# 产品采购清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 数量 | 单位 | 备注 |
| 1 | 签名验签服务平台 | 1 | 套 | 含5年平台证书 |
| 2 | 时间戳管理平台 | 1 | 套 | 含5年平台证书 |
| 3 | 数字证书受理平台 | 1 | 套 | 含5年平台证书 |
| 4 | 电子签章系统 | 1 | 套 |  |
| 5 | 智能密码钥匙 | 430 | 个 |  |
| 6 | 个人数字证书 | 430 | 张 |  |

# 产品技术要求

## 签名验签服务平台

1.提供pkcs1/Pkcs7 attach/Pkcs7 detach/xml Sign 对多种格式数据的数字签名和验证功能；

2.支持对文件提供数字签名和数字签名验证功能；

3.支持数字信封功能；

4.提供 CRL/OCSP 等多种方式的证书有效性验证；

5.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；

6.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；

7.提供证书存储功能，实现对客户端证书的存储，管理员可以通过页面进行证书导入和查找，业务系统可以通过接口获取已存储的证书；

8.支持服务端负载均衡功能，来解决不能对外提供大数据量服务的问题；

9.提供应用系统访问策略配置，包括所使用服务器证书、所使用根证书链、验证 CRL 策略等配置。

10.支持白名单设置，只有白名单里的 IP 才能访问签名验签服务器；

11.支持白名单设置，只有白名单里的 IP 才能访问签名验签服务器；

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；

15.支持记录管理系统审计日志、查询和导出查询结果，syslog 服务器地址配置；

16.支持双机、负载均衡；

17.提供C、COM、Java、Webservice、HTTP等主流开发API；

18.适用环境：千兆环境；

19.支持国密SM1、SM2、SM3、SM4算法

20.▲提供分级权限管理模式，分为管理员、操作员、审计员三级，分别赋予不同权限，实现权限分割，保证设备内存储数据和程序的安全，提供第三方权威机构出具的《检测报告》作为证明材料；

21.设备高度：2U；

22.电源：550W 1+1冗余电；

23.网络接口：2\*1000M；

24.性能参数：SM2签名≥850次/秒；SM2 验证≥680次/秒;

25.▲产品具备《商用密码产品认证证书》，提供证明材料;

## 时间戳管理平台

1．签发时间戳：接收应用系统发来的时间戳签发请求，签发时间戳后将时间戳返回给应用系统，时间戳服务请求遵循通用的RFC3161标准。

2．验证时间戳：处理应用系统发来的时间戳验证请求，将时间戳验证结果返回给应用系统。

3．支持算法： SM2、SM3等算法。

4．▲提供时间源管理：支持GPS、北斗、4G三合一信号源，提供第三方权威机构出具的《检测报告》作为证明材料；

5．时间同步: 支持NPT、SNTP等时间同步协议。

6．授时精度：0.5-3ms(毫秒)。

7．内置恒温晶振。

8．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。

9．支持双机、负载均衡功能，不需要使用其他第三方双机软件。

10．提供C、COM 、Java 等主流开发API。

11．时间戳签发性能(SM2)≥1000次/秒。

12．可以查看时间源的时间以及状态等信息。

13．提供对于外部导入时间戳服务器证书的上传、查询、导出等功能。

14．提供日志下载以及syslog服务器地址配置。

15．提供服务器IP、网关、服务端口、超时时间、连接数等配置。

16．可以测试时间戳服务器到其他网络地址的互通状态。

17．可以让某个IP或者IP段端访问服务，而不在白名单内的IP或者IP段不能访问服务器的服务。

18．产品符合商用密码产品认证规则。

19．▲产品符合《信息安全技术 公钥基础设施 时间戳规范GB/T 20520-2006》中相关条款所述的有关要求，提供权威机构出具的《检测报告》作为证明材料；

20．产品时间信号可溯源于国家授时中心产生的标准时间。

21．电源指标：双电源。

22．网口要求：2个1000M。

23．设备高度：≤2U。

24．功耗: ≤150W。

25．作温度：0℃-30℃。

26．工作湿度：5%-95%RH，不凝结。

27.▲产品具备《商用密码产品认证证书》，提供证明材料;

## 电子签章系统

1.支持第三方CA机构签发的数字证书。

2.提供基于Web界面的电子印章的制作和管理功能，提供日志审计功能。

3.支持电子印章图片写入证书存储介质中，并与证书绑定。

4.支持自动生成电子印章图片，或支持采集的手写签名。

5.支持对多种文档格式如word\excel\html等的电子签章，实现数据完整性保护，确认签章者身份。

6.提供电子签章中间件，满足C/S环境的电子签章集成。

7.支持原文、印章图片、数字签名的绑定，能够防止篡改。

## 数字证书受理平台

1.在医院建设数字证书受理点，医院证书管理员可通过互联网远程访问CA认证机构数字证书签发系统，可自助完成数字证书生命周期服务。

2.系统提供数字证书申请、制作功能。

3.系统提供数字证书更新、解锁功能。

4.系统提供数字证书吊销、重签功能。

5.系统提供数字证书发放情况统计查询功能。

## 智能密码钥匙

1.标准USB 1.1设备，支持USB2.0接口；

2.容量不小于64K字节；

3.自身的安全要求：具备完善的PIN校验保护功能；

4.内置安全芯片，有一定容量的安全存储空间，可以存储用户的私钥及数字证书；支持证书和标准：X509 V3；

5.支持的算法：SM2、SM3、SM4、RSA2048；

6.支持PC/SC驱动，支持智能卡登录；

7.数据存储时间：不小于10年，可擦写50万次以上；

8.应至少支持建立三级应用；支持多应用，各应用间相互独立；支持多种文件类型（二进制、定长记录、变长记录、循环记录）；

## 个人数字证书

1.标识个人用户网络身份。

2.符合卫生部《卫生系统数字证书格式规范（试行）》。

3.符合卫生部《卫生系统电子认证服务规范（试行）》。

4.证书格式标准遵循x．509v3标准。

5.支持存放介质：智能密码钥匙。

6.支持自定义证书扩展域管理。

7.支持标准的国产SM2商用密码算法。

8.▲产品厂商须具有电子认证服务许可证，产品制造厂商须通过国家卫健委（原卫生部）卫生系统电子认证服务机构复审、测试。