自然资源业务系统密码平台服务项目采购合同

陕西省自然资源信息中心（陕西省地质资料档案馆）（以下简称甲方）采购，由陕西开源招标有限公司组织采购，选定 西安鲁格信息科技有限公司（以下简称乙方）为该项目成交供应商。依据《中华人民共和国民法典》和参照《中华人民共和国政府采购法》，经甲、乙双方共同协商，按下述条款和条件签署本合同。

一、合同内容

乙方负责按照合同确定的产品名称、规格型号、数量、产地、配置内容及技术标准组织供货（具体采购项目见附件 1），按时运到甲方指定的交货地点；确保所有产品各项指标达到要求；同时乙方根据产品的使用特性做好售后服务。

二、合同价格

合同价格：人民币 陆拾捌万陆仟元整 元整（¥ 686000.00 元）

说明：

（一）合同总价包含项目报价、其他费用及应缴纳的全部税款等费用。

（二）合同总价一次包死，不受市场价格变化的影响，并作为结算的唯一依据。

三、合同款项支付

付款条件说明 1：合同签订后，达到付款条件起 30 日内，支付合同总金额的 60%。

付款条件说明 2：项目验收完成后，达到付款条件起 30 日内，支付合同总金额的 40%。

四、项目实施条件

（一）项目实施地点：陕西省自然资源信息中心（陕西省地质资料档案馆）指定地点。

（二）项目完工期：合同签订后 3 个月。

（三）质保期：3 年。

五、包装运输

（一）运杂费：一次包死，已包含在合同总价内，包括从产品供应地点到交货地点所包含的运输费、保险费、搬运费等一切费用。

（二）运输方式：陆运物流

六、质量保证

（一）乙方提供给甲方的产品必须是设计科学、技术成熟、工艺优良，是用优质材料制造的、先进的、原厂生产的未曾使用过的、全新的合格产品。

（二）设计技术专利、外形专利、应用软件专利等均应符合我国有关法律及行业标准，凡因以上问题与第三方发生的任何纠纷均与甲方无关。

（三）安全可靠。在正常使用下不应对操作者造成任何人身伤害，如因产品质量或标示不明确而对操作者造成损失的，甲方将保留依法索赔的权利。

（四）有强制性安全标准的产品，乙方应提供该产品的制造许可证证明。

（五）属于国家计量检测强检的产品，供货时提供本省法定计量检测机构出具的检测证书。

（六）产品性能必须与其标示的技术指标项符合，甲方有权在产品的有效保质期内依据技术指标对该产品进行技术验收，其主要的技术参数达不到标准时，甲方有权无条件退货或依据有关法律索赔。

（七）乙方所提供设备质保期为3年。设备质保期按设备安装验收合格办理入库之日算起。质保期满后如需更换零部件，只收取零部件成本费，终身免费维护保养。

七、技术规格及标准。（详见附件2）

八、配置清单。（详见附件3）

九、技术服务

（一）技术资料：通过完善密码基础设施，建立密码服务平台，形成集约化的密码服务体系，为陕西省国土空间基础信息平台、国土空间用途管制监管系统、用地审批系统、矿业权审批管理系统、自然资源数据管理分析共享服务系统等厅内重要信息系统提供统一的密码服务接口，构建完善的商用密码保障体系，实现加强系统安全性，提高系统安全强度，降低系统威胁和风险的目标。陕西省国土

空间基础信息平台、国土空间用途管制监管系统、用地审批系统、矿业权审批管理系统、自然资源数据管理分析共享服务系统等厅内重要信息系统通过调用统一的密码服务接口，实现数字证书身份认证、签名验签、密码运算、终端密码资源调用等密码资源需求。

（二）服务承诺：

乙方承诺本项目完工期：合同签订后3个月。项目整体质保期：3年。本次项目实施服务提供原厂技术支撑团队，团队人员4人，均具备相关的专业能力，能够为本项目提供包括技术支持、服务支撑、紧急情况支持等专业化服务能力。

其中项目负责人1人，项目团队成员3人，原厂技术支撑团队将在合同签订后10个工作日内提交本项目实施计划，包括项目的分阶段工作内容、施工计划、预计开始与完成时间等，并上报采购人确认，技术支撑团队将严格按计划节点执行，若未完成，将及时汇报说明未能按计划开展或完成工作的原因，并采取措施进行改进。技术支撑团队承诺在5分钟内响应采购人需求，最长48小时内解决问题。

十、违约责任

（一）按《中华人民共和国民法典》中的相关条款执行。

（二）未按合同要求的提供产品或设备质量不能满足技术要求，采购人有权终止合同，甚至对供方违约行为进行追究。

（三）如有纠纷，双方友好协商解决，协商不成时可诉讼到甲方所在地人民法院解决。

十一、验收

货物送至采购方指定地点后，由采购方组织使用部门进行现场验收。验收须以合同、招标文件及投标文件、澄清、及国家相应的标准、规范等为依据。

十二、其他事项

（一）采购人在合同的履行期间以及履行期后，可以随时检查项目的执行情况，对采购标准、采购内容进行调查核实，并对发现的问题进行处理。

（二）本合同一式六份，甲方 四份 ，乙方 一份 ，采购代理机构一份，甲乙双方签字盖章后生效。

（三）招标文件、投标文件也是合同的组成部分，合同中未约定的以招标文

件、投标文件为准。

合同签订地点：陕西省西安市

合同签订时间：2025 年 7 月 30 日

甲　　方	乙　　方
单位名称：陕西省自然资源信息中心（陕西省地质资料档案馆）	单位名称：西安鲁格信息科技有限公司
地　　址：	地　　址：陕西省西安市高新区锦业路 6 号绿地领海大厦 B 座 0708 室
法人代表：	法人代表：
联系电话：	联系电话：18602913933
开 户 行：	开 户 行：中国银行西安软件园支行
账　　号：	账　　号：102861549413

附件 1 采购内容

货币及单位：人民币/元

序号	产品名称	型号	生产厂家	单价（元）	单位	数量	合计（元）	备注
1	密码管理平台	CSCP-PE V1.0	北京数字认证	176,000	套	1	176,000	
2	终端密码模块	Isec 密码模块	北京信安世纪	40,000	套	1	40,000	
3	服务器密码机	HSM-A8100	北京数字认证	60,000	台	1	60,000	
4	签名验签服务器	NetSign7500B-DA	北京信安世纪	70,000	台	1	70,000	
5	安全互联网关	AG1200-DA	北京信安世纪	50,000	台	3	150,000	
6	密码支撑服务	陕西 CA/龙脉 GM3000	陕西数字认证	60,000	项	1	60,000	
7	人员驻场	定制	西安鲁格信息	130,000	年	1	130,000	
合计：人民币 陆拾捌万陆仟元整 元整（¥ 686000.00 元）								

附件 2 技术规格及标准

一、技术指标

1. 密码管理平台

提供密码管理平台，需兼容国产化环境，提供包括但不限于统一设备管理、密钥管理、统一用户管理、统一资源管理、统一应用接入管理、统一运营管理、统一服务管理、统一密码服务对接规范、密码态势分析、告警管理、统一监控、日志审计分析等能力。具体服务要求如下：

1、密码设备管理：

（1）支持在密码资源管理中登记时间戳服务器、服务器密码机、签名验签服务器、协同签名服务器、密码模块、安全认证网关的设备信息，登记完成后可以查看设备 IP、端口号、设备厂商、设备类型、设备型号、注册时间等信息；

（2）支持在密码资源管理中对时间戳服务器、服务器密码机进行资源监控及监控配置支持按小时、天等维度，以图表化形式显示设备 CPU、内存和磁盘使用情况；

2、支持密码服务监控，包括密码服务监控、服务器监控、组件监控、中间件监控等，支持以图表形式展示监控结果。（需提供国家相关部门认可的检测机构出具的产品检测报告佐证）；

3、支持密钥管理功能：

（1）支持将 A 业务系统的密钥授权给 B 业务系统使用。支持密钥授权策略的配置，包括密钥信息、密钥用途、授权周期等；

（2）支持对称密钥与非对称密钥的统计分析，包括正常、禁用、注销等各个状态下密钥数量、算法等多维度统计；

（3）不用应用之间的密钥未经授权，不能使用其他密钥进行密码运算。

4、性能要求

（1）在单台服务器密码机设备提供支撑条件下，密码服务管理平台的对称加密（SM4）处理能力 800Mbps，且平均响应时间 4ms；密码服务管理平台的对称解密（SM4）处理能力≥800Mbps，且平均响应时间≤4ms；

（2）在单台签名验签服务器设备提供支撑条件下，密码服务管理平台的签名性能（SM2）处理能力≥25000 次/秒，且平均响应时间≤2ms；密码服务管理平台的验签性能（SM2）处理能力≥18000 次/秒，且平均响应时间≤2ms。

5、提供所有密码服务的统一整合、发布，支持密码服务接口的创建、发布、上线、下线等生命周期管理，支持高性能、高可用的密码服务接口的托管服务；

6、提供所有密码服务的统一运维，支持密码服务接口的分组管理，标签管理，请求和响应参数管理，备份与恢复管理等；

7、提供密码服务接口的版本管理，支持应用兼容访问不同版本的接口；

8、提供密码服务管理平台外部密码接口的管理，支持外部密码服务接口注册到统一密码服务网关，支持外部密码服务接口的接入、发布、上线、下线、监控、统计等生命周期管理；

9、提供对密码服务限流熔断的配置，支持流控阈值请求速率、请求数、并发数的配置和返回参数信息的自定义，支持对负载服务的健康检查，服务熔断的请求间隔时间、请求超时时间、请求成功次数、请求失败次数等的配置；

10、提供统一的密码服务访问入口，支持对访问入口的配置，如 AK/SK 认证方式、防重放攻击、限流熔断、http 方法（GET、POST、PUT、DELETE、PATCH）等；

11、提供应用访问密码服务数据的统计分析，可查看服务使用、服务活跃、服务调用等情况统计分析结果，结果以图表化形式进行展现，支持按年、月、日维度展现。

12、针对各类密码设备进行统一管理、统一调度、统一监控、统一配置、动态扩展、按需分配，以密码资源池组的方式为业务系统提供密码能力，实现资源利用率的最大化；

13、支持设备、虚机等资源的连通性健康检查；

14、支持负载均衡，包括硬负载与软负载的接入配置，保证服务的高可用性，可实现弹性业务伸缩，确保流量均衡；

15、支持密码资源池调度的服务管理，包括服务一键发布、一键启动、一键升级、一键回滚、一键扩容、克隆实例、移动实例、上下架等；

16、支持日志审计功能，记录不同操作者登录、登出、密码修改、服务操作内容、操作模块、操作结果等，支持日志的搜索查询、归档与恢复；

17、提供 IP 黑白名单的配置，支持以全局维度配置 IP 黑名单，支持以业务应用、业务单位的维度配置 IP 黑白名单；

18、支持 CORS 跨域配置，支持配跨域域名、IP 网段、是否服务在身份凭证等信息；

19、能够适配以下国产化环境：

（1）操作系统：包括麒麟、统信等国产化操作系统；

（2）数据库：包括电科金仓、达梦等国产化数据库；

（3）芯片：包括飞腾、鲲鹏、海光等国产化 CPU；

（4）中间件：东方通、金蝶等国产化中间件。

20、具备《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》第二级及以上的要求；

21、具有《信息技术产品安全测试证书》；

2. 终端密码模块

提供终端密码模块，该密码服务用于 PC 客户端和业务系统服务端之间在“应用和数据安全”层面重要数据传输过程的机密性和完整性保护。

1、终端密码模块适用于 win/银河麒麟/中标麒麟/统信 UOS 等操作系统；

2、密码模块产品形态为 API 库，供其他应用程序集成调用，API 库分别包含 C、Java、JS、ArkTS 开发语言编译生成的类库，可供 C、C++、C#、Java、Objective-C、JS、ArkTS 等应用开发语言调用；

3、支持 SM2、SM3、SM4 国家标准密码算法；

4、支持 HMAC、CMAC 等消息鉴别码生成和校验；

5、支持后量子算法(Falcon（512、1024），Dilithium（level2、3、5），Kyber（512、768、1024），SphincsPlus)；

6、支持对证书请求 P10 进行解析，获取 P10 关键要素；

7、使用私钥文件进行数字信封解密操作，支持带签名和不带签名的数字信封格式；

8、使用私钥文件、公钥证书进行签名、验签操作；

9、支持客户端和服务端通过密钥协商方式实现报文和加解密及完整性保护功能；

10、支持单双向国密、国际 SSL 通道建立；

11、支持国密和国际算法自动切换；

12、支持 IPv4/IPv6 环境下优先使用 IPv6，支持 IPv6 的 HappyEyeBall 连接竞速算法；

13、支持 X86、ARM、MIPS 等 CPU 架构；

14、支持 Windows、Linux、AIX、安卓、麒麟、统信、鸿蒙等操作系统；

15、包含 C 密码模块、Java（Android）密码模块、JS 密码模块、鸿蒙密码模块、Android-SSL-SDK、Java-SSL-SDK、C-SSL-SDK、ArkTS-SSL-SDK 等。

3. 服务器密码机

1、服务器密码机要求采用国产化 CPU 及操作系统，标准机架式设备（带导轨或托盘等相关安装配件），支持双电源，实现电路冗余。

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。

3、支持基于 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。；

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。

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；

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≥1.9 万对/秒；SM4 加/解密≥2.9Gbps；SM2 签名≥6.2 万次/秒，验签≥4.3 万次/秒。

11、具备《计算软件著作权登记证书》；

12、具备《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》第二级及以上的要求。

4. 签名验签服务器

签名验签服务器为信息系统的数据和文件提供“应用和数据安全”层面的电子签名、验签服务，同时支持对称、非对称密钥产生。

1、产品要求：标准机架式设备（带导轨或托盘等相关安装配件），双电源冗余，国产飞腾≥4 核 CPU X1，硬盘≥1T，≥16G 内存，≥7 个千兆电口、≥4 个千兆光口，银河麒麟 V10 国产操作系统；

2、签名：SM2 签名≥16KTPS，SM2 验签≥11KTPS；

3、支持 PKCS7 标准和 CMS 标准签名验签；

4、支持制作、解密数字信封；支持制作、解密带签名数字信封；

5、支持 SM2、SM3、SM4 等国密标准算法；

6、支持对非对称算法、摘要算法、对称算法进行弱算法过滤的设置；

7、支持导入多级 CA 证书，证书级别不受限制；

8、支持 CRL、OCSP 方式检查证书作废列表；

9、支持配置相同主题的两张 CA 根证书，并在验签时自动识别；

10、支持 KEK 和默认两种方式的密钥加密导入导出功能以实现多机部署；

11、支持产生对称、非对称密钥；可通过导入分段的方式生成对称密钥；

12、支持对称密钥、非对称密钥、证书进行分组管理；

13、可配置连接 CA 进行在线证书的申请、下载操作；

14、支持通过 webui 上传升级包进行版本升级；

15、支持实时监控，可监控设备资源、网络、电气、签名服务等实时情况；

16、支持对指标项监控进行风险预警；支持对系统资源、加密卡、服务进程、证书密钥、日志信息等进行监控预警；

17、支持多台设备（包括生产系统和灾备系统）之间机构证书、对称密钥、非对称密钥同步；

18、支持 Java、C、C#、Restful 接口；

19、支持 HA 高可用性配置，支持通过网络和服务状态进行 HA 切换；

20、支持双因素认证登录功能；管理员证书可采用外部证书和自签证书两种方式；

21、支持管理用户分级权限管理；

22、可批量执行巡检指令实现一键巡检并生成巡检报告；包括日常巡检、应急巡检和深度巡检，支持管理员进行指令的上传、下载、删除、单个执行等操作。

23、具有《商用密码产品认证证书》，符合 GM/T 0029《签名验签服务器技术规范》、GM/T 0028《密码模块安全技术要求》第二级及以上的要求。

5. 安全互联网关

安全互联网关用于省厅、各单位的业务专线链路传输数据的机密性和完整性保护，保障省厅链路接入安全。

1、提供3台安全互联网关，产品要求：标准机架式设备（带导轨或托盘等相关安装配件），双电源冗余，国产海光CPU ≥8核8线程 X1，硬盘≥1T，内存≥16G，千兆电口≥6个，千兆光口≥4个；

2、最大并发用户数≥3000，最大加密吞吐率（国密）≥1Gbps；

3、支持SM2、SM3、SM4等国密标准算法；

4、支持SPA单包敲门，每个站点单独管理单包敲门功能。既可以单独开启、关闭此功能，相关配置相互独立。使用SM4/HMAC-SM3保证敲门包安全性；

5、支持SSLv3、TLSv1.0、TLSv1.2、TLS1.3、DTLS、TLCP等通信加密协议；

6、支持国密算法协商建立IPSec安全隧道，支持定期监测网络状态，实现隧道断线自动重建；

7、支持IKE/AH/ESP/PFS等标准IPSec协议，支持IPSec链路探测、动态隧道等；

8、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，可组合多种认证方式进行多因素认证；

9、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；

10、▲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（需提供功能截图证明）；

11、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），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；

12、支持内网3层/4层/7层的内外网应用发布；

13、支持基于多种TCP/UDP的B/S或C/S结构的业务系统，支持自定义内容改写，支持多种使用动态端口的应用协议，如：FTP、TFTP、Telnet、Oracle、SQL Server等；

14、支持远程桌面应用的发布和访问管理以及远程桌面的单点登录，用户登录后，无需 2 次登录即可直接访问远程桌面应用；

15、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；

16、▲支持应用层动脱，可通过抑制、加密、替换、散列等脱敏方式实现用户侧敏感数据脱敏，内置多种脱敏算法，如身份证、日期、Email 地址等；

17、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；

18、具备 IPv4/IPv6 双协议栈工作模式，满足 IPv6 环境部署要求；支持 IPv6 的资源访问，包括 IPv6 的 Web 资源和网络资源；

19、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；

20、支持多种高可用性模式：A/A 模式，A/S 模式，Cluster 模式，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；

21、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；

22、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；

23、具有《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》第二级及以上的要求。

6. 密码支撑服务

智能密码钥匙支撑服务：提供满足 669 个智能密码钥匙，作为密钥安全存储和个人证书载体，提供签名验签、杂凑等密码运算能力，实现用户信息的完整性、真实性保护。

数字证书支撑服务：提供满足669个合规数字证书，用于标识用户身份，实现身份真实性保护。

二、实施和售后服务

项目实施服务：本项目需提供原厂技术支撑团队，团队人员应4人，并具备相关的专业能力，为本项目提供包括技术支持、服务支撑、紧急情况支持等专业化服务能力。其中项目负责人1人，项目团队成员3人，技术支撑团队应在合同签订后10个工作日内提交本项目实施计划，至少包括项目的分阶段工作内容、施工计划、预计开始与完成时间等，并报采购人确认，严格按计划节点执行，若未完成，需汇报说明未能按计划开展或完成工作的原因，并采取措施进行改进。技术支撑团队要求能够在5分钟内响应采购人需求，最长48小时内解决问题。

驻场保障服务：要求提供一年现场密码安全运维服务，协助用户提高原有密码设备的使用率和利用率，需提供具备CISP或网络工程师证书资质的驻场工程师1人，驻场服务范围涵盖为本次项目所提供的密码产品和原有密码设备提供定期巡检和日常运维，及时发现密码配置方面的不合规或薄弱点，并进行即时整改，出具运维巡检报告及整改建议。

附件 3 配置清单

序号	产品名称	型号	技术参数
1	密码服务平台	CSCP V1.0	兼容国产化环境，提供包括但不限于统一设备管理、密钥管理、统一用户管理、统一资源管理、统一应用接入管理、统一运营管理、统一服务管理、统一密码服务对接规范、密码态势分析、告警管理、统一监控、日志审计分析等能力。
2	终端密码模块	Isec 密码模块	该密码服务用于 PC 客户端和业务系统服务端之间在“应用和数据安全”层面重要数据传输过程的机密性和完整性保护。 1、终端密码模块适用于 win/银河麒麟/中标麒麟/统信 UOS 等操作系统； 2、密码模块产品形态为 API 库，供其他应用程序集成调用，API 库分别包含 C、Java、JS、ArkTS 开发语言编译生成的类库，可供 C、C++、C#、Java、Objective-C、JS、ArkTS 等应用开发语言调用； 3、支持 SM2、SM3、SM4 国家标准密码算法；
3	服务器密码机	HSM-A8100	1、服务器密码机要求采用国产化 CPU 及操作系统，标准机架式设备（带导轨或托盘等相关安装配件），支持双电源，实现电路冗余。 2、SM2 密钥对产生≥1.9 万对/秒；SM4 加/解密≥2.9Gbps；SM2 签名≥6.2 万次/秒，验签≥4.3 万次/秒。 11、具备《计算软件著作权登记证书》； 12、具备《商用密码产品认证证书》，符合 GM/T 0028《密码模块安全技术要求》第二级及以上的要求。
4	签名验签服务器	NetSign7500 B-DA	1、产品要求：标准机架式设备（带导轨或托盘等相关安装配件），双电源冗余，国产飞腾≥4 核 CPU X1，硬盘≥1T，≥16G 内存，≥7 个千兆电口、≥4 个千兆光口，银河麒麟 V10 国产操作系统； 2、签名：SM2 签名≥16KTPS，SM2 验签≥11KTPS； 3、支持 PKCS7 标准和 CMS 标准签名验签； 4、支持制作、解密数字信封；支持制作、解密带签名数字信封；

			5、支持 SM2、SM3、SM4 等国密标准算法；
5	安全互联网关	AG1200-DA	3 台安全互联网关，产品要求：标准机架式设备（带导轨或托盘等相关安装配件），双电源冗余，国产海光 CPU 8 核 8 线程 X1，硬盘 1T，内存 16G，千兆电口 6 个，千兆光口 4 个；最大并发用户数 3000，最大加密吞吐率（国密）1Gbps；支持 SM2、SM3、SM4 等国密标准算法；
6	密码支撑服务	陕西 CA/龙脉 GM3000	智能密码钥匙支撑服务：提供满足 669 个智能密码钥匙，作为密钥安全存储和个人证书载体，提供签名验签、杂凑等密码运算能力，实现用户信息的完整性、真实性保护。 数字证书支撑服务：提供满足 669 个合规数字证书，用于标识用户身份，实现身份真实性保护。
7	人员驻场	西安鲁格信息定制	提供一年现场密码安全运维服务，协助用户提高原有密码设备的使用率和利用率，需提供具备 CISP 或网络工程师证书资质的驻场工程师 1 人，驻场服务范围涵盖为本次项目所提供的密码产品和原有密码设备提供定期巡检和日常运维，及时发现密码配置方面的不合规或薄弱点，并进行即时整改，出具运维巡检报告及整改建议。