黄河水利职业技术学院政府采购项目

合同书

（合同年度编号：2024-056）

项 目 名 称 ：	校园可信认证系统及设备采购项目
项目资金来源：	可信校园密码服务平台（双高校建设项目）
项目方案核准编号：	发规（2024 年第 1 号）（2024 年 1 月 24 日）
项目招标编号：	豫财磋商采购-2024-41
采购单位(甲方)：	黄河水利职业技术学院
供货单位(乙方)：	北京数字认证股份有限公司
合同签订时间：	2024 年 8 月 16日

项目采购合同书

采购单位（甲方）：黄河水利职业技术学院

供货单位（乙方）：北京数字认证股份有限公司

根据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《中华人民共和国民法典》等相关法律法规、规范性文件以及校园可信认证系统及设备采购项目的招标磋商文件、投标响应文件、中标（成交）通知书等文件的相关内容，甲乙双方经平等协商，就该项目的有关事项达成如下协议，以资共同遵守。

一、甲方向乙方采购货物一览表

序号	货物名称	规格型号	数量	单价（元）	金额（元）	生产厂商	备注
1	教育数字证书认证系统	DICA	1 套	290000	290000	北京数字认证股份有限公司	/
2	教育密码综合服务子系统	CSCP-BA	1 套	393600	393600		一次报价¥430000.00
3	教育部权威平台对接服务	CERT-E-RSA	1 套	50000	50000		/
4	电子签章系统（含服务器）	ESS4000-PDF-A8001	1 台	198000	198000		/
5	时间戳服务器	TSS-HG8001	1 台	95000	95000		/
6	鲲密一体机	TrustCM-Kunpeng2400	1 台	210000	210000		/
7	安全认证网关	NAG-A3001	2 台	147000	294000		/
8	签名验签服务器	DSVS-HG8001	1 台	130000	130000		/
9	协同签名系统（含服务器）	COSS-A8001	1 台	210000	210000		/
10	服务器密码机	HSM-A8001	1 台	79000	79000		/
合计（人民币）		（大写）壹佰玖拾肆万玖仟陆佰元整			¥1949600.00 元		

备注：1.本项目采用**竞争性磋商**方式招标，合同价为最终报价；2.合同总价包括货物及配套货物的设计、制造、包装、运输、保险、安装调试、验收、培训、技术服务（包括技术资料、工具、图纸等的提供）及保修期内保修服务与备品备件发生的所有含税费用。

二、交货期、地点及方式

2.1 交货期：甲乙双方签订合同后，乙方负责在 **45 日历天** 内完成项目所有设备的到货及安装调试和必要的技术培训等工作。

2.2 交货地点：甲方指定交货地点。

2.3 交货要求：

2.3.1 乙方发货前，应当先与甲方沟通，共同确认本次发送货物设备的参数、运送方式、

时间、双方对接人员安排等问题，经甲方确认后，乙方安排发货。

2.3.2 货物到达交货地点之前的货损风险由乙方承担，乙方应当为货物和派往甲方进行服务人员购买相应的意外险和人身险等有关保险，相关费用由乙方承担。

2.3.3 货物设备到达指定交货地点后，由甲乙双方确认的对接人对货品进行初验，初验时乙方除应交付货物设备，还应当同时交付所供货物经国家有关部门颁发的货物鉴定证书、使用许可证、用户手册、产品合格证、保修手册、有关图纸、技术资料及配件、随机工具等。甲方初验合格的，为乙方出具初验合格单，乙方开始对设备进行安装调试。

2.4 初验过程中，发现货物存在短缺、次品、损坏的情况的，或者乙方未能完整交付设备及 2.3.3 款规定的资料和工具的，乙方应及时安排补充、更换，直到初验合格，方可视为乙方完成交货；因此所需费用全部由乙方承担。导致逾期交付的，由乙方承担相关的违约责任。

2.5 在到货、初验至安装、调试、验收期间，乙方必须有技术人员到场，否则出现货物缺少或丢失，甲方不承担任何责任。

三、货物安装、调试、测试与验收

3.1 货物安装、调试均由乙方负责并承担相关费用，乙方在安装和调试的过程中同时对甲方进行设备安装的基本技术培训指导，甲方应在现场监督和学习。

3.2 乙方安装调试完成后，在 5 个工作日内由甲、乙双方共同进行测试和验收，甲方可根据实际需要，对设备进行多次测试，测试合格后在进行验收。测试和验收过程中发生的一切费用均由乙方承担。

3.3 测试及验收时，乙方交付的货物及相关资料、证书、配件、工具应同时满足国家法律法规和规范性文件对货物的质量要求、甲方招标文件对货物的质量、参数要求、乙方在投标文件中或其他对货物质量、参数、包装作出的书面承诺、声明或保证。

3.4 验收合格后甲乙双方签订验收报告书，验收报告书一式三份，甲方二份，乙方一份。有大型贵重仪器的，另行签订大型贵重仪器设备验收报告书。大型贵重仪器设备验收报告书，一式四份，甲方三份，乙方一份。

3.5 经验收，发现乙方货物不符合技术质量要求，致使不能实现合同目的且乙方又不能在合理期限内提出解决方案的，甲方可退货并解除合同。甲方解除合同的，乙方应当立即将所供货物设备撤出甲方场地，在此期间，货物设备的毁损、丢失的风险由乙方承担。

3.7 甲乙双方在验收结果有争议时，由甲方邀请其他具有检测资质的检测机构（下称第三方检测机构）进行检测，如果第三方检测机构检测后认定质量合格且符合招标文件和对方投标文件相关要求及承诺，则第三方检测所发生费用由甲方负担；如果第三方检测机构检测后认定争议货物质量不合格或达不到招投标文件承诺及要求，则第三方检测所发生费用由乙方负担，并且后续再次检测所有第三方检测的费用均由乙方负责，乙方承担因质量不合格对甲方造成的一切损失和承担一切后果，同时甲方有权终止合同。

3.8 乙方为执行本合同而提供的技术资料、软件的使用权归甲方所有。

3.9 乙方保证其提供的货物的全部及部分，均不存在任何侵犯第三方知识产权的情形。

否则，乙方应向甲方承担违约责任及赔偿由此给甲方造成的名誉及经济损失。

四、质量保证及售后技术服务

4.1 乙方保证货物来源合法、合规、全新且未使用过，所有权没有瑕疵的（即不存在资产抵押或其他可能影响货物所有权的事宜），其质量、规格及技术特征要符合国家法律法规和规范性文件对货物的质量要求及本合同及合同所附资料的要求。

4.2 乙方所提供的所有设备免费保修 叁 年（保修期内提供免费上门保修服务，提供终身维护）。有特殊要求的以厂家三包条件为准，由乙方提供或承诺延长保修期的由乙方提供免费保修。乙方承诺，保修期以外所有设备的维护和维修由乙方负责，乙方只收取材料费、人工成本费。

4.3 所有货物保修服务方式均为乙方上门保修，乙方收到甲方的维护和维修通知后，应在 4 小时内，派员到甲方货物使用现场维修，由此产生的一切费用均由乙方承担。

4.4 乙方应于验收后向使用方提供项目各项详细验收报告、技术文档的归纳、整理、提交，并提供完整的技术资料。

4.5 进口设备在办理货款支付前，需提供“海关进出口货物征免税证明”等相关报关手续证明，并且提供翻译后的中文说明书。

4.6 乙方为甲方免费提供操作及维护培训，主要内容为设备的基本结构、性能、主要部件的构造及原理，日常使用操作、保养与管理，常见故障的排除，紧急情况的处理等，培训地点主要在货物安装现场或按甲乙双方协商安排。

4.7 其他售后服务要求，均按照乙方投标文件中有关承诺执行。

五、付款方式

5.1 在项目安装、调试、培训等验收合格后 15 个工作日内支付合同总金额的 100%。由甲方项目负责部门凭中标通知书、合同、乙方开具的增值税专用发票、验收报告等凭证办理付款手续。乙方未向甲方开具符合甲方要求票据的，甲方有权拒绝向乙方付款。

5.2 本合同款项由财政部门国库集中支付以银行转账方式支付，合同与发票上乙方银行开户和账号等信息须完全一致，请乙方认真核对有关支付信息。

5.3 项目付款前，乙方应当向甲方提交合同金额 5%的质量保函，质量保函有效期自验收合格之日起 365 天（按日历日计），到期后质量保函自动失效。

六、索赔、违约金

6.1 乙方在参与本项目采购活动过程中如存在提供虚假承诺、证明、串通投标等违法违规行为，除承担相应的行政责任外，甲方有权解除合同，并要求乙方承担合同总金额 30% 的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

6.2 若乙方不能按期交付设备的，乙方应向甲方支付违约金。违约金为每延期壹周支付延误部分设备金额的 0.5%。延期不足壹周的按照壹周计算。支付违约金后，乙方仍对以上提及的合同产品和技术文档有继续交货的义务。乙方逾期 30 天不能交付的，按不能交付处理，乙方向甲方另行支付合同金额 10%的违约金，同时甲方有权解除合同。

6.3 乙方交付的货物不符合质量约定或乙方未履行相应的质量保证责任及售后服务义务或存在侵权行为的，甲方有权退货，并要求乙方支付合同总金额 30%的违约金，违约金不足以赔偿甲方损失的，甲方有权要求乙方赔偿经济损失。

6.4 若甲方无正当理由而拒收货物，甲方应向乙方偿付拒收设备款额 1 %的违约金。

6.5 如甲方未能按照合同如期付款，则应向乙方支付逾期违约金。违约金为每延期壹周支付延误部分金额的 0.5%的违约金。延期不足壹周按照壹周计算。支付违约金后，甲方仍必须继续按合同履行付款义务。

七、不可抗力

7.1 不可抗力是指不能预见、不能避免并不能克服的客观情况。

7.2 任何一方由于不可抗力而影响合同义务履行时，可根据不可抗力的影响程度和范围延迟或免除履行部分或全部合同义务。但是受不可抗力影响的一方应尽量减小不可抗力引起的延误或其他不利影响，并在不可抗力影响消除后，立即通知对方。任何一方不得因不可抗力造成的延迟而要求调整合同价格。

7.3 受到不可抗力影响的一方应在不可抗力事件发生后 2 周内（含本数），取得有关部门关于发生不可抗力事件的证明文件，并以书面形式提交另一方确认。否则，无权以不可抗力为由要求减轻或免除合同责任。

7.4 进口货物由于出口国限制出口导致不能供货、政策变化等原因导致本采购项目不能继续实施，不属于不可抗力范围。

八、争议的解决

8.1 合同履行过程中发生争议时，双方本着真诚合作的精神，通过友好协商解决。

8.2 若执行本合同的过程中发生纠纷，双方当事人应当及时协商解决；协商不成时，则提交甲方所在地人民法院提起诉讼。

8.3 在诉讼期间，合同中未涉及争议部分的条款仍须履行。

8.4 因一方违约导致本合同解除的，守约方为主张权益引发诉讼产生的诉讼费用（包括但不限于：律师费、诉讼费、保全费、鉴定费、翻译费等全部费用损失）由违约方承担。

九、合同构成及保存

9.1 本项目的招标磋商文件、投标响应文件、报价文件、中标通知书、补充协议、会议纪要、甲乙双方商定的其他文件等均为本合同不可分割之部分。解释的顺序除特别说明外，以文件生成时间在后的为准。

9.2 本合同所列货物的技术规格、技术要求及其他有关货物的特定信息由合同附件说明。

9.3 本合同正本一式陆份，甲方肆份，乙方贰份。合同自双方法人代表或授权代表或项目负责人签字并加盖合同专用章或公章之日起生效。本合同签订的甲乙双方地址是甲乙双方认可的有效通讯地址，如有争议引发诉讼，该地址将作为法院文书送达地址。

十、其他

10.1 除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下义务。合同

履行期间，发生特殊情况时，任何一方需变更本合同的，要求变更一方应及时书面通知对方，征得对方同意后，双方签订书面变更协议，该协议将成为合同不可分割的部分。未经双方签署书面文件，任何一方无权变更本合同，否则，由此造成对方的经济损失，由责任方承担。

10.2 货物的技术规格、性能指标、培训计划及售后服务方案等以招投标文件为依据。本合同中未尽事宜，由双方协商处理或另行签定补充协议，补充协议与本合同为不可分割的组成部分。

10.3 本合同附件：货物技术参数表。

甲方：黄河水利职业技术学院（盖章）	**乙方：北京数字认证股份有限公司**（盖章）
开户银行：农行开封市东京支行	开户银行：北京银行双清苑支行
开户帐号：16-106501040000945	开户帐号：01090327800120102315712
统一社会信用代码：12410000416305577XM	统一社会信用代码：91110108722619411A
单位地址：开封市东京大道西段 1 号	单位地址：北京市海淀区北四环西路 68 号 1501 号
法定代表人或委托代理人：申浩	法定代表人：[illegible]
项目负责人：[illegible]	委托代理人：[illegible]
项目联系人：侯栢成	供货联系人：陈盟盟
联系人电话：13103787009	联系电话：15838102250
日　　期：2024 年 8 月 26 日	日　　期：2024 年 8 月 26 日

附件　设备技术参数表

序号	设备名称	规格、技术参数及功能描述
1	教育数字证书认证系统	1.提供数字证书生命周期管理服务，实现基于 Web 的证书申请、审核、提交签发请求、用户管理、系统管理等功能。能够支持传统的硬件介质证书和新型的移动数字证书发放。系统的设计及建设符合国家密码管理局、工业和信息化部等国家有关标准规范要求。证书符合 ITU X.509 V3 标准及具有标准扩展域的证书。 2.支持最大用户数量 100 万用户；RSA2048 双证书签发速度 500 张/秒；SM2 单证书签发速度 3000 张/秒； SM2 双证书签发速度 800 张/秒；最大并发用户数 100 用户； 3.支持 SM2、RSA 算法，其中 RSA 算法支持 2048、4096 位。支持双证书（加密证书和签名证书）和双中心（证书管理中心和密钥管理中心）结构。 4.支持 SPKM 安全通讯协议。 5.支持证书策略管理，对密钥用法、扩展密钥用法、有效期、生效时间进行配置管理；支持多种内置证书模板，可签发普通用户单双证书、机构证书、设备证书、VPN 证书、代码签名证书、微软域证书；具有自定义数字证书扩展项。 6.证书模板支持动态字段和固定值配置，支持主题 DN 强制校验和主题 DN 不校验等多种验证模式。 7.支持多种证书存储格式和导出功能，包括 PEM、DER、Base64 和 PKCS#12 格式。 8.支持黑名单（CRL）的生成、发布，支持 CRL 策略管理；CRL 发布支持分片 CRL，全量和增量 CRL 多种模式。支持基于 HTTP/HTTPS 协议、LDAP 协议的 CRL 发布点。 9.具备安全审计功能：支持各个功能模块的运行事件记录、系统重要策略、权限变更，证书操作记录，

序号	设备名称	规格、技术参数及功能描述
		并有相应的审计机制，日志支持签名验证。支持证书查询和汇总统计报表生成。审计记录支持防篡改。 10.证书对中文和特殊符号有良好的支持，证书主题 DN 项支持逗号，加号，双引号，百分号，括号等功能。 11.支持证书签发有效期灵活配置，包括以申请时间、审核时间、下载时间三种模式配置。 12.系统提供证书申请、作废、更新、查询和下载等功能，支持用户身份审核，支持多级授权。支持证书批量申请、批量制证。支持人员批量注册，提供文件导入方式。支持手动和自动证书审核方式。 13.支持划分多个层次的管理域，包括机构域和权限域，每个域管理该区域内的证书用户，每个域可以设置相应的管理员。 14.证书注册审核中心系统操作员可以查看指定用户的证书信息，包括证书的当前状态、有效期、颁发者等。 15.系统具备独立的审计模块，可以对操作日志进行审计，签名验证。支持对证书发放数量，证书状态统计功能。 16.证书签发可验证介质序列号是否在授权之内，只有已授权的介质允许签发证书。 17.提供证书生命周期接入服务，包括 Restful API 和 SDK。SDK 支持多种语言，包括 Java、C、c#、python 语言。 18.支持按照国密标准规范与部级教育数字认证系统（CA）对接。 19.提供移动端数字证书发放服务，包括：移动端数字证书申请信息提交、接收 CA 签发的数字证书、下发数字证书等。 20.提供在线证书服务模块，支持证书用户在线自助完成更新、解锁、变更等操作服务。 21.数字证书认证系统具备国家密码管理局颁发的《商用密码产品认证证书》。 22.数字证书认证系统具备公安部颁发的《网络安全专用产品安全检测证书》。 23.至少支持麒麟、统信、中科方德操作系统，飞腾、龙芯、鲲鹏、海光 CPU，人大金仓、南大通用、达梦数据库，东方通、金蝶、宝兰德、中创中间件，以上每类至少提供一家兼容性证明报告，并加盖投标人公章。 24.数字证书认证系统具备国家网络与信息系统安全产品质量监督检验中心出具的《信息技术产品安全测试证书》，确保产品不存在漏洞库中已知的中、高风险漏洞。 25.数字认证子系统中的密钥管理系统具备飞腾、龙芯、鲲鹏、海光等国产 CPU 的兼容性测试证明。
2	教育密码综合服务子系统	1.具备 API 管理能力：支持 API 分组管理：添加 API 分组、修改 API 分组、查询 API 分组、添加分组的管理员和 API 负责人。支持 API 版本管理：在分组中添加不同版本的 API、修改 API、删除 API、查询 API 列表、通过 API ID 查询一个 API。 2.具备白名单管理：提供 API 访问白名单管理：支持单 API 访问授权，支持 API 分组配置白名单。 3.API 接入安全防护支持 Appkey 认证、HMAC 认证、数字签名认证，支持请求防重放。 4.支持可视化 API 实时监控，包括：调用量、调用方式、响应时间、错误率，并支持历史情况查询。 5.支持可自定义配置的预警方式（短信、Email 等），订阅预警信息，以便实时掌握 API 运行情况。 6.提供密钥全生命周期包括密钥生成、派发、导入、导出、备份、恢复、查询等。支持 SM2，SM3,SM4 等算法。 7.支持应用通过 API 接口或者租户通过开放平台来创建用户主密钥，主密钥可以用来加密保护数据密钥，也可以直接加解密数据；支持应用主密钥的启用、禁用和删除等管理功能。 8.支持 CA 数字证书有效性验证，支持同时配置多条证书链，验证不同 CA 系统签发的数字证书，兼容第三方 CA 和自建 CA 签发的数字证书，包括不限于 SSL 证书、SM2 签名证书、RSA 签名证书。 9.支持数字签名、签名验签、数字信封、数据加密、时间戳等功能。 10.支持密码设备作为密码资源，以池化方式进行统一调度管理，为应用系统提供密码服务。支持密码设备资源池的创建、启用、停用等，支持向密码设备资源池中动态增减设备，该过程不会中断已有应用。 11.能够根据密码资源的使用情况动态调整密码资源池中的虚拟密码机数量，合理利用资源。 12.提供硬件服务器 CPU、内存、磁盘、网络等监控项，满足服务器的基本监控运维需求。监控项提供报警功能，可以直接在硬件监控图表中使用报警功能，也可以将服务器添加到应用分组后，在分组中使用报警功能。 13.支持对不同厂商物理密码设备统一管理：支持不同厂商密码设备统一注册、统一管理；包括物理密码设备 IP 登记管理、端口管理、设备类型管理、设备型号管理、设备厂商管理等。 14.在密码设备支持 SNMP 协议的情况下，能够对池中设备负载情况（CPU、内存、硬盘占用率）进行监控，使得管理人员能够及时发现资源使用情况，按需调整池中资源数量。 15.支持对密码服务平台的统一运维监管，包括对应用接入情况、服务器使用情况、日志服务器运行情况、应用系统对密码设备的密码应用请求情况、密码设备 CPU、内存、磁盘使用情况、异常告警情况的全面监控，提供监控情况大屏展示。 16.密码服务管理平台具备统一密码接入管理功能、物理密码设备管理功能、密码设备资源池管理功能、应用管理功能、日志管理功能，提供国家认可专业机构出具的功能检验检测报告

序号	设备名称	规格、技术参数及功能描述
		17.密码服务管理平台具备国家密码管理局颁发的《商用密码产品认证证书》，且满足密码模块安全等级第二级相关要求。 18.产品支持密钥存储机制、密钥调用鉴别流程满足系统功能需求；能实现密钥协商机制和密钥隔离机制，保护密钥安全；采取了相应的安全保护机制，满足等保三级要求，具有数据存储、链路安全、运维管理、系统安全保障等技术能力。提供国家认可专业机构的测评证书。
3	教育部权威平台对接服务	1.支持电子凭证系统与教育部权威机构的验证平台对接。对接后，我校签发的可信电子成绩单可在教育部权威机构在线“电子成绩单验证平台”上进行快速验证。 2.与教育部权威机构的验证平台对接，对接时间 1-2 天。 3.包含单位数字证书（国密算法），采用 SM2 国产算法签发；单位数字证书（国际算法 Adobe 认证），采用 RSA 国产算法签发；时间戳数字证书（国密算法），采用 SM2 国产算法签发；时间戳数字证书（国际算法 Adobe 认证），采用 RSA 国产算法签发。以上四种数字证书用于标识凭证签发单位相关业务处室的网上真实身份，证书格式须遵循 x．509v3 标准，数字证书有效期 3 年。
4	电子签章系统（含服务器）	1.支持灵活的签章定位方式，支持关键字定位签章，支持对 PDF 文档中的单个或全部关键字进行签章，支持指定在第几个关键字进行签章；支持坐标定位签章，支持对 PDF 文档中指定的页码和坐标位置进行签章；支持表单域定位签章，支持对 PDF 文档中的某个表单域位置进行签章。 2.支持 PDF 文档生成服务，支持将业务系统提交的 XML 等格式的业务数据与 PDF 模板合并，生成 PDF 文档；支持将多个图片合并生成 PDF 文档；支持将 word 文档转换成 PDF 文档。 3.支持 PDF 空签名域生成，可以对签名域规则进行配置，包括在 PDF 中生成空签名域的所在位置、区域大小、覆盖类型、签名状态，以及多个签名域之间的相对位置等。 4.支持印章透明化，能够满足签章后的 PDF 文件内容不会被公章红色字体掩盖，同时保证印章外观不失真； 5.多页批量签章：支持在多页的 PDF 文档中每页的相同位置加盖相同的印章，签章的位置支持坐标方式定位，每页的签章都有电子签名。针对 1000 页文档的 PDF 进行多页签章每页签名，签章效率小于 3 秒。 6.支持骑缝章签章，可配置骑缝章模式，如页面右侧加盖骑缝章或左侧加盖骑缝章，并支持文档保护限制，控制文档是否可打印或复印。 7.支持条形码生成管理，支持条形码的类型包括但不限于 QR 码、PDF417 码、CODE128 码或 CODE39 码等，可自动生成条形码编号。 8.可根据用户需求灵活扩展配置“PDF 模板管理与应用模块”，支持 PDF 文档生成与模板管理，实现用 Office 编辑的 docx 文档和 xslt 文档作为 PDF 模板进行 PDF 文档的生成。 9.支持应用环境：Windows server；Linux；AIX；Solaris；Unix 等；提供 C、Java 等主流开发 API； 10.支持 OFD 文档签章，可根据用户需求灵活扩展配置“OFD 批量签章模块”，实现 OFD 格式文档服务端批量签名和签章功能，符合国标 GB/T38540-2020、GM/T0031-2014 标准规范。 11.可根据用户需求灵活扩展配置“大文档签章加速模块”，用于提供 20M 以上文件大小 PDF 格式文档的签章的加速功能，支持坐标和关键字及多规则组合方式签章，支持普通签章和多页签章。 12.管理运维功能：系统管理：支持对组织机构、角色、管理员进行管理，对系统配置的维护和管理。用户管理：支持根据不同的组织机构、部门来配置用户信息。印模管理：支持印章图片管理功能，印模文件类型支持 PNG、GIF 格式，提供印章图片导入和自动生成印章图片功能。印章管理：支持对印模印章制作、停用、启用、删除等功能的管理。权限控制：对电子印章的使用进行控制，提供在线获取印章、印章权限管理功能，支持印章授权给用户、部门使用，非授权用户无法使用印章，确保电子印章使用的全程可控。 13.签章处理能力在千兆网络环境下，签发 200K PDF 文件效率≥200 次/秒。 14.具备国家密码局颁发的《商用密码产品认证证书》。 15.为了确保产品支持国产化环境，需提供该产品客户端软件/程序与统信桌面系统或其他国产桌面系统的基于龙芯、兆芯、海光等 CPU 平台的兼容性互认证明，提供兼容性互认证明文件。 16.为了确保产品支持国产 OFD 签章环境，需提供该产品与不少于 3 家 OFD 阅读器厂商的兼容性适配证明（如数科、福昕、点聚、永中等），提供兼容性适配证明文件。 17.产品具备国家网络与信息系统安全产品质量监督检验中心出具的《信息技术产品安全测试证书》，确保产品不存在漏洞库中已知的中、高风险漏洞。
5	时间戳服务器	1.支持管理员配置功能，管理员配置支持基于数字证书的方式配置“超级管理员模式”和“三权分立模式”。 2.支持多种格式动态密钥时间戳的签发及验证功能。 3.支持多种时间戳服务接口，满足各类应用开发平台调用。 4.支持可信时间发布功能，支持时间同步机制。 5.支持应用平台：Windows server; Linux；AIX；Solaris；Unix。 6.支持应用接口：Java、C、COM。 7.支持算法标准：SM2、SM3。

序号	设备名称	规格、技术参数及功能描述
		8.内置权威时间源模块，符合国家授时中心的时间精度标准，并且经国家授时中心的权威鉴定测试，网络时间同步精度优于 10ms。（提供国家授时中心检测证书证明材料） 9.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，支持通过密钥对备份数据进行加密，支持通过口令解密实现备份数据恢复。 10.提供时间源管理：支持 GPS 或北斗或 4G 授时方式。 11.时间戳生成速率 4000 次/秒，验证速率 8000 次/秒。 12.电源指标：双电源。 13.产品具备 IPv6 Ready Logo 认证证书。 14.产品具备国家网络与信息系统安全产品质量监督检验中心出具的《信息技术产品安全测试证书》，确保产品不存在漏洞库中已知的中、高风险漏洞。 15.产品具备国家密码管理局颁发的《商用密码产品认证证书》且满足密码模块安全等级第二级相关要求。 16.产品具备麒麟软件等支持国产化的 NeoCertify 认证的认证证书。
6	鲲密一体机	1.产品内置可信执行环境密码系统必须为混合软件密码模块，采用 TEE 技术架构开发，并具备商用密码产品认证证书（二级）资质。 2.可信执行环境密码系统需支持集群化部署，支持统一管理，支持统一密钥分发。 3.可信执行环境密码系统支持与业务系统部署在同一台配置有鲲鹏 920 CPU 的服务器中，为业务系统直接提供内生的密码服务。 4.可信执行环境密码系统提供符合 GM/T0018《密码设备应用接口规范》、Java Cryptography Extension、SSL 加速等多规范的 SDK，同时还可提供 C/C++、Java、Go 等多种语言形式的集成开发库。 5.SM2 签名性能不低于 40000 次/秒，SM2 验签性能不低于 17000 次/秒，SM4 算法加/解密性能不低于 41Gbps，SM3 杂凑算法性能不低于 1Gbps，支持通过 POC 测试进行验证。 6.支持容器化部署，能够实现各容器间密钥的安全隔离、运行环境安全隔离。 7.支持自动到管理端注册、自动初始化。 8.支持扩展服务配置，包括 SSL 卸载服务、签名验签服务，支持通过 POC 测试进行验证。SSL 卸载服务包含基于 SSL/TLS 构建安全通道功能；支持 SSL 卸载；签名验签服务包含基于数字证书的身份认证功能、数据签名与签名验证功能、加解密服务和数字信封功能。
7	安全认证网关	1.支持多种认证方法，包括 UKEY 证书、协同签名、动态口令等。 2.支持基于数字证书的服务器端与客户端的双向认证，多种形式的证书透传功能可以非常方便地在应用层实现基于数字证书的安全认证。 3.支持 SSL 加速、SSL 卸载、HTTP 压缩、Web 高速缓存功能、HTTP 请求和响应改写、HTTP 内容改写、HTTP 反向代理转发和 HTTP 重定向。 4.支持国产密码算法：SM2、SM3、SM4 等；支持 ECC-SM4-SM3、ECDHE-SM4-SM3 密钥套件。 5.支持 IPsec 协议，需支持国密 AH 和 ESP 模式下 IKE 协议。 6.支持证书作废状态的 CRL 验证；支持 OCSP 在线验证证书作废状态。 7.支持 Windows、Linux、IOS 和 Android 等安全终端接入。 8.不依赖客户端，支持 HTML、JavaScript 和插件参数。 9.支持视图查看 SSL 加速状态、CPU 使用率、内存使用率、并发连接数、新建连接数等。 10.性能：SSL 最大并发连接数（个）200,000，SSL 每秒新建连接（个/秒）7000，SSL 加解密吞吐率 500Mbps。 11.具备国家密码局颁发的《商用密码产品认证证书》，且满足密码模块安全等级第二级相关要求。 12.产品具备公安部颁发的《网络安全专用产品安全检测证书》。 13.产品支持 IPV6，具备全球 IPV6 测试中心的《IPV6 Ready Logo 认证》证书。 14.产品具备麒麟软件等支持国产化的 NeoCertify 认证的认证证书。
8	签名验签服务器	1.支持管理员配置功能，管理员配置支持基于数字证书的方式配置“超级管理员模式”和“三权分立模式”。 2.支持一键检测功能，包括服务接口检测和加密卡检测，保证设备处于正常工作状态。 3.具备完善的身份鉴别机制，支持基于数字证书的身份认证，同时管理员通过管理界面可进行证书管理、应用管理、系统管理以及日志管理等管理操作。 4.支持 PKCS1/ PKCS7 attach/PKCS7 detach/XML Sign 等多种格式的数字签名和验证，同时支持大文件数字签名和验证。 5.支持多证书链配置，验证不同 CA 的用户证书，支持 CRL/OCSP 等多种方式的证书有效性验证。 6.支持国密 SM1、SM2、SM3、SM4 算法。 7.支持数字信封和带签名的数字信封功能。 8.支持备份恢复功能，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。 9.支持双机、负载均衡。 10.提供 C、COM、Java 等主流开发 API。

序号	设备名称	规格、技术参数及功能描述
		11.SM2 签名速率 10000 次/秒，验签速率 4000 次/秒。 12.电源指标：双电源。 13.产品具备 IPv6 Ready Logo 认证证书。 14.产品具备公安部计算机信息系统安全产品质量监督检验中心出具的检测报告，确保产品符合《信息安全技术 签名验签服务器技术规范 GB/T 38629-2020》和《信息安全技术 通用渗透测试检测条件 JCTJ 005-2016》（6.2.1、6.2.2）相关要求。 15.产品具备国家密码管理局颁发的《商用密码产品认证证书》且满足密码模块安全等级第二级相关要求。 16.产品具备麒麟软件等支持国产化的 NeoCertify 认证的认证证书。
9	协同签名系统（含服务器）	1.支持可视化的用户管理、证书管理，实现数字证书得申请、更新、吊销等。 2.支持对接入应用的授权管理。 3.提供 restful API 的形式接口与业务系统对接，产品提供对业务系统请求报文的真实性完整性校验。 4.产品支持基于数字证书的安全认证登录管理功能，能实现多种角色管理，包括但不限于管理员、操作员、审计员等。 5.支持基于服务端的签名任务发起和签名结果获取；基于协同密钥技术来实现移动端用户私钥的生成和使用。 6.支持在统一页面实现对用户的集中管理，包括用户导入、用户新增、用户照片和签章图片导入、单个冻结和批量冻结、单个删除和批量删除、批量导出、签章样式自定义编辑等功能。 7.支持在线、离线证书签发模式、日志及审计功能；支持用户量、签名量、证数量的统计分析。 8.支持管理员一键授权管理：能够在单一页面实现自由勾选功能模块对管理员进行权限分配，包括对用户管理功能的授权、对证书验证管理的授权、CSS 高级配置的授权、系统设置的授权、日志的授权、配置管理的授权等。 9.支持一人多设备、一设备多人的应用场景；支持授权签名：用户只需要使用手机在 PC 端完成一次授权即可多次签名，并可以关闭授权；支持推送签名：用户以推送的方式发起签名，签名者在手机端收到推送后直接完成签名；支持在签名任务中添加签名描述信息。 10.支持通过系统唯一用户标识绑定用户身份；支持通过接口添加用户信息，支持 CRL 配置和根证书配置，支持标准签名验证，能够与 USBKey 签名互通，支持证书有效性验证。 11.性能指标：SM2 签名能力 350TPS。 12.支持算法标准：SM1、SM2、SM3、SM4。 13.产品具备国家密码管理局颁发的《商用密码产品认证证书》且满足密码模块安全等级第二级相关要求。 14.具备全球 IPV6 测试中心的《IPV6 Ready Logo 认证》。 15.产品具备麒麟软件等支持国产化的 NeoCertify 认证的认证证书。
10	服务器密码机	1.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。采用由国家密码管理局批准使用的双物理噪声源。 2.支持 SM4 算法的 ECB、CBC、OFB、CFB、CTR 等模式的数据加密和解密运算；支持基于 SM4 算法的保留格式加解密。 3.消息鉴别码产生和验证：支持基于 SM4 算法的 MAC 产生及验证。 4.数据签名/验证：支持 SM2 算法的私钥签名，使用对应的公钥签名验证。 5.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。 6.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。 7.支持国产密码算法：SM2、SM3、SM4 等。 8.支持审计日志的记录，查询和导出功能；支持多方协同签名、多方协同解密功能；支持密钥分散功能。 9.双机热备：对外可提供高稳定、高性能的服务，支持热备负载功能，支持多 机并行，提供容错功能，当有密码机出现故障时不影响业务运算。 10.性能指标，SM2 算法密钥对产生（对/秒）≥5000；SM2 签名/验签（次/秒）≥8000/4000；SM2 算法加/解密≥80Mbps/80Mbps；SM4 算法加/解密≥400Mbps/400Mbps；SM3 运算≥400Mbps/400Mbps。 11.产品具备国家密码管理局颁发的《商用密码产品认证证书》且满足密码模块安全等级第二级相关要求。 12.产品须具备《计算机信息系统安全专用产品销售许可证》。 13.产品支持 IPV6，具备 IPV6 测试中心的《IPV6 Ready Logo 认证》证书或国内 IPV6 认证证书。