如有建议或意见，请以书面形式并加盖公章、注明联系人、联系方式，于 2024 年10月 7日 17:00 之前送至我单位，逾期不受理（如邮寄，2024年 10 月7日 17:00 之后到达本公司的邮件将不再受理）。

采购需求

**一、项目预算金额**

本项目预算金额为 55万人民币，最高限价为55万元人民币 （如报价超过最高限价，将作为无效投标）。投标人报价应包括全部货物及服务的价格及相关税费、运费、安装调试、培训、售后服务等其他有关的所有费用，用户不再支付报价以外的任何费用。

**二、项目背景**

徐州市住房公积金管理中心主要负责徐州市全辖区内企事业单位的住房公积金归集、提取以及发放个人公积金贷款等工作。为了健全规章制度、强化资金风险意识、防止网络欺诈、信息泄密、信息抵赖、确保单位用户网络信息安全，我中心已建成电子认证平台系统并正常运行。我中心于2018年推出单位版网上业务工作，截止2024年9月25日，缴存单位用户7164个，开发商用户377个，共计7541用户，依据电子认证相关法律法规及公积金应用系统安全建设要求，为了确保数字证书安全和电子认证应用平稳运行及有效应用，满足未来业务拓展需要，我中心拟就2024-2025年证书延期及电子认证平台运维服务、公积金网上业务系统与数字证书、电子签章系统集成对接服务以及业务系统等级保护测评服务等进行招标。

项目建设应严格按照《中华人民共和国网络安全法》、《中华人民共和国电子签名法》等国家网络安全法律法规要求，本次招标中涉及到数字证书必须支持国密SM2、SM3、SM4等算法，必须符合国家密码管理局《安全电子签章密码应用技术规范》，按照信息安全等级保护三级系统要求，确保数据保密性、完整性和可用性,保障数据安全。

## 三、建设目标

1、通过本项目的全面建设与实施，满足采购人徐州住房公积金网上业务大厅对身份认证、数据加密、电子签章和数据防篡改等方面的安全需求；为缴存单位用户、开发商用户、银行发放CA锁，建立云章系统，为公积金内部人员提供电子签章服务，确保公积金中心电子回单的真实性和完整性，防止篡改和伪造。除上述功能应用外，还通过手写签名服务、手写板应用，实现公积金柜台无纸化业务办理，用户业务办成后直接通过手写板完成业务办理表单手写签字确认，确保电子表单真实性、完整性以及签名人的不可否认性。构建数字证书与电子签章发放与服务机制，为徐州住房公积金业务相关用户提供数字证书和电子签章的申领、开通、延期、挂失、补办、解锁、信息变更、技术支持等服务。同时本期采购内容与我中心现有电子认证基础设施能够兼容对接，并且能够满足我中心2024-2025年业务系统和数字证书、电子签章应用对接需要，保障电子认证服务连续性和可持续性，不得影响现有业务的正常使用。

2、按照信息安全等级保护三级系统要求对现有的业务系统进行测评，并根据测评结果对安全建设提出进一步整改建议。

项目建设遵循标准

1. 《中华人民共和国电子签名法》
2. 《中华人民共和国网络安全法》
3. 《电子认证服务管理办法》
4. 《电子认证服务密码管理办法》
5. 《国家信息化领导小组关于我国电子政务建设指导意见》（中发[2002]17号）
6. 《国务院关于加快推进“互联网+政务服务”工作的指导意见》（国发〔2016〕55号）
7. 《“互联网+政务服务”技术体系建设指南》（国办函〔2016〕108号）
8. 《关于加强网络信息保护的决定》（全国人大2012年12月）
9. 《关于信息安全等级保护管理办法》的通知（公通字〔2007〕43号）
10. 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）
11. 《信息安全技术信息系统安全等级保护实施指南》（GB/T 25058-2010）
12. 《信息安全技术信息系统等级保护安全设计技术要求》（GB/T 25070-2010）
13. 《信息安全技术公钥基础设施 电子签名格式规范》（GB/T 25064-2010）

## 四、技术参数要求

### **1、业务办理身份认证应用系统**

身份认证应用系统，须采用多层防御体系，确保印章的合法、准确和不可抵赖性，包括事前防范和事后防篡改；确保系统安全可靠，须支持大用户并发、快速响应和满足一体化信息系统和各类应用系统的并发对接访问需要；系统结构和软硬件配置须具备稳定性、安全性、可扩充性；需采用人性化设计，要求用户界面设计友好、美观，操作符合日常习惯和工作流程需要，能和通用的字处理软件、网页紧密地结合，做到易学习、易操作，系统提示和帮助信息准确、完整、清晰易懂。系统采用应用基础平台的软件设计架构，能够支持多种应用环境、多种系统的应用集成，具有良好的扩展性和适应能力，以便于通过模块化的扩展能够满足未来各种新的需求。

#### （1）发证系统（RA）

|  |  |
| --- | --- |
| **指标项** | **技术要求** |
| 数字证书签发管理 | 接收数字证书业务对接系统提交的数字证书申请数据 |
| 受理点人员通过在线方式访问数字证书签发业务管理系统，实时为用户签发数字证书 |
| 提供数字证书申请、续期、注销、补办、解锁等业务功能 |
| 签发个人、单位数字证书 |
| 证书有效期最长不超过10年 |
| 系统安全性 | 身份认证 |
| 访问控制 |
| 文件/信息加密 |
| 文件/交易信息的完整性与不可抵赖性 |
| 时间戳服务 |
| 全球可信站点认证 |
| 格式支持 | 发放的数字证书均遵循 ITU X.509 V3 标准 |
| 支持用户按照规范在自定义域扩展增加自己的定义 |
| SM2证书公私钥长度不低于256位 |
| 证书支持中英文显示 |
| 业务管理 | 提供数字证书业务查询功能； |
| 提供各类数字证书业务统计报表功能 |
| 提供用户授权管理功能 |
| 提供证书信息管理功能 |
| 实现与电子认证系统证书签发管理系统软件的证书业务互联互通操作 |
| 证书管理 | 审核：通过审核的信息，获得系统返回的用于下载证书的参考号和授权码。对于不合格的信息，可以拒绝审核通过。被拒绝的信息可以重新做“信息编辑”或者“删除信息”。 |
| 查询：用户证书查询支持按照用户的证件类型、证件号码、用户名称、证书类型、证书状态、时间、DN 等条件进行查询。 |
| 补发、换发：支持在证书有效期内，因证书存储介质损坏或遗忘口令等原因进行证书补发。原有证书撤销，补发后的证书过期日为原证书的过期日。证书即将到期的时候，用户需要换发证书。RA系统进行换发操作后，提供用户新的参考号和授权码。将原有证书撤销。 |
| 撤销：证书永久丢失、密钥泄漏时，审核后可以通过注销证书来停止此证书的使用。证书撤销后，证书序列号永久的发布在目录的撤销列表中（CRL），应用系统检查 CRL 即可拒绝该证书的正常登录。 |
| 冻结：由于用户未交费、临时丢失或某些不确定的原因， 可以暂时冻结该证书，使其证书暂时不可使用。证书冻结后，证书序列号暂时的发布在目录的撤销列表中（CRL），应用系统检查 CRL 即可拒绝该证书的正常登录 |
| 解冻：在得到许可的情况下，可以解除证书的冻结状态，恢复证书的正常使用。证书解冻后，CRL不再有该证书的序列号，从而可以登录应用系统。 |
| CA服务能力要求 | CA服务支持上亿级的证书应用和管理 |
| CA服务可用率不低于99.99% |
| CA服务机房金融级别多级分区管理，保证根证书密钥安全 |
| CA机房至少异地灾备，要求BGP双线 |
| 信息编辑 | 对已经录入的信息可以进行修改和编辑，可以按照一定的条件进行证书查询，然后对用户信息进行编辑修改。 |
| 制证功能 | 对于某些特定的用户（主要是指使用智能卡的用户），申请证书的请求得到批准，并取得了参考号和授权码后，需要RA可以直接为用户下载证书。常见证书的存储介质包括硬盘的文件、智能卡（USBkey）。 |
| 接口功能 | 提供电子认证系统证书签发管理系统之间的通信接口，包括证书管理（注册、审核、更新、注销、密钥恢复等）和证书下载等接口。 |
| 兼容性功能 | 需要提供证书兼容的开发包，实现多家证书和签章的兼容，方便业务系统的统一开发。 |
| ★本次需求 | 1、能够与徐州市住房公积金管理中心业务系统数据、业务实现无缝对接和协同联动，实现网上查询、网上申报、网上审批业务的办理需求，必须保证以往发放的证书接续可用，不得影响现有网上业务的正常使用需求。  2、发证系统壹年系统使用、升级、维护服务 |

#### **五、数字证书安全应用开发套件**

数字证书保存在USBkey中，使用数字证书实现公积金网上业务系统中用户身份证验证，保证用户身份的合法性和唯一性。

|  |  |
| --- | --- |
| **指标项** | **技术要求** |
| 数字证书解析 | 支持国家相关标准的数字证书及PKI/CA公钥体系 |
| 支持标准CSP接口 |
| 支持USBKey介质数字证书读取 |
| 提供数字证书验证、根据证书验证、CRL验证功能 |
| 数字签名 | 实现基于数字证书的数字签名和验签功能 |
| 支持PKCS#1、PKCS#7等数字签名格式 |
| 使用SM2非对称算法 |
| 支持SM3摘要算法 |
| 支持多人数字签名 |
| 加密解密 | 使用SM2非对称加密 |
| 支持SM4等对称加密 |
| 数据编码 | 提供BASE64编码、BASE64解码 |
| 兼容性 | 支持IE、Firefox、Chrome等浏览器至最新版本 |
| 接口要求 | 可支持.Net、Java等接口 |
| 性能指标 | 支持网上营业厅用户数字证书的申请与注册 |
| 至少满足 200 个数字证书注册请求的并发数 |
| 签名验签效率不低于20M/秒 |
| 加解密效率不低于20M/秒 |
| ★本次需求 | 1、能够与徐州市住房公积金管理中心业务系统数据、业务实现无缝对接和协同联动，实现网上查询、网上申报、网上审批业务的办理需求，必须保证以往发放的证书接续可用，不得影响现有网上业务的正常使用需求。  2、数字证书安全应用开发套件系统壹年系统使用、升级、维护服务 |

#### （3）电子签章系统

|  |  |  |
| --- | --- | --- |
| **指标项** | | **技术要求** |
| 基础功能 | 安装平台 | 电子签章客户端软件支持多平台安装，支持Internet Explorer 6.0及以上版本所提供的产品完全兼容Windows XP/Vista/7/8/10 等32位和64位操作系统及IE8/9/10/11、Firefox和Chrome等32位和64位浏览器 |
| 规范性 | 产品支持国产SM2加密算法密钥；  遵循《中华人民共和国电子签名法》关于电子签名的规范，支持SM2算法，符合国家安全标准  支持在国产化环境下电子签章 |
| 系统使用 | 提供仿真放大镜功能，人性化阅读 |
| 中英文字显示可提供工具栏上按钮 |
| 提供产品白皮书或者技术开发文档 |
| 文本格式支持 | 支持PDF、HTML、OFD等数据格式进行数字签名/印章的签入、验证、数据保护、证书查看与数字签名信息查看  支持pdf1.1到1.7版本各种版本的文件 |
| 文档验证 | 支持文档验证功能，电子签章客户端对所签文档进行完整性认证，确定是否被篡改。验证方式包括在线验证和离线验证。 |
| 盖章批注 | 既支持对电子文档“先审批后盖章”，也支持“先盖章后审批”的功能。 |
| 文档保护 | 对文档指定内容进行保护，锁定后的文档只有浏览权限，不能修改 |
| 签章功能 | 单人签章 | 单人签章在3S内；提供接口获取该签完章的签章信息，并提供在服务器端将原文信息和签章信息可以合成的接口；支持多人同时签章然后合成，提供相应的压力测试数据（时间） |
| 签章撤销 | 只有盖章用户才有权限也只能撤销自己所盖的签章。在多级审批盖章或者文档上有多个签章的情况下，用户的撤销签章，并不会直接影响其他已盖签章的效果。 |
| 云章功能 | 支持服务端电子签章，即云签章。区别一般将数字证书和电子签章存放于USB\_KEY中模式，采用集中式管理系统方式，将电子签章和数字证书统一存放于服务端电子签章管理系统并采用硬件加密卡加密存储。通过唯一标识符，将电子签章与数字证书进行绑定，在服务端完成电子签名的过程。 |
| 手写签名功能 | 提供手写板、手写签名服务，个人用户在柜台业务办理通过手写板直接获取个人签名完成对表单的签字 |
| 骑缝章 | 支持文档中签盖骑缝章，支持右骑缝章、中缝章。 |
| 透明签章 | 使用电子签章客户端进行盖章后，签章位于被签内容上面，但并不覆盖内容，效果与纸质盖章相似。 |
| 签章信息查看 | 支持验证结果、盖章时间、盖章人、数字证书、签章外观、签章名称、签章来源、所属单位等签章信息查看  提供签章右键菜单功能，并提供接口控制菜单是否显示  提供通过移动鼠标自选签章位置功能；  提供获取当前文档里签章个数功能；  支持带章打印功能；  支持带章浏览功能 |
| 盖章方式 | 支持鼠标自选位置盖章、关键字盖章、指定位置盖章、批量盖章等方式 |
| 其他功能 | 软件功能 | 输入书签名称，跳转到该书签的位置正常 |
| 获取硬件介质号，获取锁内签章信息 |
| 可以提供第三方时间戳接口 |
| 获取一个PDF总页数 |
| 判断PDF是否盖过章 |
| 功能拓展  要求 | | 包括手写板、指纹设备、公安部设备。采用本地设备进行离线盖章方式时，在导入签章时，可对设备内签章使用次数进行授权设置，用完了需连接到服务器自动更新使用权限。 |
| 提供第三方调用接口；  支持与手机APP进行集成；  支持在移动端进行签章； |
| ★本次需求 | | 1、能够与徐州市住房公积金管理中心业务系统数据、业务实现无缝对接和协同联动，实现网上查询、网上申报、网上审批业务的办理需求，必须保证以往发放的证书接续可用，不得影响现有网上业务的正常使用需求。  2、电子签章系统壹年系统使用、升级、维护服务 |

#### （4）USB KEY 介质

|  |  |  |
| --- | --- | --- |
| **指标项** | | **技术指标要求** |
| 介质硬件要求 | 存储容量： | ≥64K Bytes，可创建私有文件区，实现扩展应用，扩展区的空间不低于30K |
| CPU芯片位数 | ≥32位 |
| 硬件接口 | USB 2.0及以上，不需额外插电 |
| 显示 | USB-Key带LED状态指示灯，能够进行通讯状态指示和电源指示 |
| 功能要求 | 加密算法 | 支持2048/1024位RSA算法密钥对在芯片内生成，芯片内完成2048/1024位RSA算法的签名、认证、加密、解密运算；支持RSA、SM2非对称加密；支持3DES、AES、RC4、SM1、SM4等对称加密 |
| 数字签名 | 实现基于数字证书的数字签名和验签功能，支持PKCS#1、PKCS#7等数字签名格式，支持SHA1、SHA256、SM3等摘要算法，支持多人数字签名 |
| 内置算法 | 内置芯片完成算法实现，密钥不在USB Key以外出现 |
| 加密模块 | 支持MSCSP和PKCS#11标准加密模块，所提供的CSP模块通过微软签名 |
| 随机数生成 | USB-Key内置随机数发生器 |
| 密钥存储 | 支持ITU-T X.509 V3标准证书存储 |
| 删除密钥 | USB-KEY可以根据需要删除不使用的密钥对 |
| 私钥保护 | 设备内部的私钥及其他私密信息必须通过PIN码校验才能访问，PIN码至少支持12个字符，且连续错误次数达到上限时设备自动锁定，必须解锁后才能继续使用，连续输错次数最大不超过10次。验证设备PIN码和修改PIN 码时采用加密传输模式 |
| 技术标准 | | 符合CE、FCC和CSP标准 |
| 使用  要求 | 多密钥 | USBKEY可支持多个密钥和应用，每个应用相互独立 |
| 浏览器： | 支持IE 8/9/10/11和Chrome、Firefox 等最新版本的32或64位浏览器，完全支持HTTPS协议的应用 |
| 支持二次开发 | 提供用户在USBKEY上进行二次开发使用（提供DLL动态库和Active X 控件），方便用户与系统进行无缝集成； |
| 操作系统 | 支持Windows XP/7/Vista/8/10 和Linux等32和64位操作系统 |
| 驱动和控件 | 具有完善的驱动和控件，能够兼容主流操作系统，支持客户在线下载驱动。 |
| ★本次需求 | 1、能够与徐州市住房公积金管理中心业务系统数据、业务实现无缝对接和协同联动，实现网上查询、网上申报、网上审批业务的办理需求，必须保证以往发放的证书接续可用，不得影响现有网上业务的正常使用需求。  2、USB KEY壹年产品使用、系统升级维护服务，包含往年中心已发放使用用户的产品服务。 | |

### **注：招标文件中标“★”项不得负偏离，如出现负偏离则视为不能满足采购方需求而拒绝其投标。**

### **★**2、等保测评服务

根据徐州市住房公积金管理中心要求开展2024年度信息安全等级保护测评，对于此项工作的资质要求：必须要具有测评机构推荐证书的测评机构。测评完成后出具年度信息安全等级保护测评报告。

**此项工作可以由中标单位进行分包。**

## 六、项目实施要求

1、投标人需对本项目涉及的硬件和软件产品提供完整的实施方案，且符合本项目的用户实际业务情况和配置要求，以便最佳的发挥和实现整个系统的性能。

**★**2、项目实施期间，需保障已发放的用户业务办理身份认证系统（包括发证系统、数字证书安全应用套件、电子签章系统、USB KEY介质）的正常使用，业务不中断。

3、项目服务期间，需配合用户单位可能的业务调整需求，不涉硬件设备增加的部分不再额外增加费用。

**★**4、要求至少1名所投产品厂家自有，且经所投产品厂家认证具备系统运维能力人员在中心提供驻场服务，负责系统的日常运行、故障处理、USB KEY产品的办理和管理工作、负责解答用户产品使用过程中的咨询，执行中心上下班考勤时间，服从相关部门科室的管理要求，未经采购人许可，不得随意更换驻场服务人员，每周工作时长不得低于3个工作日，投标时提供拟驻场人员近六个月（不含开标当月）内任意一个月的社保缴纳证明。

5、信息安全等级保护测评工作要依据《信息系统安全等级保护基本要求》、《信息系统安全等级保护测评要求》等文件内容严格开展测评，并形成测评报告。

## 六、售后服务要求

1、项目服务期限：自签订合同后，提供不少于**壹年**的系统维护服务（含软硬件）。

2、售后服务响应时间及维护承诺：

7\*24小时的硬件和软件现场服务；

维护期间出现自身系统故障5分钟内响应，1小时内解决故障问题并提交问题报告；

建立系统服务台账，及时更新用户信息；

## 七、培训要求

1、中标人必须提供相应的应用软件技术和系统操作等方面的培训。有关应用软件的操作培训课程，培训应该在系统试运行前完成，同时提供培训手册。

2、中标人应对采购人相关业务人员进行培训，确保参训的使用人员完全掌握培训内容，技术人员能够完全独立维护整个软件系统。提供操作指南，业务指导手册等使用说明文档。

**八、其他要求**

1、其他见招标文件《拟签订的合同文本》。