ICS 35.240
CCS L76

T/CCUA

中 国 计 算 机 用 户 协 会 团 体 标 准

T/CCUA XXXX—XXXX

电子印章互通互认服务平台 接入要求

Electronic seal interoperability and mutual recognition service platform-Requirements for access

（征求意见稿）

（本草案完成时间：2024 年 3 月）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国计算机用户协会　　发 布

目　　次

前言 II
引言 III
1　范围 1
2　规范性引用文件 1
3　术语、定义和缩略语 1
3.1　术语和定义 1
3.2　缩略语 3
4　系统构成 3
4.1　系统结构 3
4.2　电子印章互通互认服务平台组成 3
4.3　电子印章系统组成 4
5　基本要求 4
5.1　提供服务功能 4
5.2　业务持续性保障 4
5.3　安全要求 4
5.4　统一电子印章格式 4
5.5　证书介质 4
6　电子印章互通互认服务平台接入接口要求 5
6.1　基础接口要求 5
6.2　电子印章互通互认服务平台云证书接口要求 8
6.3　电子印章互通互认服务平台 UKey 证书接口要求 10
6.4　文档验真 12
7　数据安全 13
8　安全运维 13
8.1　日志管理 13
8.2　密码管理 13
8.3　安全事件处置管理 13
参考文献 15

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。

本文件由中国计算机用户协会提出并归口。

本文件起草单位：中国计算机用户协会政务信息化分会、国家市场监督管理总局竞争政策与大数据中心、工业和信息化部电子第五研究所（中国赛宝实验室）、安徽省数据资源管理局、海南省大数据管理局、 湖北省大数据中心、山西省大数据中心、人民网股份有限公司、北京安证通信息科技股份有限公司、国富安电子商务安全认证有限公司、江苏省国信数字科技有限公司、北京世纪龙脉科技有限公司、山西云时代技术有限公司、人民数据管理有限公司、人人签数据科技有限公司。

本文件主要起草人：童晓民、刘权、贾洋、刘佳莎、童旭亮、刘峰、刘师学、孙聪、王海明、刘文中、李鹏飞、任贤辉。

引　言

为实现电子印章跨区域、跨行业、跨平台的互信、互通、互认，支撑保障各类“互联网+”应用深入拓展，需基于电子印章行业现行的标准，规范电子印章互通互认服务平台接入要求，特制定本文件。

本文件遵循《中华人民共和国民法典》《中华人民共和国电子签名法》和《电子认证服务管理办法》的相关规定，同时根据互联网商务和业务的特点而制定。

电子印章互通互认服务平台 接入要求

1 范围

本文件确立了电子印章互通互认平台的结构、基本要求、接口要求、数据安全和安全运维等要求。
本文件适用于电子印章互通互认服务平台的设计、开发、运维或第三方电子印章平台的接入改造。

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。

[1] GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式
[2] GB/T 20520 信息安全技术 公钥基础设施 时间戳规范
[3] GB/T 20988—2007 信息系统灾难恢复规范
[4] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
[5] GB/T 22240-2020 信息安全技术 网络安全等级保护定级指南
[6] GB/T 31508-2015 信息安全技术 公钥基础设施 数字证书策略分类分级规范
[7] GB/T 32905 信息安全技术 SM3 密码杂凑算法
[8] GB/T 32918（所有部分）信息安全技术 SM2椭圆曲线公钥密码算法
[9] GB/T 33190-2016 电子文件存储与交换格式
[10] GB/T 33481-2016 党政机关 电子印章应用规范
[11] GB/T 35273-2020 个人信息安全规范
[12] GB/T 35275-2017 信息安全技术 SM2密码算法加密签名消息语法规范
[13] GB/T 35276 信息安全技术 SM2 密码算法使用规范
[14] GB/T 35285-2017 信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求
[15] GB/T 38540-2020 信息安全技术 安全电子签章密码技术规范
[16] GB/T 33560 信息安全技术 密码应用标识规范
[17] GB/T 39204-2022 信息安全技术 关键信息基础设施安全保护要求
[18] GB 50174-2017 数据中心设计规范
[19] GM/T 0112-2021 PDF 格式文档的密码应用技术要求
[20] GM/T 0015-2012 基于SM2密码算法的数字证书格式规范
[21] GM/T 0031-2014 安全电子签章密码技术规范
[22] GA/T 1106-2013 信息安全技术 电子签章产品安全技术规范

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

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。

注：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/T25056-2018，3.1]

3.1.2

电子印章 electronic seal

一种由电子印章制章者数字签名的安全数据。

注：包括电子印章所有者信息和图形化内容的数据，用于安全签署电子文件。

[来源：GB/T38540-2020,3.1]

3.1.3

电子签章 electronic seal signature

使用电子印章签署电子文件的过程。

注：电子签章可实现与纸质文件签章操作相似的可视效果，可保障数据来源的真实性、数据完整性以及签名人行为的不可否认性

[来源：GB/T38540-2020,3.2]

3.1.4

原文 original data

需要进行电子签章或数字签名处理的电子文件。

[来源：GB/T38540-2020,3.3]

3.1.5

电子签章数据 electronic seal signafure data

电子签章过程产生的包含电子印章、原文信息和数字签名等信息的数据。

[来源：GB/T38540-2020,3.4]

3.1.6

电子印章系统 electronic seal system

电子印章管理系统和电子签章软件的统称。

注：1、电子印章管理系统具有电子印章制作与管理、安全审计等功能注；2、电子签章软件是对电子文件加盖电子印章或添加数字签名的软件。

[来源：GB/T38540-2020,3.5]

3.1.7

电子印章客户端 electronic seal client

安装了电子签章软件的电子计算机、移动终端等的统称。

3.1.8

制章者 electronic seal maker

电子印章系统中具有电子印章制作和管理权限的机构。

注：电子印章中的图像和相关信息应经制章者进行数字签名，电子印章中的制章者证书应是该机构的单位证书。

[来源：GB/T38540-2020,3.6]

3.1.9

签章者 electronic seal signer

电子印章的所有者，是具备电子印章法定使用权限的实体。

[来源：GB/T38540-2020,3.7]

3.1.10

SM2 算法 SM2 algorithm

由 GB/T 32918（所有部分） 定义的一种椭圆曲线密码算法。

[来源：GB/T38540-2020,3.8]

3.1.11

SM3 算法 SM3 algorithm

由 GB/T 32905 定义的一种杂凑算法。

[来源：GB/T38540-2020,3.9]

3.1.12

电子签名 electronic seal signature

数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

[来源：中华人民共和国电子签名法，第二条]

3.1.13

时间戳 time stamp

使用数字签名技术产生的数据。签名的对象包括了原始文件信息、签名参数、签名时间等信息。

[来源：GB/T20520-2006,3.1]

3.1.14

电子认证服务机构/CA 机构 certificate authority

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。

注：电子认证服务机构/CA机构为需要第三方认证的电子签名提供电子认证服务，帮助电子签名人和依赖方建立信任关系，并证明电子签名制作数据和电子签名人真实身份的关联关系的实体。

[来源：GB/T25056-2018,3.5]

3.2 缩略语

下列缩略语适用于本文件。

ID：标识（Identification）

JSAPI：JS应用程序编程接口（JavaScript Application Programming Interface）

ODF: 开放文档格式(Optical Distribution Frame)

PDF: 可携带文件格式(Portable Document Format)

UKey：以一种USB接口的硬件设备作为载体数字证书（USB Key）

4 系统构成

4.1 系统结构

电子印章互通互认服务平台符合《电子认证服务管理办法》等相关法律法规和标准规范的规定，面向省市印章平台、行业印章平台、第三方印章平台等电子印章系统，提供电子认证服务，实现跨区域、跨行业、跨平台电子印章交叉互信、互认。结构见图1。

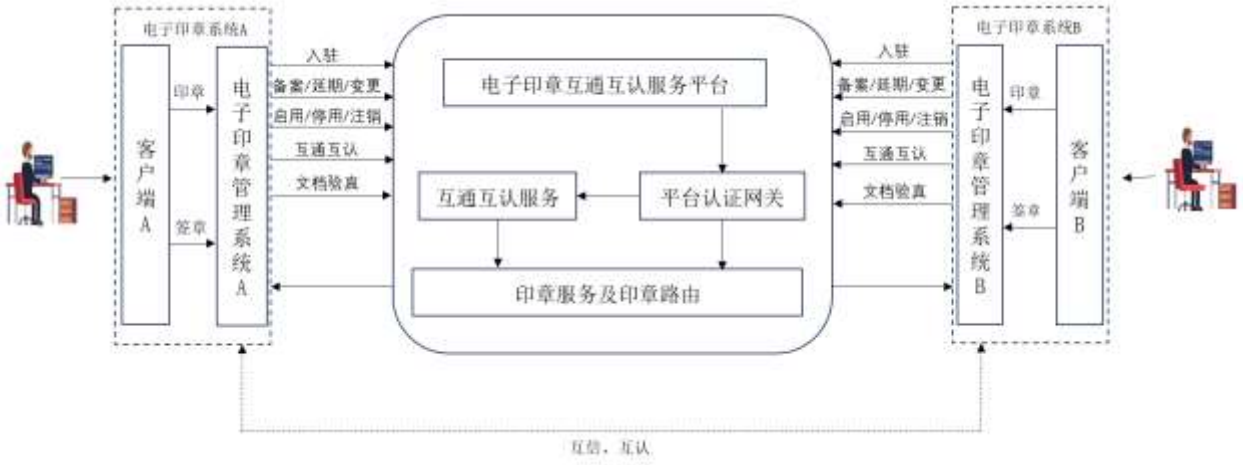

图1 系统结构

4.2 电子印章互通互认服务平台组成

电子印章互通互认服务平台由以下部分组成：

a) 平台认证网关：对接入电子印章系统所发送的请求进行合法合规性验证；

b) 互通互认服务：提供接入跨越电子印章系统的电子签章服务，对产生的电子签章文件提供跨越电子印章系统的互通互认能力、文档验真能力；

c) 印章服务及印章路由：对接入电子印章系统所发送的请求，查询电子印章备案来源，路由到电子印章所制作的电子印章系统获取电子印章、电子数据签名。

4.3 电子印章系统组成

电子印章系统由以下部分组成：

a) 电子印章管理系统：提供电子印章制作的相关服务、电子印章状态发布和查询及变更等、电子印章签章或验章等；
b) 电子印章客户端：支持对 PDF 或 OFD 格式的版式文件进行签章或验章。

5 基本要求

5.1 提供服务功能

电子印章互通互认服务平台应包括但不限于以下服务：

a) 入驻：电子印章系统接入电子印章互通互认服务平台先实名注册账号，提交入驻申请，审批通过后，根据电子印章互通互认服务平台规范进行技术对接、改造、测试，对接上线；
b) 电子印章备案/延期/变更：入驻的电子印章系统，完成电子印章制作后，同步将电子印章数据备案至电子印章互通互认服务平台，或将电子印章延期或变更状态数据同步至电子印章互通互认服务平台；
c) 电子印章启用/停用/注销：将电子印章启用或停用或注销状态数据同步至电子印章互通互认服务平台；
d) 互通互认：入驻电子印章互通互认服务平台的电子印章系统之间，实现电子印章互联互通、互验；
e) 文档验真：对文档签章真伪进行验证。

5.2 业务持续性保障

电子印章互通互认服务平台业务持续性应符合下列要求：

a) 部署在不低于 GB50174-2017 的 B 级机房；
b) 灾难恢复能力达到 GB/T20988—2007 第四级要求。

5.3 安全要求

安全方面应符合下列要求：

a) 电子印章互通互认服务平台其安全保护等级 GB/T22240-2020 第三级，并按照要求通过等级保护测评；
b) 电子印章系统其安全保护等级不低于 GB/T22240-2020 中第三级，并按照要求通过等级保护测评。

5.4 统一电子印章格式

5.4.1 数字证书

数字证书应符合GB/T20518-2018、GB/T35285-2017、GB/T31508-2015的要求。

5.4.2 电子印章

电子印章应符合GB/T20520、GB/T32905、GB/T32918、GB/T33481-2016、GB/T33560、GB/T35276、GM/T0015-2012的要求。

5.4.3 签章格式

签章格式应符合GB/T35275-2017、GB/T38540-2020、GA/T1106-2013、GM/T0031-2014的要求。

5.4.4 签章文件

签章文件应符合SM2国密PDF标准和OFD格式标准。SM2国密PDF标准应按照GM/T0112-2021编制而成。OFD支持SM2算法，所有厂商应遵守GB/T33190-2016以达到互签互验。

5.5 证书介质

电子印章互通互认服务平台应至少支持下列证书介质进行互通互认：

a) 云证书：证书存储在云服务器；

b) UKey 证书：证书存储在 UKey 设备内。

6 电子印章互通互认服务平台接入接口要求

6.1 基础接口要求

6.1.1 入驻

6.1.1.1 入驻流程

入驻流程按下列步骤完成：

a) 电子印章系统在电子印章互通互认服务平台注册账号、实名；

b) 以接入单位名义提交入驻申请；

c) 根据电子印章互通互认服务平台规范进行技术对接、改造、测试；

d) 对接上线。

6.1.1.2 入驻接口

可自定义接口的创建、编辑和管理，无特殊要求。

6.1.2 电子印章备案/延期/变更

6.1.2.1 备案/延期/变更流程

已有及新办电子印章备案基本信息，包括印章主体信息、印章来源、印章类型、证书类型、印章启/停用/注销状态。电子印章备案流程见图2。

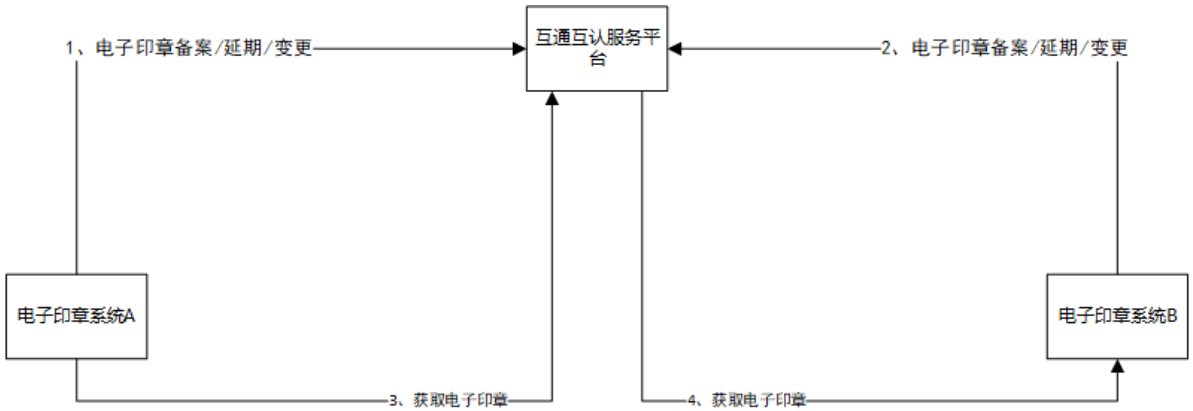

图2 电子印章备案流程

6.1.2.2 电子印章备案/延期/变更接口

接口描述：调用电子印章互通互认服务平台电子印章的备案接口实现印章备案/延期/变更，电子印章互通互认服务平台生成电子印章唯一赋码，调用方保存电子印章唯一赋码至系统。

调用方式：http post/json

请求参数见表1。

表1 电子印章备案接口请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
time	时间戳（获取当前系统时间，以毫秒为单位）	是	String
nonce	100000000内随机整数	是	Integer

表1 电子印章备案接口请求参数（续）

code	业务系统印章编码	否	String
sealCode	印章唯一赋码，印章备案为非必填，其他情况必填	否	String
name	印章名称	是	String
sealType	章类型，0：所有，01：公章（电子法定名称章），02：财务章（电子财务专用章），03：发票章（电子发票专用章）， 04：合同章（电子合同专用章），05：法人章（电子名章），06：业务专用章，07：个人名章，08：个人手绘章	是	String
UKeyId	UKey设备编号	否	String
certNumber	证书序列号	否	String
possessor	印章使用单位或用户名称	是	String
possessorCertNo	印章使用单位或用户证件号	是	String
possessorType	关联者类型，1：机构，2：个人	是	Integer
bizType	电子印章状态，1：备案，2：延期，3：变更	是	Integer
certType	证书性质，1：UKey，2：云证书	是	Integer
sign	签名值	是	String

返回数据见表2。

表2 电子印章备案接口返回数据

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	印章唯一赋码	String

6.1.3 电子印章启用/停用/注销

接口描述：电子印章注销接口实现印章启用/停用/注销。
调用方式：http post/json
请求参数见表3。

表3 电子印章注销接口请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
time	时间戳（获取当前系统时间，以毫秒为单位）	是	String
nonce	100000000内随机整数	是	Integer
sealCode	印章唯一赋码	是	String
state	状态（1：启用，3：注销，4：停用）	是	Integer
sign	签名值	是	String

返回数据见表4。

表4 电子印章注销接口返回数据

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	返回为空	String

6.1.4 获取电子印章

接口描述：获取企业指定或全部类型电子印章。
调用方式：http post/json

请求参数见表5。

表5　电子印章获取接口请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
time	时间戳（获取当前系统时间，以毫秒为单位）	是	String
nonce	100000000内随机整数	是	Integer
deviceId	设备ID，手机盾获取印章时必填	否	String
idCard	用户证件号，手机盾获取印章时必填	否	String
orgCode	企业组织机构代码	是	String
sealType	印章类型，0：所有，01：电子法定名称章，02：电子财务专用章，03：电子发票专用章， 04：电子合同专用章，05：电子名章，06：业务专用章，07：个人名章，08：个人手绘章	是	String
certType	印章证书类型，（0：所有，1：UKey证书，2：云证书）	否	Integer
certNumber	证书序列号	否	String
UKeyId	UKey设备编号	否	String
sign	签名值	是	String

返回数据见表6、表7、表8、表9。

表6　电子印章获取接口返回数据（1）

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	返回详细数据，描述信息见表7	Json Array

表7　电子印章获取接口返回数据（2）

data参数名称	data参数说明	数据类型
signId	签名ID，签名ID只针对某一个印章签名单次有效	String
sealType	印章类型，01：电子法定名称章，02：电子财务专用章，03：电子发票专用章，04：电子合同专用章，05：电子名章，06：业务专用章，07：个人名章，08：个人手绘章	String
sealRelateType	印章所属者类型（1：企业公章； 2：个人私章）	String
sealCode	印章唯一标识	String
sealName	印章名称	String
moulageData	印模数据，Base64编码返回	String
width	印模宽度，单位毫米	Integer
height	印模高度，单位毫米	Integer
dpiX	印模宽度，单位像素	Integer
dpiY	印模高度，单位像素	Integer
sealData	电子印章数据，Base64编码返回	String
sealInvalidTime	电子印章有效期，格式：YYYY-MM-DD HH:MM:SS	String
certType	印章证书类型（1：UKey证书，2：云证书）	Integer
destHost	客户端请求地址，如果印章证书类型为UKey证书时，返回相对应平台的客户端请求地址	String
platName	平台名称	String
UKeyId	UKey设备编号	String
algorithm	证书算法（1：RSA，2：SM2）	String
certList	当前用户签名公钥证书列表，返回详细数据，描述信息见表8	Json Array
state	印章状态（1：待下载，2：已下载）	Integer
userList	印章授权信息列表，返回详细数据，描述信息见表9	List

表8　电子印章获取接口返回数据（3）

certList参数名称	参数说明	数据类型
algorithm	证书算法（1：RSA，2：SM2）	Integer
certCode	证书序列号	String
invalidTime	证书失效时间	String
signPublicKey	签名公钥证书数据（cer公钥证书）	String
subjectCn	证书使用者CN	String

表9　电子印章获取接口返回数据（4）

userList参数名称	参数说明	数据类型
userName	授权人名称	String
mobilePhone	授权人手机号码	String

6.2　电子印章互通互认服务平台云证书接口要求

6.2.1 云证书电子印章互通互认流程

6.2.1.1　综述

云证书电子印章互通互认流程见图3。

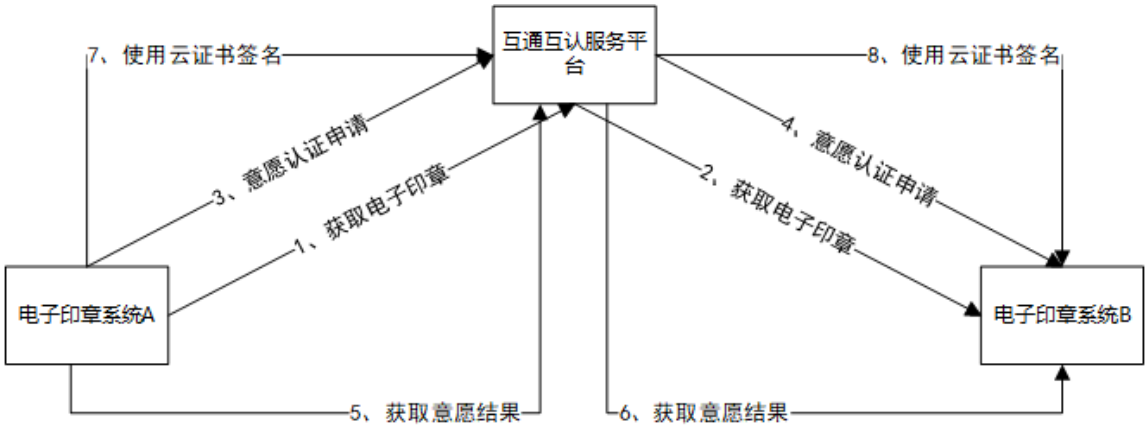

图3　基于云证书互通互认流程

6.2.1.2　获取电子印章

电子印章系统A发现需要在其他电子印章系统完成签章时，向电子印章互通互认服务平台获取电子印章，电子印章互通互认服务平台通过印章查询功能查询已备案印章，并从中获取电子印章，返回给电子印章系统A。

6.2.1.3　意愿认证申请

用户选择云印章，向电子印章互通互认服务平台发起意愿认证申请，电子印章互通互认服务平台解析用户所选印章来源（电子印章系统B），向电子印章系统B获取意愿认证地址，并返回给电子印章系统A。

6.2.1.4　获取意愿认证结果

电子印章系统A通过认证标识ID向电子印章互通互认服务平台获取意愿认证结果，电子印章互通互认服务平台通过认证标识ID向电子印章系统B获取意愿认证结果，并返回给平台A。

6.2.1.5　摘要签

电子印章系统A向电子印章互通互认服务平台发起摘要签请求，电子印章互通互认服务平台凭本次认证标识ID、意愿认证凭证向电子印章系统B获取签名数据，并返回给电子印章系统A，完成签名。

6.2.2 云证书电子印章接口

6.2.2.1 云证书签名意愿认证申请

接口描述：电子签章厂商从开放平台获取意愿认证信息，包括本次认证标识ID，意愿认证地址。调用方以二维码方式显示意愿认证地址，并通过本次认证标识ID获取最终意愿认证凭证。

调用方式：http post/json

请求参数见表10。

表10 云证书签名意愿认证申请请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
time	时间戳（获取当前系统时间，单位为毫秒）	是	String
nonce	100000000内随机整数	是	Integer
orgCode	企业统一社会信用代码	否	String
name	用户姓名	否	String
idCard	身份证号码	否	String
mobile	手机号	是	String
sealCode	印章唯一标识	是	String
redirectUrl	重定向地址	否	String
sign	签名值	是	String

返回数据见表11、表12。

表11 云证书签名意愿认证申请返回数据（1）

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	返回详细数据，描述信息见表12	JSON

表12 云证书签名意愿认证申请返回数据（2）

data参数名称	data参数说明	数据类型
authUrl	认证URL	String
clientType	认证URL地址类型（H5、PC）	String
authId	本次认证标识ID，通过该属性获取意愿认证结果凭证。	String

6.2.2.2 获取云证书签名意愿结果

接口描述：通过意愿认证标识ID获取最终意愿认证凭证。

调用方式：http post/json

请求参数见表13。

表13 获取云证书签名意愿结果请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
time	时间戳（获取当前系统时间，单位为毫秒）	是	String
nonce	100000000内随机整数	是	Integer
authId	本次认证标识ID，通过该属性获取意愿认证结果凭证	是	String
sealCode	印章唯一赋码	是	String
sign	签名值	是	String

返回数据见表14、表15。

表14　获取云证书签名意愿结果返回数据（1）

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	返回详细数据，描述信息见表15	JSON

表15　获取云证书签名意愿结果返回数据（2）

data参数名称	data参数说明	数据类型
authCode	意愿认证凭证	String
authId	本次认证标识ID	String

6.2.2.3　云证书签名

接口描述：云证书签名。
调用方式：http post/json
请求参数见表16。

表16　云证书签名请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
time	时间戳（获取当前系统时间，以毫秒为单位）	是	String
nonce	100000000内随机整数	是	Integer
sealCode	印章唯一赋码	是	String
authId	本次认证标识ID	是	String
authCode	意愿认证凭证	是	String
type	签名值结构类型（P1、P7，为p7时结构体中原文数据为非必填）	是	String
docHash	type为P1时该属性存储待签名数据，type为P7时该属性为加盖印章后的文档杂凑值	是	String
credentNo	身份证号码	是	String
orgCode	企业统一社会信用代码，企业签章必填	否	String
signId	签名ID，获取电子印章返回的signId	是	String
hashType	Hash类型（1：MD5，2：SHA1，3：SHA256，4：SM3）	是	Integer
sign	签名值	是	String

返回数据见表17、表18。

表17　云证书签名返回数据（1）

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	返回详细数据，描述信息见表18	JSON

表18　云证书签名返回数据（2）

data参数名称	data参数说明	数据类型
type	签名数据格式类型（P1,P7）	String
signData	签名数据，Base64编码	String

6.3　电子印章互通互认服务平台 UKey 证书接口要求

6.3.1 基于 UKey 证书电子印章互通互认流程

6.3.1.1 综述

基于UKey证书电子印章互通互认流程见图4。

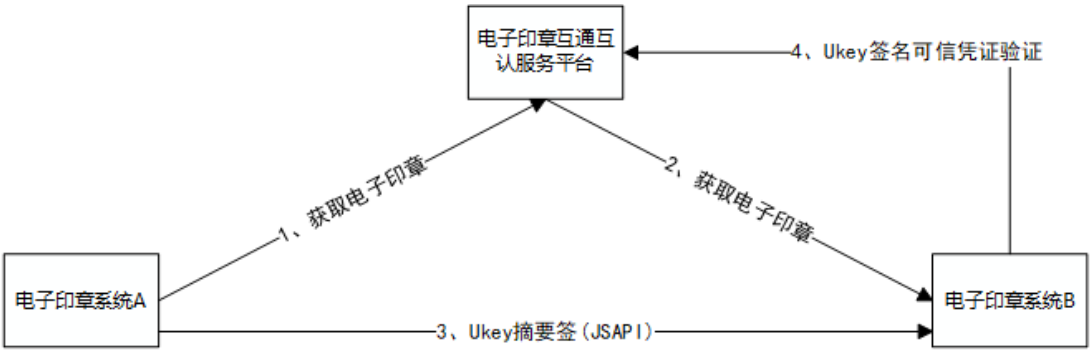

图4 基于 UKey 证书互通互认流程

6.3.1.2 获取电子印章

电子印章系统A向电子印章互通互认服务平台获取电子印章，电子印章互通互认服务平台查询备案电子印章模块，并从备案电子印章模块中获取电子印章，返回给电子印章系统A。

6.3.1.3 摘要签

用户选择UKey印章，电子印章系统A通过JSAPI调用电子印章系统B进行签名，电子印章系统B通过签名ID向电子印章互通互认服务平台进行安全验证，验证通过后将签名数据返回电子印章系统A，完成签名。

6.3.2 UKey 证书电子印章接口

6.3.2.1 UKey 证书签名

接口描述：UKey证书签名（JSAPI），PC端通过JSAPI，调用客户端程序，完成签名。
调用方式：http post/json
请求参数见表19。

表19 UKey 证书签名请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
signId	签名ID	是	String
hashType	Hash 类型（1：MD5，2：SHA1，3：SHA256，4：SM3）	否	Integer
signFormat	签名格式（1：P1，2：P7）	否	Integer
sealCode	印章唯一赋码	否	String
docHash	signFormat为P1时该属性存储待签名数据，type为P7时该属性为加盖印章后的文档杂凑值)；Base64编码传输	否	String
sign	签名值	是	String

返回数据见表20。

表20 UKey 证书签名返回数据

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	Base64编码签名值	JSON

6.3.2.2 获取 UKey 信息

接口描述：调用客户端工具，获取UKey相关信息。
请求方式：POST
请求参数见表21。

表21 获取 UKey 信息请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
type	操作类型（1：获取签名公钥证书；2：获取加密公钥证书）	是	String
sign	签名值	是	String

返回参数见表22、表23。

表22 获取 UKey 信息返回数据（1）

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	返回详细数据，描述信息见表23	String

表23 获取 UKey 信息返回数据（2）

data参数名称	data参数说明	数据类型
UKeyId	UKey设备编号	String
certData	当type为1 时，返回Base64编码签名公钥证书	String

6.4 文档验真

电子印章系统A需要对经电子印章系统B签章的文档进行验证时,向电子印章互通互认服务平台发送文档验真请求,电子印章互通互认服务平台把验证结果返回电子印章系统A，实现互通互认。

请求参数说明见表24。

表24 文档验真请求参数

参数名称	参数说明	是否必填	数据类型
version	版本	是	String
appId	AppId标识	是	String
time	时间戳（获取当前系统时间，以毫秒为单位）	是	String
nonce	100000000 内随机整数	是	Integer
file	文件	是	MultipartFile
sign	签名值	是	String

返回数据说明见表25、表26、表27、表28。

表25 文档验真返回数据（1）

参数名称	参数说明	数据类型
code	结果编码	String
message	返回详细信息	String
data	返回详细数据，描述信息见表26	JSON

表26 文档验真返回数据（2）

data参数名称	参数说明	数据类型
fileName	文件名称	String
fileSize	文件大小	Long

表26　文档验真返回数据（2）（续）

signCount	签章次数	Int
verifyResult	验签结果	Boolean
details	签章明细见表27	Lis

表27　文档验真返回数据（3）

details 参数名称	details 参数说明	数据类型
sealType	印章类型	String
signTime	签名时间	String
provider	服务商	String
certIssuer	证书颁发者信息	String
certOwner	证书使用者信息	String
certSn	证书序列号	String
certValidStart	证书开始时间	String
certValidEnd	证书结束时间	String
sealPicBase64	印章图片	String
sealCode	印章编码	String
flowVoList	验签流程见表28	List

表28　文档验真返回数据（4）

flowVoList参数名称	参数说明	数据类型
step	当前验证环节	String
hint	提示	String
status	状态	0 失败；1 成功

7　数据安全

电子印章互通互认服务平台在数据安全方面应符合GB/T39204-2022、GB/T35273-2020、GB/T22239-2019的要求。

8　安全运维

8.1　日志管理

日志管理应符合下列要求：

a)　全面收集电子印章互通互认服务系统的运行日志，并进行归一化预处理，以便后续存储和处理；

b)　原始日志信息和归一化处理后的日志信息分别进行存储。原始日志信息存储应进行防篡改签名，以便作为司法证据；已归一化的日志进行结构化存储，以便检索和深度处理；

c)　日志留存时间不低于 6 个月。

8.2　密码管理

应符合GB/T 35276、GB/T 32905、GB/T 32918的要求，采用国家密码主管部门批准的密码算法，使用国家密码主管部门认证核准的密码产品。

8.3　安全事件处置管理

8.3.1 安全事件处置规定

应建立安全事件处置规定

a)　制定安全事件处置应急预案。

b)　制定应急响应培训和应急演练规定，并定期组织培训和演练，使相关责任人掌握岗位职责和应急处置策略和规定。

c) 根据应急响应预案，制定安全事件上报规定，包括但不限于：
   1) 记录事件内容，包括但不限于：发现事件的人员、时间、地点，发生事件的系统名称，对其他互联系统的影响，是否需要联系执法机关或有关部门；
   2) 评估事件可能造成的影响，并采取必要措施控制事态，消除隐患；
   3) 按照《国家网络安全事件应急预案》等有关规定及时上报。
d) 根据相关法律法规变化情况，以及事件处置情况，及时更新应急预案和相关规定。

8.3.2 安全事件告知规定

应建立安全事件相关责任人告知规定，包括但不限于：告知形式、告知内容、安全事件影响等。

参 考 文 献

[1] 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
[2]《中华人民共和国电子签名法》 主席令 第29号 2019年
[3]《商用密码管理条例》 国务院令 第760号 2023年
[4]《国务院关于印发“十四五”数字经济发展规划的通知》 国发 29号 2021年
[5]《关于加快推进电子证照扩大应用领域和全国互通互认的意见》 国办发 3号 2022年
[6]《国务院办公厅关于进一步优化营商环境降低市场主体制度性交易成本的意见》 国办发 30号 2022年
[7]《国家网络安全事件应急预案》中央网络安全和信息化领导小组办公室 4号 2017年
[8]《电子认证服务管理办法》 工业和信息化部令 第1号 2009年
[9]《电子认证服务密码管理办法》 国家密码管理局公告 第17号 2009年
[10]《信息安全等级保护管理办法》 公安部、国家保密局、国家密码管理局、国务院信息化工作办公室 公通字第43号 2007年