**将乐县总医院电子签名采购参数**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **货物名称** | **数量** | **基本技术参数** |
| 1 | 签名验签设备 | 1台 | 1. 签名验签设备性能要求：2048位RSA签名速度：>=2200次/秒；2048位RSA验证速度：>=19000次/秒；256位SM2签名速度：>=2000次/秒；256位SM2验证速度：>=2200次/秒；SM3杂凑算法：>=1.5Gbps；SHA1杂凑算法：>=22Gbps；
2. 支持国密非对称加密算法SM2；
3. 支持国际非对称加密算法RSA（2048、4096）；
4. 签名验签设备须符合国家密码管理局2014年颁布的GM/T 0029-2014《签名验签服务器技术规范》，具备国家密码管理局颁发的签名验签服务器《商用密码产品型号证书》,须提供证书复印件且加盖投标人公章及国家密码管理局官网截图与链接证明；
5. ★签名验签设备须支持互联网云环境下的签名，设备所集成的云签功能须符合《计算机信息系统安全产品部件第一部分：安全功能检测GA216.1-1999》中完整性鉴别类有关要求，须提供国家部级检测机构出具的云签平台相关检验报告复印件且加盖投标人公章；
6. 采用专用工控机结构和高效冷却智能散热系统，具备物理安全能力，增强主板与内存的接触，防止内存松动和接触不良，提升稳定性，采用固定材料要求具有抗静电性和阻燃性，须提供固定套件和服务器相关的震动、跌落、高低温的测试报告，报告中须明确包含相关测试的环境照片及测试结果，提供测试报告复印件且加盖投标人公章；
7. 采用工控专用冗余双电源；
8. 支持配置时间源设备，自动同步时间；
 |
| 2 | 身份认证设备 | 1台 | 1. 身份认证设备性能要求：2048位RSA身份验证速度：>=19000次/秒；256位SM2身份验证速度：>=2200次/秒；
2. 认证服务支持RSA和SM2算法进行身份有效性验证；
3. 采用证书验证，支持CRL查询；
4. 支持针对不同应用独立提供用户红名单服务；
5. ▲身份认证设备须支持证书安全认证服务，所集成的证书安全认证系统功能须符合公安部《信息安全技术公钥基础设施安全技术要求 GA/T 687-2007》第三级中的相关要求，须提供国家部级检测机构出具的证书安全认证系统相关产品检验检测报告复印件且加盖投标人公章；
6. ★身份认证设备须支持信任管理功能，所集成的信任管理功能须符合《信息安全技术访问控制产品检验规范MSTL\_JGF\_04-010 》（基本级）相关条款所述的有关要求，须提供国家部级检测机构出具的信任管理服务相关检验检测报告复印件且加盖投标人公章；
7. ▲身份认证设备所集成的终端软件系统须符合公安部GA216.1-1999《计算机信息系统安全产品部件第1部分：安全功能检测》不可否认性鉴别相关条款，须提供国家部级检测机构出具的密码终端相关产品检验报告复印件且加盖投标人公章；
8. 身份认证设备所集成的支持包含生物特征在内的多种互联网上身份快速鉴别能力须符合国际FIDO（Fast IDentity Online）规范，须提供资质证书复印件且加盖投标人公章及FIDO Alliance官网截图与链接证明；
9. ★身份认证设备须集成4路或4路以上密码芯片，支持SM1、SM2、SM3、SM4运算，可验证每路密码芯片的SM1算法、芯片ID和设备证书，每路密码芯片须装载至少1本SM2设备证书和1本RSA2048设备证书且设备证书须由权威数字证书机构颁发；
10. 采用专用工控机结构和高效冷却智能散热系统，具备物理安全能力，增强主板与内存的接触，防止内存松动和接触不良，提升稳定性，采用固定材料要求具有抗静电性和阻燃性，须提供固定套件和服务器相关的震动、跌落、高低温的测试报告，报告中须明确包含相关测试的环境照片及测试结果，提供测试报告复印件且加盖投标人公章；
11. 采用工控专用冗余双电源；
12. 支持配置时间源设备，自动同步时间；
 |
| 3 | 电子签章设备 | 1台 | 1. 支持最大印章数：10000；
2. 批量签章速率:>=1Gbps；
3. 提供印章全生命周期管理；包括印章制作、印章颁发、印章吊销；
4. 有完善的权限控制机制，系统管理与应用管理分开；避免超级权限用户；
5. 印章数据只能由制章人制作，使用合法制章人的签名私钥对印章数据进行签名；
6. 签章应用具备安全性设计，具备只能由印章数据中指定的经授权的签章人签章，签章人在电子签章时，在线验证身份和电子印章有效性验证；
7. 签章文件采用PDF和OFD版式，满足签章文件安全、可信、通用和互认的需求；
8. 电子签章设备须符合国家密码管理局2014年颁布的GM/T 0031-2014《安全电子签章密码应用技术规范》，设备所集成的电子签章系统须具备国家密码管理局颁发的电子签章系统《商用密码产品型号证书》,须提供证书复印件且加盖投标人公章及国家密码管理局官网截图与链接证明；
9. ★电子签章设备所集成的存证服务功能须符合《计算机信息系统安全产品部件第一部分：安全功能检测GA216.1-1999》、《信息安全技术通用渗透测试检测条件JCTJ005-2016》中相关条款所述的有关要求，须提供国家部级检测机构出具的存证服务相关检验检测报告复印件且加盖投标人公章；
10. ★电子签章设备须集成4路或4路以上密码芯片，支持SM1、SM2、SM3、SM4运算，可验证每路密码芯片的SM1算法、芯片ID和设备证书，每路密码芯片须装载至少1本SM2设备证书和1本RSA2048设备证书且设备证书须由权威数字证书机构颁发；
11. 采用专用工控机结构和高效冷却智能散热系统，具备物理安全能力，增强主板与内存的接触，防止内存松动和接触不良，提升稳定性，采用固定材料要求具有抗静电性和阻燃性，须提供固定套件和服务器相关的震动、跌落、高低温的测试报告，报告中须明确包含相关测试的环境照片及测试结果，提供测试报告复印件且加盖投标人公章；
12. 采用工控专用冗余双电源；
13. 支持配置时间源设备，自动同步时间；
 |
| 4 | 时间戳设备 | 1台 | 1. 时间戳设备性能要求：2048位RSA时间戳签名速度：>=2100次/秒；2048位RSA时间戳验证速度：>=17000次/秒；256位SM2时间戳签名速度：>=2000次/秒；256位SM2时间戳验证速度：>=2200次/秒；
2. 时间源同步性能〉1000并发；CDMA时间源授时精度为5ms ；GPS/北斗授时精度为10μs；北斗接收通道6，接收灵敏度：-157.6dBW；
3. CDMA工作频率为：800MHz，无SIM卡，接收灵敏度为-166dBW;冷启动时间为：10秒，热启动时间为1秒；GPS工作频率为575.42MHz；接收灵敏度为-163dBW，冷启动时间为：15秒，热启动时间为2秒；
4. 支持CDMA、GPS、北斗三种时间源；在一路不通的情况下，可互相切换，保证时间准确性；
5. 签发时间戳：对客户端发起的时间戳请求进行响应，签发有效；
6. 验证时间戳：验证包含时间戳信息的有效性；
7. 内置设备数字证书，用于支持签发和验证时间戳；
8. 提供的可信时间源，符合国家授时中心的时间精度标准，并且经国家授时中心的权威鉴定测试，时间误差小于7毫秒；
9. 提供验证时间戳请求、获取标准时间、签发时间戳、生成时间戳响应、配置服务密码接口服务；
10. 时间戳设备所集成的授时服务须具有中科院国家授时中心颁发的授时相关的检定证书,须提供证书复印件且加盖投标人公章；
11. 采用专用工控机结构和高效冷却智能散热系统，具备物理安全能力，增强主板与内存的接触，防止内存松动和接触不良，提升稳定性，采用固定材料要求具有抗静电性和阻燃性，须提供固定套件和服务器相关的震动、跌落、高低温的测试报告，报告中须明确包含相关测试的环境照片及测试结果，提供测试报告复印件且加盖投标人公章；
12. 采用工控专用冗余双电源；
 |
| 5 | 加解密设备 | 1台 | 1. 加解密设备性能要求：128位SM系列加解密算法加密/解密速度>=470Mbps；SM系列杂凑算法速度>=2.7Gbps；
2. 服务基于国密SM1和SM4对称算法的数据加密和解密：支持CBC模式的数据加密和解密计算；
3. 数据摘要的产生和验证：支持SM3杂凑算法；
4. 物理随机数的产生：采用由国家密码管理局审批的物理噪声源产生器芯片生成的随机数；
5. 加解密设备须符合国家密码管理局规范GM/T 0030-2014《服务器密码机技术规范》，设备所集成的服务器密码机须具备国家密码管理局颁发的服务器密码机《商用密码产品型号证书》,须提供证书复印件且加盖投标人公章及国家密码管理局官网截图与链接证明；
6. ▲加解密设备须支持网络文件的集中加密管理，所集成的产品须具备国家密码管理局颁发的文件加密相关的产品型号证书，须提供证书复印件且加盖投标人公章及国家密码管理局官网截图与链接证明；
7. 采用专用工控机结构和高效冷却智能散热系统，具备物理安全能力，增强主板与内存的接触，防止内存松动和接触不良，提升稳定性，采用固定材料要求具有抗静电性和阻燃性，须提供固定套件和服务器相关的震动、跌落、高低温的测试报告，报告中须明确包含相关测试的环境照片及测试结果，提供测试报告复印件且加盖投标人公章；
8. 采用工控专用冗余双电源；
9. 支持配置时间源设备，自动同步时间；
 |
| 6 | 个人证书介质USB Key | 500枚 | 1. 证书符合标准：X.509；
2. 支持RSA/SM1/SM2/SM3/SM4算法；
3. 证书中包含身份信息和公钥，用于标识证书持有人的身份；
4. 数字安全证书和对应的私钥存储于硬件USB Key中；
5. USB 2.0全速，通讯速率最高可达12Mbps；
6. 数据存储年限，至少10年；
7. 写次数：至少30万次；
8. 支持Windows、Mac、Linux和国产操作系统；
9. ★投标所采用CA机构须同时支持颁发国密标准SM2证书和国际标准RSA2048或更高级别的证书，证书介质USB Key须支持IE、火狐、Chrome、Safari、360浏览器；投标人须提供与个人证书配套对应数量的互联网微信签名证书，用于备用签名或互联网环境下的签名应用，实现基于USB KEY 与微信帐户的互通；
 |