# 招标项目技术、服务、政府采购合同内容条款及其他商务要求

前提：本章中标注“\*”的条款为本项目的实质性条款，投标人不满足的，将按照无效投标处理。

## 一、 项目概述

**（一）项目概况：**

本项目共1个包，采购成都市公共卫生临床医疗中心CA签名系统

**（二）标的名称及所属行业：**

|  |  |  |  |
| --- | --- | --- | --- |
| 包号：01 | 品目号 | 标的名称 | 所属行业 |
| 1-1 | CA签名系统 | 软件和信息技术服务业 |

## \*二、 商务要求

1．服务期限及实施地点

1.1 服务期限：合同签订后2个月内完成系统安装、调试、培训。

1.2 实施地点：成都市公共卫生临床医疗中心。

2．付款方法和条件

合同签订后7日内预付合同总金额的30%，系统安装、调试验收合格后30日内支付合同总金额的65%，余下5%合同款待质保期满后7日内无息支付。

3.质保期

3.1质保期：验收合格之日起一年。

4.安装调试及验收

4.1中标供应商负责系统安装、调试。

4.3中标供应商应就系统的安装、调试、操作、维修、保养等对采购人维修技术人员进行培训。系统安装、调试完毕后，中标供应商应对采购人操作人员进行现场培训，直至采购人的技术人员能独立操作，同时能完成一般常见故障的维修工作。

4.4根据《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号），相关国家行业规范及招标文件要求为验收依据进行验收。双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由采购人在招标文件与投标文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。如产品验收不能满足招标文件要求，或者中标供应商虚假响应招标文件要求导致产品不能达到招标文件要求的，合同设备经中标供应商1次优化、维修或设备上线后5个工作日内仍不能达到上述质量及验收标准的，采购人有权退货，并视作中标供应商不能交付货物而须支付违约赔偿金给采购人，采购人还可依法追究中标供应商的违约责任。

## 三、技术、服务要求

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **功能参数要求** | **单位** | **数量** | **备注** |
| **（一）成品软件部分** |
| 1 | 电子签名网关系统 | 1. 支撑数字证书的签名验证。
2. 数字签名功能：支持PKCS#1/PKCS#7格式的签名，支持RSA1024、2048、SM2算法的证书。
3. 签名验证：支持PKCS#1/PKCS#7格式的签名验证功能。
4. 数字信封：支持PKCS#7、10方式数字信封封装和解封。
5. 证书有效性验证：支持对获得的证书进行CRL的有效性验证。
6. 获取证书信息：具备证书解析功能，获取证书中的任意主题信息以及扩展项信息。
7. \*提供系统生产厂商的《电子认证服务使用密码许可证》、《电子认证服务许可证》，两证齐全（提供证书复印件）。
 | 套 | 1 | 　 |
| 2 | 电子签章系统 | 1. 支持跨平台部署，实现统一部署，分级管理；支持Windows，Linux等主流服务器操作系统。
2. 支持IE6到IE11以及其他以IE为内核的浏览器。
3. ▲系统同时支持C/S和B/S模式；需支持用户数量≥100,000人，并发用户数≥2,000人，在线用户数≥20,000人。（提供国家应用软件产品质量监督检验中心/信息安全测评中心/CNAS等国家认可的具有检测检验资质的第三方检测检验机构出具的测试报告复印件）
4. 支持查看报表、生成报表、删除报表，以EXCEL文档在IE浏览器生成。
5. 支持通过签章服务器进行证书管理。
6. 支持以APPCODE的方式对应用系统使用电子签章进行权限认证和控制。
7. 支持局域网。
8. 支持手写签名批注功能（包括手写板输入），配合数位手写板，实现电子签名批注与传统纸张批注相同效果，笔锋、顺畅、方便手写，真迹保留。
9. 支持根据创建不同权限角色。
10. 支持发放管理员。
11. 具备数据定日备份、数据手动备份、数据手动还原、管理员Key密码修改、密钥盘签章迁移、管理员手机管理、密钥盘密码初始化、打印机审核等功能。
12. 支持在服务器端对用户秘钥进行在线初始化。
13. 系统支持第三方验证登录方式（AD域认证）。
14. 提供在线升级签章客户端软件。
15. 支持在office、wps、pdf、html、cad、xml、OFD等多种格式上盖章校验。
16. ▲为业务系统提供PDF文档后台批量签章、数字签名、批量验证等功能：服务器后台PDF生成、文档合并、文档抽取、插入附件、文档水印、电子签章、二维条码、数字签名、域签名、电子签章等，支持多种模式印章调用，支持自动批量签章。（提供国家应用软件产品质量监督检验中心/信息安全测评中心/CNAS等国家认可的具有检测检验资质的第三方检测检验机构出具的测试报告复印件）
17. ▲系统为国家自主安全可控，且通过国家认可的第三方权威机构安全可靠软硬件测试。（提供中国电子技术标准化研究院赛西实验室/信息安全测评中心/CNAS等国家认可的具有检测检验资质的第三方检测检验机构出具的测试报告复印件）
18. ▲提供公安部出具的光学防伪打印系统检验报告。（提供检验报告复印件）
19. 需通过信息系统安全保护等级评测。（不低于三级，四级最高）
20. 支持VPN专网的数据传输。
21. 支持生成带防伪标识的电子文档，输出纸质后，可通过防伪鉴真系统识别真伪。
22. ▲支持对微软OFFICE/金山WPS/PDF文档/HTML表单进行电子签章，手写签名加盖。（提供功能截图证明材料复印件）
23. ▲支持指定打印名称、打印机电脑、打印机IP、拥有人密钥盘、申请日期、指定打印机、指定打印电脑授权打印，打印份数控制等功能，并且能够控制文档是否打印签章，打印黑白签章及原章输出打印。（提供功能截图证明材料复印件）
24. ▲系统须提供电子印章与业务系统集成的文档中间件，该中间件须通过国家版权局或国家知识产权局或公安部信息安全产品检测中心的认证。（提供国家版权局或国家知识产权局或公安部信息安全产品检测中心出具的证书复印件）
 | 套 | 1 |  |
| 3 | 电子签章客户端系统 | 1. 支持操作系统版本：同一版本签章软件适用于Windows2000/XP/2003/VISTA/Windows7/Windows8/Windows10，同时支持32位和64位系统。
2. 支持Office版本：同一版本签章软件适用于OFFICE2000/2003/2007/2010/2013/2016/2019，同时支持32位和64位系统。
3. 支持电子签章与数字签名：对Word/Excel/PDF电子文档加盖电子印章，能同时自动调用数字证书进行数字签名，电子印章与数字签名绑定，保护文档安全性、有效性、完整性和防抵赖，签章在需要时可撤销。
4. 支持手写签名和批注：提供键盘输入文字批注，或者原笔迹手写批注，同时加盖电子印章，保护文档安全。
5. ▲系统需支持MS Office文档和WPS Office文档互验：支持MS Office签章结果可以实现通过WPS Office打开验证文档内容有效性,WPS Office签章结果可以实现通过MS Office打开验证文档内容有效性，达到“互验、互看”的功能。（提供WPS Office或MS Office厂商兼容测试证明复印件）
6. 支持验证文档数字签名有效性，查看数字证书有效性。
7. 支持根据用户应用系统的情况进行功能定制开发（部分功能）各版本签章软件可以同用户应用系统进行开发整合。
8. 包含个人或单位签章的制作。
 | 套 | 200 |  |
| 4 | PDF云签系统 | 1. 支持PDF文档后台批量签章、数字签名、批量验证等。
2. 支持底层基于数字证书数字签名功能实现。
3. 支持提供多重密码控制和证书身份控制，完全满足信息安全的要求。
4. 支持基于国家标准PKI（公共密钥基础设施）体系开发；支持标准的CA认证以及X.509格式数字证书。
5. 证书支持使用USBKEY方式存在。
6. 支持多种定位方式。
7. 提供二次开发应用接口：支持B/S和C/S等架构，具有良好的扩展性。
8. 提供电子签章集成应用的配套文档中间件OFFICE /PDF类。
 | 套 | 1 |  |
| 5 | 数字证书管理系统 | 1. 提供证书签发与管理功能，支持实现：申请、更新、吊销等功能。
2. 支持对最终用户身份证书进行统一管理。
3. 支持为最终用户签发可证明其身份的、具有法律效力的唯一电子标识。
4. 所签发的证书支持完善的电子签名应用集成系统。
5. 支持证书版本：x509 v3。
6. 支持自定义证书扩展项，支持三个扩展项。
7. 能够提供CRL证书吊销列表服务。
8. 能够提供证书策略配置管理，可扩展的配置CA所签发证书的有效期、证书主题、证书扩展、证书版本、密钥长度、证书类型等。
9. \*提供系统生产厂商的《电子认证服务使用密码许可证》、《电子认证服务许可证》，两证齐全（提供证书复印件）。
 | 套 | 1 | 　 |
| 6 | 移动安全认证系统 | 1. APP首页：具备签名数据图形化统计，针对每一个医护人员能够实现对于已签、待签、作废等数据实时统计；各种医院签名的快速导航，包括门诊处方、影像、诊断报告、病历记录、检验报告、医嘱等。
2. 签名管理：支持对待签名、已签名、废弃的签名信息进行分类展现，并且能够快速查询各种信息；对于待签数据能够对医疗数据进行签名；对于已签名的记录可以进行作废处理；能够查看签名数据信息。
3. ▲签名功能：支持移动APP端自动签名功能，在医护人员设置好的自动签名时段内，医疗系统的待签名数据自动完成签名。（提供功能截图证明材料复印件）
4. 用户中心：支持对医护人员基本信息进行管理，并且实现对移动数字证书的申请，医护人员实名认证等；并且，实现对签名的管理，能够实现手写签名、签章的管理；用户中心能够实现自动签名的有效设置，可以根据医护人员排班情况，设置自动签名的时段。
5. 医护人员账号管理：支持对医疗机构的医护人员的账号进行有效管理，包括姓名、身份证号、手机号、所属科室、账号状态等信息。
6. 签名数据管理：支持对通过进行签名的原始数据进行查询、查看，待签名的数据来源于各个医疗系统。
7. 医疗数据类型：支持定义多种类型的待签名数据的数据类型。
8. 待签名数据项自定义：支持自定义不同类型的签名数据的具体数据项。
9. 支持采用SM2算法密钥分割技术来实现对数字证书申请、发放、安装、吊销的生命周期管理。
10. 医疗系统签名接口：支持通过统一的签名接口调用，实现对医疗数据的电子签名，签名完成通过接口回调实现返回医疗签名值反馈给医疗系统。
11. \*提供系统生产厂商的《电子认证服务使用密码许可证》、《电子认证服务许可证》，两证齐全（提供证书复印件）。
 | 套 | 1 | 　 |
| 7 | 数据存储安全管理系统 | 1. 存储容量≥8G，对存储介质进行注册、注销、挂失、权限控制、日志审计。
2. 产品的启动区属于只读状态，可防止攻击者进行篡改；在身份认证之前不能访问数据区密文；在身份认证过程中，存在口令尝试次数限制，可有效防止暴力破解。口令认证过程受安全芯片保护。
3. 在身份认证之后，对安全U盘用户数据区的访问，需要通过调用安全芯片接口。接口会对访问的进程进行合法性校验，第三方进程无法成功通过校验，从而阻止第三方的访问与篡改。
4. 在身份认证之前无法访问数据区密文，无法获取数据明文密文的配对；加密方法无法被第三方程序调试，密钥的生成和维护机制受安全芯片保护。
 | 套 | 1 |  |
| 8 | 数据存储安全认证系统 | 1. 系统采用B/S架构，支持云虚拟化环境安装部署，系统数据库支持集中式或分离式部署；用户可以随时通过升级平台达到扩展端口、增加链路；本次配置并发用户数：≥30000个永久正式授权，无感知准入授权：≥32000个；
2. 系统支持未来扁平化的接入认证功能，支持Cisco 1K和9K系列、华为ME60系列、中兴、华三、阿尔卡特、爱立信、Juniper E系列和Mx系列、锐捷等的外置式Portal认证及RADIUS属性集；支持标准RADIUS协议，符合RFC2865、RFC2866、RFC3576协议。可以与第三方RADIUS、微软AD域控、LADP等配合完成认证，也可以根据RADIUS SERVER扩展RADIUS属性；
3. 支持基于RADIUS的无感知认证，解决用户终端无法通过重定向传递MAC、IP地址、URL、baseName等多种参数问题，同时支持基于MAC数量及共享用户数量实现用户唯一性身份准入，解决用户共享接入网络的安全问题；支持基于客户端类型与认证网关设备联动下发ACL、NAS端口属性，实现IP绑定、VLANID绑定、SSID绑定属性类型，实现用户灵活准入控制；
4. 安全型配置：能够识别恶意请求：跨站脚本(XSS)、SQL注入式攻击、DDOS、恶意扫描、CC攻击、Web ShellCode、恶意爬虫、JAVA攻击、暴力破解等应用层攻击行为；能基于访问行为特征进行分析，能识别盗链、爬虫攻击的能力；内置主流ShellCode特征库，对上传内容进行检查，防止恶意ShellCode上传。
5. 支持通过AI机器自学习能生成安全防护策略；通过自学习能发现参数的名称、类型、匹配频率，可配置匹配到自学习特征后放行，可配置匹配不到自学习特征直接阻断请求。
6. 支持第三方标准OWASP防护规则直接导入，实现快速上线服务及攻击策略修改部署；
7. 黑名单功能，有效防止国内外指定区域攻击；支持基于AI机器学习模式下的智能IP黑名单功能（提供功能截图证明材料复印件）；
8. 系统支持对用户并发及连接频率限制，实现DDOS防御特性，支持一键禁ping功能，支持一键加固系统功能，一键将全部规则全部设置为阻断/拒绝功能，简化运维，提高网络安全性（提供功能截图证明材料复印件）；
9. 支持基于IP、账号组实现认证首页及认证后重定向页面的指定及页面定制功能；支持与统一门户或单点登录系统对接实现网络准入认证、业务统一认证的一体化整合（提供功能截图证明材料复印件）；
10. 系统易维护性要求：支持基于时间的文件、数据库的备份功能，提高系统易用性；提供WEB、CLI等多种配置方式；支持基于知识库的数据库优化功能，配置图形化的一键或者自定义的数据库内存优化器技术，保证系统数据库服务高效运行。
 | 套 | 1 |  |
| **（二）集成服务软件部分** |
| 9 | 时间戳系统 | 1. 支持时间戳的签发及验证功能。
2. 支持时间戳服务器签发的信息包的验证功能。支持验证时间戳信息的有效性、签名证书的有效性等内容。
3. 支持可信时间发布功能。
4. 支持NPT协议，能够与第三方授时中心（如：国家授时中心）、卫星授权时间源进行时间同步，确保所签发时间戳时所获取时间的有效性。
5. 支持获取时间戳信息功能，包含时间戳的时间、数据信息、消息摘要算法等。
6. 支持第三方CA证书导入、导出、备份和恢复等管理功能。
7. 支持多种非对称算法：RSA、SM2非对称加密算法等。
8. 支持配置服务器证书；支持对硬件设备进行配置；支持对时间源签名服务加密设备的配置管理；配置界面操作简单易用。
9. 支持系统自行记录日志，将日志以SYSLOG的方式发送到指定服务器，并提供对日志审计功能。
10. 支持系统备份当前所有配置，保证系统瘫痪时能快速恢复。
11. 支持多种开发接口：客户端提供C/C++、Java、ActiveX/COM组件及定制接口等多种时间戳服务接口，满足各类应用开发平台调用。
12. ▲提供工业液晶触摸屏，支持设备状态查询、监控。（提供截图证明材料复印件）
13. 时间戳签发≥1000次/秒。
 | 套 | 1 |  |
| 10 | 证书集成中间件软件系统 | 1. 支持为业务系统提供统一的、标准的证书管理、数字签名验签、加密解密等功能。
2. 支持证书申请、下载、安装、证书过滤、解析等功能。
3. 支持数字签名验签。
4. 支持windows应用，兼容IE8到IE11、谷歌、火狐、360等浏览器。

支持数据加密解密。 | 套 | 1 |  |
| 11 | 智能USBKEY系统 | 1. 接口支持标准USB1.1，兼容USB2.0,兼容USB3.0。
2. 处理器：32位以上智能卡芯片。
3. 存储空间：≥77K。
4. 证书和标准：X.509 V3,PKCS#11,MS CAPI,SSL V3,IPSec。
5. 内置安全算法：RSA,SHA-1,DES,3DES，SM3，SM2。

支持操作系统：WindowsXP/2003/Vista/Windows 7/Windows 8/Windows 10。 | 个 | 200 |  |
| 12 | 个人证书服务 | 1. 颁发给个人的证书，在有效期内具有区分、标识个人身份的功能。
2. 功能支持身份认证、数字签名和抗抵赖。
3. 服务内容支持证书新增或更新（含吊销、加密密钥恢复、CRL及LDAP查询等）。
4. 格式：X509 V3。
5. 签名算法：SM3/SM2。
6. \*提供系统生产厂商的《电子认证服务使用密码许可证》、《电子认证服务许可证》，两证齐全（提供证书复印件）。
 | 张/年 | 200 |  |
| 13 | 机构证书服务 | 1. 颁发给机构的证书，在有效期内具有区分、标识机构身份的功能。
2. 功能支持身份认证、数字签名和信息加解密、抗抵赖。
3. 服务内容支持证书新增或更新（含变更、吊销、加密密钥恢复、CRL及LDAP查询等）。
4. 格式：X509 V3。
5. 签名算法：SM3/SM2。
6. \*提供系统生产厂商的《电子认证服务使用密码许可证》、《电子认证服务许可证》，两证齐全（提供证书复印件）。
 | 张/年 | 1 |  |