

第三章 招标项目技术、服务、商务及其他要求

（注：当采购包的评标方法为综合评分法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

（注：当采购包的评标方法为最低评标价法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1 采购项目概况

随着信息化的快速发展，IT数据的激增，信息安全重要性已经上升到国家安全层面，密码作为信息安全的基石更为重要，为确保密码算法的自主可控，降低敏感信息泄露以及信息系统遭受攻击的风险，国家密码管理局自2012年开始制定并发布了基于自主知识产权的国产密码算法。依据《中华人民共和国网络安全法》、《中华人民共和国密码法》、《商用密码管理条例》及GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等标准规范，从密码功能要求、密码技术应用要求等方面进行密码应用实训仿真环境建设。建设完成后具备签名验签、对称加解密、非对称加解密、MAC/HMAC、电子签章、数字信封、数字证书签发、时间戳、SSL、动态口令认证、二维码扫码认证、数字证书认证、移动认证等密码服务，通过这些密码服务为师生提供密码应用的教学、科研、实验及考试。增强学院课程内容的丰富，提升学院学生密码相关的个人技术能力，提高整体就业率，同时增强学院密码相关科研成果的输出能力。

3.2 采购内容

3.2.1 标的清单

采购包1:

采购包预算金额（元）：2,000,000.00

采购包最高限价（元）：2,000,000.00

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否涉及核心产品	是否涉及采购进口产品	是否涉及采购节能产品	是否涉及采购环境标志产品
1	应用安全网关/安全认证网关	50.00	163,000.00	套	软件和信息技术服务业	否	否	否	否
2	电子签章系统	50.00	129,000.00	套	软件和信息技术服务业	否	否	否	否
3	移动统一认证安全管理平台	50.00	148,500.00	套	软件和信息技术服务业	否	否	否	否

4	数据加解密服务系统	50.00	168,000.00	套	软件和信息技术服务业	否	否	否	否
5	签名验签客户端	1.00	60,000.00	套	软件和信息技术服务业	否	否	否	否
6	国密门禁系统安全网关	1.00	37,500.00	套	软件和信息技术服务业	否	否	否	否
7	密码应用一体化系统	4.00	117,800.00	台	软件和信息技术服务业	是	否	否	否
8	USB-KEY	100.00	3,000.00	个	软件和信息技术服务业	否	否	否	否
9	密评工具箱系统	1.00	105,000.00	套	软件和信息技术服务业	是	否	否	否
10	手机令牌	2.00	50,000.00	套	软件和信息技术服务业	否	否	否	否
11	动态令牌认证系统	50.00	143,000.00	套	软件和信息技术服务业	否	否	否	否
12	SSL VPN安全网关	50.00	166,000.00	套	软件和信息技术服务业	否	否	否	否
13	移动安全认证客户端软件	2.00	126,000.00	套	软件和信息技术服务业	否	否	否	否

14	签名验签服务器 (系统)	50.00	160,000.00	套	软件和 信息技 术服务 业	否	否	否	否
15	数字证书认证系 统	50.00	175,000.00	套	软件和 信息技 术服务 业	否	否	否	否
16	安全浏览器	100.00	50,000.00	套	软件和 信息技 术服务 业	否	否	否	否
17	时间戳服务器 (系 统)	50.00	165,000.00	套	软件和 信息技 术服务 业	否	否	否	否
18	视频监控数据安全 与防护系统	1.00	30,000.00	套	软件和 信息技 术服务 业	否	否	否	否
19	视频摄像头	4.00	3,200.00	个	软件和 信息技 术服务 业	否	否	否	否

3.3技术要求

采购包1:

标的名称: 应用安全网关/安全认证网关

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、同时支持单向、双向SSL卸载，同时支持标准的国际算法和国密算法（TLS1.2，TLS1.3，SM2V1.1）协议（需提供清晰功能截图）；</p> <p>3、支持RSA1024位、RSA2048位及SM2三种密钥的客户端以及服务器证书，且可同时支持RSA和SM2证书提供服务；</p> <p>4、SSL算法可配置，过滤弱算法，拒绝未配置的客户端算法请求；支持通用的主流加密算法，包括SM2、SM3、SM4算法（需提供清晰的截图）；</p> <p>5、传输客户端证书到后台，支持header和cookie方式传递用户整张证书信息，同时支持header、cookie、url三种方式传输证书某一项信息到后台服务器（需提供清晰的截图）；</p> <p>6、支持同时使用多个信任CA，用户证书作废状态验证，支持下载CRL或在线OCSP来检测客户端证书是否作废，后台服务健康检查，支持icmp、tcp、HTTP等等多种主动式服务器健康检查方法；</p> <p>7、服务器负载均衡功能，支持OSI 模型中二层、三层、四层和七层的负载均衡。（二层负载均衡基于网络接口。三层负载均衡基于服务器IP地址。四层负载均衡与TCP或UDP端口有关。七层负载均衡是基于应用层的信息，如URL、HTTP表头或Cookie等）负载算法不小于22种（需提供清晰的功能截图）；</p> <p>8、支持IPv4和IPv6的相互地址转换，支持混合资源负载,支持NAT64、NAT46、NAT66、NAT44，支持IPv4/v6双栈（需提供清晰的功能截图）；</p> <p>9、命令行页面（OS命令行）无需安装辅助软件即可运行ping、tcpdump、telnet等排错命令，管理页面可查看证书算法、证书有效期起止时间等所有信息（需提供界面截图）；</p> <p>10、同时支持支持工业标准的SOAP 和REST API 的全功能接口，实现与第三方管理软件的无缝集成（需提供清晰功能截图）；</p> <p>11、节点之间支持VRRP和心跳线两种主/备切换方式。支持多种高可用模式：A / A模式，A / S模式，最多可以支持32台设备的集群。支持双节点切换功能。切换时间小于200ms；基于CPU、内存占用率、SSL加速卡状态进行条件筛选进行主备节点切换或服务重启（需提供清晰功能截图）；</p> <p>▲12、安全客户端：支持提供对应的安全客户端，客户端支持签名验签功能、SSL加解密功能及证书认证功能，支持国密算法；提供客户端产品的《商用密码产品认证证书》、《著作权证书》（需提供清晰的证明材料和证书影印件）；</p> <p>▲13、产品具有国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“应用安全网关”关键字，提供证书影印件；</p>
---	--

标的名称：电子签章系统

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、产品符合GM/T0031《电子签章密码技术规范》、GB/T38540《信息安全技术安全电子签章密码技术规范》；</p> <p>3、支持Word、Excel、PDF、OFD、SVG等格式文件签章（需提供清晰功能截图）；</p> <p>4、支持多页骑缝章功能，支持同一文件多人轮流签章功能，支持同一文件多人不特定顺序同时签章功能，支持在不安装签章客户端软件的计算机上实现防止非法打印和非法截屏功能；</p> <p>5、支持电子印章制作、管理、发放、挂失、停用、更新、重新生成颁发等功能；</p> <p>6、支持一个电子印章对应多个印章使用人证书，支持一个印章使用人证书可授权使用多个电子印章；</p> <p>7、产品提供服务端印章存储功能，可以统一存储、监管电子印章；</p> <p>8、支持服务器签章、服务器验章功能；</p> <p>9、支持关键字定位和坐标定位签章功能，支持坐标定位多页签章功能，支持即时制章同时签章的功能；</p> <p>10、支持用户管理功能，可对用户进行的浏览、添加、设置、修改、删除与查询等操作，可对接CA等安全管理设施，进行统一用户管理（需提供清晰功能截图）；</p> <p>11、支持系统监控功能；</p> <p>12、支持对电子印章数据和电子印章状态数据的查询、统计功能；</p> <p>13、支持对用户管理、印章管理等操作进行日志记录以供审计；日志的内容包括操作用户，被操作人员，操作对象，操作时间，操作描述等；</p> <p>14、具备《计算机软件著作权登记证书》；</p> <p>▲15、产品具备国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“电子签章系统”关键字，提供证书影印件；</p>
---	--

标的名称：移动统一认证安全管理平台

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、支持用户管理：用户新增、修改、删除、用户注册授权码管理，设备管理：对用户移动终端设备进行管理，包括设备绑定、解绑、挂失等；</p> <p>3、证书管理：后台通过与数字证书认证系统对接，为移动端客户提供证书申请、更新、冻结、解冻、作废等证书管理；</p> <p>4、数字签名/验签：移动端数字签名请求及业务系统数字签名验签服务，二维码服务：可信二维码生成、验证；</p> <p>5、支持通过移动数字证书实现 SSL/TLS 协议的加密传输功能；</p> <p>6、具备客户端电子签章功能，移动电子签章服务管理模块需集成在安全管理平台中，负责电子印章的管理与认证、电子签章的审计等功能；</p> <p>7、支持与移动安全中间件SDK进行无缝整合，提供秘钥分散管理技术，基于用户行为特征、移动硬件特征、OS特征派生证书私钥，支持将私钥打散存放在手机APP及后台，支持签名门限合成技术保证在数字签名、数据加解密过程中私钥永不合体，保障私钥安全；</p> <p>8、管理员可以管理用户操作员和审计操作员，分别负责用户的操作以及系统的审计，包括操作员的添加、维护、授权和删除功能；</p> <p>9、支持数字证书签发、动态密码生成验证、电子签章验证、数字签名验签功能，并且支持配置外接不同数字证书签发系统、动态密码服务器系统、电子签章验证、签名验签服务器功能（需提供清晰功能截图）；</p> <p>10、密钥管理功能：提供密钥安全生成、存储、使用及销毁功能，数字证书私钥由各参与实体(用户、设备、服务器等)各自形成和维护自己的分散私钥片段，公开自己的公钥片段，需要参与签名运算时，各分散私钥片段独立计算得到分段签名结果，由门限签名算法负责将分段签名结果整合成完整签名结果；</p> <p>▲11、产品具备国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“移动统一认证安全管理平台”关键字，提供证书影印件；</p>
---	--

标的名称：数据加解密服务系统

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、支持对称密码算法：SM4；</p> <p>3、支持对称密钥、非对称密钥对象的管理，包括：状态管理和属性管理等；</p> <p>4、支持密钥对象的生成、更新、备份、恢复、归档、销毁等安全生命周期管理操作；</p> <p>5、支持以密钥分量方式导入、导出对称密钥，支持密码信封方式导入/导出非对称密钥；</p> <p>6、支持三级密钥体系：根密钥、客户主密钥、工作密钥，每级逐级向下派生密钥；</p> <p>7、支持对称密钥和非对称密钥加解密，支持对结构化数据加解密，支持签名验签、生成随机数、生成数字信封、生成数字摘要，支持在线加密和本地加密；</p> <p>8、支持KMIP客户端管理：支持新增、删除、停用KMIP客户端，可配置KMIP客户端认证方式、通信方式、操作权限等；</p> <p>9、支持应用系统无需改造的数据库切面加密功能（需提供清晰功能截图）；</p> <p>10、支持应用系统无需改造的数据库透明加密功能；</p> <p>11、支持字段级的数据库加解密能力，支持保留格式加密，数据格式长度不变；</p> <p>12、支持敏感数据脱敏，并支持自定义脱敏策略；</p> <p>13、支持基于角色的访问控制，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；（需提供清晰的截图证明）</p> <p>14、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、网络的使用情况、展示版权、产品型号和License信息（需提供清晰的截图证明）；</p> <p>▲15、产品具有国家认可的第三方认证机构颁发的《商用密码产品认证证书》，达到GM/T 0028 《密码模块安全技术要求》二级安全要求，且证书中包含“数据加解密”关键字，提供证书影印件；</p>
---	--

标的名称：签名验签客户端

参数性质	序号	技术参数与性能指标
	1	<p>1、支持IE10及以上版本所有浏览器数字签名，支持非IE（Edge、Chrome、Firefox、360、密信）浏览器所有版本数字签名，支持HTML5数字签名方式；</p> <p>2、同时支持国密算法数字签名、国际算法数字签名方式；</p> <p>3、签名控件需要提供应用开发商调用API接口详细开发手册；</p> <p>4、产品支持银河麒麟、中标麒麟、统信操作系统，提供兼容性测试通过证明文件，提供证书影印件；</p> <p>5、产品具有中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》，提供证书影印件；</p> <p>▲6、品牌一致性要求：密码应用一体化系统、签名验签客户端、移动安全认证客户端软件、动态令牌认证系统、密评工具箱系统为同一品牌，提供原厂授权函及中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》，提供证书影印件；</p>

标的名称：国密门禁系统安全网关

参数性质	序号	技术参数与性能指标
	1	<p>1、国密门禁管理系统+加密系统+完整性审计系统+服务器+加密卡+门禁卡+键盘读卡器+四门控制器+门磁锁；</p> <p>2、标配管理16门管理授权，含发卡器；</p>

标的名称：密码应用一体化系统

参数性质	序号	技术参数与性能指标
	1	<p>★1、标准2U设备，双电源，硬盘≥4T，内存≥96G，千兆电口≥2个、万兆光口≥4个；</p> <p>★2、L4：新建：≥2.9M CPS、并发：≥32M、吞吐：≥140Gbps；L7：新建：≥800KRPS、并发：≥4.8M、吞吐：≥100Gbps；</p> <p>3、采用密码超融合架构将计算、网络、密码的虚拟化整合到同一个设备中，对外提供云化的密码应用服务，支持提供签名验签、对称加解密、非对称加解密、MAC\HMAC、电子签章、数字信封、数字证书签发、时间戳、SSL、动态口令认证、二维码扫码认证、数字证书认证、移动认证、移动加解密、移动电子签章、移动SSL等服务（需提供清晰功能截图）；</p> <p>▲4、产品具备国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“密码应用一体化系统”关键字，提供原厂授权函及证书影印件；</p>

标的名称：USB-KEY

参数性质	序号	技术参数与性能指标

1	<p>1、数字证书存储介质，每个介质中装载由CA证书认证系统签发的数字证书，可以与CA证书认证系统无缝对接；</p> <p>2、密钥处理和运算均在存储硬件内部进行；</p> <p>3、处理器采用32位智能卡芯片；</p> <p>4、存储空间：$\geq 64K$(用户空间)；</p> <p>5、数据存储年限：至少10年；</p> <p>6、室温下最少擦写次数为50万次；</p> <p>7、支持USB1.1、2.0、3.0接口；</p> <p>8、支持算法：RSA1024/2048、DES、3DES、SHA256、SHA-1、MD5、SM1、SM2、SM3、SM4；</p> <p>9、支持操作系统：Windows 10及以上版本/Linux；</p> <p>10、符合国密的GM/T 0002、GM/T 0003、GM/T 0004、GM/T 0005、GM/T 0006规范；</p>
---	---

标的名称：密评工具箱系统

参数性质	序号	技术参数与性能指标
1	1	<p>1、密评工具箱系统是商用密码应用安全性评估工作的一体化专业便携笔记本设备，包括IPSECVPN检测工具、SSLVPN检测工具、SSL协议在线检测工具、随机数检测工具、证书检测工具、算法检测工具、端口检测工具等（需提供清晰功能截图）；</p> <p>2、支持为用户提供定期备份数据库功能（需提供清晰功能截图）；</p> <p>3、支持日志审计功能，可以审计用户对密评工具箱系统的所有操作；</p> <p>4、提供密评任务的创建以及任务数据的维护，提供单位信息的新建、修改、删除和拉取，提供信息系统以及相关资产数据的导入和查看，提供信息系统测评表单的自动生成；提供测评表单的任务分解；</p> <p>5、支持密评报告管理，包括管理密评报告的生成、预览及下载（需提供清晰功能截图）；</p> <p>6、支持生成测评任务、生成调查表、生成测评检查表单、生成测评报告（需提供清晰功能截图）；</p> <p>7、支持SSLVPN协议、IPSECVPN协议的离线和在线分析功能，并展示检测报告（需提供清晰功能截图）；</p> <p>8、支持检测证书的有效期、格式、信任域及吊销验证并出具报告；</p> <p>9、支持对随机数样本的检测并展示检测结果；</p> <p>10、具备知识库管理功能，包括电子文档的归档管理以及在线预览和下载（需提供清晰功能截图）；</p> <p>▲11、品牌一致性要求：密码应用一体化系统、签名验签客户端、移动安全认证客户端软件、动态令牌认证系统、密评工具箱系统为同一品牌，提供原厂授权函及中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》，提供证书影印件；</p>

标的名称：手机令牌

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<p>1、独立移动应用APP，支持Android OS 4.4及以上移动操作系统；</p> <p>2、支持多种加密算法和杂凑运算，支持RSA、SHA1、SHA256、SM2、SM3和SM4等密码算法；</p> <p>3、支持产生动态密码，且动态密码长度可以手动切换；</p> <p>4、APP登录支持指纹认证、手势密码等认证方式，APP支持多账号管理（需提供清晰功能截图）；</p> <p>5、APP端支持扫码添加动态密码账号，同时支持APP端生成动态密码账号加密同步到服务端。</p>
---	---

标的名称：动态令牌认证系统

参数性质	序号	技术参数与性能指标
	1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、产品同时支持管理模块、生成模块、验证模块，三个模块独立运行，独立管理，支持单独模块的负载均衡；</p> <p>3、支持操作系统（如Windows，UNIX、Linux、Solaris、AIX等）的动态密码验证；</p> <p>4、支持业务系统与应用开发接口（验证API）相结合；支持RADIUS PEAP、PAP、CHAP、MSCHAP/MSCHAPV2协议；</p> <p>5、支持RSA算法，支持国密算法，支持动态增加算法，以扩展系统对多种不同算法的支持，支持各种加密算法；</p> <p>6、支持最终用户自主选择动态密码终端类型，如：矩阵卡、刮刮卡、手机短信、手机令牌，支持基于事件同步动态令牌，支持基于时间同步动态令牌，支持基于挑战-响应动态令牌；</p> <p>▲7、产品具有国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“动态令牌认证系统”关键字，提供原厂授权函及证书影印件；</p>

标的名称：SSL VPN安全网关

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、产品支持标准TLS1.2/SM2v1.1 协议,支持国际算法及国密算法，包括SM4、SM3、SM2等（需提供清晰的截图证明）；</p> <p>3、产品支持SITE TO SITE功能，并支持零客户端、零终端部署，解决LAN to LAN组网方式（需提供清晰的截图证明）；</p> <p>4、产品支持Android系统的L3访问，PC客户端支持Windows平台、国产PC平台（包括X86架构、ARM架构、MIPS架构，系统支持统信、麒麟）；</p> <p>5、产品必须支持隧道模式，可安全的访问所有基于IP的（TCP、UDP）应用，B/S、C/S结构及其他网络服务（需提供清晰的截图证明）；</p> <p>6、产品必须支持多种SSL VPN认证方法，包括LDAP、RADIUS、AD、证书、本地数据库、SAML、OAuth等（需提供清晰的截图证明）；</p> <p>7、产品必须支持VRRP和心跳线两种主/备切换方式，支持多种条件切换主备状态，CPU利用率阈值、内存利用率阈值、CPU温度、链路检查等（需提供清晰的截图证明）；</p> <p>8、产品命令行页面（OS命令行）可进行ping、tcpdump、telnet等排错命令，不可安装其他辅助软件（需提供清晰的运行界面截图证明）；</p> <p>9、具备良好的兼容性，可支持目前主流的浏览器平台，如Firefox、Netscape、IE等；支持主流操作系统Linux、Windows及国产操作系统（中标麒麟、银河麒麟、统信）；</p> <p>▲10、产品具有国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“安全接入网关”关键字，提供证书影印件；</p>
---	--

标的名称：移动安全认证客户端软件

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<p>1、支持Android OS 4.4及以上操作系统；</p> <p>2、支持多种加密算法和杂凑运算，支持RSA、SHA1、SHA256、SM2、SM3和SM4等密码算法；</p> <p>3、用户管理：用户签约、用户PIN管理、用户行为监测；</p> <p>4、支持用户密钥安全生成与安全计算，用户私钥分散，用户私钥移动端分散片段不保存，各分散私钥片段独立计算得到分段签名结果，由门限签名算法负责将分段签名结果整合成完整签名结果；</p> <p>5、支持移动端数字证书申请、更新与安全存储；</p> <p>6、支持数字签名与验签，与移动统一认证安全管理平台配合生成完整签名，任何一方均不能单独生成签名；</p> <p>7、移动威胁感知：实时监测移动终端安全态势、并把采集的数据发送到移动统一认证安全管理平台进行安全分析；</p> <p>8、支持国际和国密SSL安全链接，保障移动通信安全；</p> <p>▲9、品牌一致性要求：密码应用一体化系统、签名验签客户端、移动安全认证客户端软件、动态令牌认证系统、密评工具箱系统为同一品牌，提供原厂授权函及中华人民共和国国家版权局颁发的《计算机软件著作权登记证书》，提供证书影印件；</p>
---	---

标的名称：签名验签服务器（系统）

参数性质	序号	技术参数与性能指标
	1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、支持按照PKCS#10标准生成证书请求并导出请求包；支持1024/2048位RSA算法、256位SM2算法的数字签名和签名验签功能，支持带签名的数字信封，解密带签名的数字信封；信任域列表管理支持跨域，检查证书作废列表可配置，支持导入多级CA证书，时检查证书作废列表，检查CRL有效期；</p> <p>3、支持多节点（3节点以上）之间机构证书同步，支持机构证书列表管理，按机构名称、证书DN、证书有效期搜索证书，下载、更新机构名称，证书黑名单管理（需提供清晰功能截图）；</p> <p>4、API接口要求：支持长连接和短连接，支持JAVA、.Net、C/C++语言的API接口；</p> <p>5、通过DownloadCRL配置下载CRL列表，可以通过LDAP、HTTP方式下载，并支持OCSP方式验证证书有效性；登陆系统所需的权限管理，设置超级管理员、系统管理员和日志审计员；</p> <p>6、支持生产系统和灾备系统之间的设备远程证书同步，支持弱算法过滤，且可灵活配置，支持通过管理界面进行补丁升级，且具有回退功能（需提供清晰功能截图）；</p> <p>7、支持PDF印章管理，支持多个印章管理，PDF签章及数字签名验签，并且提供JAVA/.NET接口调用方式，并且提供国密算法PDF阅读器（需提供清晰功能截图）；</p> <p>▲8、产品具备国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“签名验签”关键字，提供证书影印件；</p>

标的名称：数字证书认证系统

参数性质	序号	技术参数与性能指标
	1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、功能要求：支持数字证书管理：证书申请、证书审核、证书签发、证书发布、证书撤销、证书挂起、证书更新、日志管理、安全管理等基本证书管理功能；</p> <p>3、性能要求：含证书容量1000张，支持扩容容量≥1万张，支持CRL（证书撤销列表）下载与更新服务，能自行设置证书撤销列表更新频率；</p> <p>4、日志管理：提供日志管理功能，具体包括系统运行日志、系统管理日志、帐户日志、证书日志和证书撤销列表日志；</p> <p>5、双证书支持：支持通过一个p10请求，同时发放两张证书（一张签名证书，一张加密证书），到期管理：支持证书到期提醒（提供截图证明）；</p> <p>6、协议支持：支持SCEP协议（提供截图证明）；</p> <p>7、扩展性：产品需要有良好的扩展性，支持双机热备技术及负载均衡技术；系统备份：支持通过管理界面对系统进行备份、恢复；</p> <p>8、算法要求：支持RSA与国密算法，标准要求：证书符合ITU X.509 V3格式，证书撤销列表符合ITU X.509 V2标准，证书存储格式支持Base64、DER、PKCS#7等格式，中文支持：证书对中文有良好的支持，并具有中文DN功能；</p> <p>▲9、产品具有国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“数字证书认证”关键字，提供证书影印件；</p>

标的名称：安全浏览器

参数性质	序号	技术参数与性能指标
------	----	-----------

1	<p>1、支持对中标麒麟、银河麒麟、中科方德、UOS、深度、普华、国心、一铭、新支点等国产操作系统，需提供至少5种与国产操作系统厂商的互认证证书的影印件；</p> <p>2、支持对龙芯、兆芯、飞腾、鲲鹏等国产芯片，需提供至少3种与国产芯片厂商的互认证证书的影印件；</p> <p>3、支持对南大通用、达梦、神州通用、人大金仓等国产数据库，需提供至少3种与国产数据库厂商的互认证证书的影印件；</p> <p>4、支持对东方通、金蝶等国产应用中间件，需提供至少2种与国产应用中间件厂商的互认证证书的影印件；</p> <p>5、双算法支持，同时支持国密算法和国际通用算法，同时支持 SSL 单项及双向链接；</p> <p>6、支持客户端信息汇集功能，可以根据用户身份信息、访问地址信息、客户端启动关闭信息、应用系统页面脚本运行错误信息、插件及证书加载异常信息等数据进行用户行为审计；</p> <p>7、支持安全策略推送功能，提供对于安全浏览器客户端软件的某些安全管控功能的策略配置和推送、下发、更新；</p> <p>8、支持安全策略配置项的推送：兼容模式配置、插件管控、证书管控、完整性校验、隐私设置、防拷贝、数字水印；</p> <p>▲9、产品具有国家认可的第三方认证机构颁发的《商用密码产品认证证书》，提供证书影印件。</p>
---	--

标的名称：时间戳服务器（系统）

参数性质	序号	技术参数与性能指标
	1	<p>1、以虚拟化镜像的方式部署在密码应用一体化系统上面（需提供清晰功能截图）；</p> <p>2、支持签发时间戳、验证时间戳、查看时间戳、检索时间戳（需提供清晰功能截图）；</p> <p>3、支持多种可信时间源获取方式：包括国家授时中心等NTP服务器，北斗、GPS等卫星导航系统，4G-LTE蜂窝无线通讯基站；</p> <p>4、支持证书的CRL验证及OCSP验证；</p> <p>5、同时支持国际算法、国产算法，签名算法：RSA 1024/2048/4096、SM2，摘要算法：SHA-1/SHA-2(SHA-256、SHA-512)、SM3；</p> <p>6、支持日志管理功能，包括服务日志、系统日志、HA日志、SNMP日志、DownloadCRL日志、OCSP日志、WatchDog日志；</p> <p>7、支持SNMP、SYSLOG；</p> <p>▲8、产品具有国家认可的第三方认证机构颁发的《商用密码产品认证证书》，且证书中包含“时间戳”关键字，提供证书影印件；</p>

标的名称：视频监控数据安全与防护系统

参数性质	序号	技术参数与性能指标
------	----	-----------

1	桌面式结构，产品支持8路视频接入；内置国密安全芯片，支持SM1/SM2/SM3/SM4算法，至少支持8路1080P视频接入，支持UDP协议，兼容H.264和H.265编码协议，支持对符合GB/T28181的视频流进行传输的机密性保护，支持对NVR存储的视频数据进行机密性保护，支持对符合GB/T28181的视频流进行传输的完整性保护，支持对NVR存储的视频数据进行完整性保护；
---	--

标的名称：视频摄像头

参数性质	序号	技术参数与性能指标
	1	≥400万像素，焦距：4MM,星光夜视，≥30M红外夜视距离。

3.4商务要求

3.4.1交货时间

采购包1:

自合同签订之日起90日

3.4.2交货地点

采购包1:

四川轻化工大学（宜宾校区）

3.4.3支付方式

采购包1:

分期付款

3.4.4支付约定

采购包1: 付款条件说明：签订合同后，采购人接到成交供应商通知、成交供应商出具的合法、有效、完整的票据资料后，达到付款条件后15日内，支付合同金额的30%作为项目预付款；，达到付款条件起15日内，支付合同总金额的30.00%。

采购包1: 付款条件说明：全部货物安装调试完毕并验收合格，采购人接到成交供应商通知、成交供应商出具的合法、有效、完整的全额增值税专用发票后，达到付款条件后30日内，支付合同金额的70%。，达到付款条件起30日内，支付合同总金额的70.00%。

3.4.5验收标准和方法

采购包1:

验收方法：按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）、《政府采购需求管理办法（财库〔2021〕22号）》、《四川轻化工大学采购项目验收管理办法（川轻化〔2020〕11号）》以及招标文件的质量要求和技术指标、中标投标人的投标文件及承诺与合同约定标准的要求进行验收；招投标双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由招标人在招标与投标文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。

3.4.6包装方式及运输

采购包1:

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

3.4.7质量保修范围和保修期

采购包1:

质量保修范围和保修期：保修期：验收合格通过之日起3年；提供设备原厂维修服务，即时响应（包括电话响应）；电话

响应无法解决4小时内到达现场，24小时内修复，如在48小时内无法修复，则提供部件冗余服务或采取应急措施，提供相同产品或不低于故障产品规格档次的备用产品供采购人使用，以确保货物的正常使用。

3.4.8违约责任与解决争议的方法

采购包1:

按照合同的执行

3.5其他要求

★1、交货期限：合同签订之日起90天。★2、交货地点：四川轻化工大学（宜宾校区）★3、付款方式：（1）签订合同后，采购人接到成交供应商通知、成交供应商出具的合法、有效、完整的票据资料后，达到付款条件后15日内，支付合同金额的30%作为项目预付款；（2）全部货物安装调试完毕并验收合格，采购人接到成交供应商通知、成交供应商出具的合法、有效、完整的全额增值税专用发票后，达到付款条件后30日内，支付合同金额的70%。★4、质量保修范围和保修期：保修期：验收合格通过之日起3年；提供设备原厂维修服务，即时响应（包括电话响应）；电话响应无法解决4小时内到达现场，24小时内修复，如在48小时内无法修复，则提供部件冗余服务或采取应急措施，提供相同产品或不低于故障产品规格档次的备用产品供采购人使用，以确保货物的正常使用。★5、验收方法：按照《财政部关于进一步加强政府采购需求和履约验收管理的指导意见》（财库〔2016〕205号）、《政府采购需求管理办法（财库〔2021〕22号）》、《四川轻化工大学采购项目验收管理办法（川轻化〔2020〕11号）》以及招标文件的质量要求和技术指标、中标投标人的投标文件及承诺与合同约定标准的要求进行验收；招投标双方如对质量要求和技术指标的约定标准有相互抵触或异议的事项，由招标人在招标与投标文件中按质量要求和技术指标比较优胜的原则确定该项的约定标准进行验收。6、其他要求（对应评分表内容）：（1）投标供应商根据本项目采购需求在有利于项目实施的角度有针对性的编制技术服务方案，主要包含以下内容：①需求分析；②总体设计；③进度计划；④项目管理方案（2）。投标供应商根据本项目采购需求在有利于项目实施的角度有针对性的编制培训及售后服务方案（3）投标供应商通过一体化平台，对密码应用一体化系统相关功能进行演示内容（4）投标供应商对产品部署上线时间提供承诺（5）为保证履约能力，产品生产厂家或供应商需具有相关体系证书认证与技术人员专业资质认证。