**上海市干部保健审核监督服务信息系统(2024升级改造)**

**项目需求**

上海市保健事务中心

# 项目背景

## 项目概述

为落实相关法律法规对于信息系统密码应用的要求，结合《国家政务信息化项目建设管理办法》《政务信息系统政府采购管理暂行办法》等规范性依据，本次项目围绕上海市干部保健审核监督服务信息系统进行国密改造，以确保系统严格符合GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》。通过本项目的改造和建设措施，为上海市干部保健审核监督服务信息系统打造一个更加安全、高效和可靠的技术环境，确保保健审核监督工作的顺利开展。

## 建设内容

本次项目内容如下：

1. 通过对上海市干部保健审核监督服务信息系统现状和密码应用需求分析，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称《密码应用基本要求》），从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理等层面，设计该系统密码应用的技术方案、安全管理方案和实施保障方案。
2. 依据《中华人民共和国数据安全法》、《关键信息基础设施安全保护条例》等国家策略要求。本次项目建设一套全面适配国产化环境，服务器私有部署、自主可控的即时通讯产品，实现通讯安全性、使用灵活性以及功能实用性，兼容现有业务系统、适合信创环境，以提升系统的通讯效率和安全性。

## 建设周期

本项目建设周期共4个月，自合同签订之日起2个月内完成项目交付，4个月完成项目验收，期间为试运行期。

# 项目需求清单及参数

## 应用系统改造要求

* + 建设目标

供应商应综合考虑上海市干部保健审核监督服务信息系统在物理和环境、网络和通信、设备和计算、应用和数据等层面的密码应用需求，针对本系统设计合规、正确、有效的密码应用技术方案，应达到《密码应用基本要求》中二级指标要求，并为后续密码保障体系建设、密码应用测评和密码应用安全性评估奠定坚实基础。

* + 建设原则

密码应用技术方案设计遵循以下原则：

1）总体性原则。供应商应根据密码应用安全要求等级，结合密码应用需求和预期目标，对系统的密码应用开展顶层设计，形成涵盖技术、管理和实施保障的整体方案，为在系统中落实密码应用相关要求奠定基础。

2）完备性原则。供应商应围绕本系统实际业务应用与安全要求等级，通过自上而下的体系化设计，综合考虑物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等多个层面密码应用需求，设计系统密码应用技术方案。

3）经济性原则。供应商应在合理、够用的前提下，结合系统规模、并发数、冗余、部署方式、管理模式等情况，设计符合《密码应用基本要求》的密码应用技术方案，确保系统密码应用建设投资合理，规模适度，避免资金浪费和过度保护。

* + 标准规范
* GB/T 36968-2018《信息安全技术 IPSec VPN 技术规范》
* GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》
* GM/T 0023-2014《IPSec VPN 网关产品规范》
* GM/T 0024-2014《SSL VPN 技术规范》
* GM/T 0025-2014《SSL VPN 网关产品规范》
* GM/T 0026-2014《安全认证网关产品规范》
* GM/T 0027-2014《智能密码钥匙技术规范》
* GM/T 0028-2014《密码模块安全技术要求》
* GM/T 0029-2014《签名验签服务器技术规范》
* GM/T 0030-2014《服务器密码机技术规范》
* GM/T 0031-2014《安全电子签章密码技术规范》
* GM/T 0033-2014《时间戳接口规范》
* GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》
* GM/T 0071-2019《电子文件密码应用指南》
  + 建设内容

供应商应通过对上海市干部保健审核监督服务信息系统现状和密码应用需求分析，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称《密码应用基本要求》），从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理等层面，设计该系统密码应用的技术方案、安全管理方案和实施保障方案。

依据《中华人民共和国网络安全法》、等级保护规范要求，为上海市干部保健审核监督服务信息系统规划异地灾难备份系统，可以预先配置自动化复制策略，以确保数据在备份地点的持续更新。在灾难事件发生时迅速启动备份的系统，并在更有安全保护的地方继续运行业务，以保证业务系统的连续可用性。

### 密码应用功能模块建设内容

* + - 1. 身份认证使用证书体系

要求设计并开发用户身份认证模块，对接智能密码钥匙接口，绑定应用系统的用户数字证书和用户ID，实现应用系统对用户的安全身份鉴别。

* + - 1. 应用系统访问控制信息签名验签模块

要求设计并开发应用系统访问控制信息签名验签模块，调用服务器密码机提供的SM2算法数字签名验签功能接口，实现应用服务访问控制信息的完整性保护。

当关键业务流程在系统留下痕迹时（数据落地时），需要对请求信息进行 SM3 摘要算法计算，并调用签名服务器对摘要进行签名。将签名数据一同存储到数据库中，以实现关键业务流程的完整性。

* + - 1. 应用系统重要数据安全传输模块

要求设计并开发重要业务数据安全传输模块，对接安全认证网关SSL安全通信接口，并对HTTPS加密信道进行升级改造，实现应用系统重要数据传输的机密性和完整性保护。

要求利用SSL/TLS协议对数据进行加密，并在后台系统接收请求时进行解密。

* + - 1. 重要数据存储时的加解密

要求设计并开发应用系统重要数据加解密模块，调用服务器密码机提供的SM2算法加解密功能接口，实现应用系统重要数据存储的机密性和完整性保护。

* + - 1. 数据库性能损耗分析；数据库性能优化；数据库读写加解密验证

数据库在进行存储加密后，需要进一步测试和分析数据库系统中的性能问题。涉及检查和评估查询、索引、表结构、数据库配置等方面，供应商需找出潜在问题并采取相应的优化措施，提高响应速度、并发处理能力和整体性能，尽可能避免或减少加解密过程中所带来的性能损耗。此外，还需要对敏感数据进行加密和解密双向验证，确保只有授权用户能够访问数据，并验证读写操作以保证数据的完整性和安全性。

* + - 1. 其他应用安全接口要求

针对包含重要数据或敏感数据的接口，供应商需要配合以下功能来确保接口的安全性：

1. 记录接口的访问日志、异常日志和安全事件，用于安全审计和调查。

2. 对接口的输入参数进行验证和过滤，使用安全的编码方式，确保输入数据的安全性，防止恶意输入和非法数据。

3. 实施适当的防护措施和会话管理机制，控制接口访问频率，避免过度请求对系统造成压力。

4. 进行安全评估和渗透测试，扫描接口的安全漏洞，发现并修复潜在的安全问题等。

## 系统集成总体要求

1. 总集成服务内容包括组织协调项目建设所涉及到所有内容，供应商需制定合理可行的项目管理计划，保证所有建设内容按计划保质保量地开展，供应商对本项目的总体质量和进度负责。
2. 总集成需在保健局现有信息化建设基础上，充分考虑本次项目建设需要、未来业务扩展以及设备采购清单，完成上海市干部保健审核监督服务信息系统差距分析、密码应用改造建设部署、专用通讯系统信创适配等进行合理性规划，供应商需充分考虑到业务实时性要求，全面保障业务的连续性，给出科学、合理的系统集成方案，须在响应文件中以独立章节对此详细描述。同时，供应商具备类似系统的集成能力、交付和运维客诉数据中心的能力，响应时需提供相应的证明材料。
3. 供应商成交后需与采购人共同制定项目进度计划方案，并负责按项目进度计划方案进行实施方案设计、产品到货、集成实施、调试测试和验收及售后服务工作。供应商需要严格按项目进度计划方案执行相关的集成工作，包括新购设备的安装、参数配置，以及未来业务扩展时的系统调整。
4. 供应商在调试前应提出完整的调试计划并经采购人确认，包括设备调试的内容、项目、指标、方法和进度，并提供相应的仪器和工具。供应商有责任对采购人的技术人员提出的问题作出解答。调试中应进行详细记录，系统调试结束后，由供应商做出分析总结并签字后交给采购人验收。
5. 供应商负责提交符合采购人需求的项目施工文档，包含但不限于：实施方案、货物点交单、到货验收单、设备／软件随带资料配件移交单、现场环境核对表、设计变更单、加电测试报告、设备参数配置表、系统软件安装表、现场测试报告、施工日志、竣工图、项目完工报告、试运行申请报告、试运行报告、初步验收申请报告、初步验收报告、项目验收申请报告、项目验收报告等。
6. 本次采购设备安装、调试及集成达到验收标准后，方可进行验收测试。验收标准（包括项目、指标、方式和测试仪器等）应由供应商在验收前10天前提交给采购人，采购人可根据合同及技术规范书进行合理的修改与补充，经双方确认后形成最终验收文件作为验收依据。验收测试合格后，双方签署验收文件，设备开通投入运行，双方签署最终验收文件。
7. 双方签署最终验收文件时，供应商应提交全套、完整的项目手册、配置、管理及维护的全面技术资料，以及所有与用户、设备等相关联的说明、固定资产登记表等资料，并有责任帮助采购人整理、装订、归档。
8. 供应商需安排具备大型信息系统集成经验的工程师作为项目实施期间驻场的技术接口人，对采购人碰到重大集成技术问题进行处理，在接到采购人报告后负责处理相关事务和协调集成方资源。

## 技术参数要求

本项目采购的配套设备总体要求如下：

1. 供应商提供的产品需是市场主流设备，不接受厂商已停产或即将停产的设备，并按照后续章节设备清单要求提供合法获得产品的说明或证明材料（需提供产品授权书、原厂售后服务承诺函等有效证明材料）。

2. 供应商所提供的硬件产品是指：满足本项目功能需求、应用完整的设备或系统。

3. 以下设备清单表中设备，优选国产主流产品，并在业界有良好的口碑的品牌。

4. 本项目摘取下述设备清单中性能指标（下表指标与设备清单中描述重复的以本表为准）作为系统关键指标（带▲标注），供应商需根据下述关键指标进行响应，标明偏离情况，提供关键指标技术参数偏离表，并且提供满足该指标的相关证明材料（需提供相应的第三方测试报告、适配证明、加盖原厂公章的产品官方技术资料白皮书或官方网页截图等证明文件或支持承诺文件）

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 采购参数 |
| 1 | 安全认证网关 | ▲可支持服务器负载均衡功能，负载均衡算法提供最少连接数、轮询、最快响应时间、最小带宽使用率等负载均衡算法，支持20种以上负载均衡算法。 |
| 2 | 安全认证网关 | ▲支持丰富的健康检查方法，包括但不限于：ICMP、TCP、UDP、HTTP、HTTPS、FTP、SNMP、DNS等多种服务器健康检查方式，且设备能够支持通过SCRIPT-TCP、SCRIPT-UDP应用脚本方式，对服务器的FTP, SMTP, LDAP, RADIUS, POP3, DNS, TELNET等多种应用进行检查 |
| 3 | 安全认证网关 | ▲支持客户端证书过滤功能，支持基于issus、subject等项拒绝连接； |
| 4 | 安全认证网关 | ▲安全认证网关及SSL客户端需为同一厂商，均需具备国家密码管理局所颁发的《商用密码产品认证证书》,其中安全认证网关/具备国家版权局颁发的《计算机软件著作权登记证书》/具备全球IPv6测试中心颁发的《IPv6 Logo 认证证书》/具备两种以上商密浏览器的产品兼容性认证证书/响应产品CPU、操作系统具备原厂产品兼容性认证/同系列产品具备两家以上第三方检测中心出具的检测报告 |
| 5 | 密钥管理系统 | ▲具备国家密码管理局所颁发的《商用密码产品认证证书》/具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 6 | 签名验签服务器 | ▲支持基于IP地址校验和基于访问口令校验的安全访问，只允许合法的业务应用通过API访问，防止恶意访问。 |
| 7 | 签名验签服务器 | ▲支持设备监控包括可监控CPU温度、风扇转速、CPU使用率、网口流量等状态。 |
| 8 | 签名验签服务器 | ▲支持弱算法过滤，可灵活配置摘要算法是否允许签名和验签名、非对称算法的秘钥长度、对称算法是否允许加密或解密； |
| 9 | 签名验签服务器 | ▲签名验签服务器及完整性保护工具需为同一厂商，均需具备国家密码管理局所颁发的《商用密码产品认证证书》，并标明GM/T 0028-2014密码模块技术要求中第三级要求/具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 10 | 服务器密码机 | ▲支持通过前面板钥匙销毁密钥、带电开机箱销毁密钥和不带电开机箱销毁密钥。 |
| 11 | 服务器密码机 | ▲具备国家版权局颁发的《计算机软件著作权登记证书》/具备国家密码管理局所颁发的商用密码产品认证证书，满足GM/T 0030《服务器密码机技术规范》、GM/T 0028《密码模块安全技术要求》第二级要求/设备原厂商通过CMMI5认证 |
| 12 | VPN网关 | ▲不依赖第三方软件即可实现OTP认证 |
| 13 | VPN网关 | ▲支持单点登录，支持为文件共享、Web资源、远程桌面资源开启单点登录 |
| 14 | VPN网关 | ▲具备零信任特性，集网络隐身、自适应身份认证、动态访问控制、持续性环境检测等能力于一体 |
| 15 | VPN网关 | ▲具备国家密码管理局所颁发的《商用密码产品认证证书》/具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 16 | 身份认证管理系统 | ▲系统以及数字证书必须符合国家、行业以及《商用密码管理条例》、《中华人民共和国电子签名法》和《电子认证服务管理办法》等相关法规标准，能满足实际的业务环境要求，具备扩展性以满足定制化改造需求；应提供标准的、通用的、多样化的接口形态，并满足与各类应用系统的集成需求； |
| 17 | 数据库加密系统 | ▲切面加密功能要求:支持业务代码无需改造的数据库切面加密功能，加密粒度支持字段级;支持切面加密细粒度权限管理：配置特定应用查看明文权限、配置特定应用使用特定策略;支持存量数据转加密;切面加密任务运行失败时支持任务重置;支持保留格式加密，保持数据格式和长度不变;支持密文检索;支持数据的明密文识别;支持切面加密配置的生命周期管理，防止数据库重复加密或二次解密;提供可视化工具，进行加密数据运维管理;支持达梦、人大金仓、南大通用等主流国产数据库 |
| 18 | 数据库加密系统 | ▲切面脱敏功能要求:支持字段级的切面脱敏能力，同时保持数据库数据不做修改;支持自定义脱敏策略，支持脱敏配置的产生、分发、生效、失效等全生命周期管理;提供可视化工具，进行脱敏数据运维管理 |
| 19 | 数据库加密系统 | ▲具备国家版权局颁发的《计算机软件著作权登记证书》/具备国家密码管理局所颁发的《商用密码产品认证证书》，达到GM/T 0028-2014《密码模块安全技术要求》二级安全要求 |
| 20 | 专用通讯系统平台 | ▲支持发送阅后即焚消息，在查看消息后手机端文字10秒，文件30秒，PC端文字5秒自动消失。安全设置支持:Mac地址绑定；IP地址绑定；移动端设备号验证；首次登录修改密码；消息传输加密；禁止移动端下载文件；禁止移动端登录；公告/云盘文件加密；文件传输加密；文件流转记录；账号/部门有效期；多设备在线；要求兼容支持所有国际国内主流客户端与服务器端操作系统与CPU芯片、数据库、中间件并实时更新升级 |

54. 以下清单可供响应参考，由供应商自行开展深化设计，参考清单数量为最低配置，对于未列出的但对系统的正常运行和维护必不可少的配件、辅助材料等，供应商应补充并包含在总报价中，确保系统的可用性，满足采购文件要求。如供应商原因引起缺漏项，造成系统无法搭建完成，由供应商免费增补至验收合格，采购人不再额外增补费用。

| 序号 | 名称 | 数量 | 单位 | 维保期限（年） | 提供产品授权书、原厂售后服务承诺函 |
| --- | --- | --- | --- | --- | --- |
|  | 安全认证网关 | 2 | 台 | 3 | 是 |
|  | 密钥管理系统 | 1 | 台 | 3 | 是 |
|  | 签名验签服务器 | 1 | 台 | 3 | 是 |
|  | 服务器密码机 | 2 | 台 | 3 | 是 |
|  | VPN网关 | 10 | 台 | 3 | 是 |
|  | 身份认证管理系统 | 1 | 套 | 3 | 是 |
|  | 完整性保护工具 | 1 | 套 | 3 | 是 |
|  | 数据库加密系统 | 1 | 台 | 3 | 是 |
|  | 站点证书 | 1 | 套 | 1 | 是 |
|  | 专用通讯系统平台 | 1 | 套 | 1 | 是 |

### 安全认证网关

|  |  |  |
| --- | --- | --- |
| **编号** | **指标项** | **采购要求** |
| 1 | 硬件要求 | 标准1U设备，支持双电源，支持国产操作系统，不少于4核4线程国产CPU X1，不少于1T硬盘，不少于8G内存，不少于4个千兆电口，不少于2个千兆光口 |
| 2 | 性能要求 | SSL吞吐率（国密）不低于450Mbps SSL每秒新建连接数（国密）不低于800 SSL最大并发连接数（国密）不低于200,000 |
| 3 | 算法要求 | 对称算法：SM4、3DES、AES等 非对称算法：SM2、RSA2048、等 摘要算法：SM3、SHA-1、SHA256等 |
| 4 | 功能要求 | 支持证书字段透传功能，转发模式包括URL、cookie、header且可自定义名称； |
| 5 | 支持SSL拦截白名单，只允许通过指定的域名访问特定的SSL服务； |
| 6 | 支持透明模式、反向代理模式以及三角传输模式，支持旁路连接方式（单臂模式）和串连连接方式（双臂模式）。 |
| 7 | 支持多种高可用性模式：A/A模式，A/S模式，支持多台设备的集群，支持双机failover切换功能，能够及时发现设备故障，支持会话同步； |
| 8 | 支持通过WEBUI、CLI进行完整配置以及设备管理； |
| 9 | 可支持服务器负载均衡功能，负载均衡算法提供最少连接数、轮询、最快响应时间、最小带宽使用率等负载均衡算法，支持20种以上负载均衡算法。 |
| 10 | 支持丰富的健康检查方法，包括但不限于：ICMP、TCP、UDP、HTTP、HTTPS、FTP、SNMP、DNS等多种服务器健康检查方式，且设备能够支持通过SCRIPT-TCP、SCRIPT-UDP应用脚本方式，对服务器的FTP, SMTP, LDAP, RADIUS, POP3, DNS, TELNET等多种应用进行检查 |
| 11 | 支持高可靠性HA，支持以CPU温度、CPU使用率、SSL加速卡等作为阈值监控对象，并支持基于“与”、“或”等逻辑关系运算组合监控对象进行HA切换，并且HA设备之间能够实现配置同步和会话状态同步。 |
| 12 | 支持客户端证书过滤功能，支持基于issus、subject等项拒绝连接； |
| 13 | 产品资质 | 安全认证网关及SSL客户端需为同一厂商，均需具备国家密码管理局所颁发的《商用密码产品认证证书》,其中安全认证网关 |
| 14 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 15 | 具备全球IPv6测试中心颁发的《IPv6 Logo 认证证书》 |
| 16 | 具备两种以上商密浏览器的产品兼容性认证证书 |
| 17 | 响应产品CPU、操作系统具备原厂产品兼容性认证 |
| 18 | 同系列产品具备两家以上第三方检测中心出具的检测报告 |

### 密钥管理系统

|  |  |  |
| --- | --- | --- |
| **编号** | **指标项** | **采购要求** |
| 1 | 软硬件形态 | 支持在裸服务器、虚拟机环境运行 |
| 2 | 支持银河麒麟/中标麒麟/统信UOS等操作系统 |
| 3 | 支持达梦/人大金仓/南大通用/云图/神通等数据库 |
| 4 | 支持x86/ARM架构CPU平台 |
| 5 | 密钥管理功能 | 非对称密钥生成及生命周期管理 |
| 6 | 在用库、历史库、备用密钥库 |
| 7 | 定时、即时产生密钥 |
| 8 | 管理员、业务员角色管理（标准角色） |
| 9 | 支持多CA |
| 10 | 用户密钥恢复，司法密钥恢复（暂同用户密钥恢复） |
| 11 | 密钥统计查询 |
| 12 | 日志查询，审计 |
| 13 | 密钥库的备份与恢复 |
| 14 | 资质要求 | 具备国家密码管理局所颁发的《商用密码产品认证证书》 |
| 15 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |

### 签名验签服务器

|  |  |  |
| --- | --- | --- |
| **编号** | **指标项** | **采购要求** |
| 1 | 硬件要求 | 标准1U设备，支持双电源，支持国产操作系统，不少于国产CPU X1，不少于1T硬盘，不少于8G内存，不少于4个千兆电口，不少于2个千兆光口 |
| 2 | 性能要求 | SM2签名不低于20KTPS，SM2验签不低于11KTPS |
| 3 | 算法要求 | 对称算法：SM4、3DES、AES等 非对称算法：SM2、RSA2048等 摘要算法：SM3、SHA-1、SHA256等 |
| 4 | 功能要求 | 单台设备支持配置多个签名验签服务 |
| 5 | 支持Attached签名验签、Detached签名验签、attached事后验签、RAW签名验签、XML封皮签名验签、XML封内签名验签、XML分离签名验签； |
| 6 | 支持提供数字信封功能对原文数据高强度加解密、支持HMAC加解密； |
| 7 | 支持基于IP地址校验和基于访问口令校验的安全访问，只允许合法的业务应用通过API访问，防止恶意访问。 |
| 8 | 支持设备监控包括可监控CPU温度、风扇转速、CPU使用率、网口流量等状态。 |
| 9 | 支持弱算法过滤，可灵活配置摘要算法是否允许签名和验签名、非对称算法的秘钥长度、对称算法是否允许加密或解密； |
| 10 | 支持对PDF文件格式进行电子签名和验证，可自定义签名区域内显示的图章、说明文字及签名证书信息。 |
| 11 | 要求设备支持提供SDF接口，具备非对称、对称及杂凑运算和密钥管理SDF接口。 |
| 12 | 资质要求 | 签名验签服务器及完整性保护工具需为同一厂商，均需具备国家密码管理局所颁发的《商用密码产品认证证书》 |
| 13 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |

### 服务器密码机

|  |  |  |
| --- | --- | --- |
| **编号** | **指标项** | **采购要求** |
| 1 | 硬件架构 | 专用2U机架式设备，支持双电源，支持国产操作系统，不少于8核16线程国产CPU X1，不少于1T硬盘，不少于8G内存，不少于2个千兆电口 |
| 2 | 设备支持机械锁，开机箱需要钥匙开锁 |
| 3 | 性能要求 | SM2签名/验证速率不低于22000/18000次/秒 SM3杂凑速率不低于885Mbps SM4计算速率不低于870Mbps |
| 4 | 接口规范 | 服务器密码机API接口符合《GM/T 0018-2012 密码设备应用接口规范》。 |
| 5 | 算法要求 | 对称算法：SM4、3DES、AES等 非对称算法：SM2、RSA2048等 摘要算法：SM3、SHA-1、SHA256等 |
| 6 | 物理随机数的产生 | 采用国家密码管理局认可的双WNG系列物理噪声源芯片生成真随机数。 |
| 7 | 密钥产生 | 支持通过设备内密码卡物理噪声源生成和存储RSA、SM2密钥对。 |
| 8 | 数字签名验签 | 可以根据需要使用内部存储的私钥或外部私钥进行数字签名和验签，实现对各类电子数据的数字签名功能，支持多种数字签名格式，支持文件签名验签功能。 |
| 9 | 数字信封功能 | 支持基于RSA和SM2密码算法的数字信封，并支持由内部密钥保护到外部密钥保护的数字信封转换。 |
| 10 | 三级密钥管理体系 | 分别为系统保护密钥、用户密钥对及密钥加密密钥KEK、会话密钥，逐层加密。 |
| 11 | 密钥存储 | 设备内密码卡可存储签名密钥对和加密密钥对，并且私钥部分受系统保护密钥加密保护，以密文的形式存储在服务器密码机中。 |
| 12 | 密钥备份及恢复 | 支持基于备份密钥保护下的密钥备份和恢复，保证系统的安全性和可靠性。 |
| 13 | 密钥销毁 | 支持通过前面板钥匙销毁密钥、带电开机箱销毁密钥和不带电开机箱销毁密钥。 |
| 14 | 用户权限控制 | 具有用户管理功能，对访问用户分级管理，提高密码设备自身的安全性。 |
| 15 | 连接白名单 | 通过对连接白名单的支持，实现了密码机对应用服务器的授权认证，进一步提高了系统的安全性。 |
| 16 | 多机并行 | 多机并行可以提供容错功能，当有密码机出现故障时不影响业务密码运算。多机并行还可以提高密码运算性能。 |
| 17 | 资质要求 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 18 | 具备国家密码管理局所颁发的商用密码产品认证证书，满足GM/T 0030《服务器密码机技术规范》、GM/T 0028《密码模块安全技术要求》第二级要求 |
| 19 | 设备原厂商通过CMMI5认证 |

### VPN网关

|  |  |  |
| --- | --- | --- |
| **编号** | **指标项** | **采购要求** |
| 1 | 硬件要求 | 标准1U设备，支持双电源，支持国产操作系统，不少于4核国产CPU X1，不少于1T硬盘，不少于16G内存，不少于6个千兆电口，不少于4个千兆光口，不少于500个并发用户授权 |
| 2 | 性能要求 | 最大并发用户数不低于6,000 最大加密吞吐率不低于500Mbps 每秒新建连接数不低于700 |
| 3 | 算法模式 | 支持SM2、SM3、SM4等商用密码算法 |
| 4 | 通信加密 | 支持SSLv3、TLSv1.0、TLSv1.2、TLS1.3等通信加密协议 |
| 5 | 身份认证 | 支持用户名口令、证书认证、扫码登录、短信验证码、复杂验证码、邮箱等认证方式，支持LocalDB、LDAP、RADIUS、NTLM、HTTP/HTTPS认证等 |
| 6 | 支持证书认证，并支持指定证书字段和认证用户名进行唯一绑定 |
| 7 | 支持OAuth、SAML2.0认证，支持企业微信、微信、支付宝、钉钉等第三方认证 |
| 8 | 不依赖第三方软件即可实现OTP认证 |
| 9 | 支持协同签名的国密双向认证，支持协同签名证书下载、双向证书认证功能，协同签名产品要求与网关产品为同一品牌 |
| 10 | LocalDB支持认证模式选择、动态码绑定、服务器、账户和组设置、密码过期处理、账号锁定功能等 |
| 11 | LDAP认证支持LDAPv3协议所有的LDAP服务器，包括OpenLDAP和活动目录（AD），单个虚拟站点支持配置32个LDAP服务器 |
| 12 | 支持硬件绑定认证，用户可唯一绑定终端的CPU、操作系统、硬盘等硬件信息，满足绑定关系的账号才可登录；支持自动绑定和手动绑定；并支持针对domain和sid的正则表达式过滤，满足条件方可登录 |
| 13 | 权限控制 | 支持基于角色的访问控制（按照用户名、组名、登录时间、源IP和登录方法定义角色） |
| 14 | 支持IP、端口、协议、URL级别的访问控制，支持配置允许和拒绝策略，对于不同用户，不同角色实现不同的控制 |
| 15 | 支持外部服务器的组映射授权,支持LDAP的memberOf属性和OU属性进行授权 |
| 16 | 应用发布 | 支持内网3层/4层/7层的内外网应用发布 |
| 17 | 支持基于多种TCP/UDP的B/S或C/S结构的业务系统，支持多种使用动态端口的应用协议，如：FTP、TFTP、Telnet、Oracle、SQL Server等 |
| 18 | 支持所有基于Web的B/S、C/S应用的访问，支持自定义内容改写 |
| 19 | 支持单点登录，支持为文件共享、Web资源、远程桌面资源开启单点登录 |
| 20 | 可以扩展支持最多256个虚拟站点，可配置独立管理员、独立访问门户、认证方式、访问控制列表、用户源等，多站点安全策略互不干扰 |
| 21 | 支持自定义门户界面，支持门户主题导入，支持自定义响应页面、登录页面、注销页面、SMS认证页面、欢迎页面、修改用户密码等页面 |
| 22 | 终端接入 | 支持客户端的安全检查机制，可以检查客户端的个人防火墙、防病毒系统，检查客户端的文件、进程、注册表、操作系统及其版本等信息，并且可以根据检测的结果赋予不同的访问权限 |
| 23 | 支持VPN客户端可使用不少于两种虚拟网卡类型进行连接 |
| 24 | 客户端支持多个接入点最优自动优选接入 |
| 25 | 支持VPN客户端可自定义界面显示信息，支持默认接入点的自定义封装，安装完后即可直接连接 |
| 26 | 支持安全终端接入，支持Windows、Linux、iOS、Android、MacOS、统信UOS、银河麒麟等，支持以Web方式接入VPN设备，包括常见浏览器（如IE、Firefox、Chrome、Microsoft Edge和Safari等） |
| 27 | 支持通过XML-RPC、Restful API接口实现与应用程序对接 |
| 28 | 系统要求 | 具备零信任特性，集网络隐身、自适应身份认证、动态访问控制、持续性环境检测等能力于一体 |
| 29 | 支持管理员手动创建用户，支持从文件（CSV文件）批量导入用户 |
| 30 | 支持在线用户状态查看，支持在线用户的强制下线，支持对同一个账号登录会话个数限制，且能自定义策略，对超出限制的会话请求可拒绝或者踢出旧的会话让新的会话登录 |
| 31 | 支持多种高可用性模式：A/A模式，A/S模式，Cluster模式 |
| 32 | 可根据系统健康检查、硬件类、软件类、网络环境类等健康状态与使用率等自定义HA失效切换规则 |
| 33 | 支持独占型虚拟网关，每个虚拟网关独占IP地址和域名，用户可以通过域名或者IP地址访虚拟网关 |
| 34 | 日志格式符合Syslog标准，每种类型日志的表象都支持WELF格式的完整审计日志 |
| 35 | 支持SNMP v1、v2和v3版本；维护并提供自有SNMP MIB供管理员对设备进行监控和管理；支持SNMP Trap |
| 36 | 支持Email系统告警功能，支持通过Email方式将管理员预设的告警信息发送至指定邮箱，完成对设备的监控 |
| 37 | 支持记录系统日志、访问日志、管理日志、流量日志等，并支持日志建模，实现对用户的所有访问、操作行为的监控和审计；系统支持将审计信息发送到第三方统一审计平台和其他Syslog服务器 |
| 38 | 支持对系统硬件资源使用率的实时监控:通过图形界面方式动态实时监测系统 CPU资源、存储空间、系统内存的使用情况以及各网络接口的网络流量监测，便于系统的维护和问题定位；支持自定义日志显示等级，包含（信息、警告、错误、调试） |
| 39 | 支持支持基于WEB和SSH方式的远程管理方式，进行安全的配置管理，并且支持Console和SNMP协议的管理 |
| 40 | 支持单臂模式、主备模式、集群模式、分布式集群模式的部署 |
| 41 | 支持系统备份、系统升级功能，支持双分区、四分区一键版本升级与切换功能，管理员可一键切换至任意版本，无需重新配置 |
| 42 | 产品资质 | 具备国家密码管理局所颁发的《商用密码产品认证证书》 |
| 43 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |

### 身份认证管理系统

|  |  |  |
| --- | --- | --- |
| **编号** | **指标项** | **采购要求** |
| 1 | 功能指标要求 | 能够利用现有数字证书认证系统，实现与合法第三方CA机构运营系统对接，实现第三方权威数字证书的注册、受理、发放、状态变更等业务功能。 |
| 2 | 支持多种格式证书，包括个人证书、单位数字证书。 |
| 3 | 签发的数字证书遵循x．509v3标准证书格式，支持自定义证书扩展域管理。 |
| 4 | 证书业务办理（申请、更新）要求能同时支持三种模式的证书办理方式：一种是面对面由管理员代为进行系统资料填写、提交、证书业务办理的模式；第二种是由业务系统的用户的申请信息，由业务系统、用户身份管理系统或虚拟身份所在系统提供身份信息并进行审核。申请信息提交后审核由后台系统接口自动完成；第三种是要求RA系统面向应用系统提供证书申请、证书下载、证书更新、证书查询和验证等接口服务，即用户或管理员可以直接通过应用系统侧完成证书发放和状态管理功能。 |
| 5 | 能够面向企业提供统一的数字证书服务，实现用户证书信息查询和管理；提供证书批量制作功能，支持用户信息的批量导入。 |
| 6 | 系统管理功能：系统管理，包括对CA机构管理（可多CA机构接入）、用户管理、业务系统管理、系统证书管理、权限角色管理。 |
| 7 | 受理点管理：能支持受理点管理（LA），能进行受理点的授权和管理员管理。 |
| 8 | 证书到期提醒：提供证书到期提醒功能，可以通过设置时间、邮件等方式进行提醒。 |
| 9 | 能够提供详尽的查询、统计、报表功能，能统计用户、证书、机构、时间段内、应用领域等不同维度的证书发放和使用情况，可进行柱状图形展现，能导出excel报表。 |
| 10 | 能够支持完整的权限管理功能，支持业务管理员、操作员、审计员多级管理机制。 |
| 11 | 能够提供业务日志管理功能，能记录系统所有的业务操作日志，包括系统登录、权限变更、业务办理、系统维护等记录。 |
| 12 | 能够提供数据备份、恢复功能，为管理员提供基于web页面的操作界面实现数据备份、恢复，降低系统维护复杂度。 |
| 13 | 系统以及数字证书必须符合国家、行业以及《商用密码管理条例》、《中华人民共和国电子签名法》和《电子认证服务管理办法》等相关法规标准，能满足实际的业务环境要求，具备扩展性以满足定制化改造需求；应提供标准的、通用的、多样化的接口形态，并满足与各类应用系统的集成需求； |
| 14 | 支持SSL通道加密：提供通道加密功能，保障数据传输安全。 |
| 15 | 非功能指标要求 | 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 |
| 16 | 提供日志记录，可将日志以syslog的方式发送到指定服务器 |

### 完整性保护工具

|  |  |  |
| --- | --- | --- |
| **编号** | **指标项** | **采购要求** |
| 1 | 产品形态 | 基于签名验证服务器开发的文件签名和验证的软件，要求提供内置密码算法模块组件产品形态为API |
| 2 | API库支持C、JAVA、JS开发语言编译生成的类库。 |
| 3 | 算法要求 | 支持SM2、SM3、SM4国家标准密码算法和AES、DES、3DES、SHA系列、RSA等国际算法。 |
| 4 | 功能要求 | 支持密钥生成：支持生成RSA或者SM2非对称密钥对，支持生成3DES、AES、SM4算法密钥。 |
| 5 | 支持使用非对称密钥对数据进行加解密，支持RSA、SM2等密码算法。 |
| 6 | 支持使用对称密钥对数据进行加解密，支持3DES、SM4、AES等密码算法。 |
| 7 | 支持使用RSA、SM2密码算法对数据进行签名验签运算。 |
| 8 | 支持使用SM3、SHA256等密码算法对数据进行摘要运算。 |
| 9 | 支持使用HMAC、CMAC等密码技术实现消息鉴别码生成和校验。 |
| 10 | 支持attached和detached签名/验签 |
| 11 | 资质要求 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 12 | 具备国家密码管理局所颁发的《商用密码产品认证证书》 |

### 数据库加密系统

|  |  |  |
| --- | --- | --- |
| **编号** | **指标项** | **采购要求** |
| 1 | 硬件要求 | 模块化1U设备，支持双电源，支持国产操作系统，不少于4核4线程国产CPU X1，不少于1T硬盘 X1，不少于16G内存，不少于6个千兆电口，不少于4个千兆光口 |
| 2 | 性能要求 | 最大在线加解密吞吐量（SM4）：650Mbps 最大每秒在线加解密处理能力（SM4）：4000 |
| 3 | 算法要求 | 支持SM2、SM3、SM4等商用密码算法 |
| 4 | 密钥管理要求 | 支持对称密钥和非对称密钥的生成、更新、备份、恢复、归档、销毁等全生命周期管理操作：支持以密钥分量方式导入/导出根密钥，支持以密码信封方式导入/导出对称密钥，支持多种门限方案的密钥备份与恢复机制，并且支持密钥跨版本恢复 |
| 5 | 支持三级密钥体系 |
| 6 | 支持密钥轮转机制，并可自定义轮转周期 |
| 7 | 支持密钥别名管理 |
| 8 | 通用加解密功能要求 | 支持对结构化数据和非结构化数据加解密，支持对称密钥和非对称密钥加解密 |
| 9 | 支持签名验签、生成随机数、生成数字信封、生成摘要 |
| 10 | 支持浏览器和后台服务器之间的报文加密功能，保证传输的机密性和完整性 |
| 11 | 支持RESTful接口，支持JSON编码格式、UTF-8编码 |
| 12 | 切面加密功能要求 | 支持业务代码无需改造的数据库切面加密功能，加密粒度支持字段级 |
| 13 | 支持切面加密细粒度权限管理：配置特定应用查看明文权限、配置特定应用使用特定策略 |
| 14 | 支持存量数据转加密 |
| 15 | 切面加密任务运行失败时支持任务重置 |
| 16 | 支持保留格式加密，保持数据格式和长度不变 |
| 17 | 支持密文检索 |
| 18 | 支持数据的明密文识别 |
| 19 | 支持切面加密配置的生命周期管理，防止数据库重复加密或二次解密 |
| 20 | 提供可视化工具，进行加密数据运维管理 |
| 21 | 支持达梦、人大金仓、南大通用等主流国产数据库 |
| 22 | 切面脱敏功能要求 | 支持字段级的切面脱敏能力，同时保持数据库数据不做修改 |
| 23 | 支持自定义脱敏策略，支持脱敏配置的产生、分发、生效、失效等全生命周期管理 |
| 24 | 提供可视化工具，进行脱敏数据运维管理 |
| 25 | 认证与访问控制要求 | 支持基于角色的访问控制（RBAC），支持系统管理员、安全管理员、审计管理员、审核管理员形式的权限划分 |
| 26 | 支持管理员双因素认证，支持国密数字证书的USBKEY方式登录系统 |
| 27 | 支持应用认证，认证方式支持：AK/SK、用户名口令 |
| 28 | 支持基于属性的访问控制（ABAC），支持应用密钥操作权限管理、应用IP白名单管理以及资源管理 |
| 29 | 系统管理要求 | 支持系统数据的备份与恢复功能，支持系统跨版本升级和恢复，支持全量升级和补丁升级 |
| 30 | 支持独立的服务管理：支持启停服务，配置SSL证书等 |
| 31 | 支持一键巡检：对网络、加密卡、HA、SSL、密码算法等关键系统功能进行检查，并输出巡检结果 |
| 32 | 支持服务日志、业务日志、操作日志和归档日志，并提供操作日志审计功能，支持syslog，支持通过HMAC保护系统日志的完整性 |
| 33 | 支持国密SSL实现安全通信 |
| 34 | 支持web管理平台按时间维度统计密钥数量、新增趋势、使用量、使用排行，展示CPU、内存、磁盘、网络等的使用情况 |
| 35 | 支持系统告警，包括：计划删除告警、对称库/非对称库容量不足告警、keepalived告警、数据库同步告警、系统备份告警、CPU占用告警等 |
| 36 | 支持双机主备、集群等部署方式，支持HA配置，实现SSL、DB、密钥、服务配置等自动同步 |
| 37 | 资质要求 | 具备国家版权局颁发的《计算机软件著作权登记证书》 |
| 38 | 具备国家密码管理局所颁发的《商用密码产品认证证书》，达到GM/T 0028-2014《密码模块安全技术要求》二级安全要求 |

### 站点证书

使用具备资质的电子认证服务机构签发的应用系统站点数字证书。

### 专用通讯系统平台

**即时通讯系统的总体架构要求**

**先进性：**具有一定的先进性、前瞻性、扩充性。在充分考虑技术上先进性的同时，采用成熟技术，保证建成的系统具有良好的稳定性。考虑到一定时期业务的增长，系统应具有一定的可扩充性。

**实用性：**在满足功能需求的前提下，要适应实际工作特点，做到简单实用、界面人性化、过程自动化。

**可靠性：**由于系统的特定用户群，必须在系统平台上保证系统的可靠性。数据应有保护措施，具有容错性、健壮性等。实现不同用户身份和权限的管理。

**开放性：**充分考虑目前或将来的网络发展和需求，采用标准的开放协议来构架整个系统。既有自己独特优势，又能与多家优秀的产品组合，共同构成一个开放的、易扩充的、稳定的、统一的系统。

**可维护性：**系统应提供友好的应用维护界面、模块化设计、采用标准的高级语言编程、灵活的功能模块重组等，保证系统具有良好的可维护性。

**可扩展性：**要求系统能适应不断扩大的要求，能升级以及扩容；适应新技术不断发展的要求，使系统能不断引入新技术，能方便地向新产品过渡，使系统具有很强的生命力，能不断地平滑升级，不被淘汰。

**安全性：**从技术和管理上确保网络和信息的高度安全，使信息安全流转并得到充分利用。

同时，系统作为一个统一的消息平台，应具有即时通讯、统一架构和协同应用、后台管理等模块。

工作人员可以通过客户端方便的进行即时通讯，同时和办公系统等功能模块集成，实现消息到达提醒和单点登录等功能。

**1.PC客户端功能要求：**  
**1.1.即时通讯**

在客户端互相展现组织机构通讯录，可以不经对方同意，将对方加入个人通讯录，互相用即时消息沟通；

支持文字消息、图片、语音消息、文件、文件夹在线离线发送，支持截图涂鸦、远程控制、远程屏幕、字体大小、自定义表情、自定义快捷短语、窗口抖动功能；

支持本地历史消息查看、漫游消息查看、对消息/文件/图片撤回、转发、收藏、回复、引用、重发等功能；

支持消息多人/部门群发、回复、转发、阅读查看记录  
**1.2.用户登录验证**

能够实现注册用户的登录，并能保存登录信息，以方便用户下次登录。

支持域环境验证及第三方身份验证登录。

支持二维码手机扫码验证登录。  
**1.3.群聊、讨论组**

具有群聊天功能，既可以跟自己的好友进行点对点聊天，支持多点聊天。

支持创建群组，可通过检索查找所有人员，自行添加群/讨论组。

支持客户端创建群组权限控制，群@功能、群公告、群共享、群重命名、转让群主、设置群管理员、消息置顶、禁言、禁止群成员私聊功能

支持客户端群添加、删除、退出、解散、搜索功能

支持群聊消息提醒设置，接收不提醒

**1.4.历史消息**

具有即时消息、群组消息等历史记录功能，为方便历史消息的浏览。

提供按部门分组和按时间、人员排序的功能。

提供按文件记录、图片记录、链接记录分类查询

支持消息记录漫游。  
**1.5.消息回执**

消息发送，对方接收之后自动有回执，未读消息标记显示，保证消息零丢失。  
**1.6.文件传输**

支持文件在线和离线的发送，支持断点续传。

文件传输支持服务器中转和P2P传输两种方式，接收端可以自由选择，接收端离线则自动选择服务器中转传输。

支持大容量文件传输。  
**1.7、组织结构**

提供多层组织结构查询功能，提供多种查询方式，用户可通过组织结构查询联系人，发送即时消息。

具有显示和屏蔽用户的权限，可由管理员在后台进行授权。

支持一人多岗，人员可在多个部门同时展示，个人资料中可自定义选择显示其中一个部门。

**1.8、部门通讯录**

支持显示用户所属部门通讯录。

支持通过查询快速定位到联系人。  
**1.9、我的联系人**

支持好友功能，可以方便的将常用的联系人加入自己创建的联系人分组，方便用户查找。  
**1.10、自定义应用**

提供标准插件开发文档，支持对插件进行权限管理，做到自由启用和禁用插件。  
**1.11、升级更新**

支持自动更新功能，当用户登录系统后，发现有新版本或增加新功能，系统自动提示用户安装。

**1.12、网盘功能**

提供文件共享功能，支持以部门、联系人、群组为单位的云盘划分并可以对文件（夹）浏览、下载、上传、删除等操作；  
 支持根据用户角色权限确定用户的查看、编辑等权限范围；

支持对文档的快速检索、查看功能。

**1.13、签收消息**

支持签收消息，即接收方必须输入自己的登录密码方可查看到签收消息内容，防止重要消息内容泄露。

**1.14、安全设置**

支持账号限制IP地址、IP地址段绑定登录；

支持账号Mac地址绑定、移动端设备号验证登录。

**1.15、阅后即焚**

支持发送阅后即焚消息，在查看消息后手机端文字10秒，文件30秒，PC端文字5秒自动消失。

**1.16、定时发送**

支持设置指定时间发送定时消息，支持查看等待发送的消息和全部消息。

**1.17、组织架构用户数显示**

支持组织架构人员显示，显示在线用户数/部门总用户数。

**1.18、文件密级管理**

支持PC客户端发送文件时对文件设置等级，接收者低于文件密级无法发送

**1.19、客户端水印背景**

支持显示个人账号水印背景，防止截图拍照消息泄露，并支持后台自定义设置开关。

**1.20、群发**

支持发送文字、图片、文件消息群发功能，按部门/联系人选择发送，转发群发消息，下载群发消息中的文件，双击文件，直接调用本地软件打开，回复群发消息，查看群发人员已读状态。

**1.21、公告/广播**

支持发送、接收查看公告通知功能，支持公告发送文字、图片、附件，支持查看公告人员已读状态。

**1.22、多端消息漫游同步**

支持消息漫游，更换设备也能查看历史消息，支持PC端、移动端多端消息同步漫游。

**1.23、敏感词过滤功能**

支持自定义设置敏感词组，客户端在发送消息中含敏感词组会提示、\*替代和禁止发送等类型。  
**1.24、移动端接收文件不落地**

支持可设置部门账号在手机登录在线时，手机接收到文件不能下载本地，只能在电脑端接收查看，防止文件外泄。

**1.25、高管模式功能**

支持管理台设置密级，没有设置密级的人员为0级，等级最低。下级可以向上级发起会话，但不能越级发起。比如2级可以对3级发起会话，但是不能对4级发起会话。

**1.26、密码强度设置**

保证客户端登录的安全，支持客户端密码复杂强度设定，并满足客户端首次登录强制修改密码。

**2、服务端后台管理**

提供后台操作管理功能，以保证系统的正常运行和应用。支持人员管理、群组管理、部门管理、分级管理、系统全局设置、消息查询、角色控制等。支持管理端多员管理，不同的管理员登录后台查看权限不一样（系统管理员、安全管理员、审计管理器、超级管理员）

**2.1、即时通讯管理台**

提供即时通讯系统的相关配置功能，如服务器名、服务器参数的管理。

数据监控，可统计所有人员、部门、群组总数量，可统计每月账号总登录数、消息发送总数等。

登录策略，可设置系统管理员账号登录ip绑定登录策略及对管理员账号增加、删除、修改。

监控管理，支持展示服务器实时硬盘空间、CPU使用率、内存使用率，方便维护。

数据库管理，管理台提供数据库自动备份，数据库还原、数据库初始化及数据库迁移功能。

系统工具，提供客户端平滑升级，后台添加更新包，客户端能检测自动升级。

群聊管理，可以创建、维护群聊室的相关信息，可以对群历史记录、群成员进行管理。

消息广播管理，可以把消息广播权限给指定的用户和组。

为保证系统的安全运行，对即时通讯的日志有详细的记录，包括但不限于聊天记录日志、广播消息日志、用户登录日志、用户在线日志等。

提供完善的即时通讯统计报表功能，包括但不限于用户登录统计报表、在线人数统计报表。

**2.2、用户管理**

提供用户、组织架构、权限管理。支持用户、组织架构批量导入导出（需满足：TXT/EXECEL/XML/JSON导入、AD导入、LDAP导入等）

提供用户的管理功能，支持用户账号的增加、删除、修改等操作。可以设定用户姓名、账号、性别、密码、职务、手机号、座机、邮箱、头像、房间号、工号、短号、生日、账号有效期及账号激活状态。

提供用户可以按目录树进行分级管理，支持分级授权，每个机构可以设置自己的管理员，维护自己机构的用户。方便进行用户及用户权限的增、删、修改等操作。

根据单位的特点，灵活实现现有部门用户单位内部及不同单位之间的修改调整等操作。

管理员分为超级管理员和普通管理员两类。超级管理员可以定义机构，而普通管理员则不可。普通管理员可以定义部门和二级单位。

日常的用户管理由普通管理员完成。通过权限的划分，实现普通管理员对相应数据的分级授权管理。

支持人员排序，可设置安排设置的值排序或者按照在线状态排序。

分级管理，提供后台设置分级管理员，指定某账号为某部门的管理员，他的账号可登录后台对对应的部门进行人员调整。

**2.3、组织机构管理**

根据单位的特点，要求对各个单位、部门、分支机构、直属机构都可以进行多级管理，并能方便、灵活实现部门组织机构的重组、改名、撤消、人员变动等应用操作。

支持部门排序。

支持部门访问可见设置，可设置部门人员账号登录后只能看到部分组织架构。

**2.4、人员权限、系统设置管理**

支持自定义设置消息、文件、群聊消息、通知及日志的保存时间，也可永久保存。

支持设置移动端禁止登录、消息传输加密类型、禁止语音功能、禁止视频功能、禁止客户端修改密码、禁止共享群文件、客户端首次登录强制修改密码、禁止群成员私聊、禁止发送文件、禁止远程、禁止截图、禁止创建群组等功能。

支持设置部分人员权限，如：发送公告的权限、发送文件的权限、云盘文件管理权限及其他应用的特定权限。

**2.5、文档共享管理**

根据各组织情况自由设定组织人员对于文档的操作权限。

**2.6、消息审计**

支持服务端查看所有的消息记录，包括文字、图片、附件，支持一对一的单聊消息及群组聊天记录，并提供时间、账号、人员等检索功能。

**3、安全模块**

**3.1、安全设置**

|  |  |
| --- | --- |
| **Mac地址绑定** | 支持后台设置账号绑定Mac地址，客户端登录时验证Mac地址一致允许登录 |
| **IP地址绑定** | 支持后台设置账号绑定IP地址，客户端登录时验证IP地址一致允许登录 |
| **移动端设备号验证** | 支持后台设置移动端登录后自动获取移动端设备号，下次移动端登录时验证设备号一致允许登录 |
| **首次登录修改密码** | 支持客户端在第一次登录时强制修改密码，后台可设置高中低密级强度 |
| 消息传输加密 | 支持后台设置发送消息时选择加密方式（SM4国密、AES256） |
| **禁止移动端下载文件** | 支持设置不同人员不用角色，账号在移动端登录时，禁止下载文件，避免文件外泄 |
| 禁止移动端登录 | 支持后台设置账号禁止在移动端登录 |
| 公告/云盘文件加密 | 支持应用中公告/云盘中的文件加密存储 |
| **文件传输加密** | 支持后台设置发送文件时选择加密方式（SM4国密、AES256）；开启加密传输后，服务器储存为密文，移动端接收的文件也为密文（只能通过大蚂蚁APP打开查阅） |
| **文件流转记录** | 支持后台设置开启文件流转记录，开启后对同一文件可监控下载人员记录 |
| **移动端密聊** | 支持后台开启移动端密聊功能，开启后移动端可选择发起密聊沟通模式（消息禁止拷贝或转发、头像名字打码防截屏、消息阅后即焚不留痕、不可被录屏） |
| **账号/部门有效期** | 支持后台设置账号/部门有效期限，到期后账号自动为禁用状态，客户端无法登录 |
| 多设备在线 | 支持后台开启PC端与移动端同时在线，消息同步漫游 |

**3.2、**权限设置

|  |  |
| --- | --- |
| P2P传输 | 支持后台开启客户端P2P文件传输，并自定义设置阈值 |
| 头像常亮 | 支持后台开启客户端头像常亮，开启后所有人头像为在线，不存在状态变更 |
| 发起公告权限 | 支持后台设置允许发起、删除公告的账号人员 |
| 创建群组权限 | 支持后台设置禁止创建群组的账号人员 |
| **文件发送大小限制** | 支持后台设置特定账号人员发送最大文件大小限制权限 |
| 群发权限 | 支持后台设置群发人员最多个数限制 |
| 部门访问控制 | 支持后台设置账号访问部门范围，不同权限登录账号显示的组织架构不同 |
| 个人资料展示/修改控制 | 支持后台设置人员账号自定义选择展示/禁止修改个人资料消息 |
| 其他禁用功能 | 禁止发送文件、禁止语音、禁用视频、禁止远程、禁止截图、禁止客户端修改密码、禁止群共享文件、账号状态开启/禁用 |

**4、通讯软件系统集成要求**

**4.1、统一用户和单点登录**

实现与办公系统集成实现单点登录，并实现从即时通讯客户端单点登录到行政办公系统的功能模块。

使用即时通讯系统的消息、短信、群组实现实时的沟通交流。

对接入统一用户和单点登录的应用系统进行管理。

对接入系统的用户进行管理，可以对用户进行增、删、改操作。要求可对用户按组织结构进行分组，支持用户组的分级授权。

具有系统登录日志记录管理功能，可以记录用户登录的IP、MAC地址、时间。

对于不能实现统一用户的系统，要求能以映射方式实现单点登录。  
**4.2、二次开发和开放性**

具有良好的扩展性，可以方便的进行二次开发，并需提供以下的接口：

即时消息发送接口、统一用户接口、第三方调用等接口。需提供详细的接口文档和接口实例。

需提供与第三方应用系统紧、松偶合整合实例，提供接口和开发文档。

具有完善的接口，可跟第三方业务系统进行集成，为不同业务系统及不同工作人员提供安全保障。

提供SDK接口，能与办公系统进行无缝集成。

提供Web Service接口，用于用户、组织架构信息的维护，实现办公系统与即时通讯系统的集成、单点登录、消息推送、消息提醒。

**5、即时通讯系统平台兼容性支持要求**

**5.1、客户端**

|  |  |
| --- | --- |
| **系统OS** | **处理器CPU** |
| windows7及以上 | X86 |
| Linux（centos7） | X86 |
| 乌班图Ubuntu | X86 |
| 安卓Android6及以上 | —— |
| 苹果iOS9及以上 | —— |
| 鸿蒙HarmonyOS | —— |
| 统信UOSV20 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 银河麒麟KylinV4/V10/V10SP1 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 中标麒麟NeokylinV4/V6/V7 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 深度Deepin | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 中科方徳V5.0 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |

**5.1、服务器**

|  |  |
| --- | --- |
| windows server2012及以上 | X86 |
| Linux（centos7） | X86 |
| 统信UOSV20 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 银河麒麟KylinV4/V10 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 中标麒麟NeokylinV6/V7 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 深度Deepin | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 中科方徳V5.0 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |

**5.1、数据库**

|  |  |
| --- | --- |
| Mysql（MariaDB） | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| SQL Server2019及以上 | X86 |
| 达梦DM8 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 人大金仓KingbaseES | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 阿里OceanBase | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 南大通用GBASE | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 神舟通用 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |

**5.1、中间件**

|  |  |
| --- | --- |
| PHP | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| Apache | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| Ngaix | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 东方通 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |
| 金蝶 | ARM架构(飞腾、鲲鹏、麒麟)、MIPS架构(龙芯)、X86架构(Intel、AMD、兆芯、海光) |

# 项目实施、验收与售后服务要求

## 项目实施

### 实施进度

供应商须在响应文件中给出详细、合理的项目进度安排，明确各阶段建设目标、建设内容，确定各平台间相互关系，协调各平台建设进度。合同签订前，供应商需与采购人共同商定项目进度安排，并按项目进度安排签署合同，依次开工建设，项目建设中应严格遵守项目进度安排。

项目建设过程中，如果各个阶段的里程碑能够提前达成，经双方协商，可提前进行阶段性验收。

在建设过程中，供应商应该接受采购人委托的监理单位的监理，按照监理单位的要求提交项目相关的文档。

### 实施人员

供应商应为本项目建立专用的技术实施团队，项目团队人员配置科学合理、分工明确。团队成员须保持稳定，并由采购人与供应商共同管理，项目经理、技术负责人、实施人员必须专职承担本项目工作，采购人认可人员后原则上不得更换，其他人员的更换也需征得采购人同意。

为保证项目顺利实施，供应商在项目实施期间提供现场项目经理1人、技术负责人1人、应用开发人员不少于2人、集成工程师不少于3人的项目团队。具体要求如下

1. 项目经理负责整体项目协调及质量进度把控定期反馈项目进展；需具备信息系统项目管理师认证、高级工程师（计算机相关专业），同时具有10年以上类似信息系统项目经理工作经验的评定优先考虑。

2. 技术责任人负责整体项目中一体化设计方案及实施方案的评审确保方案的可执行性；需具有国产云计算、国产数据库相关能力，需提供相关证书或其他证明材料，具有注册信息安全专业人员认证（CISP）证书，供应商应明确技术负责人在本项目中管理权限和调动相关资源的权力，以确保项目顺利实施。

3. 应用开发人员不少于2人，其中软件工程师1人，软件测试工程师1人。

4. 系统集成工程师不少于3人

系统集成工程师负责硬件设备的安装、部署、调试、安全应急等工作，需具备注册信息安全专业人员认证（CISP），具备虚拟化、国产数据库、国产中间件工程师、国产云计算相关能力，需提供相关证书或其他证明材料。

供应商应详细列出项目实施团队人员姓名、相关认证资质、项目经验、近三个月任意一个月的社保缴纳等证明材料。

### 安装、调试

1) 合同签定一周内，供应商须向业主提交安装实施环境的要求。实施安装7天以前，供应商向采购人提交安装、测试和安装验收的计划方案，该计划方案须经过采购人同意方可作为安装、测试和安装验收的依据。

2) 供应商应承担所供产品的安装、调试和配置工作，同时应提供完整的安装调试文档及系统配置文件。

3) 供应商应全力与采购人及其他相关产品供应商配合，保证系统按时、正常地投入运行。

4) 供应商需保证所配置的软件产品有合法的使用权。

### 项目验收

1) 系统验收合格的条件必须至少满足以下三个要求：试运行时性能满足合同要求；性能测试和试运行验收时出现的问题已被解决；已提供了合同的全部货物和资料。

2) 所有业务系统正式投入运行后进行系统验收。用户将邀请相关行业专家、监理与用户方一起验收，同时就系统的安全性、完整性、易用性、适用性等请第三方专业评测机构进行评测，届时验收专家由用户方指定。

## 工期要求

自合同签订之日起2个月完成项目总体建设，4个月完成验收，其中包括1个月的试运行。

## 技术文档

系统验收后供应商需向采购人提供项目准备、需求分析、设计、集成、实施、上线、交付各阶段及项目管理全过程中的有关文档。文档包括但不限于以下内容：

* 项目计划书、用户需求分析报告。
* 项目概要设计书。
* 安装、测试报告等。
* 使用手册、培训手册等。
* 系统维护手册。
* 验收报告等。

## 项目管理要求

供应商与采购人共同组成工作组，各工作组与采购人项目负责人、供应商项目经理组成项目组。项目组建立固定的工作会制度，各工作组定期召开平台建设工作会，项目组定期召开项目协调会。各平台协调形成统一的调研计划，同步进行，一次完成，不能多次重复调研。

供应商须在项目实施过程中制定项目管理制度和工作流程，合理规划项目的组织架构、沟通方式和工作职责，并报采购人备案，提供项目管理工具平台和项目版本控制管理平台辅助项目管理工作，定期向采购人提供工程实施进展情况报告。

供应商须制定严格的项目质量控制规范和流程，并在采购人认可的情况下按照制定的规范和流程严格执行。采购人须在应答中详细阐明质量管理措施以及方法。

## 质量保障要求

供应商需采用ISO20000质量标准体系要求针对项目实施过程及交付结果进行质量规划、管理和控制，提供完整的质量保证体系，对项目实施的全过程进行监控和管理，对项目进度和工程实施进度进行控制。

在项目实施前，供应商应会同采购人及具体使用部门明确相关的实施方案、实施进度安排、过渡迁移对接方案和应急处置方案等内容，确保相关业务的正常有序运行。

## 风险控制要求

供应商要能在充分理解本项目需求的基础上，对可能出现的各类风险进行评估和制定应对措施，以保证本项目的顺利实施。

## 项目培训要求

培训工作是整个系统得以正常运行的关键，供应商应据此制定详细的培训方案。培训对象除包含普通业务人员的专项培训以外，还应对系统维护人员进行系统维护人员进行系统维护的培训。

供应商须为采购人进行现场安装指导，使采购人掌握产品安装、调试、验收、故障诊断的基本技能；供应商须提供高水平的、全面的专业技术培训，培训内容应涵盖设备功能介绍、设备维护管理、设备故障诊断等要点。使采购人的人员达到能独立进行管理、维护测试、故障处理等工作，保证系统平台能够正常、安全地运行。

本次响应报价须包含培训产生的相关费用。

## 系统维护、售后服务

免费维护期：

供应商需提供验收合格后整体质保一年，硬件设备三年、软件产品一年。在项目验收合格后，供应商必须提供至少一年的免费技术维护服务，其中包括系统维护、常规检查等,保证系统的正常运行。

售后服务

（1）技术支持

供应商须证明有能力常年为采购人提供7×24小时快速响应技术支持服务，确保技术人员能够在接到报修电话通知后2小时内达到现场，接到技术支持要求时，应为系统使用人员提供如何使用系统的咨询服务。

（2）故障响应

供应商须保证在售后服务期内，各类故障应在接到报修电话通知后30分钟内响应，对于影响系统正常运行的严重故障，2小时内达到现场查找故障原因并提出解决方案，如非硬件故障 4 小时内解决故障；如遇硬件故障，8 小时内解决故障或及时提供备机维持上海市干部保健审核监督服务信息系统运行正常。

若供应商未能按时派员到现场或未能按时限解决问题，采购人有权自行处理，所发生费用由供应商承担。

（3）热线服务

供应商应保证在质保期内为采购人的所有应用单位提供电话客服服务，并且供应商须提供本单位的热线电话、E-mail、传真、网站等途径，随时接受采购人及项目使用单位提出的各种技术问题，并在24小时内提供解决方案。

其他服务：

1) 供应商负责所供软件及配套产品的售后服务，包括提供所供产品技术咨询、技术培训、到货验收、安装调试以及负责所供产品的保修及其它售后技术服务。

2) 在特殊时段（国定假日、采购人重大系统测试、季度停机、应急演练、投产）等重保期间，供应商需按照采购人要求安排7×24小时应急小组，增派工程师提供现场技术支持服务，确保整体系统安全稳定运行。

3) 供应商须作出无推诿承诺。即供应商应提供特殊措施，无论由于哪一方产生的问题而使系统发生不正常情况时，在得到采购人通知后，须立即派工程师到现场，使系统尽快恢复正常。

4) 在质保期结束前，须由供应商工程师和业主代表进行一次全面检查，任何缺陷必须由供应商负责修理，在修理之后，供应商应将缺陷原因、修理内容、完成修理及恢复正常的时间和日期等报告给采购人，报告一式两份。

5) 供应商需在响应文件中对售后服务的任务内容和服务方式进行详细罗列与界定，对于需要采购人方面配合的内容也可同时加以说明。

# 其他要求

1) 响应文件需对采购文件相应章节的采购内容予以解答，响应文件需满足所有实质性的指标要求。

2) 本项目是针对上海市干部保健审核监督服务信息系统建设，前期经过论证和严格测算，业务模式较为复杂，因此需供应商对本项目有深入理解，合理评估响应总价。

3) 供应商应承诺在实施和维护过程中，任何涉及采购人的信息，包括但不限于采购人数据、特有的业务功能需求等，未得到采购人同意的情况下不得对任何第三方展示、举例乃至销售，否则供应商将承担由此产生的一切后果。

4) 供应商具有近三年类似项目建设开发经验，ISO20000信息技术服务管理体系认证证书、ISO9001质量管理体系认证证书、ISO27001信息安全管理体系认证证书、信息系统建设和服务能力等级认证证书（CS2及以上）、ITSS信息技术服务运行维护证书、CCRC信息安全服务资质认证证书（二级及以上）、国家信息安全测评信息安全服务资质证书（安全工程类）、信息系统建设和服务能力评估（CS3及以上）的优先考虑。