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
采购需求和采购实施计划

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	预留
1	1	2022 年度房管信息系统密码应用建设	C0202	项	1	否	否	否	专门面相中小企业

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：

1.供应商在响应文件《采购需求响应、偏离说明表》中应对技术要求进行响应描述或偏离说明。

2.磋商文件中“★”标注的技术服务及商务要求，应满足或优于，如有不满足的其响应按照无效响应处理。

3.“▲”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

密码是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。《密码法》的颁布实施，从法律层面为开展商用密码应用提供了根本遵循，《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57号）以及《关于进一步加强全省政务信息化项目密码有关工作的通知-鄂密局发[2021]2 号》的

颁布实施，进一步促进了商用密码的全面应用。

武汉市住房保障和房屋管理局（以下简称“武汉房管局”）为贯彻落实《密码法》及《国家政务信息化项目建设管理办法》关于信息系统密码应用的要求，决定对武汉房管局房管信息系统进行密码应用改造。

通过对现状和密码应用需求进行分析，依据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等 4 个层面，以及密钥管理、安全管理等方面，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。

（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保密、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：1）供应商在投标文件《技术、服务要求响应、偏离说明表》中未对以下技术要求逐条说明响应或偏离情况的，其投标按照**无效投标处理**。

2）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：

（一）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 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）

（二）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		产品制造商通过了 CMMI-DEV V2.0（能力成熟度模型集成）3 级及以上评估
2.3		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）
2.4		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。
2.5		▲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）
2.6		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。
2.7		支持端口聚合、VLAN、支持动态路由协议包括 RIPv1、RIPv2、OSPFv1、OSPFv2。
2.8		▲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）
2.9		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。
2.10		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。
2.11		支持客户端 IP 透传，通过 HEADER，URL,COOKIE 方式透传用户客户端 IP。
2.12		支持用户名口令、动态口令，数字证书等多种认证方式。
2.13		支持角色白名单及黑名单配置，细粒度的访问控制策略。
2.14		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。
2.15		▲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）
2.16		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。
2.17		▲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）

2.18		▲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）
2.19		▲具备设备升级与回滚功能，保障系统稳定性。(提供产品功能截图证明材料)
2.20		▲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）
2.21		支持 IPV4/IPV6 双栈协议

（三）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

（四）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 位高性能、高容量智能卡芯片，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

（五）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		产品制造商通过了 CMMI-DEV V2.0（能力成熟度模型集成）3 级及以上评估。（须提供证书扫描件）
5.3		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。
5.4		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。
5.5		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。
5.6		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。
5.7		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。
5.8		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。
5.9		restful 风格接口，统一的接口说明文档，方便第三方应用接入。
5.10		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。
5.11		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。
5.12		密码安全服务大平台策略。一个平台承载多种密码安全服务。综合底层开发平台和系统设计能力，提供持续增量部署各种密码业务能力，避免形成多个密码安全服务信息孤岛，确保密码服务 API 一致性，密码设备统一运维，安全管理统一规范。
5.13		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，便于业务功能扩展。
5.14		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。
5.15		支持双活、集群、负载均衡等部署方式，支持横向扩展。
5.16		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。

5.17		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。
5.18		▲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）
5.19		▲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）
5.20		▲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）
5.21		▲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）
5.22		▲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）

（六）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		▲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）
6．3		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。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。
6．4		▲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）
6．5		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；
6．6		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。
6．7		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，可用于实现互备或负载的多台设备间的密钥同步。密钥支持远程管理。
6．8		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。
6．9		▲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）
6．10		▲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）

（七）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		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）
7.3		▲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）
7.4		产品制造商通过了 CMMI-DEV V2.0（能力成熟度模型集成）3 级及以上评估。（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 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。

2.2.1.2.4 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。

2.2.1.2.5 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

2.2.1.2.6 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质证书：

信息系统项目管理师；

网络规划设计师高级证书。

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。

2.2.1.2.7 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和未列入本标书但对项目实施必不可少的设备。供应商必须承担所投标设备(含软件)和未列入本标书招标的相关设备(含软件)的集成，并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.（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（以合同约定为准）

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，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 保密条款

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秘密和专有信息负有保密义务，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保密义务的， 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） 为了保证项目实施的质量，供应商需提供本项目的项目经理具有信息系统项目管理师、网络规划设计师证书，需提供劳动合同及资格证扫描件加盖公章；

（2） 近两年供应商具有类似业绩；

（3） 供应商具有 GB/T27922-2011 售后服务四星及以上认证证书；

（4） 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）；

（5） 供应商所投 SSL VPN 安全网关产品的制造商通过了 CMMI-DEV V2.0（能力成熟度模型集成）3 级及以上评估；

（6） 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）；

（7） 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）；

（8） 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）；

（9） 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）；

（10） 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）；

（11） 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）；

（12） 供应商所投 SSL VPN 安全网关产品具备设备升级与回滚功能，保障系统稳定性。(提供产品功能截图证明材料)；

（13） 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）

（14） 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）；

（15） 供应商所投密码支持服务平台的产品制造商通过了 CMMI-DEV V2.0（能力成熟度模型集成）3 级及以上评估。（须提供证书扫描件）；

（16） 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）；

（17） 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）；

（18） 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）；

（19） 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《计算机软件著作权登记证书》。（需提供相应证明文件）；

（20） 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);

（21） 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);

（22） 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);

（23） 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);

（24） 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);

（25） 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);

（26） 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);

（27） 供应商所投签名验签服务器的制造商通过了 CMMI-DEV V2.0（能力成熟度模型集成）3 级及以上评估。(提供证书扫描件);

（28） 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);

（29） 供应商所投签名验签服务器需支持多台（3 台以上）设备之间机构证书同步。(提供产品功能截图证明材料);

（30） 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);

（31） 供应商须针对本项目制订切实可行的项目总体设计方案;

（32） 供应商须针对本项目制订切实可行的项目组织实施方案;

（33） 供应商须针对本项目制定售后服务方案;

（34） 供应商须针对本项目制订切实可行的项目培训方案；

三、采购实施计划

3.1 合同订立安排

3.1.1 采购项目预（概）算、最高限价

本项目预算：122.08 万

最高限价：122.08 万

3.1.2 开展采购活动的时间安排

计划 11 月上旬发布磋商公告，11 月底公示中标结果并签订合同。

3.1.3 落实政府采购政策功能情况

按照武汉市集中采购目录限额标准，100 万以上项目委托政府采购中心进行采购，落实政采电子招标采购要求，项目采购采用电子标形式进行发标。

3.1.4 采购组织形式和委托代理安排

本项目采购委托招标代理开展采购工作，委托武汉市政府采购中心进行采购。

3.1.5 采购包划分与合同分包

本项目不分包。

3.1.6 供应商资格条件

1.满足《中华人民共和国政府采购法》第二十二条规定，即：

（1）具有独立承担民事责任的能力；

（2）具有良好的商业信誉和健全的财务会计制度；

（3）具有履行合同所必需的设备和专业技术能力；

（4）有依法缴纳税收和社会保障资金的良好记录；

（5）参加政府采购活动前三年内，在经营活动中没有重大违法记录；

（6）法律、行政法规规定的其他条件。

2.单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加本项目同一合同项下的政府采购活动。

3.为本采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的，不得再参加本项目的其他招标采购活动。

4.未被列入失信被执行人、重大税收违法案件当事人名单，未被列入政府采购严重违法失信行为记录名单。

5.落实政府采购政策需满足的资格要求：无

6.本项目的特定资格要求：无

3.1.7 采购方式

本项目采用竞争性磋商方式采购。

3.1.8 竞争范围

本项目在湖北省政府采购网公开发布竞争性磋商公告。

3.1.9 评审规则

本项目采用综合评分法。

3.2 合同管理安排

3.2.1 合同类型

本项目合同采用固定总价合同。

3.2.2 定价方式

依据采购人与成交供应商的成交金额确定合同价款。

3.2.3 合同文本的主要条款（仅作示例，合同条款以实际签订为准）

本合同由武汉市住房保障和房屋管理局（以下简称为“甲方”）为一方，以（以下简称“乙方”）为另一方,按下述条款和条件签署。鉴于甲方对进行公开招标采购，并接受了乙方为项目中标单位，乙方投标金额为人民币：　　元整（¥　　元）（以下简称“合同价”）。

本合同再次声明如下：

1. 本合同中的词语和术语含义与合同条款中的定义相同。
2. 考虑到甲方将按照本合同向乙方支付合同价，乙方再次保证全部按照合同的规定向甲方提供服务。
3. 考虑乙方要向甲方提供各项服务，甲方在此保证按照合同的时间和方式向乙方支付合同价。
4. 本合同一旦签订，代表乙方已同意完成投标书中承诺的内容以及招标文件中甲方要求完成的内容。

第一条 定义

本合同中，下列名词、术语具有下述特定含义：

第一章　“合同”系指买方（甲方）和卖方（乙方）签署的、合同格式中载明的买卖双方所达成的协议，包括所有的附件、附录和上述文件所提到的构成合同的所有文件。

第二章　“合同价”系指根据合同规定乙方在正确地履行完合同义务后，甲 方应支付给乙方的价格。

第三章　“安装”是指安装工作，按照合同要求的所有设备进行组装、连接和就位，安装完成通电后系统可正常运行。

第四章 “服务”系指根据本合同规定乙方承担的辅助服务。例如：技术培训、缺陷修补、维护服务和合同中规定乙方应承担的其他义务。

第五章 “调试”是指对安装完成的合同货物进行检查、调整、校正、启动、临时运行。

第六章 “甲方”均系指负责项目招标采购、建设管理、合同支付、检验验收的当事人。本合同中的甲方是指武汉市住房保障和房屋管理局，地址：武汉市建设大道 702 号。

第七章 “甲方范围”系指武汉市住房保障和房屋管理局。甲方委托其下属事业单位武汉市房产信息中心履行甲方合同部分权利和义务。

第八章 “乙方”系指与甲方签订合同,承担本项目开发任务的当事人。本合同中的乙方是指，单位地址:。

第九章 除非文档另作要求，凡提及一方、对方或各方，均包括其合法权利义务承受方和许可的受让方。

第十章 凡提及的天、日期、星期、月份和年份，即指公历日历的日历天、日期、星期、月份和年份。“工作日”指国家所规定的节假日之外的所有工作日,未指明为工作日的日期指连续的日期。

第十一章 凡本合同提及“当事人”或“各方”的措辞应指具有法人资格的任何组织。

第十二章 如果合同中的某些规定或条件被限制或宣布无效，则不影响其他规定或条件的有效性。

第十三章 凡提及合同和／或协议，均指所列举的合同和／或协议及其附件，在任何情况下，也指不时修改和补充的合同和／或协议。

第二条 合同组成

以下文件与合同具有同等法律效力，在合同文件中若有不一致的地方，则图纸和文字发生

矛盾时，以文字说明为准；前后文件有矛盾时，以时间在后者为准，标准或要求不一致时，以标准或要求高的为准；在合同实施过程中，合同各方的一切联系、通知均以书面通知为准，合同各方共同签署的其它文件，都属于合同补充文件。

2.1　合同正文；

2.2　招标编号为 号的招标文件；

2.3　乙方公开响应 号的政府采购投标文件；

2.4　中标通知书；

2.5　经双方授权代表签字确认的，在投标期间形成的书面文件；

第三条 设备清单及交货

3.1　需求清单

3.2　项目要求：

（一）报价要求

（二）项目要求。

（三）产品及安装

1.产品要求

2.安装要求

第四条 双方权利义务

4.1　　甲方权利义务：

4.2　　乙方权利义务：

第五条 合同总金额及付款方式

5.1　本合同价为　元整（¥　　元）（为含税包干价）。

5.2　　合同款由甲方按照工程进度，依据合同款支付流程分期支付给乙方。具体付款安排如下：

5.2.1　合同付款方式：签订合同后甲方向乙方支付合同款的 60%；项目验收合格后甲方向乙方支付合同款的 40%。

第六条 变更

6.1　变更的范围包括合同变更、期限变更等。

6.2　如一方有重大的问题或重要的变更发生，应当在变更发生之日起 5 工作日内向对方做出书面报告。对方也应当在 5 工作日内作出回复。如某一方违反本条的规定，该方应该承担由此而引起的项目迟延或不能及时付款及配合项目进行的后果。

6.3　如乙方对设备安装部署方案进行调整,乙方应该以书面形式提出申请,由甲方签字认可。

6.4　不应随意对合同条款进行任何变更或修改，除非双方同意并签署书面的合同修改协议，成为本合同不可分割的组成部分，具有与本合同同样的效力。

第七条 知识产权

7.1　乙方保证甲方在使用本项目或其任何一部分时不存在权利上的瑕疵，不会发生侵犯第三方专利权、版权、商标权和工业设计权等知识产权的情况。若发生侵犯第三方权利的情况，应由乙方负责处理并承担由此产生的全部责任，甲方因纠纷对外承担的赔偿，为维护权利支付的诉讼费、律师费等相关费用都应由乙方承担。

7.2 本项目工作成果所产生一切的所有权及版权归甲方所有。

7.3 项目实施和验收时乙方应向甲方提交全部设备说明书及培训资料。

7.4 本规定不因本合同的终止和到期而失效。

第八条 安全及保密

第九条 违约责任

9.1 交付违约

9.2 付款违约

9.3 保密违约

9.4 其他条款违约

第十条 不可抵抗力

第十一条　合同生效及终止

第十二条　纠纷处理

3.2.4　履约验收方案

满足采购方需求，完成采购建设内容密码改造、测试、部署、培训及试运行。依据《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）及《政务信息系统密码应用与安全性评估工作指南》（2020 版），采购方组织专家组对项目完成情况进行评审，采取项目组汇报、系统功能演示、现场答疑等方式开展项目履约验收工作。

3.2.5　风险管控措施

为防范政府采购风险，建立透明的政府采购工作流程，规范采购意向公开、采购计划、采购实施等环节，提高政府采购工作透明度，自觉接受供应商和社会群众的监督，不断提高政府采购工作的规范性。

武汉市住房保障和房屋管理局

2022 年 11 月 7 日