西安教育统计基础数据库平台三级等保、

密码评估及改造项目采购需求

# 项目概况

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **项目名称** | **项目内容** | **数量** | **单价****(万元)** | **总价****(万元)** |
| 西安教育统计基础数据库平台三级等保、密码评估及改造项目 | 完成西安教育统计基础数据库平台三级等保、商用密码评测所必须得平台密码安全及网络安全系统改造、现有教育统计系统升级以及技术支持服务 | 1项 | **79.00** | **79.00** |

西安教育统计基础数据库平台的网络安全等级保护确定为第三级，并须通过商用密码应用安全性评估。目前该系统硬件和应用软件均无法满足商用密码评测及网络安全三级等保要求，需要根据三级等保和商用密码评测要求完成改造，以确保西安教育统计基础数据库平台通过三级等保和商用密码评测。

# 采购内容

## 密码产品采购

根据三级等保及商用密码评测需要，采购2台服务器密码机，对统计平台敏感信息进行加密。

## 应用软件升级

采用国密算法机制对西安教育统计系统进行升级改造，对敏感数据进行机密性、完整性和可用性保护，提升信息安全水平。

## 安全网关

根据三级等保及商用密码评测需要，采购1台安全网关。

## 其他计算机网络安全产品

采购签名服务器、堡垒机各1台，国密数字证书40张，双算法SSL证书1张，智能密码钥匙40块，国密浏览器40套。

## 采购清单：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 名称 | 单位 | 数量 | 备注 |
| 一 | 密码产品 |
| 1 | 服务器密码机 | 台 | 2 |  |
| 二 | 其他计算机网络安全产品 |
| 2 | 安全认证网关 | 台 | 1 |  |
| 三 | 其他计算机安全产品 |
| 3 | 签名服务器 | 台 | 1 |  |
| 4 | 堡垒机 | 台 | 1 |  |
| 5 | 国密数字证书 | 张 | 40 |  |
| 6 | 双算法SSL证书 | 张 | 1 |  |
| 7 | 智能密码钥匙 | 块 | 40 |  |
| 8 | 国密浏览器 | 套 | 40 |  |
| 四 | 应用软件 |
| 9 | 西安教育统计系统升级 | 项 | 1 |  |

# 产品技术要求

按照评测所需要求，配置必要的密码软硬件系统，完成对平台进行系统的改造，满足三级等保和商用密码评测的要求。

## 服务器密码机：

1. 产品规格：设备高度≥2U，支持双电源，实现电路冗余（提供产品图片）。
2. ▲支持密钥安全产生、安装、存储、使用、销毁以及备份恢复全生命周期的管理。（提供第三方权威机构检测报告佐证，提供检测报告复印件）。
3. ▲支持基于RSA/SM2密码算法的数字信封功能，并支持由内部密钥保护到外部密钥保护的数字信封转换功能。（提供第三方权威机构检测报告佐证，提供检测报告复印件）。
4. ▲支持密钥安全存储,保证关键密钥在任何时候不以明文形式出现在设备外，密钥备份文件也受到备份密钥的加密保护。（提供第三方权威机构检测报告佐证，提供检测报告复印件）。
5. 消息鉴别码产生和验证：支持基于SM4 算法的 MAC 产生及验证。
6. 支持设备初始化配置包括密钥产生安装、生成管理员、按照安全机制对密钥安全存储和备份、系统配置、一键检测等功能，保证设备处于正常工作状态。
7. ▲支持访问控制，可通过管理界面设置管理员权限和密钥产生、安装、备份恢复以及日志查询等操作；（提供产品功能截图证明）。
8. 支持国产密码算法：SM2、SM3、SM4等。
9. 支持密钥分散功能。
10. SM2密钥对产生≥1.3万对/秒 ；SM4加/解密≥700Mbps；SM2签名≥3.9万次/秒，验签≥1.8万次/秒。
11. 产品具备公安部产品检测报告。（提供检测报告复印件）
12. 产品制造厂商须具有该产品完全自主知识产权，提供服务器密码机系统软件著作登记证书。（提供证书证明材料）
13. 产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供证书证明材料）
14. ▲具备国家密码局颁发的《商用密码产品认证证书》，满足密码模块二级要求；（提供证书证明材料）。

## 安全认证网关

1. 产品规格：设备高度≥2U；网络接口：≥2个RJ-45 100/1000M电口。
2. 支持基于数字证书的服务器端与客户端的双向认证，多种形式的证书透传功能可以非常方便地在应用层实现基于数字证书的安全认证。
3. 支持国产密码算法：SM2、SM3、SM4等；支持ECC-SM4-SM3、ECDHE-SM4-SM3密钥套件。
4. ▲支持IPsec协议，需支持国密AH和ESP模式下IKE协议; （提供产品功能截图证明）。
5. 支持虚拟站点功能，单台设备要求支持不少于128个虚拟站点。
6. ▲支持安全防护：包括蜜罐、2-7层DDOS、SSL DDoS防御、单包授权、防SQL注入，跨站脚本攻击、WebShell检测。（提供产品功能截图证明）。
7. 访问控制要求：设备能够基于用户和组作细粒度的授权，不同的用户或用户组分配不同的访问权限。能够对3层到7层的访问方式进行控制。能够基于证书字段进行授权。
8. 审计要求：支持对用户日常访问业务系统的行为进行集中审计；支持根据不同条件精确定位相关审计信息；支持对管理员操作审计；支持流量日志采集。
9. 每秒新建连接数≥3,800，最大并发连接数≥275,000，吞吐率800Mbps；支持SSL加密隧道功能，默认含≥25个用户license，最大并发用户数≥500；
10. ▲具备国家密码局颁发的《商用密码产品认证证书》，满足密码模块二级要求（提供证书证明材料）。
11. 产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供证书证明材料）。
12. 产品制造厂商须具有该产品完全自主知识产权，提供安全认证网关系统软件著作登记证书。（提供证书证明材料）
13. ▲提供所投安全认证网关与国内任意一家国密浏览器软件产品兼容性互认证明。

## 签名验签服务器：

1. 产品规格：机架式设备，设备高度≥2U，（提供产品图片）。
2. ▲支持管理员配置功能，管理员配置支持基于数字证书的方式配置“超级管理员模式”和“三权分立模式”（提供第三方权威机构检测报告佐证，提供检测报告复印件）。
3. ▲支持一键检测功能，包括服务接口检测和加密卡检测，保证设备处于正常工作状态（提供产品功能截图证明）。
4. ▲具备完善的身份鉴别机制，支持基于数字证书的身份认证，同时管理员通过管理界面可进行证书管理、应用管理、系统管理以及日志管理等管理操作（提供第三方权威机构检测报告佐证，提供检测报告复印件）。
5. 支持配置NTP同步功能，自动同步时间。
6. 支持多证书链配置，验证不同CA的用户证书，支持 CRL/OCSP 等多种方式的证书有效性验证。
7. 支持国密SM1、SM2、SM3、SM4算法。
8. 主要性能参数：SM2签名7000次/秒，SM2验签2700次/秒。
9. 产品制造厂商须具有该产品完全自主知识产权，提供签名验签服务系统软件著作登记证书。（提供证书证明材料）
10. 产品具备公安部颁发的《计算机信息系统安全专用产品销售许可证》（提供证书证明材料）
11. ▲产品具备国家密码管理局颁发的《商用密码产品认证证书》（提供证书证明材料）。

## 堡垒机

1. 基本规格：标准2U工控机，冗余电源，端口数量：≥2\*USB；≥6千兆电口，支持接口扩展槽；内置≥DDR4-16G内存；内置≥4TB企业级硬盘。
2. 授权数量：最高支持图形连接并发≥50路，字符连接并发≥100路。
3. 资源管理：
4. 需支持对资源及登录账户进行管理功能，包括新增、查询、修改、批量导入、导出、删除、分组等操作；
5. 需支持批量导入阿里云、华为云、腾讯云、AWS、Azure和UCloud等平台云主机；（提供产品功能截图证明）；
6. 需支持主机资源通过IP地址和端口号进行自动发现功能；（提供产品功能截图证明）。
7. 用户管理：
8. 需支持本地账号、USBkey、手机令牌、手机短信和动态令牌等多因子认证功能；（提供产品功能截图证明）；
9. 需支持对用户的创建、删除、编辑、查询等操作功能；
10. 需支持对用户的批量导入功能，导入格式包括xls/xlsx/csv等；
11. 批量导入用户支持覆盖已有用户（提供产品功能截图证明）；
12. 需支持用户USBkey签发功能；（提供产品功能截图证明）；
13. 需支持命令控制类和数据库控制类策略管理功能，命令控制策略内容包括执行动作、有效时间等；有效时间段需满足以周为单位，精确到小时级；执行动作包括断开连接、拒绝执行、动态授权、允许执行等（提供产品功能截图证明）；
14. 需支持对关键资源进行双人授权功能；（提供产品功能截图证明）；
15. 需支持操作命令和命令集管理功能，包括增加、删除、修改、查询、自定义添加等；
16. 需支持可根据用户、用户组、部门、角色、资源、IP段、命令集、生效时间为核心要素设置详细的策略功能；需支持同时以用户、用户组、资源、资源组、账户、账户组为核心要素设置多对多的资源访问授权功能。
17. 运维管理：
18. 需提供类主机网盘存储功能，支持RDP、SSH、VNC协议类型主机的文件上传和下载，并进行审计；需支持邀请其他用户加入自己的会话进行协同操作功能（提供产品功能截图证明）；
19. 需支持对运维脚本管理功能，包括在线编辑、文件导入、修改、下载、查询等；
20. 需支持快速运维管理功能，包括命令运维、脚本运维、文件传输等内容（提供产品功能截图证明）；
21. 需支持同时访问多台设备以及同时对多台设备执行相同命令功能（提供产品功能截图证明）。
22. 需支持SSH、RDP、VNC、Telnet、FTP等协议，需支持通过Xshell、putty、MAC terminal等客户端和Remote Broswer（HTML5）访问目标资源；通过应用发布实现对IE、Chrome、FireFo等应用程序的扩展支持
23. 需支持用户向管理员主动申请资源的运维权限功能，内容上传下载、文件管理、运维时间、资源账号等。
24. 需支持对工单审批管理功能，包括批准、驳回、撤销等（提供产品功能截图证明）。
25. 审计管理：
26. 需支持实时会话审计管理功能，支持查看当前正在进行的会话详情、监控当前会话的操作、中断当前会话等。
27. 需支持可根据文本审计的内容为关键字进行图形搜索功能，搜索出来的结果可以直接定位到相关图形画面进行在线播放；（提供产品功能截图证明）。
28. 需满足运维报表类型包括运维时间分布、运维Top分析、资源访问次数、会话时长、会话协同、双人授权、传输文件等功能；
29. 需支持以PDF/DOC/XLS/HTML等多种格式以天、周、月为粒度自动发送运维报表功能；（提供产品功能截图证明）。
30. 审计安全：需支持审计日志的完整性保护，防止审计日志被恶意篡改。
31. 密评管理：需满足密评要求，支持国产化算法SM2,可通过支持SM2算法的证书认证登录。
32. 产品资质：
33. 需要具有中华人民共和国国家版权局颁发的软件著作权登记证书；并提供证明材料。
34. 需要具有公安部颁发的产品销售许可证；并提供证明材料。
35. 需要具有中国网络安全审查技术与认证中心颁发的IT产品信息安全认证证书；并提供证明材料。
36. 需要具有国家保密科技测评中心颁发的涉密信息系统产品检测证书；并提供证明材料。

## 国密个人数字证书：

1. 能够标示个人在网络身份，证书格式标准遵循x．509v3标准。
2. 证书支持自定义证书扩展域管理。
3. ▲设备证书的颁发机构为可信第三方电子认证服务机构。证书的颁发机构须具备中华人民共和国工业和信息化部颁发的《电子认证服务许可证》，提供复印件证明材料。
4. ▲第三方电子认证服务机构需要通过国家密码管理局安全性审查，提供国家密码管理局的通过安全性审查证明材料。

## 双算法SSL证书：

1. SSL证书服务能力：须满足验证网站域名或IP使用权，提供RSA和SM2双算法证书。
2. 须支持360、奇安信等国密浏览器的SM2算法SSL证书。
3. 须满足RSA、SSL证书支持谷歌、火狐、IE等全球主流浏览器。
4. ▲提供SSL证书与国内任意一家国密浏览器产品兼容性互认证明。
5. ▲SM2国密算法SSL证书的颁发机构为可信第三方电子认证服务机构。SSL证书的颁发机构须具备中华人民共和国工业和信息化部颁发的《电子认证服务许可证》，提供复印件证明材料。
6. ▲第三方电子认证服务机构需要通过国家密码管理局安全性审查，提供国家密码管理局的通过安全性审查证明材料。

## 智能密码钥匙：

1. 支持多种类型的密钥、支持多个密钥的安全存储，支持证书的导入、导出、安全存储
2. 支持通过密码算法实现文件和数据的电子签名及签名验证
3. 公钥私钥对生成时间≤30秒；数字签名和验证时间<1秒/次；SM2签名运算速率≥100次/秒。
4. ▲提供智能密码钥匙与国内任意一家国密浏览器产品兼容性互认证明。
5. ▲产品具备国家密码管理局颁发的《商用密码产品认证证书》，且满足密码模块安全等级第二级相关要求（提供证书证明材料）

## 国密浏览器：

1. 在 Windows 平台支持 Chrome、IE 双核，在国产操作系统支持 Chrome 内核；支持系统环境检测；
2. 基于 SM2/SM3/SM4 密码算法套件的单双向 SSL 协议。

# 应用软件升级技术要求

采用国密算法机制对西安教育统计基础数据库平台进行安全改造，在对敏感数据进行机密性、完整性和可用性保护的同时，减少对外部密码产品的依赖，提升信息安全水平。改造要求如下：

## 用户登录动态验证

将原学校级用户“账号+密码+静态验证码”的登陆方式，整改为“手机号+动态验证码”的登陆方式；动态验证码采用第三方手机短信验证服务；根据学校用户身份设计并研发登陆界面；设计实现短信验证码对接与验证功能。

## 管理员登陆国密加密

将原市级、21个区县级等管理员“账号+密码+静态验证码”的登陆方式，整改为使用国密智能密码钥匙登陆方式；根据用户身份设计并研发登录界面；设计实现用户身份与智能密码钥匙认证功能；设计实现用户身份与智能密码钥匙绑定颁发机制。

## 用户数据国密加密

考虑到用户身份信息数据的机密性与完整性，设计研发用户身份信息国密密码机对接服务；设计研发用户身份信息数据加密流程；实现通过国密密码机对用户身份进行加密的功能。

## 用户权限国密加密

考虑到用户权限访问控制的机密性与完整性，设计研发用户权限访问控制国密密码机对接服务；设计研发用户功能权限、接口访问权限等验证策略；实现通过国密密码机对用户权限访问控制进行加密的功能。

## 业务数据国密加密

考虑到业务数据的机密性与完整性，设计研发业务数据国密密码机对接服务；设计研发对学生、教职工、统计人员等业务数据的存储策略、处理及展示流程，包括上学年数据结转、数据查重等核心业务流程；实现通过国密密码机对业务数据进行加密的功能。

## 日志数据国密加密

设计研发日志数据国密密码机对接服务，保障操作记录等日志数据的机密性和完整性；设计研发操作记录等日志数据的存储策略、处理及展示流程；实现通过国密密码机对日志数据进行加密的功能。

# 项目实施及服务要求

1. 投标人应组织专业技术人员，完成本项目的实施，并提供专业技术服务。
2. 根据三级等保和商用密码评测的要求完成平台网络、安全系统、平台应用系统的升级改造。
3. 根据评测机构的要求进行系统的专项整改。

# 商务要求

1. 、供货期

合同签订后一个月内，完成产品供货、应用系统升级和系统升级改造。

1. 设备质保期

硬件设备质保期一年。

1. 付款方式

合同签订后支付总金额的30%，系统升级完成后支付40%，验收合格后支付剩余尾款。