## 附件：

## 数字签名验签服务系统要求及参数

|  |  |
| --- | --- |
| 序号 | 功能指标要求 |
| 1 | ★为保证医院业务系统数字签名验签服务使用的流畅性，以及后期责任举证的便利性，产品及功能必须与医院前期已部署电子认证服务体系无缝对接。签名验签服务器技术符合GM/T0029《签名验签服务器技术规范》的要求。包含三年维保。 |
| 2 | 提供pkcs1/Pkcs7 attach/Pkcs7 detach/xml Sign 等对多种格式数据的数字签名和验证功能，提供对文件数字签名和验证功能，支持对文件进行SHA256、SM3等方式的数字摘要签名；提供加解密PKCS7格式数字信封功能；提供证书解析功能，获取证书中的任意主题信息以及扩展项信息；支持RSA算法及SM2算法 |
| 3 | 提供通用密码服务，包括摘要运算、随机数、对称加解密、非对称加解密、数字信封、base64编解码等功能，支持SM3、SHA256、RSA、SM2等常见算法。设备支持国密最新算法； |
| 4 | 提供审计监测服务，包括应用日志采集，并与电子认证管理平台审计监测系统配合进行电子认证应用记录集中存储、管理等功能，用于监测电子认证应用情况、事后责任追溯等应用场景； |
| 5 | 证书本地验证服务，主要为业务系统提供局域网方式的证书有效性验证，提速证书认证和局域网运行效率； |
| 6 | 虚拟化服务功能：能支持将系统进行虚拟化分区处理，分别面向不同的接入单位提供独立的安全管理帐户和界面，各接入单位之间的密钥和数据相互逻辑隔离； |
| 7 | 提供证书验证功能，支持对X.509 Version 3、PKCS系列证书的DER和PEM格式的应用与验证 |
| 8 | 提供数据加密、解密功能，支持数字信封加密，支持DES、Tri-DES算法、以及国产密码算法 |
| 9 | 提供CRL的证书有效性验证，CRL更新配置可自动定时进行  |
| 10 | 服务器证书管理：实现对业务系统服务器端密码设备及服务器证书进行配置与管理，可生成服务器证书申请文件。 |
| 11 | 信任源管理：可同时配置多条证书链，验证不同CA的用户证书。 |
| 12 | 动态黑名单管理：可自动更新CRL黑名单、动态更新，不需要重新启动服务。 |
| 13 | 安全存储：基于密码技术构建安全存储区，用于对可信根证书及黑名单文件进行分类安全存储，防止非法操作。 |
| 14 | 提供备份恢复功能，可通过界面备份当前所有配置，保证系统瘫痪时的快速恢复 |
| 序号 | 非功能指标要求 |
| 1 | 提供日志记录，可将日志以syslog的方式发送到指定服务器 |
| 2 | 支持双机、负载均衡 |
| 3 | 提供C、COM 、Java 等主流开发API |
| 4 | 签名能力：大于等于2000次/秒，签名验证：大于等于3500次/秒 |
| 5 | 适用环境：千兆环境，并发用户多 |
| 6 | 支持性能扩展，提供增加硬件加密引擎或并行负载扩展方式。 |
| 序号 | 产品规格要求 |
| 1 | 设备高度：2U |
| 2 | 网络接口: 4个千兆网口 |
| 3 | 电源指标：1个工控电源 |
| 4 | 硬件加密卡：有 |
| 序号 | 资质要求 |
| 1 | ★生产厂商提供的签名验签服务器为自有知识产权（具有软件著作权证书） |
| 2 | ★生产厂商具有国家密码管理局商用密码检测中心颁发的《商用密码产品认证证书》 |