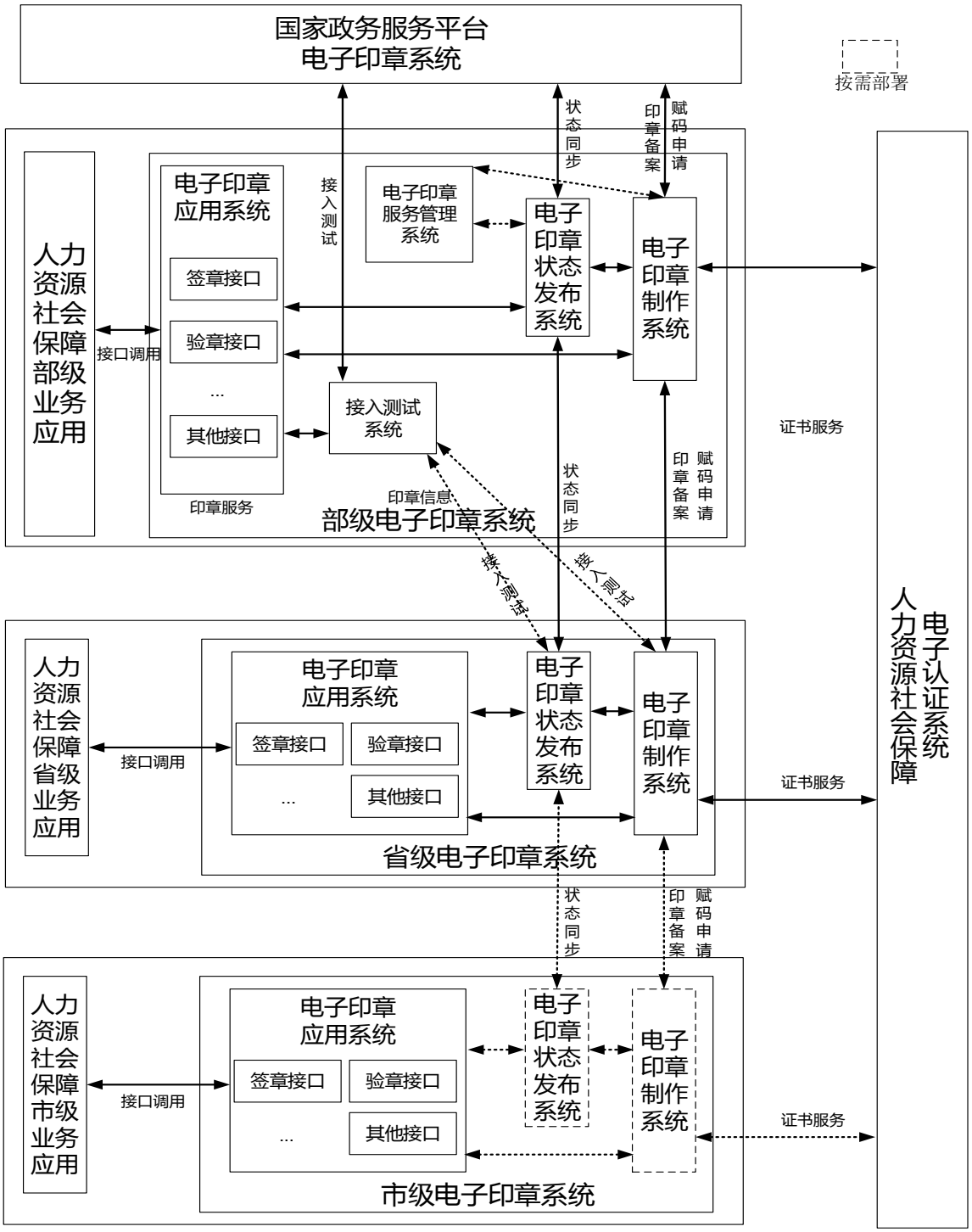

图 1　人力资源社会保障电子印章体系总体结构

如图1 所示，人力资源社会保障电子印章体系整体上分为部、省、市三级结构，各级电子印章系统主要由电子印章制作系统、电子印章状态发布系统、电子印章应用系统等组成。电子印章数字证书由人力资源社会保障行业电子认证系统签发管理。部级电子印章系统与国家政务服务平台电子印章系统对接，地方人社电子印章系统可通过部级电子印章系统接入国家政务服务平台电子印章系统，实现与地方政务服务平台电子印章系统的信任接入。

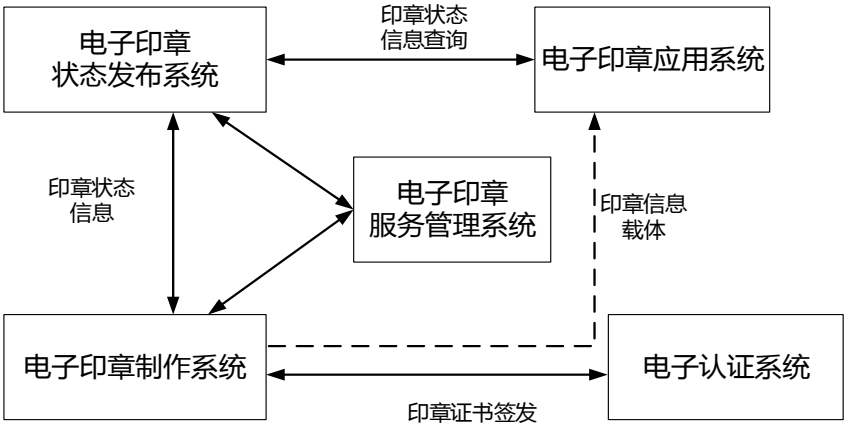

图 2　电子印章系统组成关系

部级电子印章系统组成如下：

电子印章制作系统，提供电子印章制作的相关服务，与部级人力资源社会保障电子认证系统对接实现电子印章数字证书发放，与国家政务服务平台电子印章系统对接实现信任接入，面向省级电子印章制作系统提供国家政务服务平台电子印章系统信任接入服务。

电子印章状态发布系统，提供电子印章的状态发布、查询、下载及变更服务，与国家政务服务平台电子印章系统对接实现状态同步，面向省级电子印章状态发布系统提供状态同步相关服务。

电子印章应用系统，面向部级各种业务的用户管理、授权管理及电子印章签章、验章等服务。

电子印章服务管理系统， 面向省级电子印章制作系统和电子印章状态发布系统提供注册信任接入服务。

省级电子印章系统组成如下：

电子印章制作系统，提供电子印章制作的相关服务，与省级人力资源社会保障电子认证系统对接实现电子印章数字证书发放，与部级电子印章系统对接实现国家政务服务平台电子印章系统的信任接入，面向市级电子印章制作系统提供部级电子印章系统的信任接入服务。

电子印章状态发布系统，提供电子印章的状态发布、查询、下载及变更服务，与对接实现状态同步，面向市级电子印章状态发布系统提供状态同步相关服务。

电子印章应用系统，面向省级各种业务的用户管理、授权管理及电子印章签章、验章等服务。

市级电子印章系统组成如下：

电子印章制作系统，提供电子印章制作的相关服务，与省（市）级人力资源社会保障电子认证系统对接实现电子印章数字证书发放，与省级系统对接实现国家政务服务平台电子印章系统的信任接入，按需建设。

电子印章状态发布系统，提供电子印章的状态发布、查询、下载及变更服务，与省级系统对接实现状态同步，按需建设。

电子印章应用系统，面向市级各种业务的用户管理、授权管理及电子印章签章、验章等服务。

6　电子印章系统部署结构

人力资源社会保障各级电子印章相关系统部署于业务专网，公众服务网可按需要部署电子印章应用系统，如图3 所示。

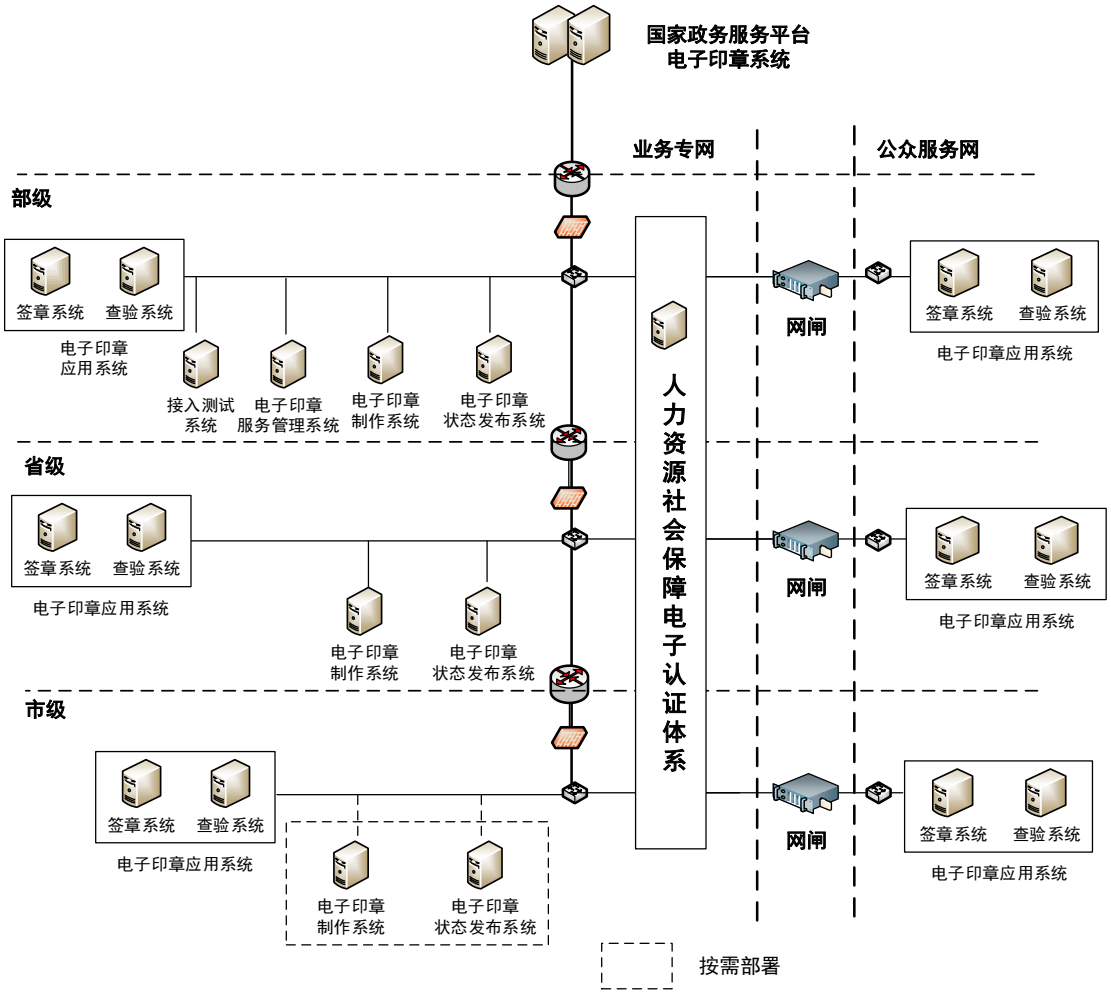

图 3　典型部署应用

人力资源社会保障电子印章纵向应用分为部、省、市三级。部级电子印章系统与国家政务服务平台电子印章系统进行互通，代理各地方电子印章系统完成行业内印章的备案、赋码的申请；省市两级统建或分级建设，由省级按照实际情况按需部署；市级电子印章系统向省级电子印章系统提交注册，省级电子印章系统向部级电子印章系统提交注册，与部级平台交互完成印章的备案、赋码的申请和互通互认。

人力资源社会保障电子印章横向应用为业务专网和公众服务网的跨域应用。业务专网署电子印章制作系统、电子印章状态发布系统、电子印章应用系统等；公众服务网部署电子印章应用系统。

详细描述：

a)　部级业务专网部署电子印章制作系统、电子印章状态发布系统、电子印章接入测试系统、电子印章服务管理系统、电子印章应用系统。其中电子印章制作系统、电子印章状态发布系统通过政务外网与国家平台交互，完成赋码申请、印章备案、状态同步等业务；电子印章接入测试系统是各地方接入部级电子印章制作系统、电子印章状态发布系统前的预检测测试系统，主要验证各地方系统是否满足国办接口要求；电子印章服务管理系统是各地方接入部级电子印章制作系统、电子印章状态发布系统的注册服务管理系统，需通过电子印章服务管理系统注册后才可接入。公众服务网部署电子印章应用系统，电子印章应用系统包含签章系统和查验系统两个子系统，为公众服务网业务系统提供签章服务及跨行业文件验证服务。

b) 省级业务专网部署电子印章制作系统、电子印章状态发布系统、电子印章应用系统；公众服务网部署电子印章应用系统，为公众服务网业务系统提供签章服务及跨行业文件验证服务。

c) 市级业务专网与公众服务网建设电子印章应用系统；电子印章制作系统、电子印章状态发布系统根据省级应用情况可按需部署。

d) 人力资源社会保障电子印章系统由人力资源社会保障电子认证体系提供电子认证服务；包含证书申请、延期、变更、吊销。

e) 各地方电子印章制作系统、电子印章状态发布系统，通过部级代理接口与国家电子印章系统交互，完成赋码申请、印章备案、状态同步等业务。

f) 各省电子印章验证通过本省电子印章状态发布系统验证，跨省业务通过部级电子印章状态发布系统验证。

g) 数字证书模板应以国办C0122 附录D 为蓝本，可在此基础上扩充人社内部业务项，比如增加印章来源（政府或人社行业）等。

6.1 电子印章基础设施业务

6.1.1 电子印章制作和状态发布系统对接流程

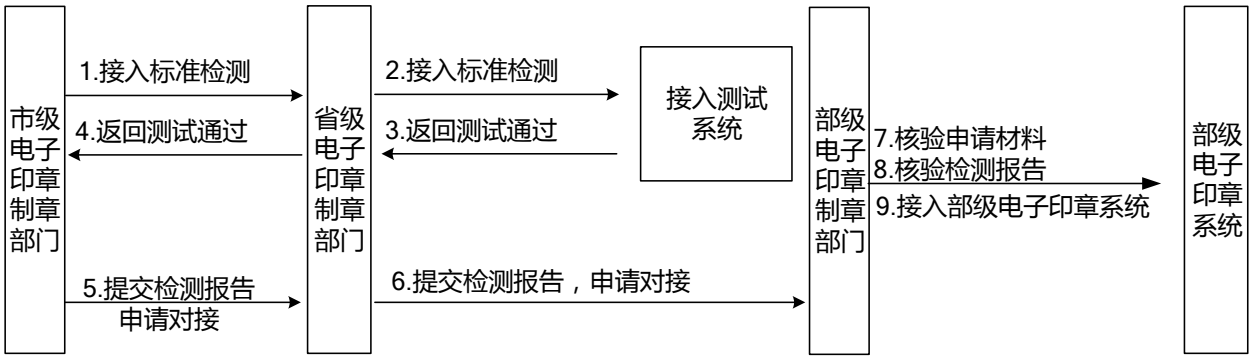

图 4 系统对接业务流程

对接业务流程描述：

a) 各地人力资源社会保障电子印章系统建设完成后，首先经电子印章接入测试系统检测电子印章制作系统、状态发布系统国办接口的正确性。

b) 各地人力资源社会保障电子印章系统测试通过后，逐级提交测试报告和系统对接申请，即市级向省级平台提交测试报告和系统对接申请，省级向部级平台提交测试报告和系统对接。

c) 部级审核部门核验申请材料的完整性和检测报告的正确性，通过后进行正式系统对接。

6.1.2 电子印章制作系统注册

当各地方的电子印章制作系统通过电子印章接入系统测试后，方可与部级电子印章系统进行对接，各地方电子印章制作系统应通过部级电子印章服务管理系统在部里注册，由人力资源社会保障行业CA为其签发电子印章制作系统数字证书，用于电子印章制作和身份鉴别。注册流程见图5 。

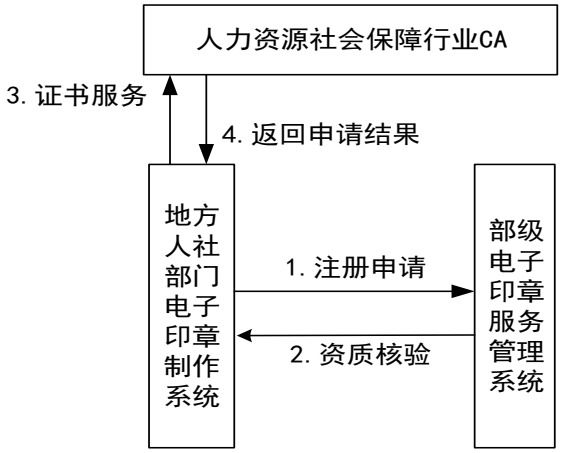

图5　电子印章制作系统注册

注册流程如下：

a) 管理人员将电子印章制作系统注册申请信息录入电子印章服务管理系统。申请信息包括系统名称、系统IP 地址和端口号、系统所在省市、系统公钥等。

b) 人力资源社会保障行业CA 为电子印章制作系统颁发数字证书，用印章根签发。

c) 将数字证书返回电子印章制作系统。

6.1.3　电子印章状态发布系统注册

当各地方的电子印章状态发布系统通过电子印章接入测试系统测试后，方可与部级电子印章系统进行对接，各地方电子印章状态发布系统应通过部级电子印章服务管理系统在部里注册，由人力资源社会保障行业CA 印章根为其签发电子印章状态发布系统数字证书，用于身份鉴别，具体流程见图6 。

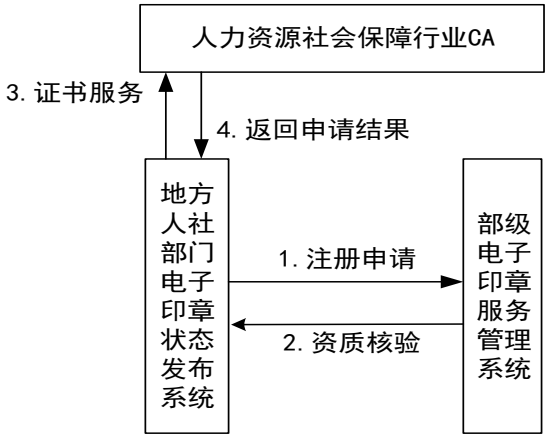

图 6　电子印章状态发布系统注册

注册流程如下：

a) 管理人员将电子印章状态发布系统注册申请信息录入国家政务服务平台统一电子印章管理系统。申请信息包括系统名称、系统IP 地址和端口号、系统所在省市、系统公钥等。

b) 人力资源社会保障行业CA为电子印章状态发布系统颁发数字证书，用印章根签发。

c) 将数字证书返回电子印章状态发布系统。

6.2 电子印章业务

电子印章按应用范围可分为跨行业应用和行业内应用，跨行业应用的电子印章在申领时，唯一赋码的申请应按照国办要求进行申请，并完成印章备案；行业内应用的电子印章在申领时，唯一赋码的申请应按行业内的赋码要求进行填写，且无需到国办平台备案。

6.3 电子印章申领

电子印章使用主体可向电子印章制发主体申领电子印章，具体流程见图 7 。

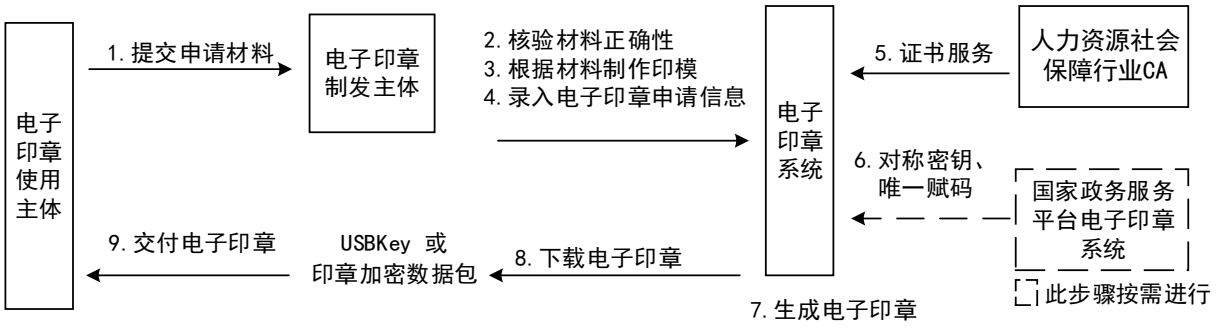

图 7 电子印章申领

电子印章申领流程描述如下：

a) 电子印章使用主体向电子印章制发主体提交申领材料，其中电子印章印模采集通过物理实物印章加盖到采集表后，扫描获取，电子印章印模须与实物印章印模保持一致。

b) 电子印章制发主体核验申领材料正确性。

c) 电子印章制发主体根据提交的申领材料制作电子印章印文图像，印文图像规格和样式在1 :1 打印下应实物印章有关规定和标准。

d) 电子印章制发主体登录电子印章系统根据申请单位提交的材料，录入提交电子印章申请信息，包括：单位统一社会信用代码、单位行政区划码、单位类型（国家行政机关或事业单位）、单位名称、经办人姓名、经办人公民身份号码、经办人手机号码、单位地址、审批单位名称、审批单位行政区划码、电子印章名称、电子印章印文图像（如果制作电子印章要导入电子印章应用系统，还应提交从电子印章应用系统导出的电子印章申请数据包）。

e) 由人力资源社会保障行业CA 为电子印章颁发数字证书（一个数字证书只能对应一枚电子印章）。

f) 从国家政务服务平台电子印章信任支撑系统获取电子印章唯一赋码、公安对称密钥、公安印章信息，并完成印章备案。（如电子印章无需跨行业使用，仅行业内应用的情况，省略此步骤）。

g) 电子印章系统根据申请材料生成电子印章。

h) 电子印章制发主体下载制作完成的电子印章。

i) 电子印章制发主体向电子印章使用主体交付电子印章。

j) 电子印章的存储包括USB-Key 和印章加密数据包两种方式，其中印章加密数据包存储于服务器中，在服务端进行电子签章。

k) 数据包的格式和安全参见GB/T 35291 和GB/T 36322 中密钥导入机制。

申请材料内容见表1 。

表1　电子印章申领需提交的材料

业务类型	电子印章申领申请材料
印章申领	加盖公章的电子印章申请文件
	经办人身份证
	经办人联系方式
	成立该单位的有关文件、批文、编办文件或证照

6.4　电子印章变更

电子印章使用主体因机构变动、名称变更等原因需要更换电子印章时，应进行电子印章变更，具体流程见图8 。

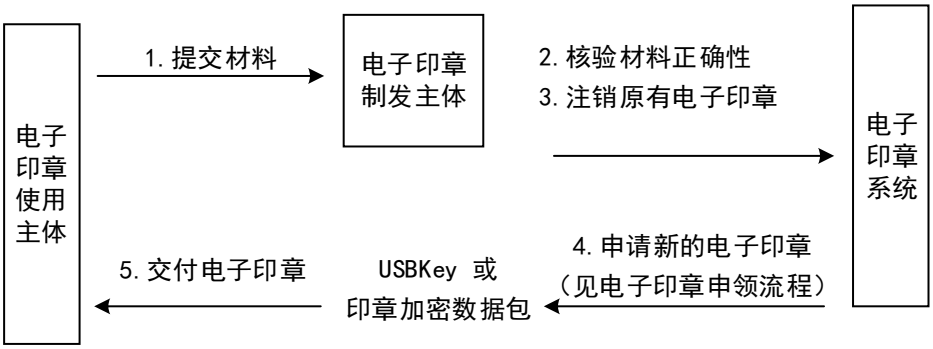

图 8　电子印章变更

电子印章变更流程描述如下：

a)　电子印章使用主体向电子印章制发主体提交变更申请材料。

b)　电子印章制发主体核验电子印章变更申请材料正确性。

c)　电子印章制发主体核验后，登录电子印章系统注销原有电子印章。

d)　电子印章制发主体申请新电子印章（新电子印章申请见电子印章申领流程）。

e)　电子印章制发主体向电子印章使用主体交付变更后的电子印章。

申请材料内容见表2 。

表 2　　电子印章变更需提交的材料

业务类型	电子印章变更申请材料
印章变更	加盖单位公章的电子印章变更原因说明书
	经办人身份证
	经办人联系方式
	成立该单位的有关文件、批文、编办文件或证照

6.5　电子印章挂失

电子印章使用主体因电子印章载体遗失时，应进行电子印章挂失，具体流程见图9 。

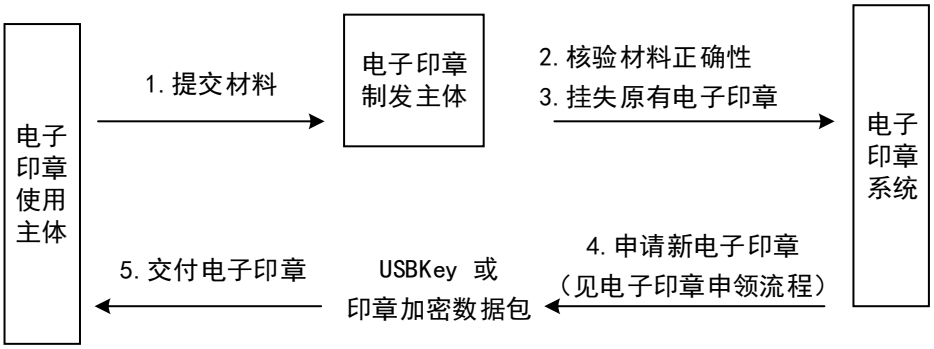

图 9　电子印章挂失

电子印章挂失流程描述如下：

a)　电子印章使用主体向电子印章制发主体提交电子印章挂失申请材料。

b)　电子印章制发主体核验电子印章变更申请材料正确性。

c)　电子印章制发主体核验后，登录相应的电子印章系统挂失原有电子印章。

d)　电子印章制发主体申请新电子印章（新电子印章申请见电子印章申领流程）。

e)　电子印章制发主体向电子印章使用主体交付新电子印章。

申请材料内容见表3 。

表3　电子印章挂失需提交的材料

业务类型	电子印章挂失申请材料
印章挂失	加盖单位公章的电子印章丢失原因说明书
	经办人身份证
	经办人联系方式
	成立该单位的有关文件、批文、编办文件或证照

6.6 电子印章注销

电子印章使用主体因自身业务原因需要注销本单位电子印章时，可通过电子印章系统实现，具体流程见图1 0 。

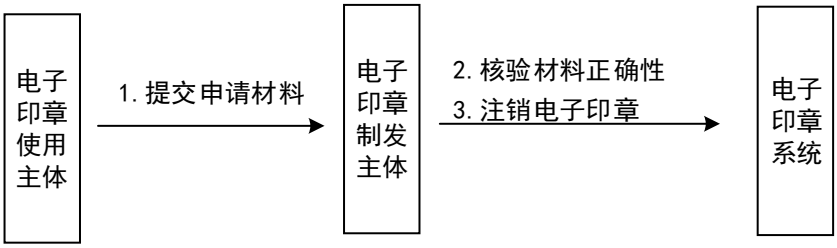

图 10　电子印章注销

电子印章注销流程描述如下：

a)　电子印章使用主体向电子印章制发主体提交电子印章注销申请材料。

b)　电子印章制发主体核验电子印章注销申请材料正确性。

c)　电子印章制发主体核验后，登录相应的电子印章系统注销指定的电子印章。

申请材料内容见表4 。

表4　电子印章注销需提交的材料

业务类型	电子印章注销申请材料
印章注销	加盖单位公章的电子印章注销原因说明书
	经办人身份证
	经办人联系方式
	成立该单位的有关文件、批文、编办文件或证照

6.7 电子印章续期

电子印章使用主体因电子印章或数字证书到期，向电子印章制发主体提交续期申请材料，具体流程见图1 1 。

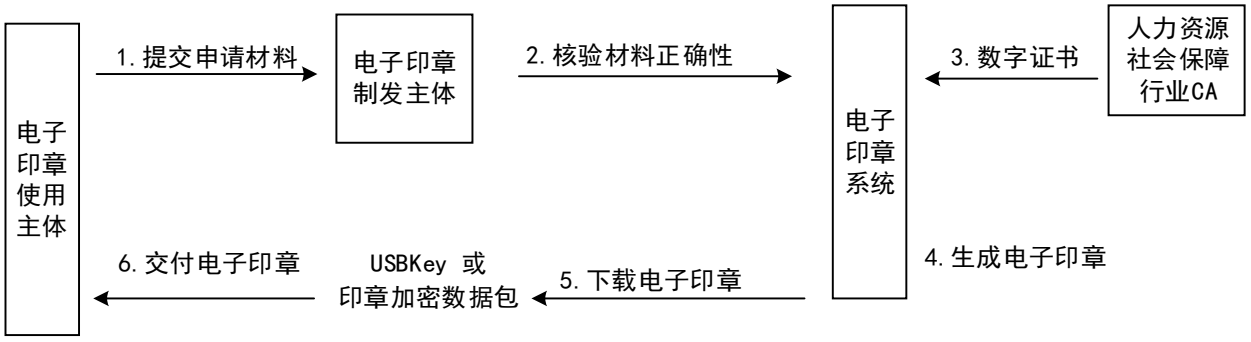

图11　电子印章续期

电子印章续期流程描述如下：

a）电子印章使用主体向电子印章制发主体提交电子印章续期申请材料。

b）电子印章制发主体核验电子印章续期申请材料正确性。

c）电子印章制发主体核验后，登录相应的电子印章系统进行电子印章续期操作。

注：电子印章续期宜支持在线申请，由电子印章使用主体进行自助申请：用户登录电子印章续期网站，插入USB-Key 或者提交密码设备产生的申请包，由电子印章系统完成数字证书续期和电子印章续期。

申请材料内容见表5 。

表 5　电子印章续期需提交的材料

业务类型	电子印章续期申请材料
印章续期	加盖单位公章的电子印章续期申请书
	经办人身份证、联系方式

6.8 电子印章更换

电子印章使用主体因电子印章载体损坏等原因需要更换载体时，向电子印章制发主体提交更换申请材料，具体流程见图1 2 。

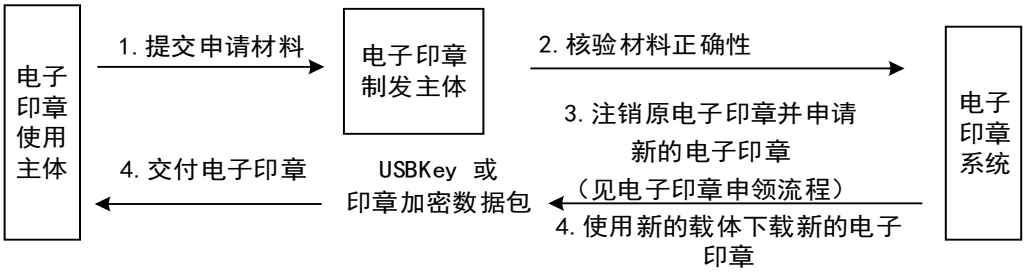

图12　电子印章更换

电子印章更换流程描述如下：

a) 电子印章使用主体向电子印章制发主体提交更换申请材料。

b) 电子印章制发主体核验电子印章更换申请材料的正确性。

c) 电子印章制发主体核验后，登录电子印章系统注销原有电子印章。

d) 电子印章制发主体申请新电子印章（新电子印章申请见电子印章申领流程）。

e) 电子印章制发主体向电子印章使用主体交付更换后的电子印章。

申请材料内容见表6 。

表6　电子印章更换申请需提交的材料

业务类型	电子印章更换申请材料
印章更换	加盖单位公章的电子印章更换原因说明书
	经办人身份证
	经办人联系方式
	成立该单位的有关文件、批文、编办文件或证照

7　电子印章应用

7.1　应用模式

电子印章使用主体可根据自身情况设计建设不同模式的电子印章应用系统,满足自身电子印章应用需求。电子印章的应用模式主要分为分散式和集中式两种：

⑴ ）分散式用章

电子印章存储在电子印章使用主体的智能密码钥匙（UKEY ）中，电子印章使用主体使用电子印章客户端软件进行签章或验章，可完成离线或在线电子签章和验章操作。

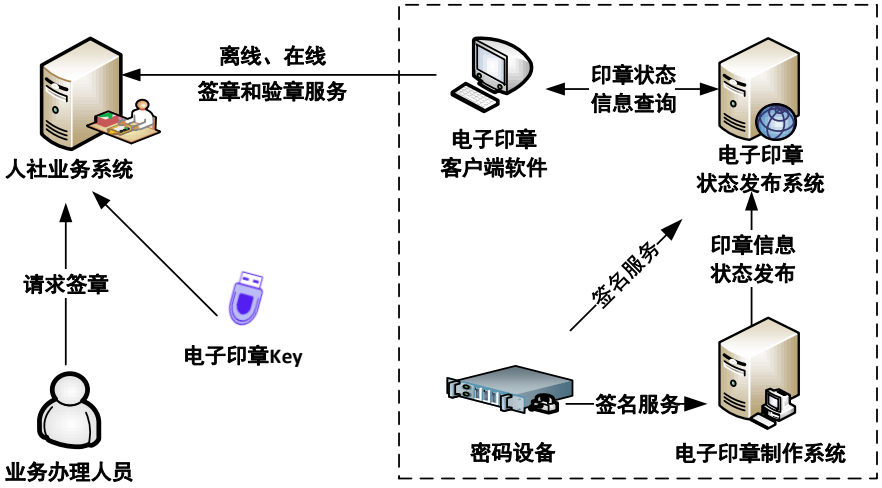

图 13　分散式用章

分散式用章描述：

a）　业务办理人员在人社业务系统办理签章相关业务时，人社业务系统通过调用电子印章客户端软件完成签章操作。

b）　电子印章客户端软件签章时，通过UKEY 读取电子印章、签名运算，完成离线或在线的电子签章操作。

⑵ ）集中式用章

电子印章存储于集中式用章系统中，电子印章使用主体使用电子印章应用系统（集中式用章系统）进行签章或验章，可在线完成电子签章和验章操作，电子印章应用系统可扩展用章用户管理、权限管理、日志审计等功能。

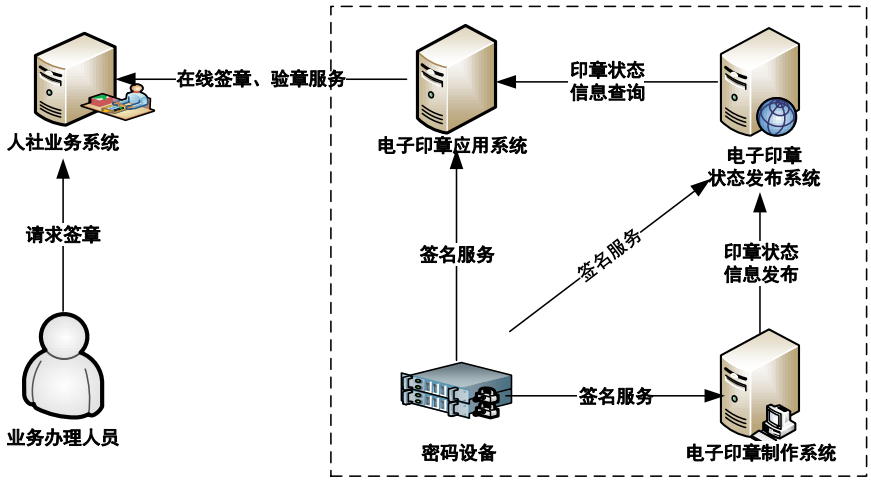

图 14　集中式用章

集中式应用描述：

a）　业务办理人员在人社业务系统办理签章相关业务时，人社业务系统通过接口调用方式向电子印章应用系统发起签章请求。

b）　电子印章应用系统响应签章请求并把已签文件返回给人社业务系统。

c）　密码设备在整个签章流程中提供安全可靠的签名服务。

d）　电子印章状态发布系统在签章、验章过程中提供电子印章有效性查询服务。

7.2 签章

7.2.1 总体要求

对签章的总体要求如下：

电子印章使用主体应通过电子印章应用系统完成签章。

电子印章使用主体可按实物印章使用要求制定本单位的电子印章管理办法。

7.2.2 签章申请

申请信息应包括但不限于申请实体、隶属机构、申请时间、电子印章应用对象。如果该过程由电子印章应用系统内部申请流程实现，申请环节应记录申请信息和申请实体数字签名，用于事后审计。

7.2.3 签章审核

电子印章使用主体应指定具有审核权限的电子印章审核员，对电子印章使用申请进行审核，同时要核对电子印章自身的有效性，给出审核意见，记录申请信息、审核人信息、审核结果。如果该过程由电子印章应用系统内部审核流程实现，审核各环节应记录保存申请信息、审核员信息、审核结果和审核员数字签名，用于事后审计。

7.2.4 签章操作

签章操作要求如下：

a) 分散式用章

1）应由电子印章管理员对用章对象进行签章；

2）电子印章管理员应核对印章使用申请者、用章对象、用章审核员、电子印章名称等信息；

3）宜对签章操作人、签章时间、用章申请和审核情况记录日志。

b) 集中式用章

1）在用章审核通过后，由申请人在电子印章应用系统内对用章对象进行签章；

2）电子印章应用系统应对申请人的身份以及用章权限进行验证；

3）电子印章应用系统应对用章对象、电子印章名称、签章操作人、签章时间记录日志。

7.3 验章

7.3.1 分散式用章

1）电子印章使用主体可根据业务需求和验章环境选择离线验章或在线验章；

2）离线验章主要包括验证电子印章和已签章文件的真实性、完整性；

3）在线验章是在离线验章的基础上，通过查询电子印章状态发布服务确认签章时电子印章的有效性。

7.3.2 集中式用章

1）集中式用章模式下对签章文件进行验章时，应验证电子印章和签章文件的完整性、真实性，同时验证签章时电子印章的有效性；

2）验证电子印章有效性时，可在线查询电子印章状态发布服务，也可下载电子印章吊销列表进行查询。

8 电子印章安全要求

8.1 平台安全要求

电子印章制作系统、电子印章状态发布系统、电子印章应用系统等应满足《GB/T 22239-2019 信息安全技术网络安全等级保护基本要求》和《GM/T 0054-2018 信息系统密码应用基本要求》三级系统相关要求，应定期开展系统网络安全等级保护、商用密码应用安全性测评，电子印章系统软硬件应具备商用密码产品型号证书。

8.2 通讯安全要求

电子印章制作系统、电子印章状态发布系统、电子印章应用系统等应采用基于国产密码技术实现的SSL 安全网关等设备进行通道加密，保护业务数据、电子印章数据、电子签章数据等机密性与完整性，系统内部通讯应采用数字签名技术保护传输数据的完整性。安全网关等设备应满足国家密码管理机构相关要求，具备商用密码产品型号证书。

8.3 数据安全要求

电子印章制作系统、电子印章状态发布系统、电子印章应用系统等应使用硬件加密机、硬件数字签名服务器等；制章人数字证书密钥、签章人数字证书密钥和电子印章需存储于加密机、数字签名服务器、智能密码钥匙等硬件设备中。密码硬件设备应满足国家密码管理机构相关要求，具备商用密码产品型号证书。移动端电子印章密码模块应用满足《GM/T 0028-2014 密码模块安全技术要求》二级或以上安全要求，并具备商用密码产品型号证书。

电子印章制作系统、电子印章状态发布系统、电子印章应用系统等应具备数据备份与恢复机制。数据备份和恢复可采用人工数据库备份或通过第三方软件备份数据库等方式实现。

8.4 管理安全要求

电子印章制作系统、电子印章状态发布系统、电子印章应用系统等应采用分权管理机制，各系统应具备独立的业务管理员与审计管理员，且为管理员分配最小管理权限。

印章管理、印章使用等流程应具备申请、审核机制，关键操作应采用数字签名技术进行签名确认，以满足事后追溯与审计要求。