# 采购需求

**一、项目基本情况**

**1.1 项目名称**：武汉市住房保障和房屋管理局2022年度房管信息系统密码应用建设

**预算金额：**122.08万

**1.2 项目目标：**综合考虑武汉市住房保障和房屋管理局业务系统的物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的密码应用技术方案，满足GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中三级指标要求，并为通过密码应用安全性评估奠定基础。

本项目服务范围覆盖2022年度房管信息系统密码应用建设的集成实施服务。

1.3 预算绩效目标

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 目标名称 | 一级指标 | 二级指标 | 三级指标 | 指标值 | | | 指标值确定依据 |
| 前年 | 上年 | 预计当年实现 |
| 预期产出 | 产出指标 | 数量指标 | 系统开发改造的数量 | / | / | 1 | 计划数据 |
| 质量指标 | 硬件验收合格率 | =100% | =100% | =100% | 历史数据 |
| 质量指标 | 系统运行响应时间 | ≤5秒 | ≤5秒 | ≤5秒 | 历史数据 |
| 预期效果 | 效益指标 | 成本指标 | 预算支出控制率 | / | / | ≤100% | 计划数据 |
| 社会效益指标 | 保障业务系统密码安全 | / | / | 完成 | 计划数据 |
| 社会公众或服务对象满意度指标 | 服务对象满意率 |  |  | ≥98% | 历史数据 |

**二、采购需求**

**2.1 采购标的汇总表：**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 包号 | 标的  序号 | 标的名称 | 品目  分类  编码 | 计量  单位 | 数量 | 是否进口 | 是否创新产品 | 绿色发展 |
| 1 | 1 | 2022年度房管信息系统密码应用建设 | C0202 | 项 | 1 | 否 | 否 | 否 |

**2.2 技术要求和商务要求**

**2.2.1 采购标的1（2022年度房管信息系统密码应用建设）**

说明：**“▲”标注的技术服务及商务要求，为重要指标。**

**2.2.1.1.项目概况；**

##### （一）项目现状

为贯彻落实《密码法》及《国家政务信息化项目建设管理办法》及相关信息系统密码应用的要求，武汉市住房保障和房屋管理局将密码应用建设纳入到年度信息化建设工作。2021年优先开展3个系统的密码应用安全性评估工作。

根据初步测评结果，房地产市场综合管理系统、智慧档案系统、房管政务服务平台3个系统密码应用不符合GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的第三级别要求。急需对相关业务系统进行密码应用建设。现状如下：

在物理环境方面，使用密码技术对进出机房人员进行身份鉴别。机房存储设备仅存储了电子门禁记录数据，未使用密码技术对电子门禁进出记录完整性进行保护；

在网络和通信安全方面，系统运维管理员远程接入时，使用SSL VPN网关远程访问堡垒机，通过查看SSL VPN设备证书中使用的密码算法为RSA-1024，server hello包中的算法套件为TLS\_RSA\_WITH\_RC4\_128\_SHA，未使用合规的密码算法保证通信实体的真实性、通信数据的机密性完整性以及访问控制信息的完整性；

在设备和计算安全方面，运维管理员使用堡垒机管理其他设备，堡垒机通过账号加口令登录，未使用密码技术实现用户登录设备时的身份鉴别，应用服务器、数据库服务器、日志审计系统均未采用密码技术对资源访问控制信息完整性进行保护；在应用和数据安全方面比如口令登录和数据存储管理未使用密码技术对访问控制信息进行完整性保护。

##### （二）项目建设目标

综合考虑武汉房管局业务系统的物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的业务系统密码应用方案，满足GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中三级指标要求，具体目标如下：

1）保障基础设施安全，保障网络周边环境和业务系统的持续使用和连续性。

2）保障网络连接安全，保障网络传输中的安全，尤其保障网络边界和外部接入的安全

3）保障主机系统的安全、保障操作系统、数据库、服务器、用户终端及相关关键资产的安全。

4）保障应用系统安全，保障应用系统在传输中的BM、完整和可用，防止和抵御当前的安全威胁和攻击。

5）安全管理体系保障，依据国家有关标准和规范要求，结合实际情况，建立一套切实可行的安全管理体系。

##### （三）项目建设依据

项目建设依据《密码法》、《国家政务信息化项目建设管理办法》、《武汉市政务信息化项目建设管理办法》、GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》等相关法规、政策、标准要求：

 《中华人民共和国网络安全法》

 《中华人民共和国密码法》

 《国家政务信息化项目建设管理办法》（国办发[2019]57号）

 《国家密码管理局关于进一步加强国家政务信息系统密码应用与安全性评估工作的函》（国密局函 [2020]119号）

 《关于进一步加强全省政务信息化项目密码应用有关工作的通知》（鄂密局发[2021]2号）

 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

 GM/T 0071-2019《电子文件密码应用指南》

 GB/T 33482-2016《党政机关电子公文系统建设规范》

 GB/T 38625-2020《信息安全技术 密码模块安全检测要求》

 GB/T 38629-2020《信息安全技术 签名验签服务技术规范》

 GB/T 38635.1-2020《信息安全技术 SM9标识密码算法 第1部分：总则》

 GB/T 38635.2-2020《信息安全技术 SM9标识密码算法 第2部分：算法》

 GB/T 38636-2020《信息安全技术 传输层密码协议(TLCP)》

 GB/T 38647.1-2020《信息技术 安全技术 匿名数字签名 第1部分：总则》

 GB/T 38647.2-2020《信息技术 安全技术 匿名数字签名 第2部分：采用群组公钥的机制》

 GM/T 0004-2012《SM3密码杂凑算法》

 GM/T 0005-2012《随机性检测规范》

 GM/T 0006-2012《密码应用标识规范》

 GM/T 0008-2012《安全芯片密码检测准则》

 GM/T 0009-2012《SM2 密码算法使用规范》

 GM/T 0010-2012《SM2 密码算法加密签名消息语法规范》

 GM/T 0011-2012《可信计算可信密码支撑服务功能与接口规范》

 GM/T 0012-2012《可信计算可信密码模块接口规范》

 GM/T 0013-2012《可信计算可信密码模块接口符合性测试规范》

 GM/T 0014-2012《数字密码认证系统密码协议规范》

 GM/T 0018-2012《密码设备应用接口规范》

 GM/T 0019-2012《通用密码服务接口规范》

 GM/T 0021-2012《动态口令密码应用技术规范》

 GM/T 0022-2014《IPSec VPN 技术规范》

 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 0028-2014《密码模块安全技术要求》

 GB/T38629-2020 《信息安全技术 签名验签服务器技术规范》

 GM/T 0030-2014《服务密码机技术规范》

 GM/T 0031-2014《安全电子签章密码技术规范》

 GM/T 0032-2014《基于角色的授权与访问控制技术规范》

 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 0037-2014《密码认证系统检测规范》

（项目执行期间，如国家技术标准调整，按新生效的标准执行）

##### （四）项目验收标准依据

《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）

《政务信息系统密码应用与安全性评估工作指南》（2020版）

**2.2.1.2服务内容**

本项目遵循国家密码相关政策文件及标准规范要求，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、管理制度、人员管理等方面，为武汉市住房保障和房屋管理局相关信息系统提供国产商用密码应用改造服务，并确保平台满足国产商用密码应用安全性评估要求。本次服务将为武汉市住房保障和房屋管理局搭建一套密码服务平台，为上层应用提供密码基础服务支撑，实现上层应用的密码安全增强。实现本密码服务平台功能需在平台下部署密码基础运算资源，由基础运算资源组合成密码资源池，满足武汉市住房保障和房屋管理局相关信息系统密码应用要求。基础运算资源主要由以下产品提供，分别为1套国密门禁系统，2台SSL VPN安全网关，200个国密浏览器，200个USBKEY，1套密码支持服务平台，1台云服务器密码机、2台签名验签服务器等。具体服务清单如下：

**2.2.1.2.1 服务清单**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 服务项目 | 单位 | 数量 | 服务内容 |
| 1 | 国密门禁系统 | 套 | 1 | 采用国产密码技术对进、出机房人员进行身份鉴别，确保重要区域进入人员身份的真实性，基于密码技术保证电子门禁系统进出记录数据的存储完整性。 |
| 2 | SSL VPN 安全网关 | 台 | 2 | 提供客户端到服务端传输通道是加密，基于国密SSL技术，实现信息在传输过程中的机密性，同时还能够实现通信双方的身份鉴别。 |
| 3 | 国密浏览器 | 个 | 200 | 基于国产密码算法套件和SSL/TLS技术，在客户端和服务端之间建立加密隧道，确保传输数据的机密性、完整性。 |
| 4 | 智能密码钥匙(USBKEY) | 个 | 200 | 主要提供签名验签、杂凑等密码运算服务，实现信息的完整性、真实性和不可否认性保护，同时提供一定的存储空间，用于存放数字证书等用户数据。 |
| 5 | 密码支持服务平台 | 套 | 1 | 提供对密码服务的统一分配、管理和调度、密码应用服务和封装，支持对上层业务应用以密码服务总线形式提供统一密码服务接口API 和统一密码服务SDK。 |
| 6 | 云服务器密码机 | 台 | 1 | 为应用系统提供数据加解密、签名验签、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护，同时提供安全、完善的密钥管理功能 |
| 7 | 签名验签服务器 | 台 | 2 | 提供基于PKI体系和数字证书的数字签名、验证签名等运算功能，保证用户身份的真实性、完整性和关键操作的不可否认性。 |
| 8 | 软硬件集成及安装服务 | 套 | 1 | 业务系统对接、SDK集成服务。 |

**2.2.1.3技术要求**

**说明：**下述技术参数中标注有“▲”号的条款，为**“四、评审因素及评分标准”**中的评分

内容。

**具体技术参数如下：**

1. **国密门禁系统**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术指标要求 |
| 1.1 | 国密门禁系统 | ★具备国家密码管理局颁发的国密门禁管理系统《商用密码产品认证证书》（须提供证书扫描件） |
| 1.2 | 国密门禁卡：支持SM4国密算法，支持采用国密算法实现身份鉴别，运行速度最大支持848Kbps，数据容量不低于256K，擦写次数不低于10万次，使用时间不低于10年。性能要求：支持卡容量不少于3万张，支持记录容量不少于10万条，开门延时小于0.5秒。 |
| 1.3 | 国密门禁读卡器：支持SM4国密算法，支持采用国密算法实现身份鉴别或其他安全保护方式，支持刷卡+密码双因子方式识别 |
| 1.4 | 门禁控制器：能够支持单门和双门的模式，支持输入格式RS 485/Wiegand 26/Wiegand 34，支持通信格式TCP/IP、RS485 |
| 1.5 | 门禁记录完整性审计系统：支持采用消息鉴别码(MAC)实现视频记录完整性保护或其他安全保护方式，支持日志采集、日志存储、日志检索、合规审计、实时监控、事件告警等功能 |
| 1.6 | ▲国密人脸识别门禁读卡器：密码应用：采用基于SM4的对称加解密技术实现门禁用户身份鉴别，识别方式：RFID+人脸/指纹，显示屏：不低于5寸TP彩屏（须提供产品彩页证明文件） |

1. **SSL VPN 安全网关**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术指标要求 |
| 2.1 | SSL VPN 安全网关 | ★具备国家密码管理局颁发的《商用密码产品认证证书》,（提供证书扫描件） |
| 2.2 | 具备第三方检测报告或信息技术产品安全测试证书或《计算机软件著作权登记证书》（提供证书扫描件） |
| 2.3 | 网络接口不少于4个千兆电口和2个千兆光口，国密加密吞吐量不小于300Mbps，支持双机热备，支持不小于2个模块的集群及Active－Active或Active-Backup工作模式，当系统之间出现故障的时候可自动切换。 |
| 2.4 | ▲支持以内存、cpu、进程、链路等多种条件作为阈值监控对象，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。（提供产品功能截图证明材料） |
| 2.5 | 支持RSA、国密算法套件，支持1024/2048位RSA、256位SM2非对称算法，支持SHA1、SHA256、SHA512、SM3摘要算法。 |
| 2.6 | 支持端口聚合、VLAN、支持动态路由协议包括RIPv1、RIPv2、OSPFv1、OSPFv2。 |
| 2.7 | ▲SSL VPN客户端控件需支持主流操作系统平台和终端必须提供Java、ActiveX两种客户端，支持MAC OS,Linux,Windows 平台。（提供产品功能截图证明材料） |
| 2.8 | 支持终端使用包括IE、Firefox、Safari、Google Chrome、Opera浏览器来登录SSLVPN系统，登录后可完整支持通过SSL VPN发布的各种IP层以上的B/S和C/S应用。 |
| 2.9 | 支持Ctrix，FTP 、Windows远程桌面、TFTP、等瘦客户端，登录VPN后客户端无需安装该类客户端，即可通过VPN直接使用。 |
| 2.10 | 支持客户端IP透传，通过HEADER，URL,COOKIE方式透传用户客户端IP。 |
| 2.11 | 支持用户名口令、动态口令，数字证书等多种认证方式。 |
| 2.12 | 支持角色白名单及黑名单配置，细粒度的访问控制策略。 |
| 2.13 | 支持提供从三层到七层的安全接入，SSL VPN需支持L3方式进行访问。 |
| 2.14 | ▲支持通过命令行方式对产品进行批量配置，可以通过命令行进行全功能配置，并提供命令行配置手册。（提供产品功能截图证明材料） |
| 2.15 | 支持单点登陆（single sign on ），只需要在SSL VPN服务器上进行一次登陆，就可以实现对系统中多个需要认证的服务器实现身份认证和授权。 |
| 2.16 | ▲VPN客户端支持密码键盘功能，提供随机分布式虚拟按键，从键盘的数据输入、数据存储、内存数据换算等全过程加密，有效防止数据侦听、数据窃取、键盘劫持、键盘截屏等攻击行为。（提供产品功能截图证明材料） |
| 2.17 | ▲VPN客户端支持动态口令生成和验证，能够基于策略和密钥种子生成一次性动态口令，支持时间型、事件型、挑战型令牌，生成的令牌有效期为30秒、60秒等可以进行调整。（提供产品功能截图证明材料） |
| 2.18 | ▲具备软件版本升级与回滚功能，保障系统稳定性。(提供产品功能截图证明材料) |
| 2.19 | ▲为方便平台的对接联调，SSL VPN 安全网关与密码支持服务平台、签名验签服务器需为同一品牌（提供对应证明文件） |
| 2.20 | 支持IPV4/IPV6双栈协议 |

1. **国密浏览器**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术指标要求 |
| 3.1 | 国密浏览器 | ★具备国家密码管理局颁发的《商用密码产品认证证书》（提供证书扫描件） |
| 3.2 | 支持龙芯、兆芯、飞腾、鲲鹏等国产CPU芯片 |
| 3.3 | 支持中标麒麟、银河麒麟、统信UOS、中科方德等国产操作系统 |
| 3.4 | 支持人大金仓、神舟通用、达梦等数据库管理系统；支持金山WPS、永中、重庆软航等办公软件及控件；支持福昕、点聚、数科网维、书生等办公套件，支持宝兰德、金蝶、东方通等中间件； |
| 3.5 | 支持HTML和CSS解析，支持JavaScrip引擎，可以正确的渲染显示页面，支持基本的浏览器操作功能； |
| 3.6 | 支持国密算法SM2、SM3、SM4，支持国密SSL协议，符合GM/T 0024-2014《SSL VPN技术规范》； |
| 3.7 | 支持NPAPI控件； |
| 3.8 | 浏览器可以提供Chrome、火狐内核版本 |

1. **智能密码钥匙(USBKEY)**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术指标要求 |
| 4.1 | 智能密码钥匙(USBKEY) | ★具备国家密码管理局颁发的《商用密码产品认证证书》（提供证书扫描件） |
| 4.2 | 内嵌32位及以上智能卡芯片，存储空间不少于128KB。支持2个以上国密应用，同时支持8个以上证书 |
| 4.3 | 验证及运算过程在硬件内部完成，私钥永不出Key，具有多种对抗攻击的安全检测和保护手段 |
| 4.4 | 符合USB2、0规范，兼容USB1、1，兼容3、0规范接口 |
| 4.5 | 支持CSP/PKCS#11、SKF国密标准、支持X、509 v3标准证书格式， |
| 4.6 | 支持AES/SHA256/RSA2048/SM1/SM2/SM3/SM4(256位)，对称算法支持ECB、CBC模式 |
| 4.7 | 提供CSP/PKCS#11/SKF开发接口，支持RSA/SM2且同时支持SKF/CSP/P11接口互通调用 |

1. **密码支持服务平台**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术指标要求 |
| 5.1 | 密码支持服务平台 | ▲具备本产品《计算机软件著作权登记证书》。（须提供证书扫描件） |
| 5.2 | 支持用户及组织机构管理。管理用户支持系统管理员、安全管理员、审计管理员的角色定义，依据角色进行权限管理，满足三权分立原则。 |
| 5.3 | 提供完整的业务日志和操作记录，方便管理审计和故障排查及问题追溯。 |
| 5.4 | 提供统一的密码设备管理，包括设备自动发现，远程管理，包括关机，重启；设备分组管理。 |
| 5.5 | 提供系统监测告警和告警通知功能，支持物理机，密码业务API 告警，告警通知支持Email，短信通知。 |
| 5.6 | 系统应提供全业务配置统一UI界面，多密码服务配置统一入口，统一存储，支持在线修改配置，无需重启即可生效。 |
| 5.7 | 支持统一的安全授权管理，统一业务配置，统一告警监控，对于客户定制化需求，应具备开放性集成能力。 |
| 5.8 | restful风格接口，统一的接口说明文档，方便第三方应用接入。 |
| 5.9 | 网关API访问安全授权管理，要求业务应用必须在平台注册审批通过，平台生成安全APISecKey，业务系统在访问时携带该安全身份标识方可访问。 |
| 5.10 | 系统应支持网关，统一api入口，支持动态网关配置，根据身份标识统一路由转发，在服务压力过大时提供限流，保证系统运行稳定。 |
| 5.11 | 系统支持承载多种密码安全服务，提供持续增量部署各种密码业务能力，确BM码服务API一致性，实现密码设备统一运维，实现安全管理及统一规范。 |
| 5.12 | 新业务动态部署。业务应用开发成微服务部署，需要使用某类功能时只需把特定的微服务部署上去，无需停止系统且不影响正在运行的业务。 |
| 5.13 | 性能和容量支持横向扩展，通过新增服务器资源，扩展系统业务容量和性能。 |
| 5.14 | 支持双活、集群、负载均衡等部署方式，支持横向扩展。 |
| 5.15 | 支持灰度升级，并且不影响现有运行的业务，在业务高峰支持动态扩容，降峰后能够在线减容，不影响现有业务。 |
| 5.16 | docker容器部署，系统支持基于docker的容器编排部署方式，支持K8S 和 docker Swarm。 |
| 5.17 | ▲支持对日志文件做HMAC-SM3处理，符合密码测评要求。（提供产品功能截图证明材料） |
| 5.18 | ▲支持对关键数据做存储加密，符合密码测评要求。（提供产品功能截图证明材料） |
| 5.19 | ▲对数字签名服务，统一接口支持国密SM2、SM3、SM4算法，attached/detached/raw签名/验签；数字信封的制作与解封。（提供产品接口证明材料扫描件） |
| 5.20 | ▲为方便平台的对接联调，密码支持服务平台与SSL VPN 安全网关、签名验签服务器需为同一品牌。（需提供相应证明文件） |
| 5.21 | ▲密码支持服务平台支持与云服务器密码机对接，支持密钥的全生命周期管理及全流程管控，包括国际算法和国密算法的对称密钥、非对称密钥等密钥的生成、启用、更新、导入、导出、打印、销毁等。（须提供对接证明材料扫描件或在中标后能实现对接的承诺书。） |

1. **云服务器密码机**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术指标要求 |
| 6．1 | 云服务器密码机 | ★具备国家密码管理局颁发的《商用密码产品认证证书》。（提供证书扫描件） |
| 6．2 | ★产品需具有中国国家强制性产品认证证书（3C）。（提供证书扫描件） |
| 6．3 | ▲具备云数据库加密系统《计算机软件著作权登记证书》。（提供证书扫描件） |
| 6．4 | 机架式硬件设备，内置高性能PCI-E密码卡，冗余电源供电，支持触摸式液晶屏。不少于4个千兆电口和2个万兆光口。SM4算法ECB加解密速率不小于4000Mbps。SM4算法CBC加解密速率不小于4000Mbps。SM2密钥产生速率不小于30000次/秒。SM2签名速率不小于26000次/秒。SM2验签速率不小于18000次/秒。SM3计算Hash速率不小于4000Mbps。 |
| 6．5 | ▲支持同态密码算法，用于如数据库加密系统的密文查询、统计等场景（提供产品功能截图证明材料） |
| 6．6 | 支持SM2 算法加/解密功能、SM2 算法数字签名/验证功能、对称密钥加/解密功能(SM1/SM4 算法加密/解密)、随机数生成功能; |
| 6．7 | 服务接口：提供API接口供外围调用，包括应用接口和管理接口，应用接口应符合包括PKCS11、JCE、国密设备等接口规范。 |
| 6．8 | 密钥管理：对称密钥管理，非对称密钥管理，支持密钥生产，导入，导出，销毁等全生命周期管理。采用多级密钥管理体系，逐层保护；密钥产生，密码机支持产生随机密钥。密钥存储，密码机支持安全存储对称密钥、SM2密钥，导出密钥时必须加密。密钥备份恢复，密码机支持内部密钥的安全备份和恢复。密钥支持远程管理。 |
| 6．9 | 虚拟化：支持虚拟化功能，支持虚拟化密码机的克隆、支持虚拟化远程控制、支持虚拟设备启动停止。支持各虚拟化密码机之间的安全隔离。支持虚拟化管理接口,包括应用权限管理、用户管理、应用管理、密钥管理等。支持轻量级容器技术。 |
| 6．10 | ▲多租户管理：支持多租户的管理，可以对每个租户分配不同资源的VSM以及相应权限key，支持同一租户对多个VSM进行管理和密钥同步（提供产品功能截图证明材料） |
| 6．11 | ▲备份管理：在满足权限的情况下能够将云服务器密码机内的密钥等重要信息加密后进行备份，并且可以恢复到相同型号的云服务器密码机中，备份采用（3，5）门限方式，产生备份密钥并分割导出到5个智能密码钥匙中（提供产品功能截图证明材料） |

1. **签名验签服务器**

|  |  |  |
| --- | --- | --- |
| 序号 | 指标项 | 技术指标要求 |
| 7.1 | 签名验签服务器 | ★具备国家密码管理局颁发的《商用密码产品认证证书》（提供证书扫描件） |
| 7.2 | ★产品需具有中国国家强制性产品认证证书（3C）。（提供证书扫描件） |
| 7.3 | 具备第三方检测报告或信息技术产品安全测试证书或《计算机软件著作权登记证书》。（提供证书扫描件） |
| 7.4 | ▲具备签名验签客户端软件《计算机软件著作权登记证书》。（提供证书扫描件） |
| 7.5 | 提供标准机架式设备，支持双电源冗余，支持不少于4个千兆电口、不少于2个千兆光口；SM2签名性能不低于20KTPS；SM2验签性能不低于15KTPS； |
| 7.6 | 支持非对称秘钥算法：SM2、RSA；支持摘要算法：SM3，MD5，SHA1，SHA256,SHA512；支持对称秘钥算法：SM4, 3DES, AES, DES； |
| 7.7 | 支持PKCS#7、XML标准格式的签名与验签。支持使用多个信任CA。支持多种签名报文信息组合方法，包括（原文+签名+签名证书）、（签名+签名证书）、（签名）等。提供包括RAW签名/验签，Attached 签名/验签，Detached签名/验签等多种方式的签名验签方式； |
| 7.8 | ▲支持一维条形码、二维码生成和验证，并支持与移动SDK/APP无缝对接，实现扫码登录功能。（提供产品功能截图证明材料） |
| 7.9 | 支持生产系统和灾备系统之间的设备远程证书同步。 |
| 7.10 | ▲支持多台（3台及以上）设备之间机构证书同步。（提供产品功能截图证明材料） |
| 7.11 | 支持密钥生成与管理功能，提供1024/2048位RSA及SM2密钥生成、密钥存储、密钥备份和密钥恢复功能。支持1024/2048位RSA、256位SM2算法，支持SHA1、SHA256、SHA512、SM3算法。支持windows、linux、AIX、Solaris、Unix等主流应用平台，支持Java、com、C、Webservice等主要应用集成接口。 |
| 7.12 | ▲为方便平台的对接联调，签名验签服务器与SSL VPN 安全网关、密码支持服务平台需为同一品牌。（提供相应证明文件） |

**2.2.1.4服务要求**

**2.2.1.2.1响应时间要求**

本项目系统服务期限为一年，在服务期限内应提供以下响应时间要求：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 故障级别 | 故障  属性 | 故障描述 | 服务方式 | 承诺故障**/**  解决时间 |
| 1级 | 紧急问题 | 业务系统遭受网络攻击，出现高危事件 | 7×24  现场服务 | （1）10分钟内响应；  （2）1小时以内排除故障。 |
| 2级 | 严重问题 | 系统支撑软件报错或警告，出现中危事件。 | 7×24远程/  现场服务 | （1）30分钟内响应；  （2）2小时以内排除故障。 |
| 3级 | 普通问题 | 系统技术功能、安装或配置咨询，不影响正常使用等低危事件。 | 7×24远程/  现场服务 | （1）1小时以内达成服务；  （2）24小时排除故障。 |

**2.2.1.2.2巡检服务**

在规定服务期限内定期（每月至少 1 次）对设备状况提供一次系统性的预防性巡检，并对系统运行中可能存在的潜在问题，提出可行的解决方案并经采购方认可后安排实施，每次巡检服务完成后应提交巡检报告。

**2.2.1.2.3培训服务**

在规定服务期限内定期（每半年至少1次）对武汉市住房保障和房屋管理局相关业务操作人员及系统开发人员（10-15人）开展商用密码应用培训服务。由采购人提供培训场地。根据实际情况组织线上或线下培训。掌握了解商用密码应用的基本要求，在实际开展业务过程中，业务操作符合国家密码法的相关规定。

**2.2.1.2.4系统软件升级**

根据采购人需求或者设备原厂的更新公布、通知的有关软件升级和软件补丁的情况，响应供应商需要在保证数据安全的前提下，在发布更新提示1 个月内主动提供系统软件升级服务，并在双方协商的时间进行。

**2.2.1.2.5协助系统更新调整**

根据采购人提出的要求，响应供应商需要协助采购人对所维护的设备进行硬件或软件的升级、改造和调整，对由此产生的各种问题提出意见和解决办法，保证该设备正常运行。

**2.2.1.2.6故障报告**

对于发生的各类故障，响应供应商技术人员在规定内解决故障的同时还应帮助采购人查找故障根源，并在故障修复后 5 天内提交《故障诊断报告》及《故障分析报告》，响应供应商客服中心应对这些报告进行统一归档管理，报告包括以下内容：

1) 故障处理过程

2) 故障原因分析

3) 故障预防性维护建议

4) 后续改进计划

**2.2.1.2.7维保服务团队要求**

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 人员配置 | 人数要求 | 工作职责范围和要求 |
| 1 | 项目经理 | 1人 | 项目经理负责对整个服务团队的管理，并定期与用户方协调沟通，保证服务质量。 |
| 2 | 技术负责人 | 1人 | 配合招标方完成维护工作，技术负责人，应具备岗位要求相关能力。 |
| 3 | 技术人员 | 2人 | 投标企业根据项目实际情况进行配置，应具备岗位要求相关能力。 |

团队人员专业能力要求：

1）项目经理要求

供应商拟派本项目的项目经理应具备的以下资格证书：

信息系统项目管理师；

网络规划设计师证书。

2）技术负责人要求

供应商拟派本项目的技术负责人应具备以下资质证书：

系统集成项目管理工程师。

项目服务期内不要求供应商提供驻场维保服务，当产品设备出现问题供应商需提供7×24远程/现场服务，按照响应时间要求进行修复，保障系统正常运行。

**2.2.1.2.8集成要求**

本项目报价应包含设备制造、包装、运输（含装卸、保险）、保管、配合土建预埋、安装、调试（含调试使用的电缆）、税费、其他安装时必须的一切费用，即投标总报价为“交钥匙”价。对在合同实施过程中可能发生的其它费用（如：安装架、线材、材料涨价、人工、运输成本增加等因素），采购人概不负责。投标方应采用技术先进、定型可靠的设备和成熟可靠、运行稳定的配套软件，包括本技术规格书招标设备。供应商必须承担所投标设备(含软件)确保通过商用密码应用安全性评估。

供应商须如实对采购要求进行响应，采购人保留中标后内进行功能验证的权力，功能验证不满足的采购人有权解除合同，一切费用由供应商自行承担。

**2.2.2商务要求**

**2.2.2.1 服务要求**

1、服务期限：系统实施交付期为合同签订后3个月，系统服务期为系统实施交付验收合格之日起1年，硬件设备质保期为系统实施交付验收合格之日起 3 年。

2、验收标准：项目实施交付完成1个月内，由采购人按照国家、行业标准组织专家进行验收（详见2.2.1.1.项目概况（四）项目验收标准依据）。交付质量达到设计要求，安装调试各项指标符合技术参数（参见服务内容清单中具体技术要求）。

3、验收方法：采购人将对本项目安装调试后进行验收。采购人在任何验收过程中，发现任何问题，成交供应商应及时按照合同规定进行整改，否则，采购人将按合同规定追究成交供应商的法律责任。

4、服务地点：湖北省武汉市江岸区建设大道702号武汉市住房保障和房屋管理局

**2.2.2.2 付款方式**

1、合同签订后 7 个工作日内，采购人支付合同金额的60%作为预付款；

2、项目验收合格后，7 个工作日内采购人支付合同金额的40%；

**2.2.2.3 双方责任义务**

1）采购人应向供应商提供并允许供应商为实施工作目的而使用合同双方商议确认

的信息、数据、资料。

2）如供应商履行本合同过程中需与第三方配合，采购人可协助协调供应商与第三方的工作。

3）采购人应按本合同约定向供应商支付款项。

4）采购人应依约及时足额通过银行转账方式向供应商支付费用。

5）供应商应按照本合同的要求，如期独立完成和交付合同成果。

6）供应商每周应向采购人书面报告当前的项目实施状况，以便采购人了解项目进展状况。

7）供应商应按照本合同的约定向采购人交付合同系统和技术资料。

8）供应商必须严格遵守采购人的有关规章管理制度。

9）供应商应针对系统故障做出分析报告、并写入运维报告（周、月、季）、巡检报告、年度报告。采购人须认真审核报告内容，发现问题及时督促指导供应商进行处理，并协助整改。

10）供应商应严格遵守国家、地方的法律、法规的规定，保证在合法且不侵犯他人利益的原则下履行本合同约定的义务，并对其所进行与本项目相关所有活动负责。

11）供应商需在不同的项目阶段安排相应的培训计划，提供完善的培训方案，方案包含培训内容、培训计划、培训课时等。

具体培训要求如下：培训内容包括：实施技能培训、系统应用培训、系统维护培训等。在交付阶段针对用户使用中的疑问提供 7\*24 小时的电话和网络答疑。

供应商应负责对所有参与项目的人员进行培训，并提交详细培训计划。

12）供应商承诺在服务期内提供技术维护服务（其中包括系统维护、跟踪检测故障排除、性能调优、技术咨询等，并负责处理、协调各系统软件的相关问题等），保证供应商提供的软、硬件正常运行；保证产品的稳定运行；达到合同约定的系统功能和技术指标要求；确保项目产品及时更新、升级，并提供相关技术服务。

13）供应商负责对应急预案进行定期审查和根据实际情况进行更新，并按照执行。

14）供应商应积极配合采购人对故障做出及时响应，制订符合项目系统稳定运行的故障应急响应制度，并严格执行。

**2.2.2.4违约责任**

双方任何一方不履行合同义务或者履行合同义务不符合本合同约定，均视为违约。守约方可向违约方发出要求其履行合同义务的书面通知，违约方应在通知发出之日起 5 个工作日内采取补救措施，逾期仍未采取措施或者采取措施仍无法消除违约情形、导致合同无法继续履行或者合同目的无法实现的，则守约方有权解除本合同并要求违约方赔偿因此造成的直接经济损失。

甲乙双方在完成双方签署的书面确认事项后，采购人书面提出变更要求，导致项目进度延迟的，工期可顺延，不视为供应商违约。

**2.2.2.5 BM条款**

甲乙双方对本合同的存在、内容、双方的合作以及双方在履行本合同过程中 所获知的对方的商业MM和专有信息负有BM义务，仅用于履行本合同项下的义务，并只为履行本合同的相关人员所知悉。任何一方的相关人员违反BM义务的，由该人员所属一方承担全部法律责任；但法律另有规定的除外。

**2.2.2.6 其他要求**

* 1. 2020 年 1 月 1 日以来供应商具有类似业绩；
  2. 供应商具有GB/T27922-2011售后服务四星及以上认证证书；
  3. 供应商所投国密门禁系统具有国密人脸识别门禁读卡器，采用基于SM4的对称加解密技术实现门禁用户身份鉴别，识别方式：RFID+人脸/指纹，显示屏：不低于5寸TP彩屏（须提供产品彩页证明文件）；
  4. 供应商所投SSL VPN 安全网关产品具备第三方检测报告或信息技术产品安全测试证书或《计算机软件著作权登记证书》（提供证书扫描件）；
  5. 供应商所投SSL VPN 安全网关产品支持以内存、cpu、进程、链路等多种条件作为阈值监控对象，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。（提供产品功能截图证明材料）；
  6. 供应商所投SSL VPN 安全网关产品的客户端控件需支持主流操作系统平台和终端必须提供Java、ActiveX两种客户端，支持MAC OS,Linux,Windows 平台。（供应商所投产品应提供产品功能截图证明）；
  7. 供应商所投SSL VPN 安全网关产品支持通过命令行方式对产品进行批量配置，可以通过命令行进行全功能配置，并提供命令行配置手册。（提供产品功能截图证明材料）；
  8. 供应商所投SSL VPN 安全网关产品客户端支持密码键盘功能，提供随机分布式虚拟按键，从键盘的数据输入、数据存储、内存数据换算等全过程加密，有效防止数据侦听、数据窃取、键盘劫持、键盘截屏等攻击行为。（提供产品功能截图证明材料）；
  9. 供应商所投SSL VPN 安全网关产品客户端支持动态口令生成和验证，能够基于策略和密钥种子生成一次性动态口令，支持时间型、事件型、挑战型令牌，生成的令牌有效期为30秒、60秒等可以进行调整。（提供产品功能截图证明材料）；
  10. 供应商所投SSL VPN 安全网关产品具备软件版本升级与回滚功能，保障系统稳定性。(提供产品功能截图证明材料)；
  11. 为方便平台的对接联调，供应商所投SSL VPN 安全网关产品需与密码支持服务平台、签名验签服务器需为同一品牌（提供对应证明文件）
  12. 供应商所投密码支持服务平台需具备本产品《计算机软件著作权登记证书》。（须提供证书扫描件）；
  13. 供应商所投密码支持服务平台需支持对日志文件做HMAC-SM3处理，符合密码测评要求。（提供产品功能截图证明材料）；
  14. 供应商所投密码支持服务平台需支持对关键数据做存储加密，符合密码测评要求。（提供产品功能截图证明材料）；
  15. 供应商所投密码支持服务平台需对数字签名服务，统一接口支持支持国密SM2、SM3、SM4算法，attached/detached/raw签名/验签；数字信封的制作与解封。（提供产品接口证明材料扫描件）；
  16. 为方便平台的对接联调，供应商所投密码支持服务平台与SSL VPN 安全网关、签名验签服需为同一品牌具备本产品。（需提供相应证明文件）；
  17. 供应商所投密码支持服务平台需支持与云服务器密码机对接，支持密钥的全生命周期管理及全流程管控，包括国际算法和国密算法的对称密钥、非对称密钥等密钥的生成、启用、更新、导入、导出、打印、销毁等（须提供对接证明材料扫描件或在中标后能实现对接的承诺书）；
  18. 供应商所投云服务器密码机产品需具备云数据库加密系统《计算机软件著作权登记证书》（提供证书扫描件）；
  19. 供应商所投云服务器密码机产品需支持同态密码算法，用于如数据库加密系统的密文查询、统计等场景（提供产品功能截图证明材料）；
  20. 供应商所投云服务器密码机产品需支持多租户的管理，可以对每个租户分配不同资源的VSM以及相应权限key，支持同一租户对多个VSM进行管理和密钥同步。（提供产品功能截图证明材料）；
  21. 供应商所投云服务器密码机产品需具备备份管理功能，在满足权限的情况下能够将云服务器密码机内的密钥等重要信息加密后进行备份，并且可以恢复到相同型号的云服务器密码机中，备份采用（3，5）门限方式，产生备份密钥并分割导出到5个智能密码钥匙中。（提供产品功能截图证明材料）；
  22. 供应商所投签名验签服务器需具备第三方检测报告或信息技术产品安全测试证书或《计算机软件著作权登记证书》（提供证书扫描件）；
  23. 供应商所投签名验签服务器需具备签名验签客户端软件《计算机软件著作权登记证书》（提供证书扫描件）；
  24. 供应商所投云服务器密码机产品需支持一维条形码、二维码生成和验证，并支持与移动SDK/APP无缝对接，实现扫码登录功能。（提供产品功能截图证明材料）；
  25. 供应商所投签名验签服务器需支持多台（3台及以上）设备之间机构证书同步。（提供产品功能截图证明材料）；
  26. 为方便平台的对接联调，供应商所投签名验签服务器与SSL VPN 安全网关、密码支持服务平台需为同一品牌。（提供相应证明文件）；
  27. 供应商须针对本项目制订切实可行的项目总体设计方案；
  28. 供应商须针对本项目制订切实可行的项目组织实施方案；
  29. 供应商须针对本项目制定售后服务方案；
  30. 供应商须针对本项目制订切实可行的项目培训方案；