HHYY2026-02-001

“广西政府采购云平台”合同编号：12N4993381142026402

政 府 采 购

商用密码应用安全性评估与整改合同

项目编号：YLZC2025-J1-990518-GXRZ

计划编号：YLZC2025-J1-11771

采购人（甲方）：玉林市红十字会医院

成交供应商（乙方）：确信信息股份有限公司

签订日期：2026 年 2 月 2 日

目录

一、采购合同

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》等法律、法规规定，按照招标文件规定条款和中标供应商投标文件及其承诺，甲乙双方签订本合同。

第一条　合同标的

1.供货一览表

序号	产品名称	商标品牌	型号参数	生产厂家	数量	单位	单价（元）	金额（元）
1	VPN综合网关（综合安全网关）	确信信息	CGW V2.0 综合安全网关	确信信息股份有限公司	2	台	66000.00	132000.00
2	国密浏览器	海泰方圆	SHM1602-G V5.0	北京海泰方圆科技股份有限公司	100	套	130.00	13000.00
3	密码机服务器	确信信息	HSM V2.0 服务器密码机	确信信息股份有限公司	2	台	66000.00	132000.00
4	国密堡垒机（安全运维服务器）	确信信息	SOP V2.0 密码机服务器	确信信息股份有限公司	1	台	66000.00	66000.00
5	密码服务平台	确信信息	CSSP 2000 V1.0 密码服务平台	确信信息股份有限公司	1	套	128000.00	128000.00
6	签名验签服务器	确信信息	DSVS V2.0 签名验签服务器	确信信息股份有限公司	2	套	66000.00	132000.00
7	电子签章系统	确信信息	ESS V2.0 电子签章系统	确信信息股份有限公司	1	台	108000.00	108000.00
8	数字证书管理系统	确信信息	CAV2.0 数字证书管理系统	确信信息股份有限公司	1	台	108000.00	108000.00

9	手机盾协同签名系统	确信信息	SCM 1000 V1.0 手机盾协同签名系统	确信信息股份有限公司	1	台	166000.00	166000.00
10	时间戳服务器	确信信息	TSA V2.0 时间戳服务器	确信信息股份有限公司	1	套	66000.00	66000.00
11	SDK 接口（商用密码应用业务流程和开发流程设计服务）	\	SDK 接口服务	\	1	项	50000.00	50000.00
12	系统调用接口服务（系统密码应用开发改造服务）	\	接口服务	\	1	项	210000.00	210000.00
13	CA 证书（个人数字证书）	西部 CA	CA 数字证书	西部安全认证中心有限责任公司	1200	张	70.00	84000.00
14	国产门禁系统（国密电子门禁系统）	天津光电	STC-1 国密电子门禁系统	天津光电安辰信息技术股份有限公司	1	套	65000.00	65000.00
15	国产监控系统（国密视频监控系统）	天津光电	SJT1708 V1.0 国密视频监控系统	天津光电安辰信息技术股份有限公司	1	套	65000.00	65000.00
16	商用密码应用安全性评估服务	\	商用密码应用安全性评估服务	长沙云创信安科技有限公司	1	次	75000.00	75000.00
17	商用密码应用咨询服务（密码应用方案评测）	\	商用密码应用咨询服务	长沙云创信安科技有限公司	1	次	30000.00	30000.00

人民币合计金额（大写）人民币壹佰陆拾叁万元整　（小写）（¥1630000.00）
备注：1、合同合计金额包括货物价款、检验、技术培训及技术资料、运输、售后服务等全部费用 2、可另附清单。

2. 合同合计金额包括货物价款，备件、专用工具、安装、厂家授权、调试、校准、检验、技术培训及技术资料和包装、运输、质保期内年检等全部费用。如招投标文件对其另有规定的，从其规定。

第二条　质量保证

1. 乙方所提供的货物型号、技术规格、技术参数等质量必须与招投标文件和承诺相一致。乙方提供的节能和环保产品必须是列入政府采购清单的产品。

2. 乙方所提供的货物必须是全新、未使用的原装产品，且在正常安装、使用和保养条件下，其使用寿命期内各项指标均达到质量要求。

第三条　权利保证

乙方应保证所提供货物在使用时不会侵犯任何第三方的专利权、商标权、工业设计权或其他权利。

乙方应按招标文件规定的时间向甲方提供使用货物的有关技术资料。

没有甲方事先书面同意，乙方不得将由甲方提供的有关合同或任何合同条文、规格、计划、图纸、样品或资料提供给与履行本合同无关的任何其他人。即使向履行本合同有关的人员提供，也应注意保密并限于履行合同的必需范围。

乙方保证所交付的货物的所有权完全属于乙方且无任何抵押、质押、查封等产权瑕疵。

第四条　包装和运输

1. 乙方提供的货物均应按招投标文件要求的包装材料、包装标准、包装方式进行包装，每一包装单元内应附详细的装箱单和质量合格证。

2. 货物的运输方式：　乙方自定　。

3. 乙方负责货物运输，货物运输合理损耗及计算方法：　由乙方负责　。

第五条　交付和验收

1. 交付使用时间：自合同签订之日起 15 日历天内完成供货验收并交付使用、地点：　甲方指定地点。

2. 乙方提供不符合招投标文件和本合同规定的货物，甲方有权拒绝接收。

3. 乙方应将所提供货物的装箱清单、用户手册、原厂保修卡、随机资料、工具和备品、备件等交付给甲方，如有缺失应及时补齐，否则视为逾期交货。

4. 甲方应当在到货并安装、调试完后七个工作日内进行验收，逾期不验收的，乙方可视同验收合格。验收合格后由甲乙双方签署货物验收单并加盖采购单位公章，甲乙双方各执一份。

5. 甲方对验收有异议的，在验收后五个工作日内以书面形式向乙方提出，乙方应自收到甲方书面异议后 3 日内及时予以解决。

第六条　安装和培训

1. 甲方应提供必要安装条件（如场地、电源、水源等）。

2. 乙方负责甲方有关人员的培训。培训时间、地点：由甲方决定　　。

第七条　售后服务、保修期

1. 乙方应按照国家有关法律法规和“三包”规定以及招投标文件和本合同所附的《服务承诺》，为甲方提供售后服务。

2. 货物保修期：1年　。

3. 乙方提供的服务承诺和售后服务及保修期责任等其它具体约定事项。（见合同附件）

第八条　付款方式和保证金

1. 当采购数量与实际使用数量不一致时，乙方应根据实际使用量供货，合同的最终结算金额按实际使用量乘以成交单价进行计算。

2. 资金性质：财政性资金。

3. 付款方式：**签订合同后十五个工作日内，支付合同总额的 30%作为预付款，项目实施完成并整体验收合格后，60 天内支付合同总额的 67%，剩余 3%系统正常运行一年后支付。**（付款前供应商必须提供真实、有效、合法的正式发票，如提供假发票的，供应商除须向采购人重开合法发票外，还须按发票票面金额一倍的赔偿违约金给采购人，与此相关的行政处罚、刑事责任亦由供应商承担）。

第九条 履约保证金

本项目无履约保证金　。

第十条 税费

本合同执行中相关的一切税费均由乙方负担。

【注：除进口减免税产品外，乙方应提供货款全额的发票（如乙方供应产品为实验设备、装置和器械的，必须开具增值税专用发票）】

第十一条 质量保证及售后服务

1. 乙方应按招标文件规定的货物性能、技术要求、质量标准向甲方提供未经使用的全新产品。乙方提供货物的质量保证期按交货验收合格之日起计（期限见《招标项目采购需求》中各分标的要求）。在保证期内因货物本身的质量问题发生故障，乙方应负责免费修理和更换零部件。对达不到技术要求者，根据实际情况，经双方协商，可按以下办法处理：

⑴更换：由乙方承担所发生的全部费用。

⑵贬值处理：由甲乙双方合议定价。

⑶退货处理：乙方应退还甲方支付的合同款，同时应承担该货物的直接费用（运输、保险、检验、货款利息及银行手续费等）。

2. 如在使用过程中发生质量问题，乙方在接到甲方通知后在 24 小时内到达甲方现场。

3. 在质保期内，乙方应对货物出现的质量及安全问题负责处理解决并承担一切费用。

4. 上述的货物因人为因素出现的故障不在免费保修范围内。超过保修期的机器设备，终生维修，维修时只收部件成本费。

第十二条 调试和验收和年检

1. 甲方对乙方提交的货物依据招标文件上的技术规格要求和国家有关质量标准进行现场初步验收，外观、说明书符合招标文件技术要求的，给予签收，初步验收不合格的不予签收。货到后，甲方应当在到货并安装、调试完后七个工作日内进行验收。

2. 乙方交货前应对产品作出全面检查和对验收文件进行整理，并列出清单，作为甲方收货验收和使用的技术条件依据，检验的结果应随货物交甲方。

3. 甲方对乙方提供的货物在使用前进行调试时，乙方需负责安装并培训甲方的使用操作人员，并协助甲方一起调试，直到符合技术要求，甲方才做最终验

收。

4. 对技术复杂的货物，甲方应请国家认可的专业检测机构参与初步验收及最终验收，并由其出具质量检测报告，检测相关费用由乙 方承担。

5. 验收时乙方必须在现场，验收完毕后作出验收结果报告；验收费用由乙方负责。

6. 质保期内年检费用由乙方负责。

第十三条 货物包装、发运及运输

1. 乙方应在货物发运前对其进行满足运输距离、防潮、防震、防锈和防破损装卸等要求包装，以保证货物安全运达甲方指定地点。

2. 使用说明书、质量检验证明书、随配附件和工具以及清单一并附于货物内。

3. 乙方在货物发运手续办理完毕后二十四小时内或货到甲方四十八小时前通知甲方，以准备接货。

4. 货物在交付甲方前发生的风险均由乙方负责。

5. 货物在规定的交付期限内由乙方送达甲方指定的地点并初步验收合格后视为交付，乙方同时需通知甲方货物已送达。

第十四条 违约责任

1. 乙方所提供的货物规格、技术标准、材料等质量不合格的，应及时更换，更换不及时的按逾期交货处罚；因质量问题甲方不同意接收的或特殊情况甲方同意接收的，乙方应向甲方支付违约货款额 5%违约金并赔偿甲方经济损失。

2. 乙方提供的货物如侵犯了第三方合法权益而引发的任何纠纷或诉讼，均由乙方负责交涉并承担全部责任。

3. 因包装、运输引起的货物损坏，按质量不合格处罚。

4. 甲方无故延期接收货物、乙方逾期交货的，每天向对方偿付违约货款额 3‰ 违约金，但违约金累计不得超过违约货款额 5% ，超过 30 天对方有权解除合同，违约方承担因此给对方造成经济损失，若为甲方解除合同的，乙方应在合

同解除之日起五日内全额无息退还甲方已付款项；若为乙方解除合同的，乙方有权收回已交付的货物，运费由甲方承担，应在合同解除之日起五日内全额无息退还甲方已付款项；甲方延期付货款的，每天向乙方偿付延期货款额 0.1‰违约金，但违约金累计不得超过延期货款额 5%”。

5. 乙方未按本合同和投标文件中规定的服务承诺提供售后服务的，乙方应按本合同合计金额 5%向甲方支付违约金。

6. 乙方提供的货物在质量保证期内，因设计、工艺或材料的缺陷和其它质量原因造成的问题，由乙方负责。

7. 其它违约行为按违约货款额 5%收取违约金并赔偿经济损失。

第十五条 不可抗力事件处理

1. 在合同有效期内，任何一方因不可抗力事件导致不能履行合同，则合同履行期可延长，其延长期与不可抗力影响期相同。

2. 不可抗力事件发生后，应立即通知对方，并寄送有关权威机构出具的证明。

3. 不可抗力事件延续一百二十天以上，双方应通过友好协商，确定是否继续履行合同。

第十六条 合同争议解决

1. 因货物质量问题发生争议的，应邀请国家认可的质量检测机构按照国家标准对货物质量进行验收。货物符合国家标准的，鉴定费由甲方承担；货物不符合国家标准的，鉴定费由乙方承担。

2. 因履行本合同引起的或与本合同有关的争议，甲乙双方应首先通过友好协商解决，如果协商不能解决，可向甲方所在地人民法院提起诉讼。

3. 诉讼期间，本合同继续履行。

第十七条 合同生效及其它

1. 合同经双方法定代表人或授权代表签字并加盖单位公章后生效。

2. 合同执行中涉及采购资金和采购内容修改或补充的，须经财政部门审批，并签书面补充协议报财政部门备案，方可作为主合同不可分割的一部分。

3. 本合同未尽事宜，遵照《中华人民共和国民法典》有关条文执行。

4. 双方确认本合同落款通讯地址作为文书送达地址，该通讯地址适用于包括

双方合同履行过程中的各类通知、协议等文件以及就合同发生争议进入民事诉讼程序后的一审、二审、再审和执行程序等阶段法律文书的送达。通讯地址需要变更时应当提前 15 个工作日书面通知对方。因提供或者确认的通讯地址不准确、通讯地址变更后未及时依程序告知对方或受送达方拒绝签收等原因，导致文书未能被实际接收的，邮寄送达的，以文书退回之日视为送达之日。

第十八条　合同的变更、终止与转让

1. 除《中华人民共和国政府采购法》第五十条规定的情形外，本合同一经签订，甲乙双方不得擅自变更、中止或终止。

2. 未经甲方书面同意，乙方不得擅自转让（无进口资格的供应商委托进口货物除外）其应履行的合同义务。

第十九条　签订本合同依据

（1）成交通知书；

（2）项目采购需求；

（3）采购文件的澄清和修改（如有）；

（4）竞标报价表（最终）；

（2）商务、技术偏离表；

（6）成交供应商澄清函（如有）；

（7）其他与本合同相关的资料。

第二十条　其他

1、本合同未尽事宜，可经双方协商签订书面补充协议，补充协议的内容与本合同的内容不一致的，以补充协议的内容为准。

2、本合同一式伍份，具有同等法律效力，采购代理机构存档壹份，甲方执叁份，乙方执壹份。（可根据需要另增加）。经甲、乙双方各自授权代表签字并加盖双方各自公章或合同专用章后生效。

3、本合同甲乙双方法定代表人或授权代表签字并加盖单位公章后生效，自签订之日起二个工作日内，甲方或采购代理机构应当将合同副本在政采云系统合同公告。

此页无正文

甲方（章）：玉林市红十字会医院 2026年2月2日	乙方（章）：确信信息股份有限公司 2026年2月2日
通讯地址：玉林市玉州区金旺路1号	通讯地址：山东省济南市高新区孙村街道科嘉路粤浦科技济南科创中心8号楼
法定代表人：	法定代表人：
委托代理人：	委托代理人：黄飞
电话：0771-5330800	电话：0531-88113379
电子邮箱：	电子邮箱：
开户银行：	开户银行：中信银行济南高新支行
账号：	账号：7377010182600006670
邮政编码：	邮政编码：250000
经办人： 2026年　月　日	

二、合同附件

1、成交通知书

广西瑞真工程造价咨询有限责任公司
商用密码应用安全性评估与整改
[项目编号：YLZC2025-J1-990518-GXRZ]
成 交 通 知 书

确信信息股份有限公司：

你单位参加了本招标机构代理的：商用密码应用安全性评估与整改的竞标，项目编号：YLZC2025-J1-990518-GXRZ（采购计划文号：YLZC2025-J1-11771），经谈判小组评定，采购人确认，确定你单位为该项目的成交单位，成交内容：商用密码应用安全性评估与整改采购所包含内容，成交金额：人民币壹佰陆拾叁万元整（¥1630000.00）；交货期：自合同签订之日起 15 日历天内完成供货验收并交付使用。现将有关事项通知如下：

一、请接到本通知后，与采购单位（玉林市红十字会医院）按采购文件规定时间内签订合同。

二、签订合同详细地点：广西壮族自治区玉林市玉州区金旺路 1 号

采购单位联系人：梁宇航　　联系电话：0775-2286030

采购代理机构项目联系人：陈雪姣　　联系电话：0771-5800672

广西瑞真工程造价咨询有限责任公司

2026 年 1 月 15 日

2、项目采购需求

序号	货物名称	数量	单位	技术参数和要求
1	VPN 综合网关（综合安全网关）	2	台	**一、硬件规格：** 1、标准 2U，国产多核处理器，≥16G 内存 ，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书。 **二、性能要求：** 1、SSL VPN 性能：并发在线用户数≥3000，并发会话数≥28000，每秒新建用户数≥250，加解密速率≥1200Mbps，转发延迟＜0.1ms；IPSec VPN 性能：每秒新建隧道数≥1000，并发隧道数≥1500，加解密速率≥1200Mbps，转发延迟＜0.1ms。 **三、功能要求：** 1、支持国际通用算法和国产 SM 系列算法；支持 PKI 体系；支持身份认证、访问控制、单点登录、SSL 隧道；IPSec 支持主模式和快速模式；支持 ESP 密钥交换协议；支持 NAT 穿越和双向 NAT 穿越； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等； ▲3、算法实现对 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法和 RSA/SHA/AES/DES/3DES 等国际通用算法的支持，实现对后量子算法的支持。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲4、身份鉴别实现基于用户名口令、数字证书、短信码、动态码等多因子认证方式；实现基于零信任架构的身份认证和安全接入功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲5、协议支持实现基于 RSA、SM2、SM9、后量子等国际和国密算法的 SSL 协议和 IPSec 协议的密钥协商、密钥交换、链路通信加密、SSL 卸载功能。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章)； 6、高强度的传输链路加密，符合 GM/T 0024《SSL VPN 技术规范》； 7、基于角色授权，可将不同用户分配给不同角色，实现对不同用户访问权限细粒度的控制；

				▲8、访问控制支持基于角色用户机构的 RBAC 访问控制模型、基于用户属性客户端属性的 ABAC 访问控制模型、可修改超级管理员登录名基于 OB4LAC 的授权访问控制模型的功能。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章)； ▲9、支持基于 NTLM、FORM、BASIC、CAS、OAuth2.0、OpenID 等方式和协议的单点登录功能。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章) 10、高强度的传输链路加密，符合 GM/T 0024《SSL VPN 技术规范》； ▲11、支持常用的 Radius/LDAP/AD 第三方身份认证；支持 PKI 体系的第三方证书，支持 OCSP、CRL、LDAP 有效性校验。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章)； 12、遵循 GM/T 0022 《IPSec VPN 技术规范》，支持与标准 IPSec VPN 产品的互联互通； 13、隧道支持主模式和快速模式、支持完全向前保密 PFS、支持 DPD 协议探测隧道状态、支持隧道断线自动重建； 14、密钥交换协议支持 ESP 协议、支持隧道模式、支持 NAT 穿越和双向 NAT 穿越； ▲15、终端支持基于 IP 地址、MAC 地址等终端硬件信息的用户绑定功能；支持终端用户登录后的网络隔离功能，支持基于组策略、用户策略、网络白名单策略的网络隔离功能。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章)； 16、终端支持实现对 Windows7/10/11 主流操作系统，麒麟、统信、深度等国产操作系统，Android、iOS、鸿蒙等移动终端的支持。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章)； ▲17、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； 18、支持多线路负载均衡、支持线路切换、线路流量负载和双机热备的功能。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章)；

				19、需提供 VPN 综合网关(综合安全网关)国家相关部门颁发的电信设备进网许可证复印件并加盖供应商公章。 **四、具有国家密码管理局商用密码产品认证证书**：符合国家密码管理局 GM/T 0023《IPSec VPN 网关产品规范、GM/T 0025《SSL VPN 网关产品规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。**（在响应文件中提供有效的证书复印件加盖单位公章）**
2	国密浏览器	100	套	**▲一、功能要求：** 1、支持 SM2、SM3、SM4 算法，与身份认证网关之间建立安全通道，保证 Web 网页访问的安全性。 2、支持第三方电子认证中心签发的数字证书； 3、可按应用设置选用 Chrome 内核、IE 内核，并可按应用设置 IE 内核版本，实现对现有业务系统的兼容性适配，支持 IE/Chrome 内核的自动切换与 Cookie 共享； 4、支持国密算法 SM2、SM3、SM4，在 Chrome 内核、IE 内核下均支持国密 SSL 协议； 5、支持 X86、ARM、MIPS 等架构国产 CPU。 **二、具有国家密码管理局商用密码产品认证证书。**（在响应文件中提供有效的证书复印件加盖单位公章）
3	密码机服务器	2	台	**一、硬件规格：** 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书； **二、性能要求：** 1、SM2 密钥生成≥19900 对/秒，SM2 签名≥ 20620 次/秒，SM2 验签≥11700 次/秒，SM2 加密≥ 4700 次/秒，SM2 解密≥5940 次/秒，SM1 加解密≥ 740Mbps，SM4 加解密≥ 690Mbps，SM3 摘要≥1400Mbps，SM7 加解密≥ 320Mbps，SM9 密钥生成≥3000 对/秒，SM9 签名≥ 1500 次/秒，SM9 验签≥250 次/秒，SM9 加密≥ 1500 次/秒，SM9 解密≥350 次/秒； **三、功能要求：** 1、适用于各类密码安全应用系统，提供高速的、多任务并行处理的密码运算；可以满足应用系统数据的签名/验证、加密

				/解密的要求，保证传输信息的机密性、完整性和有效性；同时提供安全、完善的密钥管理机制。 ▲2、支持 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法；支持 ECC/RSA1024/RSA2048/RSA4096/SHA256/SHA384/SHA512/AES/3DES 等国际通用算法；支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；支持同态算法；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 3、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 4、密钥生成：密码机可提供各类型密钥对的生成功能； 5、支持 RSA 密钥管理、SM2 密钥管理、对称密钥管理、SM9 密钥管理等功能，并支持批量添加、删除密钥；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 6、杂凑密码运算：密码机可提供基于 SM3 算法的杂凑运算功能； 7、消息认证码的产生：密码机可提供基于 SM3 算法的 HMAC 的产生及验证； 8、随机数生成：密码机可提供基于双 WNG 物理随机源的随机数生成功能； 9、用户密钥对采用私钥授权码机制，使用时需要验证授权码，提高用户密钥使用的安全性；支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 10、访问用户分级管理，包含超级管理员、系统管理员、安全管理员、审计管理员三权分立。不同管理员具有不同权限；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 11、完善的密钥备份：采用门限密钥分割技术对密码机密钥进行备份，用于加密备份密钥的密钥被分割成多份子密钥，分别存在多个管理员的智能密码钥匙中。备份密钥是加密后存放到主机中，确保密钥的安全。恢复的时候需要半数以上管理员登录才可以将密钥恢复到服务器密码机内。 12、访问控制：提供服务白名单功能，实现白名单的添加查看删除；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 13、支持双机热备、负载均衡等高可用部署模式；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 14、标准接口：提供 SDF、JCE 等国密、国际标准规范口； 15、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书；

				16、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书。 **四、具有国家密码管理局商用密码产品认证证书**；符合国家密码管理局 GM/T 0030 《服务器密码机技术规范》和 GM/T 0028 《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）
4	国密堡垒机（**安全运维服务器**）	1	台	**一、硬件规格：** 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，提供密码卡商用密码产品认证证书； **二、性能要求：** 字符型协议并发会话数≥200，图形型协议并发会话数≥100，IP 管理资源授权≥100，IP 管理资源最大授权≥200，加解密速率≥220Mbps，转发延迟＜0.2ms。 **三、功能要求：** 1、通过集成数字证书强身份鉴别、国密协议安全隧道以及堡垒机模块功能为一体，满足“设备与计算安全”国密身份鉴别、访问控制、链路加密及敏感数据防护等安全要求。 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、强身份认证：支持基于国密数字证书的身份认证和登录功能，支持第三方 CA。 4、通信机密性：运维人员客户端与国密堡垒机之间采用国密算法加密通信链路进行数据的传输，保证通信数据的完整性和机密性。 5、存储机密性：对关键敏感数据采用国密算法进行加密存储，保证关键敏感信息的机密性。 6、单点登录：实现与用户授权管理的无缝连接，可以通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。 7、集中账号管理：集中账号管理包含对所有服务器、网络设备账号的集中管理。账号和资源的集中管理是集中授权、认

				证和审计的基础。集中账号管理可以完成对账号整个生命周期的监控和管理，而且还降低了管理大量用户账号的难度和工作量。 8、资源授权：提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。 9、访问控制：能够提供细粒度的访问控制，最大限度保护用户资源的安全；对访问控制信息采用国密算法进行数字签名，以保证数据完整性，防止数据被篡改，保证系统的安全性。 10、协议管理：支持字符型（SSH、Telnet）、图形（RDP、VNC）、数据库（Oracle、Sybase、MySQL、SQLServer、DB2 等）、文件传输（FTP、SFTP）、http、https 等多种协议类型； 11、支持基于管理代理的机制，安装在被管设备上，实现了运维服务器和被管设备之间的有效身份鉴别，并建立安全的加密信息传输通道。 12、操作审计：对访日志信息采用国密算法进行数字签名，以保证数据完整性，防止数据被篡改。 **四、具有国家密码管理局商用密码产品认证证书**；符合国家密码管理局 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）
5	密码服务平台	1	套	**一、硬件规格：** 1、标准 2U，国产多核处理器，≥16G 内存 ，≥480G 企业级固态硬盘，≥2 个千兆网口，触摸液晶屏，冗余电源； **二、功能要求：** 1、算法支持：支持国密 SM1、SM2、SM3、SM4、SM9 算法； 2、密码服务平台证书综合管理应包含 CA 配置、数量授权、证书管理、数量统计、存储介质管理等功能 （提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 3、密码服务平台密码资源管理应包含密码设备管理、宿主机管理、虚拟资源管理、镜像管理、密码服务等功能(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章)； 4、实现对密码设备资源的统一管理，包括签名服务器、密

				码机、云密码机、网关、电子签章服务器、时间戳服务器、手机盾服务器的增删改查。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 5、支持数字证书服务、密钥管理服务、签名验签服务、时间戳服务、电子签章服务、数据加解密服务、协同签名运算服务、数据链路加解密服务。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 6、密码服务平台身份认证功能应包含资源管理、角色管理授权管理功能（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 7、密码服务平台应用管理功能应包含应用接入管理和应用访问授权功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 8、支持第三方 CA 接入，实现数字证书全生命周期管理，包括个人数字证书、服务器证书的申请、更新、下载、注销等； 9、支持用户统一管理，能够在平台系统中对电子签章系统用户、移动互联网密码服务系统用户进行统一管理，包括用户的注册、修改、删除、查看； 10、支持对平台和密码设备资源的网络拓扑图自动生成功能； 11、对密码设备监控信息应包括：CPU 使用率、内存使用率、硬盘等； 12、支持日志审计、监控日志、归档日志等功能； 13、支持双主机热备部署。 **三、具有国家密码管理局商用密码产品认证证书**；符合国家密码管理局 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）
6	签名验签服务器	2	套	**一、硬件规格：** 1、标准 2U，国产多核处理器，≥16G 内存 ，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，提供密码卡商用密码产品认证证书； **二、性能要求：**

				SM2 密钥生成≥19860 对/秒，SM2 签名≥ 20400 次/秒，SM2 验签≥14370 次/秒，SM2 加密≥ 4680 次/秒，SM2 解密≥6640 次/秒，SM1 加解密≥ 643Mbps，SM4 加解密≥ 564Mbps，SM3 摘要≥1118Mbps； **三、功能要求：** 1、支持身份认证、数据签名、签名验证、数据加密/解密等功能。 ▲2、支持 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法；支持 ECC/RSA1024/RSA2048/RSA4096/SHA256/SHA384/SHA512/AES 等国际通用算法；支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 3、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 ▲4、支持 PKCS#1/PKCS#7(attached 和 detached)/XML 的签名验签；支持二维码、条形码的签名处理；支持基于 SM2、RSA 等算法的数字信封加密、解密功能；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲5、用户密钥对采用私钥授权码机制，使用时需要验证授权码，提高用户密钥使用的安全性；支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲6、支持服务信息功能，实现查看服务状态，系统状态，系统自检，更改服务端口，是否加密通信，服务的启动停止；支持服务测试功能，实现对签名验签，数字信封等服务功能的测试；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲7、支持应用管理功能，可管理调用签名验签服务的应用系统，包括应用的添加、删除、修改、关联证书链等功能；支持服务白名单功能，实现白名单的添加查看删除，通过连接白名单的支持，实现签名验签服务器对应用服务器的授权认证；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的

				复印件并加盖供应商公章） ▲8、支持 RSA 密钥管理、SM2 密钥管理、对称密钥管理、受信赖根证书、证书撤销列表、业务证书等管理功能；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲9、证书管理和验证、数字签名和验证等核心功能，要求符合《信息安全技术签名验签服务器技术规范 GB/T 38629 -2020》；（提供第三方检测报告复印件并加盖供应商公章佐证） 10、支持标准 X509V3 数字证书格式，支持签名证书和加密证书的双证书认证体系，提供 CRL/OCSP/LDAP 等多种方式的证书有效性验证； 11、支持最大 500M 大文件、大数据的数字签名和数字信封功能； 12、可同时配置多条证书链，验证不同 CA 的用户证书；可同时支持 20 个不同的 CA； 13、提供 CRL 的自动下载功能和证书有效性验证功能； 14、提供证书解析功能，获取证书中的任意主题信息以及扩展项信息； 15、基于 WEB 形式的图形管理界面，提供完善的配置管理、证书管理、服务管理等功能； 16、具有日志审计功能，支持第三方 SYSLOG 日志服务器； 17、支持浏览器、应用服务器、移动端的调用； 18、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； 19、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书； 20、提供 JAVA、C++等 API 开发接口和示例代码； 21、支持双主机热备部署。 **四、具有国家密码管理局商用密码产品认证证书**；符合国家密码管理局 GM/T 0029《签名验签服务器技术规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）
7	电子签章系统	1	台	**一、硬件规格：** 1、标准 2U，国产多核处理器，≥16G 内存 ，≥480G 企业

				级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书； **二、功能要求：** 1、支持国产系列算法；可提供电子签章的管理和服务、印章制作、客户端签章工具，是基于智能密码钥匙开发的一套用于保证 MicrosoftWord/Excel 电子文档、PDF 文档以及 Web 网页的完整性、防篡改性和不可抵赖性的安全应用软件，主要采用了 PKI 中的数字签名技术来实现对 Microsoft Office Word 文档、 Excel 电子表格、PDF 文档、Web 网页的安全性保护； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、支持对 PDF 格式的文档进行电子签章，并且在电子文档上显示签章图片； 4、支持指定位置盖章、指定位置签名图片盖章、指定位置审批意见盖章、单个签章验证、文档中所有签章验证； 5、支持管理员、审计员操作，能够对用户进行统一管理、监督，包含整个生命周期管理及电子印章的制作、挂失、解挂、停用等管理； 6、支持骑缝章，提供三个骑缝章位置以供选择； 7、支持对 PDF 文档签章、验证、统计文档页数、统计签章个数、获取文档数据、打印文档等功能； 8、支持移动端电子签章功能，支持移动端手写签名采集功能； 9、支持在文档中添加时间戳，保证文档行为时间的有效性和合法性； 10、支持在文档中添加图片、文字水印； 11、支持多人对文档的会签； 12、支持文档打开时自动对文档内的所有印章进行验证功能； 13、支持文档安全控制，可设置文档保护限制； ▲14、支持对 Word/Excel 格式的文档进行电子签章；（提

				供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲15、支持身份鉴别、访问控制、剩余信息保护等自身安全功能；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 16、支持安全的集中式签章，避免印章被冒用，防止数据泄露； 17、支持文档样式保护的签验章，对文字样式快速解析，加快文档验章和签章的速度。 **三、具有国家密码管理局商用密码产品认证证书**：符合国家密码管理局 GM/T 0031 《安全电子签章密码技术规范》。（在响应文件中提供有效的证书复印件加盖单位公章）
8	数字证书管理系统	1	台	**一、硬件规格：** 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书。 **二、性能要求：** 证书最大数量：20000 **三、功能要求** 1、支持国际通用算法和国产 SM 系列算法；提供数字证书整个生命周期的过程管理功能。包括用户注册管理、证书/证书注销列表的生成与签发、证书/证书注销列表的存储与发布、证书状态的查询、密钥的生成与管理、过程安全审计等； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、支持证书新办、更新、吊销、挂起、解挂和证书黑名单等证书全生命周期管理； 4、支持多种证书类型模版，个人证书、机构证书、设备证书等； 5、支持证书模板自定义配置，支持国家标准规定的私有扩展及自定义扩展； 6、证书符合国际标准 X509 V3 标准；

				7、支持产生证书黑名单，包括：定时自动产生、手动实时产生，规范符合 X509 V2 标准； 8、支持手工录入、批量导入、三方应用授权集成等方式注册证书，并为用户签发数字证书； 9、支持证书签发模块、证书注册模块、系统配置模块分权管理模式； ▲10、模版管理包括证书模板管理、证书撤销列表模板管理、在线证书状态协议模板等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》(增强级)相关要求。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章) ▲11、密钥管理包含密钥生成、密钥存储、密钥传送与分发、密钥导入导出、密钥使用、密钥备份、密钥恢复、密钥归档、密钥销毁、密钥更新等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》(增强级)相关要求。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章) ▲12、证书管理包含证书注册、证书生成、证书撤销、证书更新、证书变更等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》(增强级)相关要求。(提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章) 13、可提供证书黑名单、Ldap、OCSP 等方式数字证书身份认证服务； 14、提供基于证书的签名/验证、加密/解密等功能组件； 15、密钥独立管理体系，支持密钥自动监控、产生、分发的智能监管系统； 16、支持管理权限划分，各系统按权操作，多系统分责管理,管理员身份可鉴别； 17、支持多级 CA 部署模式； 18、支持系统管理员操作日志审查，支持操作员签名审查； 19、支持多厂家普通、蓝牙、指纹等智能 UsbKey 钥匙的无缝接入； ▲20、可以添加证书扩展，可以对证书扩展列表进行管理，

				包括修改、删除、查看查找等；可以新增证书模板，可以对证书模板进行管理，包括查看详情、删除、查看查找等（提供第三方测试报告复印件并加盖供应商公章） ▲21、可以查看日志信息，包括日志类型、客户端地址、操作者编号等；可以通过日志类型、客户端地址、操作者编号等查找日志审计列表，列表包括日志内容、操作结果、操作时间等；（提供第三方测试报告复印件并加盖供应商公章）。 **四、具有国家密码管理局商用密码产品认证证书**；符合国家密码管理局 GM/T 0034 《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》。（在响应文件中提供有效的证书复印件加盖单位公章）
9	手机盾协同签名系统	1	台	**一、硬件规格：** 1、标准 2U，国产多核处理器，≥16G 内存 ，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书。 三、功能要求 1、算法支持：支持国密 SM2、SM3、SM4 算法； 2、密钥管理：用户密钥客户端片段生成、安全存储及销毁； 3、证书管理：集成身份认证系统（CA），支持证书在线申请、更新、注销等数字证书全生命周期管理，支持第三方 CA 认证机构； 4、扫码签名：支持扫描二维码实现数字签名； 5、推送签名：支持业务系统通过密码服务系统服务端推送签名请求到移动端，实现数字签名； ▲6、支持获取二维码、推送签名消息、获取签名值、验证签名等功能； 7、支持摘要运算、非对称加解密和对称加解密运算； 8、支持口令和指纹认证方式； ▲9、用户私钥拆分成两部分密钥因子，一部分在手机端，一部分在服务端，保证移动端密钥的安全； ▲10、协同签名：支持与客户端配合，协同实现数字签名； ▲11、系统及服务监控：能够对系统服务进行监控，授权

				查看设备运行状态； 12、用户管理：对移动终端账户进行管理、统计、查询。维护账户状态，存储账户对应的设备公钥信息等； 13、管理员管理：对系统操作的管理员进行添加、删除、修改以及授权，只有授权管理员才能登陆系统进行操作； 14、支持 Android4.4.2 、IOS9 及以上以上手机系统； ▲15、安全审计：能够对系统所有的操作和接口调用进行详细的记录，非授权人员不可篡改记录； 16、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书； 17、提供 SDK 开发接口，支持移动端 APP、微信公众号/小程序，支持免安装方式与移动端应用 APP 进行集成； 18、支持双主机热备部署。 **四、具有国家密码管理局商用密码产品认证证书**；符合国家密码管理局 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）
10	时间戳服务器	1	套	一、硬件规格： 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），时间源卡，触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书； ▲3、设备内置时间源卡，时间源卡与整机为同一厂商、同一品牌。 二、性能要求： SM2 时间戳签发≥ 15080 次/秒，SM2 时间戳验证≥8421 次/秒。 三、功能要求 1、产品支持时间戳签发，验证时间戳，支持 NTP 协议，支持第三方 CA 证书，支持 CDMA、GPS、北斗卫星授时； ▲2、支持 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法；支持 ECC/RSA1024/RSA2048/RSA4096/SHA256 /SHA384/SHA512/AES/3DES 等国际通用算法；支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；（提供由 CNAS 或 CMA 认证的第三方检

				测机构出具的测试报告的复印件并加盖供应商公章）； 3、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等； 4、提供时间戳的签发和验证功能；支持验证时间戳信息的有效性、签名证书的有效性等内容； 5、提供获取时间戳信息功能，支持获取时间戳的时间、数据信息、消息摘要算法等； 6、时间设置支持 NTP、SNTP 方式，支持时间源卡方式，时间源卡可从 BD、GPS 以及 4G 信号方式同步时间。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 7、内置权威时间源卡，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检测，时间源卡精度小于 1us（提供国家授时中心检测证明材料）； 8、支持可信时间发布功能； 9、支持时间戳证书管理功能，实现时间戳证书的申请，导入，查看，导出等操作；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 10、支持时间戳检索功能，对已签发的时间戳进行查看、查找、删除、销毁；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 11、支持时间戳归档，将已签发时间戳进行归档整理；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 12、具有日志审计功能，支持第三方 SYSLOG 日志服务器； 13、支持双机热备、负载均衡； ▲14、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； 15、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书； 16、客户端提供 API 接口，包括 C 接口、C#接口、Java 接口，支持定制接口开发。标准 2U 机架式服务器；工业触摸液晶屏。 **四、具有国家密码管理局商用密码产品认证证书**；符合国家密

				码管理局 GM/T 0033 《时间戳接口规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）
11	SDK 接口（商用密码应用业务流程和开发流程设计服务）	1	项	1、密码设备对医院应用系统做接口改造服务； 2、实施项目经理需具备电子信息专业高级职称证书及防爆电气设备安装、检修、维护技术培训证书； 3、实施人员至少有一人省市级密码管理局公示商用密码应用专家(官方网站截图证明及密码管理局公示的官方网站链接)提供有效证明文件复印件加盖单位公章。
12	系统调用接口服务（系统密码应用开发改造服务）	1	项	医院业务系统为满足三级密码评测需要做业务流程改造适应密码设备的应用。包括不限于（HIS、EMR、集成平台、数据中心、PACS、LIS、B 超、心电、内镜等系统，以医院等保备案系统为准）。
13	CA 证书（个人数字证书）	1200	张	第三方 CA 机构颁发的个人数字证书。
14	国产门禁系统（国密电子门禁系统）	1	套	**一、功能要求：** 1、系统包含门禁管理系统、门禁日志审计系统和密钥管理系统等软件系统； 2、门禁用户身份鉴别：使用用户 CPU 卡和国密门禁读卡器，采用基于 SM1/SM4 的对称加解密技术，实现用户身份鉴别； 3、门禁日志记录完整性保护：采用基于 SM3 的 HMAC 技术，实现日志记录的完整性保护； 4、密钥注入和发卡设备物理分离：支持二者物理分离，采用密钥注入器进行密钥注入，采用发卡器进行发卡。 **二、具有国家密码管理局颁发的商密认证证书。**（在响应文件中提供有效的证书复印件加盖单位公章）
15	国产监控系统（国密视频监控系统）	1	套	**一、功能要求：** 1、音像记录数据机密性保护：使用国密摄像机和国密 NVR，采用基于 SM4 的对称加解密技术，实现音像记录数据的机密性保护； 2、音像记录数据完整性保护：使用国密 NVR 以及 PCI-E 密

				码卡(配合视频加密系统软件)，采用基于 SM3 的 HMAC 技术，实现音像记录数据的完整性保护。 **二、具有国家密码管理局颁发的商密认证证书。**（在响应文件中提供有效的证书复印件加盖单位公章）
16	商用密码应用安全性评估服务	1	次	依据《中华人民共和国密码法》、《中华人民共和国网络安全法》、《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）、《信息系统密码测评要求》（试行）等国家行业现行有效的标准、规范对被测系统进行商用密码应用安全性评估，信息系统的《密码应用安全性评估报告》须取得“基本符合”或以上评估结论，并完成密码应用方案商用密码应用安全性评估报告和被测系统商用密码应用安全性评估报告在密码管理局密评的备案工作。
17	商用密码应用咨询服务（密码应用方案评测）	1	次	根据 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，系统达到第三级密码应用基本要求，针对被测系统从方案制定和评审、终端密码改造、国密安全通道改造、设备层密码改造、应用和数据安全密码改造及密码应用管理体系制度编制服务等。供应商所选择的密评机构须具备有效的《商用密码检测机构资质证书》，且业务范围为“商用密码应用安全性评估”，[须在国家密码管理局公告（第 53 号）公布的“商用密码检测机构(商用密码应用安全性评估业务)目录中”可查询]。 ▲1、为满足本项目测评要求,供应商所选择的密评机构投入本项目密码测评工具，支持 SM2/SM9 椭圆曲线点压缩计算。支持 SM9 密钥生成、签名验签、加解密、密钥封装功能。支持解析 APDU 流量包并提取签名值随机数，并自动进行验签及签名攻击。需进行视频演示。 ▲2、支持哈希算法猜测功能。支持 Attach 和 Detach 签名验签，P7 签名值分析功能。支持 PRF 运算、KDF 运算、TLCP 密钥生成、SM2 加密-K 碰撞功能。支持对称密码算法工作模式检测功能。需进行视频演示。 ▲3、为满足本项目测评要求，供应商所选择的密评机构投入本项目自主研发的密码测评工具，至少包含密码资源监测系

				统、商用密码检测软件、密码应用业务管理平台字样的测评工具，需提供相关包含以上全部字样的测评工具证明材料的复印件并加盖公章或提交承诺函所用的测评工具符合要求（承诺函格式自拟） 4、供应商所选择的密评机构配备的密码测评技术工程师需同时具备持有国家密码管理局颁发的商用密码应用安全性评估从业人员考核证书，并具备 CCSK 云计算安全知识认证、网络安全管理员证书。需提供相关包含以上全部证书证明材料的复印件并加盖供应商公章或提交承诺函配备的密码测评技术工程师符合要求（承诺函格式自拟）

商务要求表

一、合同签订期：自成交通知书发出之日起 25 日内。

▲二、交货期：自合同签订之日起 15 日历天内完成供货验收并交付使用。

三、交货地点：采购人指定地点。

三、交货方式：现场交货。

五、售后服务要求：

▲1、质量保证期不少于 1 年（自交货并验收合格之日起计）。

2、故障响应时间：供应商接到故障通知后在 1 小时内到达采购人指定现场。

3、售后技术服务要求：

1）故障响应时间：供应商接到故障通知后需在 30 分钟内做出响应（电话），在 24 小时内派工程师到现场进行故障解除，如 48 小时内无法排除故障的，必须提供不低于故障产品规格型号和档次的备用产品供用户使用，直至故障产品修复，保证系统恢复正常运行。

2）在保修期内由供应商负责保修，排除故障，无偿提供非操作不当造成的部件、配件的更换，供应商从在其指定地点收到故障产品之日起 7 天内将修理后的产品或替换产品运至最终用户现场。因操作不当或外部原因损坏，造成部件的更换，应由采购人承担有关费用。保修期内，所有维修服务均为上门服务，由此产生的费用均不再收取。

3）供应商须向采购人承诺终身优惠提供配件和维修。

4）供应商应免费培训采购人维护人员，保证维护人员能进行日常运行维护工作，提供用户操作手册和维修手册；并能熟练地排除故障、管理设备、分析故障等。

5）如需升级软件，免费升级软件。

六、其他要求：

▲1、竞标报价包括但不限于：

1）货物的价格；

2）货物的标准附件、备品备件、专用工具的价格；

3）运输、装卸、调试、培训、技术支持、售后服务等费用；

4）必要的保险费用和各项税费；

5）包括安装费用；

6）检测部门产品检测费用；

7）审核部门费用；

▲2、设备在验收过程中出现无法满足招标文件规定的参数及要求的，采购人不予验收并终止合同，一切后果由供应商承担，视为虚假应标，上报监督管理部门。

▲3、为保证服务质量，供应商应承诺与医院业务系统对接，供应商与医院业务系统的对接工作自行解决，在供货期内完成上线验收，供应商无法完成对接接口服务，在供货期内采购人有权终止合同。（供应商承诺函自拟）

▲4、付款方式：**签订合同后十五个工作日内，支付合同总额的30%作为预付款，项目实施完成并整体验收合格后，60天内支付合同总额的67%，剩余3%系统正常运行一年后支付。**

3、竞标报价表

二、响应报价表

二次（最终） 报 价 表

项目名称：商用密码应用安全性评估与整改 项目编号：YLZC2025-J1-990518-GXRZ 分标：无 供应商名称：确信信息股份有限公司

序号	货物名称	货物规格型号	数量①	单价（元）②	单项合价（元）③=①×②	备注
1	VPN 综合网关（综合安全网关）	CGW V2.0 综合安全网关	2	66000.00	132000.00	
2	国密浏览器	SHM1602-G V5.0	100	130.00	13000.00	
3	密码机服务器	HSM V2.0 服务器密码机	2	66000.00	132000.00	
4	国密堡垒机（安全运维服务器）	SOP V2.0 密码机服务器	1	66000.00	66000.00	
5	密码服务平台	CSSP 2000 V1.0 密码服务平台	1	128000.00	128000.00	
6	签名验签服务器	DSVS V2.0 签名验签服务器	2	66000.00	132000.00	
7	电子签章系统	ESS V2.0 电子签章系统	1	108000.00	108000.00	
8	数字证书管理系统	CA V2.0 数字证书管理系统	1	108000.00	108000.00	
9	手机盾协同签名系统	SCM 1000 V1.0 手机盾协同签名系统	1	166000.00	166000.00	

10	时间戳服务器	TSA V2.0 时间戳服务器	1	66000.00	66000.00	
11	SDK 接口（商用密码应用业务流程和开发流程设计服务）	SDK 接口服务	1	50000.00	50000.00	
12	系统调用接口服务（系统密码应用开发改造服务）	接口服务	1	210000.00	210000.00	
13	CA 证书（个人数字证书）	CA 数字证书	1200	70.00	84000.00	
14	国产门禁系统（国密电子门禁系统）	STC-1 国密电子门禁系统	1	65000.00	65000.00	
15	国产监控系统（国密视频监控系统）	SJT1708 V1.0 国密视频监控系统	1	65000.00	65000.00	
16	商用密码应用安全性评估服务	商用密码应用安全性评估服务	1	75000.00	75000.00	
17	商用密码应用咨询服务（密码应用方案评测）	商用密码应用咨询服务	1	30000.00	30000.00	

报价合计（包含税费等所有费用）：（大写）人民币壹佰陆拾叁万元整 （￥1630000.00元）
无分标（此处有分标时填写具体分标号，无分标时填写“无”）
验收标准：按照合同要求验收
优惠及其它：无

注：

1、供应商需按本表格式填写，不得自行更改，也不得留空，如有多分标，按分标分别提供响应报价表。

2、如为联合体响应的，“供应商名称”处必须列明联合体各方名称，并标注联合体牵头人名称，且盖章处须加盖联合体各方公章，**否则其响应作无效响应处理。**

3、以上表格要求细分项目及报价，在“货物名称”一栏中，填写具体货物，**否则其响应作无效响应处理。**

4、特别提示：采购机构将对项目名称和项目编号，成交供应商名称、地址和成交金额，主要成交标的的名称、规格型号、数量、单价、货物要求等予以公示。

5、符合采购文件中列明的可享受中小企业扶持政策的供应商，请填写中小企业声明函。注：供应商提供的中小企业声明函内容不实的，属于提供虚假材料谋取中标、成交，依照《中华人民共和国政府采购法》等国家有关规定追究相应责任。

供应商名称（电子签章）：桃信信息股份有限公司

日期：2026 年 1 月 8日

4、配置清单

八、配置清单

货物配置清单

所竞分标：无

序号	货物名称	数量及单位	品牌	规格型号	制造商	原产地	参数性能、指标及配置
1	VPN 综合网关(综合安全网关)	2 台	确信信息	CGW V2.0	确信信息股份有限公司	中国山东	标准 2U，国产多核处理器，16G 内存 ，480G 企业级固态硬盘，2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； 性能配置： 1、SSL VPN 性能：并发在线用户数：4210，并发会话数：30000，每秒新建用户数：290，加解密速率：2000Mbps，转发延迟：0.08ms；IPSec VPN 性能：每秒新建隧道数：1220，并发隧道数：1990，加解密速率：1290Mbps，转发延迟：0.08ms。功能参数详见-货物需求偏离表。
2	国密浏览器	100 套	海泰方圆	SHM1602-G V5.0	北京海泰方圆科技股份有限公司	北京	支持国产密码算法 SM2、SM3、SM4 实现国产密码算法 SSL 链接功能；功能参数详见-货物需求偏

183

							离表。
3	密码机服务器	2台	确信信息	HSM V2.0	确信信息股份有限公司	中国山东	硬件规格配置： 1、标准2U，国产多核处理器，16G内存，480G企业级固态硬盘，2个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； 性能参数：1、1、SM2密钥生成：21900对/秒，SM2签名：22640次/秒，SM2验签：12800次/秒，SM2加密：5000次/秒，SM2解密：6000次/秒，SM1加解密：790Mbps，SM4加解密：820Mbps，SM3摘要：1500Mbps，SM7加解密：370Mbps，SM9密钥生成：3500对/秒，SM9签名：2000次/秒，SM9验签：300次/秒，SM9加密：2000次/秒，SM9解密：390次/秒；功能参数详见-货物需求偏离表。
4	国密堡垒机（**安全运维服务器**）	1台	确信信息	SOP V2.0	确信信息股份有限公司	中国山东	一、硬件规格配置： 1、标准2U，国产多核处理器，16G内存，480G企业级固态硬盘，2个千兆网口（支持扩展光口），触摸液晶屏，冗

							余电源； 二、性能配置：字符型协议并发会话数：240，图形型协议并发会话数：160，IP管理资源授权：160，IP管理资源最大授权：230，加解密速率：270Mbps，转发延迟：0.15ms；功能参数详见-货物需求偏离表
5	密码服务平台	1套	确信信息	CSSP 2000 V1.0	确信信息股份有限公司	中国山东	标准2U，国产多核处理器，16G内存，480G企业级固态硬盘，2个千兆网口，触摸液晶屏，冗余电源；功能参数详见-货物需求偏离表
6	签名验签服务器	2套	确信信息	DSVS V2.0	确信信息股份有限公司	中国山东	一、硬件规格：1、标准2U，国产多核处理器，16G内存，80G企业级固态硬盘，2个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； 二、性能配置：SM2密钥生成：20000对/秒，SM2签名：22000次/秒，SM2验签：14880次/秒，SM2加密：5000次/秒，SM2解密：6720次/秒，SM1加解密：678Mbps，SM4加解密：599Mbps，

							SM3 摘要：1200Mbps；功能参数详见-货物需求偏离表
7	电子签章系统	1 台	确信信息	ESS V2.0	确信信息股份有限公司	中国山东	标准 2U，国产多核处理器，16G 内存 ，480G 企业级固态硬盘，2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源；功能参数详见-货物需求偏离表
8	数字证书管理系统	1 台	确信信息	CA V2.0	确信信息股份有限公司	中国山东	标准 2U，国产多核处理器，16G 内存，480G 企业级固态硬盘，2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； 性能配置： 证书最大数量：21050；功能参数详见-货物需求偏离表
9	手机盾协同签名系统	1 台	确信信息	SCM 1000 V1.0	确信信息股份有限公司	中国山东	标准 2U，国产多核处理器，16G 内存 ，480G 企业级固态硬盘，2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源；功能参数详见-货物需求偏离表
10	时间戳服务器	1 套	确信信息	TSA V2.0	确信信息股份有限公司	中国山东	一、硬件规格配置： 1、标准 2U，国产多核处理器，16G 内存，480G 企业级固态硬盘，2

							个千兆网口（支持扩展光口），时间源卡，触摸液晶屏，冗余电源； 二、性能配置： SM2 时间戳签发：15430 次/秒，SM2 时间戳验证：8550 次/秒；功能参数详见-货物需求偏离表
11	SDK 接口（商用密码应用业务流程和开发流程设计服务）	1 项	无	无	无	无	提供密码设备对医院应用系统做接口改造服务；相关人员也具备相关资质。
12	系统调用接口服务（系统密码应用开发改造服务）	1 项	无	无	无	无	配合医院业务系统为满足三级密码评测做业务流程改造适应密码设备的应用。
13	CA 证书（个人数字证书）	1200 张	西部 CA	无	西部安全认证中心有限责任公司	无	提供 CA 证书（个人数字证书）
14	国产门禁系统（国密电子门禁系统）	1 套	天津光电	V1.0	天津光电安辰信息技术股份有限公司	天津	用于对门禁卡进行身份鉴别时提供密码服务，保证用户身份的合法性；功能参数详见-货物需求偏离表
15	国产监控系统（国密视频监控	1 套	天津光电	V1.0	天津光电安辰信息技	天津	用于实现对于音视频数据记录的机密性防护；功

	系统）				术股份有限公司		能参数详见-货物需求偏离表
16	商用密码应用安全性评估服务	1次	无	无	长沙云创信安科技有限公司	无	完成密码应用方案商用密码应用安全性评估报告和被测系统商用密码应用安全性评估报告在密码管理局密评的备案工作。
17	商用密码应用咨询服务（密码应用方案评测）	1次	无	无	长沙云创信安科技有限公司	无	目标系统达到第三级密码应用基本要求，针对被测系统从方案制定和评审、终端密码改造、国密安全通道改造、设备层密码改造、应用和数据安全密码改造及密码应用管理体系制度编制服务等

备注：

以上性能配置清单中“货物名称、数量及单位、品牌、规格型号、制造商、原产地、参数性能、指标及配置”必须如实填写完整，品牌、规格型号没有则填无，填写有缺漏的，响应文件作无效处理。货物名称、数量及单位、品牌必须与“货物需求偏离表”一致，否则响应文件作无效处理。

供应商名称（电子签章）：确信信息股份有限公司

日期：2026年1月30日

九、售后服务承诺

我司承诺：

1、质量保证期为1年（自交货并验收合格之日起计）。

2、故障响应时间：供应商（确信信息股份有限公司）接到故障通知后在1小时内到达采

5、商务、技术偏离表

商务偏离表

四、商务条款偏离表

商务条款偏离表（格式）

分标号（此处有分标时填写具体分标号，无分标时填写“无”）：无

项号	竞争性谈判采购文件的商务要求	响应文件承诺的商务条款	偏离说明
一	合同签订期：自成交通知书发出之日起25日内。	**我司完全响应，情况如下：** 合同签订期：自成交通知书发出之日起25日内。	无偏离
二	▲交货期：自合同签订之日起15日历天内完成供货验收并交付使用。	**我司完全响应，情况如下：** ▲交货期：自合同签订之日起15日历天内完成供货验收并交付使用。	无偏离
三	交货地点：采购人指定地点。	**我司完全响应，情况如下：** 交货地点：采购人指定地点。	无偏离
四	交货方式：现场交货。	**我司完全响应，情况如下：** 交货方式：现场交货。	无偏离
五	售后服务要求： ▲1、质量保证期不少于1年（自交货并验收合格之日起计）。 2、故障响应时间：供应商接到故障通知后在1小时内到达采购人指定现场。 3、售后技术服务要求： 1）故障响应时间：供应商接到故障通知后需在30分钟内做出响应（电	**我司完全响应，情况如下：** 售后服务要求： ▲1、质量保证期不少于1年（自交货并验收合格之日起计）。 2、故障响应时间：我司接到故障通知后在1小时内到达采购人指定现场。 3、售后技术服务要求： 1）故障响应时间：我司接到故障	无偏离

	话），在 24 小时内派工程师到现场进行故障解除，如 48 小时内无法排除故障的，必须提供不低于故障产品规格型号和档次的备用产品供用户使用，直至故障产品修复，保证系统恢复正常运行。 2）在保修期内由供应商负责保修，排除故障，无偿提供非操作不当造成的部件、配件的更换，供应商从在其指定地点收到故障产品之日起 7 天内将修理后的产品或替换产品运至最终用户现场。因操作不当或外部原因损坏，造成部件的更换，应由采购人承担有关费用。保修期内，所有维修服务均为上门服务，由此产生的费用均不再收取。 3）供应商须向采购人承诺终身优惠提供配件和维修。 4）供应商应免费培训采购人维护人员，保证维护人员能进行日常运行维护工作，提供用户操作手册和维修手册；并能熟练地排除故障、管理设备、分析故障等。 5）如需升级软件，免费升级软件。	通知后需在 30 分钟内做出响应（电话），在 24 小时内派工程师到现场进行故障解除，如 48 小时内无法排除故障的，必须提供不低于故障产品规格型号和档次的备用产品供用户使用，直至故障产品修复，保证系统恢复正常运行。 2）在保修期内由我司负责保修，排除故障，无偿提供非操作不当造成的部件、配件的更换，我司从在其指定地点收到故障产品之日起 7 天内将修理后的产品或替换产品运至最终用户现场。因操作不当或外部原因损坏，造成部件的更换，应由采购人承担有关费用。保修期内，所有维修服务均为上门服务，由此产生的费用均不再收取。 3)我司须向采购人承诺终身优惠提供配件和维修。 4)我司应免费培训采购人维护人员，保证维护人员能进行日常运行维护工作，提供用户操作手册和维修手册；并能熟练地排除故障、管理设备、分析故障等。 5)如需升级软件，免费升级软件。	

六	其他要求： ▲1、投标报价包括但不限于： 1）货物的价格； 2）货物的标准附件、备品备件、专用工具的价格； 3）运输、装卸、调试、培训、技术支持、售后服务等费用； 4）必要的保险费用和各项税费； 5）包括安装费用； 6）检测部门产品检测费用； 7）审核部门费用； ▲2、设备在验收过程中出现无法满足招标文件规定的参数及要求的，采购人不予验收并终止合同，一切后果由供应商承担，视为虚假应标，上报监督管理部门。 ▲3、为保证服务质量，供应商应承诺与医院业务系统对接，供应商与医院业务系统的对接工作自行解决，在供货期内完成上线验收，供应商无法完成对接接口服务，在供货期内采购人有权终止合同。（供应商承诺函自拟） ▲4、付款方式：签订合同后十五个工作日内，支付合同总额的30%作为预付款，项目实施完成并整体验收合格后，60天内支付合同总额的67%，剩余3%系统正常运行一年后支付。	**我司完全响应，情况如下：** 其他要求： ▲1、投标报价包括但不限于： 1）货物的价格； 2）货物的标准附件、备品备件、专用工具的价格； 3）运输、装卸、调试、培训、技术支持、售后服务等费用； 4）必要的保险费用和各项税费； 5）包括安装费用； 6）检测部门产品检测费用； 7）审核部门费用； ▲2、设备在验收过程中出现无法满足招标文件规定的参数及要求的，采购人不予验收并终止合同，一切后果由我司承担，视为虚假应标，上报监督管理部门。 ▲3、为保证服务质量，我司应承诺与医院业务系统对接，我司与医院业务系统的对接工作自行解决，在供货期内完成上线验收，我司无法完成对接接口服务，在供货期内采购人有权终止合同。（供应商承诺函自拟）详见P10服务质量承诺函 ▲4、付款方式：签订合同后十五个工作日内，支付合同总额的30%作为预付款，项目实施完成并整体验收合格后，60天内支付合同总额的67%，剩余3%系统正常运行一年后支付。	无偏离

注：

1. 说明：应对照谈判文件“第二章 采购需求”中的商务条款逐条作出明确响应，并作出偏离说明。

2. 供应商应根据自身的承诺，对照谈判文件要求，在“偏离说明”中注明“正偏离”、“负偏离”或者“无偏离”。既不属于“正偏离”也不属于“负偏离”即为“无偏离”。当响应文件的商务内容低于竞争性谈判采购文件要求时，竞标人应当如实写明“负偏离”，否则视为虚假应标

3. 表格内容均需按要求填写并盖章，不得留空，否则按竞标无效处理。

4. 如果采购需求为小于、小于等于、大于或大于等于某个数值标准时，响应文件承诺不得直接复制采购需求，响应文件承诺内容应为写明商务响应承诺的具体数值，否则按竞标无效处理。如该采购需求属于不能明确具体数值的，采购人应在此采购需求的数值后标注◆号，对标注◆号的采购需求不适用上述“竞标无效”条款。

服务质量承诺函

致：玉林市红十字会医院

我公司参加贵单位组织的商用密码应用安全性评估与整改（项目编号：YLZC2025-J1-990518-GXRZ）项目的响应报价，为保证服务质量，我司（确信信息股份有限公司）承诺与医院业务系统对接，供应商（确信信息股份有限公司）与医院业务系统的对接工作我方自行解决，在供货期内完成上线验收，供应商无法完成对接接口服务，在供货期内采购人有权终止合同。

供应商名称（电子签章）：确信信息股份有限公司

日期：2026 年 1 月 5 日

七、货物需求偏离表

货物需求偏离表
（注：按采购需求具体条款修改）

所竞分标：无

项号	竞争性谈判采购文件需求			响应文件承诺			偏离说明
	货物名称	数量	货物参数要求	货物名称	数量	货物参数	
1	VPN综合网关（综合安全网关）	2台	一、硬件规格： 1、标准2U，国产多核处理器，≥16G内存，≥480G企业级固态硬盘，≥2个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书。 二、性能要求： 1、SSL VPN性能：并发在线用户数≥3000，并发会话数≥28000，每秒新建用户数≥250，加解密速率≥1200Mbps，转发延迟＜0.1ms；IPSec VPN性能：每秒新建隧道数≥1000，并发隧道数≥1500，加解密速率≥1200Mbps，转发延迟＜	VPN综合网关（综合安全网关）	2台	**我司完全响应，情况如下：** 应标产品硬件配置： 1、标准2U，国产多核处理器，16G内存，480G企业级固态硬盘，2个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； 2、产品内置密码卡与设备产品为同一厂商，已提供密码卡商用密码产品认证证书。 性能配置： **1、SSL VPN性能：并发在线用户数：4210，并发会话数：30000，每秒新建用户数：290，加解密速率：2000Mbps，转发延迟：0.08ms；IPSec VPN性能：每秒新建隧道数：1220，并发隧道数：1990，加解密速率：1290Mbps，转发延迟：0.08ms。** 产品功能： 1、支持国际通用算法	正偏离

			0.1ms。 三、功能要求： 1、支持国际通用算法和国产SM系列算法；支持PKI体系；支持身份认证、访问控制、单点登录、SSL隧道；IPSec支持主模式和快速模式；支持ESP密钥交换协议；支持NAT穿越和双向NAT穿越； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等； ▲3、算法实现对SM1/SM2/SM3/SM4/SM7/SM9/ZUC国产密码算法和RSA/SHA/AES/DES/3DES等国际通用算法的支持，实现对后量子算法的支持。（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲4、身份鉴别实现基于用户名口令、数字证书、短信码、动态码等多因子认证方式；实现基于零信任架构的身份认证和安全接入功能。（提供由CNAS			和国产SM系列算法；支持PKI体系；支持身份认证、访问控制、单点登录、SSL隧道；IPSec支持主模式和快速模式；支持ESP密钥交换协议；支持NAT穿越和双向NAT穿越； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等； 3、算法实现对SM1/SM2/SM3/SM4/SM7/SM9/ZUC国产密码算法和RSA/SHA/AES/DES/3DES等国际通用算法的支持，实现对后量子算法的支持。（已提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 4、身份鉴别实现基于用户名口令、数字证书、短信码、动态码等多因子认证方式；实现基于零信任架构的身份认证和安全接入功能。（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 5、协议支持实现基于RSA、SM2、SM9、后量子等国际和国密算法的SSL协议和IPSec协议的密钥协商、密钥交换、链路通信加密、SSL卸载功能。（提	

			或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲5、协议支持实现基于 RSA、SM2、SM9 后量子等国际和国密算法的 SSL 协议和 IPSec 协议的密钥协商、密钥交换、链路通信加密、SSL 卸载功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 6、高强度的传输链路加密，符合 GM/T 0024《SSL VPN 技术规范》； 7、基于角色授权，可将不同用户分配给不同角色，实现对不同用户访问权限细粒度的控制； ▲8、访问控制支持基于角色用户机构的 RBAC 访问控制模型、基于用户属性客户端属性的 ABAC 访问控制模型、可修改超级管理员登录名基于 OB4LAC 的授权访问控制模型的功能。（提供由 CNAS 或 CMA 认证的			供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 6、支持高强度的传输链路加密功能，符合 GM/T 0024《SSL VPN 技术规范》； 7、基于角色授权，可将不同用户分配给不同角色，实现对不同用户访问权限细粒度的控制； 8、产品具有访问控制支持基于角色用户机构的 RBAC 访问控制模型、基于用户属性客户端属性的 ABAC 访问控制模型、可修改超级管理员登录名基于 OB4LAC 的授权访问控制模型的功能。（已提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 9、支持基于 NTLM、FORM、BASIC、CAS、OAuth2.0、OpenID 等方式和协议的单点登录功能。（已提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 10、高强度的传输链路加密，符合 GM/T 0024《SSL VPN 技术规范》； 11、支持常用的	

			第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲9、支持基于NTLM、FORM、BASIC、CAS、OAuth2.0、OpenID等方式和协议的单点登录功能。（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 10、高强度的传输链路加密，符合GM/T 0024《SSL VPN技术规范》； ▲11、支持常用的Radius/LDAP/AD第三方身份认证；支持PKI体系的第三方证书，支持OCSP、CRL、LDAP有效性校验。（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 12、遵循GM/T 0022《IPSec VPN技术规范》，支持与标准IPSec VPN产品的互联互通； 13、隧道支持主模式和快速模式、支持完全向前保密PFS、支持DPD协议探测隧道状			Radius/LDAP/AD第三方身份认证；支持PKI体系的第三方证书，支持OCSP、CRL、LDAP有效性校验。（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 12、遵循GM/T 0022《IPSec VPN技术规范》，支持与标准IPSec VPN产品的互联互通； 13、隧道支持主模式和快速模式、支持完全向前保密PFS、支持DPD协议探测隧道状态、支持隧道断线自动重建； 14、密钥交换协议支持ESP协议、支持隧道模式、支持NAT穿越和双向NAT穿越； 15、终端支持基于IP地址、MAC地址等终端硬件信息的用户绑定功能；支持终端用户登录后的网络隔离功能，支持基于组策略、用户策略、网络白名单策略的网络隔离功能。（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 16、终端支持实现对Windows7/10/11主流操作系统，麒麟、统信、深度	

			态、支持隧道断线自动重建； 14、密钥交换协议支持 ESP 协议、支持隧道模式、支持 NAT 穿越和双向 NAT 穿越； ▲15、终端支持基于 IP 地址、MAC 地址等终端硬件信息的用户绑定功能；支持终端用户登录后的网络隔离功能，支持基于组策略、用户策略、网络白名单策略的网络隔离功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 16、终端支持实现对 Windows7/10/11 主流操作系统，麒麟、统信、深度等国产操作系统，Android、iOS、鸿蒙等移动终端的支持。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲17、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； 18、支持多线路负载均衡、支持线路切			等国产操作系统，Android、iOS、鸿蒙等移动终端的支持。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 17、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； 18、支持多线路负载均衡、支持线路切换、线路流量负载和双机热备的功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 19、已提供 VPN 综合网关（综合安全网关）国家相关部门颁发的电信设备进网许可证复印件并加盖供应商公章。 四、具有国家密码管理局商用密码产品认证证书：符合国家密码管理局 GM/T 0023《IPSec VPN 网关产品规范、GM/T 0025《SSL VPN 网关产品规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中已提供有效的证书复印件加盖单位公章）	

			换、线路流量负载和双机热备的功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 19、需提供 VPN 综合网关（综合安全网关）国家相关部门颁发的电信设备进网许可证复印件并加盖供应商公章。 四、具有国家密码管理局商用密码产品认证证书：符合国家密码管理局 GM/T 0023《IPSec VPN 网关产品规范》、GM/T 0025《SSL VPN 网关产品规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）				
2	国密浏览器	100套	▲一、功能要求 1、支持 SM2、SM3、SM4 算法，与身份认证网关之间建立安全通道，保证 Web 网页访问的安全性。 2、支持第三方电子认证中心签发的数字证书； 3、可按应用设置	国密浏览器	100套	**我司完全响应，情况如下：** ▲一、功能配置 1、支持 SM2、SM3、SM4 算法，与身份认证网关之间建立安全通道，保证 Web 网页访问的安全性。 2、支持第三方电子认证中心签发的数字证书； 3、可按应用设置选用 Chrome 内核、IE 内核，并	正偏离

			选用 Chrome 内核、IE 内核，并可按应用设置 IE 内核版本，实现对现有业务系统的兼容性适配，支持 IE/Chrome 内核的自动切换与 Cookie 共享； 4、支持国密算法 SM2、SM3、SM4，在 Chrome 内核、IE 内核下均支持国密 SSL 协议； 5、支持 X86、ARM、MIPS 等架构国产 CPU。 二、具有国家密码管理局商用密码产品认证证书。（在响应文件中提供有效的证书复印件加盖单位公章）			可按应用设置 IE 内核版本，实现对现有业务系统的兼容性适配，支持 IE/Chrome 内核的自动切换与 Cookie 共享； 4、支持国密算法 SM2、SM3、SM4，在 Chrome 内核、IE 内核下均支持国密 SSL 协议； 5、支持 X86、ARM、MIPS 等架构国产 CPU。 **6、浏览器启动速度在 1.5 秒以内。** **HTML5 分数：520** **使用浏览器 JetStream 套件：70** **CSS3 测试分数：63%** **所有平台安装包不高于 70MB。** **均高于行业平均标准。** 二、具有国家密码管理局商用密码产品认证证书。（在响应文件中已提供有效的证书复印件加盖单位公章）	
3	密码机服务器	2 台	一、硬件规格： 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡	密码机服务器	2 台	**我司完全响应，情况如下：** 一、硬件规格配置： 1、标准 2U，国产多核处理器，16G 内存，480G 企业级固态硬盘，2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、供货产品内置密码卡与设备产品为同一厂	正偏离

			与设备产品为同一厂商，并提供密码卡商用密码产品认证证书； 二、性能要求： 1、SM2 密钥生成≥19900 对/秒，SM2 签名≥ 20620 次/秒，SM2 验签≥ 17000 次/秒，SM2 加密≥ 5700 次/秒，SM2 解密≥5940 次/秒，SM1 加解密≥740Mbps，SM4 加解密≥ 690Mbps，SM3 摘要≥ 1400Mbps，SM7 加解密≥ 320Mbps，SM9 密钥生成≥3000 对/秒，SM9 签名≥ 1500 次/秒，SM9 验签≥250 次/秒，SM9 加密≥ 1500 次/秒，SM9 解密≥350 次/秒； 三、功能要求 1、适用于各类密码安全应用系统，提供高速的、多任务并行处理的密码运算；可以满足应用系统数据的签名/验证、加密/解密的要求，保证传输信息的机密性、完整性和有效性；同时提供安全、完善的密钥管理机制。 ▲2、支持 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法；支持 ECC/RSA1024/RSA2048/RSA4096/SHA256/SHA384/SHA512/AES/3DES 等国际通用算法；			商，已提供密码卡商用密码产品认证证书； 二、性能配置： 1、SM2 密钥生成：21900 对/秒，SM2 签名：22640 次/秒，SM2 验签：12800 次/秒，SM2 加密：5000 次/秒，SM2 解密：6000 次/秒，SM1 加解密：790Mbps，SM4 加解密：820Mbps，SM3 摘要：1500Mbps，SM7 加解密：370Mbps，SM9 密钥生成：3500 对/秒，SM9 签名：2000 次/秒，SM9 验签：300 次/秒，SM9 加密：2000 次/秒，SM9 解密：390 次/秒； 三、功能配置 1、供货产品适用于各类密码安全应用系统，提供高速的、多任务并行处理的密码运算；可以满足应用系统数据的签名/验证、加密/解密的要求，保证传输信息的机密性、完整性和有效性；同时提供安全、完善的密钥管理机制。 ▲2、产品支持 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法；支持 ECC/RSA1024/RSA2048/RSA4096/SHA256/SHA384/SHA512/AES/3DES 等国际通用算法；支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；支持同态算法；（已提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件	

			支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；支持同态算法；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 3、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 4、密钥生成：密码机可提供各类型密钥对的生成功能； 5、支持 RSA 密钥管理、SM2 密钥管理、对称密钥管理、SM9 密钥管理等功能，并支持批量添加、删除密钥；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 6、杂凑密码运算：密码机可提供基于 SM3 算法的杂凑运算功能； 7、消息认证码的产生：密码机可提供基于 SM3 算法的 HMAC 的产生及验证； 8、随机数生成：密码机可提供基于双 WNG 物理随机源的随机数生成功能； 9、用户密钥对采用私钥授权码机制，使用时需要验证授权码，提高用户密钥使用的安全性；支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对；			并加盖供应商公章） 3、产品支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 4、产品具有密钥生成功能：密码机可提供各类型密钥对的生成功能； 5、支持 RSA 密钥管理、SM2 密钥管理、对称密钥管理、SM9 密钥管理等功能，并支持批量添加、删除密钥；（已提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 6、杂凑密码运算：密码机可提供基于 SM3 算法的杂凑运算功能； 7、消息认证码的产生：密码机可提供基于 SM3 算法的 HMAC 的产生及验证； 8、随机数生成：密码机可提供基于双 WNG 物理随机源的随机数生成功能； 9、用户密钥对采用私钥授权码机制，使用时需要验证授权码，提高用户密钥使用的安全性；支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对；（已提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 10、访问用户分级管理，包含超级管理员、系统管理员、安全管理员、审计管理员三权分立。不同管理员具有不同权限；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖	

			（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 10、访问用户分级管理，包含超级管理员、系统管理员、安全管理员、审计管理员三权分立。不同管理员具有不同权限；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 11、完善的密钥备份：采用门限密钥分割技术对密码机密钥进行备份，用于加密备份密钥的密钥被分割成多份子密钥，分别存在多个管理员的智能密码钥匙中。备份密钥是加密后存放到主机中，确保密钥的安全。恢复的时候需要半数以上管理员登录才可以将密钥恢复到服务器密码机内。 12、访问控制：提供服务白名单功能，实现白名单的添加查看删除；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 13、支持双机热备、负载均衡等高可用部署模式；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 14、标准接口：提			供应商公章） 11、完善的密钥备份：采用门限密钥分割技术对密码机密钥进行备份，用于加密备份密钥的密钥被分割成多份子密钥，分别存在多个管理员的智能密码钥匙中。备份密钥是加密后存放到主机中，确保密钥的安全。恢复的时候需要半数以上管理员登录才可以将密钥恢复到服务器密码机内。 12、访问控制：提供服务白名单功能，实现白名单的添加查看删除；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 13、支持双机热备、负载均衡等高可用部署模式；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 14、标准接口：提供 SDF、JCE 等国密、国际标准规范口； 15、网络协议：投标产品支持 IPV6，已提供 IPv6 Ready Logo 认证证书； 16、防止产品存在中、高风险漏洞，我方产品具有信息技术产品安全测试证书。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0030《服务器密码机技术规范》和 GM/T 0028《密码	

			供 SDF、JCE 等国密、国际标准规范口； 15、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； 16、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0030 《服务器密码机技术规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）			模块安全技术要求》第二级要求。（在响应文件中已提供有效的证书复印件加盖单位公章）	
4	国密堡垒机（安全运维服务器）	1台	一、硬件规格： 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，提供密码卡商用密码产品认证证书； 二、性能要求： 字符型协议并发会话数≥200，图形型协议并发会话数≥100，IP 管理资源授权	国密堡垒机（安全运维服务器）	1台	**我司完全响应，情况如下：** 一、硬件规格配置： 1、标准 2U，国产多核处理器，16G 内存，480G 企业级固态硬盘，2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，已提供密码卡商用密码产品认证证书； 二、性能配置： **字符型协议并发会话数：240，图形型协议并发会话数：160，IP 管理资源授权：160，IP 管理资源最大授权：230，加解密速率：**	正偏离

			≥100，IP管理资源最大授权≥200，加解密速率≥220Mbps，转发延迟＜0.2ms。 三、功能要求 1、通过集成数字证书强身份鉴别、国密协议安全隧道以及堡垒机模块功能为一体，满足“设备与计算安全”国密身份鉴别、访问控制、链路加密及敏感数据防护等安全要求。 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、强身份认证：支持基于国密数字证书的身份认证和登录功能，支持第三方 CA。 4、通信机密性：运维人员客户端与国密堡垒机之间采用国密算法加密通信链路进行数据的传输，保证通信数据的完整性和机密性。 5、存储机密性：对关键敏感数据采用国密算法进行加密存储，保证关键敏感信息的机密性。 6、单点登录：实			270Mbps，转发延迟：0.15ms。 三、功能配置 1、供货产品通过集成数字证书强身份鉴别、国密协议安全隧道以及堡垒机模块功能为一体，满足“设备与计算安全”国密身份鉴别、访问控制、链路加密及敏感数据防护等安全要求。 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、强身份认证：支持基于国密数字证书的身份认证和登录功能，支持第三方 CA。 4、通信机密性：运维人员客户端与国密堡垒机之间采用国密算法加密通信链路进行数据的传输，保证通信数据的完整性和机密性。 5、存储机密性：对关键敏感数据采用国密算法进行加密存储，保证关键敏感信息的机密性。 6、单点登录：实现与用户授权管理的无缝连接，可以通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。 7、集中账号管理：集	

			现与用户授权管理的无缝连接，可以通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控及审计。 7、集中账号管理：集中账号管理包含对所有服务器、网络设备账号的集中管理。账号和资源的集中管理是集中授权、认证和审计的基础。集中账号管理可以完成对账号整个生命周期的监控和管理，而且还降低了管理大量用户账号的难度和工作量。 8、资源授权：提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。 9、访问控制：能够提供细粒度的访问控制，最大限度保护用户资源的安全；对访问控制信息采用国密算			中账号管理包含对所有服务器、网络设备账号的集中管理。账号和资源的集中管理是集中授权、认证和审计的基础。集中账号管理可以完成对账号整个生命周期的监控和管理，而且还降低了管理大量用户账号的难度和工作量。 8、资源授权：提供统一的界面，对用户、角色及行为和资源进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。通过集中访问授权和访问控制可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。 9、访问控制：能够提供细粒度的访问控制，最大限度保护用户资源的安全；对访问控制信息采用国密算法进行数字签名，以保证数据完整性，防止数据被篡改，保证系统的安全性。 10、协议管理：支持字符型（SSH、Telnet）、图形（RDP、VNC）、数据库（Oracle、Sybase、MySQL、SQLServer、DB2 等）、文件传输（FTP、SFTP）、http、https 等多种协议类型；	

			法进行数字签名，以保证数据完整性，防止数据被篡改，保证系统的安全性。 10、协议管理：支持字符型（SSH、Telnet）、图形(RDP、VNC)、数据库(Oracle、Sybase、MySQL、SQLServer、DB2等)、文件传输(FTP、SFTP)、http、https等多种协议类型； 11、支持基于管理代理的机制，安装在被管设备上，实现了运维服务器和被管设备之间的有效身份鉴别，并建立安全的加密信息传输通道。 12、操作审计：对访问日志信息采用国密算法进行数字签名，以保证数据完整性，防止数据被篡改。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）			11、支持基于管理代理的机制，安装在被管设备上，实现了运维服务器和被管设备之间的有效身份鉴别，并建立安全的加密信息传输通道。 12、操作审计：对访问日志信息采用国密算法进行数字签名，以保证数据完整性，防止数据被篡改。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中已提供有效的证书复印件加盖单位公章）	
5	密码	1套	一、硬件规格： 1、标准2U，国产	密码服	1套	**我司完全响应，情况如下：** 一、硬件规格：	正偏离

	服务平台		多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口，触摸液晶屏，冗余电源； 二、功能要求 1、算法支持：支持国密 SM1、SM2、SM3、SM4、SM9 算法； 2、密码服务平台证书综合管理应包含 CA 配置、数量授权、证书管理、数量统计、存储介质管理等功能（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 3、密码服务平台密码资源管理应包含密码设备管理、宿主机管理、虚拟资源管理、镜像管理、密码服务等功能（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 4、实现对密码设备资源的统一管理，包括签名服务器、密码机、云密码机、网关、电子签章服务器、时间戳服务器、手机盾服务器的增删改查。（提供	务平台		1、标准 2U，国产多核处理器，16G 内存，480G 企业级固态硬盘，2 个千兆网口，触摸液晶屏，冗余电源； 二、功能要求 1、算法支持：支持国密 SM1、SM2、SM3、SM4、SM9 算法； 2、密码服务平台证书综合管理应包含 CA 配置、数量授权、证书管理、数量统计、存储介质管理等功能 （提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 3、密码服务平台密码资源管理应包含密码设备管理、宿主机管理、虚拟资源管理、镜像管理、密码服务等功能（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 4、供货产品实现对密码设备资源的统一管理，包括签名服务器、密码机、云密码机、网关、电子签章服务器、时间戳服务器、手机盾服务器的增删改查。（已提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）；	

			由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 5、支持数字证书服务、密钥管理服务、签名验签服务、时间戳服务、电子签章服务、数据加解密服务、协同签名运算服务、数据链路加解密服务。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 6、密码服务平台身份认证功能应包含资源管理、角色管理授权管理功能（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 7、密码服务平台应用管理功能应包含应用接入管理和应用访问授权功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 8、支持第三方 CA 接入，实现数字证书全生命周期管理，包括个人数字证书、服务器证			5、支持数字证书服务、密钥管理服务、签名验签服务、时间戳服务、电子签章服务、数据加解密服务、协同签名运算服务、数据链路加解密服务。（已提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 6、密码服务平台身份认证功能应包含资源管理、角色管理授权管理功能（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 7、密码服务平台应用管理功能应包含应用接入管理和应用访问授权功能。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 8、支持第三方 CA 接入，实现数字证书全生命周期管理，包括个人数字证书、服务器证书的申请、更新、下载、注销等； 9、支持用户统一管理，能够在平台系统中对电子签章系统用户、移动互联网密码服务系统用户进行统一管理，包括用户的注册、修改、删除、查	

			书的申请、更新、下载、注销等； 9、支持用户统一管理，能够在平台系统中对电子签章系统用户、移动互联网密码服务系统用户进行统一管理，包括用户的注册、修改、删除、查看； 10、支持对平台和密码设备资源的网络拓扑图自动生成功能； 11、对密码设备监控信息应包括：CPU 使用率、内存使用率、硬盘等； 12、支持日志审计、监控日志、归档日志等功能； 13、支持双主机热备部署。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）			看； 10、支持对平台和密码设备资源的网络拓扑图自动生成功能； 11、对密码设备监控信息应包括：CPU 使用率、内存使用率、硬盘等； 12、支持日志审计、监控日志、归档日志等功能； 13、支持双主机热备部署。 **14、产品具有中国软件评测中心软件产品测试证书；** **15、产品具有国产数据库兼容性证明；** 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中已提供有效的证书复印件加盖单位公章）	
6	签名验签服	2套	一、硬件规格： 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网	签名验签服	2套	**我司完全响应，情况如下：** 一、硬件规格： 1、标准 2U，国产多核处理器，16G 内存，480G 企业级固态硬盘，2 个千兆	正偏离

	务器		口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，提供密码卡商用密码产品认证证书； 二、性能要求 SM2 密钥生成≥19860 对/秒，SM2 签名≥ 20400 次/秒，SM2 验签≥14370 次/秒，SM2 加密≥ 4680 次/秒，SM2 解密≥6640 次/秒，SM1 加解密≥643Mbps，SM4 加解密≥ 564Mbps，SM3 摘要≥1118Mbps； 三、功能要求 1、支持身份认证、数据签名、签名验证、数据加密/解密等功能。 ▲2、支持 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法；支持 ECC/RSA1024/RSA2048/RSA4096/SHA256/SHA384/SHA512/AES 等国际通用算法；支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测	务器		网口（支持扩展光口），触摸液晶屏，冗余电源； 2、内置密码卡与设备产品为同一厂商，已提供密码卡商用密码产品认证证书； 二、性能配置： **SM2 密钥生成：20000 对/秒，SM2 签名：22000 次/秒，SM2 验签：14880 次/秒，SM2 加密：5000 次/秒，SM2 解密：6720 次/秒，SM1 加解密：678Mbps，SM4 加解密：599Mbps，SM3 摘要：1200Mbps；** 三、功能要求 1、支持身份认证、数据签名、签名验证、数据加密/解密等功能。 2、支持 SM1/SM2/SM3/SM4/SM7/SM9/ZUC 国产密码算法；支持 ECC/RSA1024/RSA2048/RSA4096/SHA256/SHA384/SHA512/AES 等国际通用算法；支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；（已提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 3、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 ▲4、支持 PKCS#1/PK	

			试报告的复印件并加盖供应商公章） 3、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 ▲4、支持对PKCS#1/PKCS#7(attached 和 detached)/XML 的签名验签；支持二维码、条形码的签名处理；支持基于 SM2、RSA 等算法的数字信封加密、解密功能；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲5、用户密钥对采用私钥授权码机制，使用时需要验证授权码，提高用户密钥使用的安全性；支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲6、支持服务信息功能，实现查看服务状态，系统状态，系统自检，更改服务端口，			CS#7(attached 和 detached)/XML 的签名验签；支持二维码、条形码的签名处理；支持基于 SM2、RSA 等算法的数字信封加密、解密功能；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 5、用户密钥对采用私钥授权码机制，使用时需要验证授权码，提高用户密钥使用的安全性；支持密钥批处理功能，通过设置密钥号起止位置等信息，批量生成或删除密钥对；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 6、支持服务信息功能，实现查看服务状态，系统状态，系统自检，更改服务端口，是否加密通信，服务的启动停止；支持服务测试功能，实现对签名验签，数字信封等服务功能的测试；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 7、支持应用管理功能，可管理调用签名验签服务的应用系统，包括应	

			是否加密通信，服务的启动停止；支持服务测试功能，实现对签名验签，数字信封等服务功能的测试；（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲7、支持应用管理功能，可管理调用签名验签服务的应用系统，包括应用的添加、删除、修改、关联证书链等功能；支持服务白名单功能，实现白名单的添加查看删除，通过连接白名单的支持，实现签名验签服务器对应用服务器的授权认证；（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲8、支持RSA密钥管理、SM2密钥管理、对称密钥管理、受信赖根证书、证书撤销列表、业务证书等管理功能；（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）			用的添加、删除、修改、关联证书链等功能；支持服务白名单功能，实现白名单的添加查看删除，通过连接白名单的支持，实现签名验签服务器对应用服务器的授权认证；（已提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲8、支持RSA密钥管理、SM2密钥管理、对称密钥管理、受信赖根证书、证书撤销列表、业务证书等管理功能；（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲9、证书管理和验证、数字签名和验证等核心功能，要求符合《信息安全技术签名验签服务器技术规范GB/T 38629 -2020》；（提供第三方检测报告复印件并加盖供应商公章佐证） 10、支持标准X509V3数字证书格式，支持签名证书和加密证书的双证书认证体系，提供CRL/OCSP/LDAP等多种方式的证书有效性验证； **11、支持最大550M大**	

			▲9、证书管理和验证、数字签名和验证等核心功能，要求符合《信息安全技术签名验签服务器技术规范 GB/T 38629 -2020》（提供第三方检测报告复印件并加盖供应商公章佐证）； 10、支持标准X509V3数字证书格式，支持签名证书和加密证书的双证书认证体系，提供CRL/OCSP/LDAP等多种方式的证书有效性验证； 11、支持最大500M大文件、大数据的数字签名和数字信封功能； 12、可同时配置多条证书链，验证不同CA的用户证书；可同时支持20个不同的CA； 13、提供CRL的自动下载功能和证书有效性验证功能； 14、提供证书解析功能，获取证书中的任意主题信息以及扩展项信息； 15、基于WEB形式的图形管理界面，提供完善的配置管理、证书管理、服务管理等功			**文件、大数据的数字签名和数字信封功能；** 12、可同时配置多条证书链，验证不同CA的用户证书；可同时支持20个不同的CA； 13、提供CRL的自动下载功能和证书有效性验证功能； 14、提供证书解析功能，获取证书中的任意主题信息以及扩展项信息； 15、基于WEB形式的图形管理界面，提供完善的配置管理、证书管理、服务管理等功能； 16、具有日志审计功能，支持第三方SYSLOG日志服务器； 17、支持浏览器、应用服务器、移动端的调用； 18、网络协议：支持IPV6，已提供IPv6 Ready Logo认证证书； 19、防止产品存在中、高风险漏洞，投标产品具有信息技术产品安全测试证书； 20、提供JAVA、C++等API开发接口和示例代码； 21、支持双主机热备部署。 四、具有国家密码管理局商用密码产品认证证书；	

			能： 16、具有日志审计功能，支持第三方 SYSLOG 日志服务器； 17、支持浏览器、应用服务器、移动端调用； 18、网络协议：支持 IPV6，提供 IPV6 Ready Logo 认证证书； 19、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书； 20、提供 JAVA、C++等 API 开发接口和示例代码； 21、支持双主机热备部署。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0029《签名验签服务器技术规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）			符合国家密码管理局 GM/T 0029《签名验签服务器技术规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中已提供有效的证书复印件加盖单位公章）	
7	电子签章系统	1台	一、硬件规格： 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），	电子签章系统	1台	**我司完全响应，情况如下：** 一、硬件规格配置： 1、标准 2U，国产多核处理器，16G 内存，480G 企业级固态硬盘，2 个千兆网口（支持扩展光口），	正偏离

			触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书； 二、功能要求 1、支持国产系列算法；可提供电子签章的管理和服务、印章制作、客户端签章工具，是基于智能密码钥匙开发的一套用于保证MicrosoftWord/Excel电子文档、PDF文档以及Web网页的完整性、防篡改性和不可抵赖性的安全应用软件，主要采用了PKI中的数字签名技术来实现对Microsoft Office Word文档、Excel电子表格、PDF文档、Web网页的安全性保护； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、支持对PDF格式的文档进行电子签章，并且在电子文档上显示签章图片； 4、支持指定位置盖章、指定位置签名图片盖章、指定位置审批			触摸液晶屏，冗余电源； 2、投标产品内置密码卡与设备产品为同一厂商，并已提供密码卡商用密码产品认证证书； 二、功能配置 1、支持国产系列算法；可提供电子签章的管理和服务、印章制作、客户端签章工具，是基于智能密码钥匙开发的一套用于保证MicrosoftWord/Excel电子文档、PDF文档以及Web网页的完整性、防篡改性和不可抵赖性的安全应用软件，主要采用了PKI中的数字签名技术来实现对Microsoft Office Word文档、Excel电子表格、PDF文档、Web网页的安全性保护； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、支持对PDF格式的文档进行电子签章，并且在电子文档上显示签章图片； 4、支持指定位置盖章、指定位置签名图片盖章、指定位置审批意见盖章、单个签章验证、文档中所有签章验证； 5、支持管理员、审计	

			意见盖章、单个签章验证、文档中所有签章验证； 5、支持管理员、审计员操作，能够对用户进行统一管理、监督，包含整个生命周期管理及电子印章的制作、挂失、解挂、停用等管理； 6、支持骑缝章，提供三个骑缝章位置以供选择； 7、支持对PDF文档签章、验证、统计文档页数、统计签章个数、获取文档数据、打印文档等功能； 8、支持移动端电子签章功能，支持移动端手写签名采集功能； 9、支持在文档中添加时间戳，保证文档行为时间的有效性和合法性； 10、支持在文档中添加图片、文字水印； 11、支持多人对文档的会签； 12、支持文档打开时自动对文档内的所有印章进行验证功能； 13、支持文档安全控制，可设置文档保护限制；			员操作，能够对用户进行统一管理、监督，包含整个生命周期管理及电子印章的制作、挂失、解挂、停用等管理； 6、支持骑缝章，提供三个骑缝章位置以供选择； 7、支持对PDF文档签章、验证、统计文档页数、统计签章个数、获取文档数据、打印文档等功能； 8、支持移动端电子签章功能，支持移动端手写签名采集功能； 9、支持在文档中添加时间戳，保证文档行为时间的有效性和合法性； 10、支持在文档中添加图片、文字水印； 11、支持多人对文档的会签； 12、支持文档打开时自动对文档内的所有印章进行验证功能； 13、支持文档安全控制，可设置文档保护限制； ▲14、支持对Word/Excel格式的文档进行电子签章；（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲15、支持身份鉴别、	

			▲14、支持对Word/Excel格式的文档进行电子签章；（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； ▲15、支持身份鉴别、访问控制、剩余信息保护等自身安全功能；（提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 16、支持安全的集中式签章，避免印章被冒用，防止数据泄露； 17、支持文档样式保护的签验章，对文字样式快速解析，加快文档验章和签章的速度。 三、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局GM/T 0031《安全电子签章密码技术规范》。（在响应文件中提供有效的证书复印件加盖单位公章）			访问控制、剩余信息保护等自身安全功能；（已提供由CNAS或CMA认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 16、支持安全的集中式签章，避免印章被冒用，防止数据泄露； 17、支持文档样式保护的签验章，对文字样式快速解析，加快文档验章和签章的速度。 **18、投标产品具有国产化适配能力，具有国产数据库兼容性证明、华为鲲鹏技术认证、飞腾产品兼容性证明、麒麟软件NeoCertify认证和海光处理器产品兼容性认证；** 三、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局GM/T 0031《安全电子签章密码技术规范》。（在响应文件中已提供有效的证书复印件加盖单位公章）	
8	数字证书	1台	一、硬件规格： 1、标准2U，国产多核处理器，≥16G内存，≥480G企业级固	数字证书	1台	一、硬件规格配置： 1、标准2U，采用国产多核处理器，16G内存，480G企业级固态硬盘，2	正偏离

	管理系统		态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书。 二、性能要求： 证书最大数量：20000 三、功能要求 1、支持国际通用算法和国产 SM 系列算法；提供数字证书整个生命周期的过程管理功能。包括用户注册管理、证书/证书注销列表的生成与签发、证书/证书注销列表的存储与发布、证书状态的查询、密钥的生成与管理、过程安全审计等； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、支持证书新办、更新、吊销、挂起、解挂和证书黑名单等证书全生命周期管理； 4、支持多种证书类型模版，个人证书、机构证书、设备证书等；	管理系统		个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； 2、投标产品内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书。 二、性能配置： **证书最大数量：21050** 三、功能要求 1、支持国际通用算法和国产 SM 系列算法；提供数字证书整个生命周期的过程管理功能。包括用户注册管理、证书/证书注销列表的生成与签发、证书/证书注销列表的存储与发布、证书状态的查询、密钥的生成与管理、过程安全审计等； 2、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等。 3、支持证书新办、更新、吊销、挂起、解挂和证书黑名单等证书全生命周期管理； 4、支持多种证书类型模版，个人证书、机构证书、设备证书等； 5、支持证书模板自定义配置，支持国家标准规定的私有扩展及自定义扩展； 6、证书符合国际标准	

			5、支持证书模板自定义配置，支持国家标准规定的私有扩展及自定义扩展； 6、证书符合国际标准 X509 V3 标准； 7、支持产生证书黑名单，包括：定时自动产生、手动实时产生，规范符合 X509 V2 标准； 8、支持手工录入、批量导入、三方应用授权集成等方式注册证书，并为用户签发数字证书； 9、支持证书签发模块、证书注册模块、系统配置模块分权管理模式； ▲10、模版管理包括证书模板管理、证书撤销列表模板管理、在线证书状态协议模板等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》（增强级）相关要求。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲11、密钥管理包			X509 V3 标准； 7、支持产生证书黑名单，包括：定时自动产生、手动实时产生，规范符合 X509 V2 标准； 8、支持手工录入、批量导入、三方应用授权集成等方式注册证书，并为用户签发数字证书； 9、支持证书签发模块、证书注册模块、系统配置模块分权管理模式； ▲10、模版管理包括证书模板管理、证书撤销列表模板管理、在线证书状态协议模板等，符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》（增强级）相关要求。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲11、密钥管理包含密钥生成、密钥存储、密钥传送与分发、密钥导入导出、密钥使用、密钥备份、密钥恢复、密钥归档、密钥销毁、密钥更新等，符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》（增强级）相关要求。（提供由 CNAS 或 CMA 认证的第三	

			含密钥生成、密钥存储、密钥传送与分发、密钥导入导出、密钥使用、密钥备份、密钥恢复、密钥归档、密钥销毁、密钥更新等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》(增强级)相关要求。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） ▲12、证书管理包含证书注册、证书生成、证书撤销、证书更新、证书变更等，须符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》(增强级)相关要求。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 13、可提供证书黑名单、Ldap、OCSP 等方式数字证书身份认证服务； 14、提供基于证书的签名/验证、加密/解密等功能组件；			方检测机构出具的测试报告的复印件并加盖供应商公章） ▲12、证书管理包含证书注册、证书生成、证书撤销、证书更新、证书变更等，符合 GB/T 21053-2023《信息安全技术公钥基础设施 PKI 系统安全技术要求》（增强级）相关要求。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章） 13、可提供证书黑名单、Ldap、OCSP 等方式数字证书身份认证服务； 14、提供基于证书的签名/验证、加密/解密等功能组件； 15、密钥独立管理体系，支持密钥自动监控、产生、分发的智能监管系统； 16、支持管理权限划分，各系统按权操作，多系统分责管理，管理员身份可鉴别； 17、支持多级 CA 部署模式； 18、支持系统管理员操作日志审查，支持操作员签名审查； 19、支持多厂家普通、蓝牙、指纹等智能 UsbKey	

			15、密钥独立管理体系，支持密钥自动监控、产生、分发的智能监管系统； 16、支持管理权限划分，各系统权限独立操作，多系统集中管理，管理员身份可识别； 17、支持多级 CA 部署模式； 18、支持系统管理员操作日志审查，支持操作员签名审查； 19、支持多厂家普通、蓝牙、指纹等智能 UsbKey 钥匙的无缝接入； ▲20、可以添加证书扩展，可以对证书扩展列表进行管理，包括修改、删除、查看查找等；可以新增证书模板，可以对证书模板进行管理，包括查看详情、删除、查看查找等（提供第三方测试报告复印件并加盖供应商公章） ▲21、可以查看日志信息，包括日志类型、客户端地址、操作者编号等；可以通过日志类型、客户端地址、操作者编号等查找日志审计列表，列表包括			钥匙的无缝接入； ▲20、可以添加证书扩展，可以对证书扩展列表进行管理，包括修改、删除、查看查找等；可以新增证书模板，可以对证书模板进行管理，包括查看详情、删除、查看查找等（提供第三方测试报告复印件并加盖供应商公章） ▲21、可以查看日志信息，包括日志类型、客户端地址、操作者编号等；可以通过日志类型、客户端地址、操作者编号等查找日志审计列表，列表包括内容、操作结果、操作时间等；（提供第三方测试报告复印件并加盖供应商公章）。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0034 《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》。（在响应文件中提供有效的证书复印件加盖单位公章）	

			日志内容、操作结果、操作时间等；（提供第三方测试报告复印件并加盖供应商公章）。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局《GM/T 0034-2014 《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》。（在响应文件中提供有效的证书复印件加盖单位公章）				
9	手机盾协同签名系统	1台	一、硬件规格： 1、标准 2U，国产多核处理器，≥16G 内存，≥480G 企业级固态硬盘，≥2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书。 三、功能要求 1、算法支持：支持国密 SM2、SM3、SM4 算法； 2、密钥管理：用户密钥客户端片段生成、安全存储及销毁； 3、证书管理：集成身份认证系统（CA），支持证书在线申请、更新、注销等数字证书全生命周期	手机盾协同签名系统	1台	**我司完全响应，情况如下：** 一、硬件规格配置： 1、标准 2U，国产多核处理器，16G 内存，480G 企业级固态硬盘，2 个千兆网口（支持扩展光口），触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并已提供密码卡商用密码产品认证证书。 三、功能要求 1、算法支持：支持国密 SM2、SM3、SM4 算法； 2、密钥管理：用户密钥客户端片段生成、安全存储及销毁； 3、证书管理：集成身份认证系统（CA），支持证书在线申请、更新、注销等数字证书全生命周期	正偏离

			支持证书在线申请、更新、注销等数字证书全生命周期管理，支持第三方 CA 认证机构； 4、扫码签名：支持扫描二维码实现数字签名； 5、推送签名：支持业务系统通过密码服务系统服务端推送签名请求到移动端，实现数字签名； ▲6、支持获取二维码、推送签名消息、获取签名值、验证签名等功能； 7、支持摘要运算、非对称加解密和对称加解密运算； 8、支持口令和指纹认证方式； ▲9、用户私钥拆分成两部分密钥因子，一部分在手机端，一部分在服务端，保证移动端密钥的安全； ▲10、协同签名：支持与客户端配合，协同实现数字签名； ▲11、系统及服务监控：能够对系统服务进行监控，授权查看设备运行状态； 12、用户管理：对移动终端账户进行管			管理，支持第三方 CA 认证机构； 4、扫码签名：支持扫描二维码实现数字签名； 5、推送签名：支持业务系统通过密码服务系统服务端推送签名请求到移动端，实现数字签名； ▲6、支持获取二维码、推送签名消息、获取签名值、验证签名等功能； 7、支持摘要运算、非对称加解密和对称加解密运算； 8、供货产品支持口令和指纹认证方式； ▲9、用户私钥拆分成两部分密钥因子，一部分在手机端，一部分在服务端，保证移动端密钥的安全； ▲10、协同签名：支持与客户端配合，协同实现数字签名； ▲11、系统及服务监控：能够对系统服务进行监控，授权查看设备运行状态； 12、用户管理：对移动终端账户进行管理、统计、查询。维护账户状态，存储账户对应的设备公钥信息等； 13、管理员管理：对系统操作的管理员进行添	

			理、统计、查询。维护账户状态，存储账户对应的设备公钥信息等； 13、管理员管理：对系统操作的管理员进行添加、删除、修改以及授权，只有授权管理员才能登陆系统进行操作； 14 、支持Android4.4.2 、IOS9及以上以上手机系统； ▲15、安全审计：能够对系统所有的操作和接口调用进行详细的记录，非授权人员不可篡改记录； 16、防止产品存在中、高风险漏洞，须具有信息技术产品安全测试证书； 17、提供SDK开发接口，支持移动端APP、微信公众号/小程序，支持免安装方式与移动端应用APP进行集成； 18、支持双主机热备部署。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文			加、删除、修改以及授权，只有授权管理员才能登陆系统进行操作； 14 、支持Android4.4.2 、IOS9及以上以上手机系统； ▲15、安全审计：能够对系统所有的操作和接口调用进行详细的记录，非授权人员不可篡改记录； 16、防止产品存在中、高风险漏洞，投标产品具有信息技术产品安全测试证书； 17、我方提供SDK开发接口，支持移动端APP、微信公众号/小程序，支持免安装方式与移动端应用APP进行集成； 18、支持双主机热备部署。 **19、产品具有国产化适配能力，具有国产数据库兼容性证明、华为鲲鹏技术认证、飞腾产品兼容性证明和海光处理器产品兼容性认证；** 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中已提供有效的证书复印件加盖单位公	

			件中提供有效的证书复印件加盖单位公章）			章）	
10	时间戳服务器	1套	一、硬件规格： 1、标准2U，国产多核处理器，≥16G内存，≥480G企业级固态硬盘，≥2个千兆网口（支持扩展光口），时间源卡，触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并提供密码卡商用密码产品认证证书； ▲3、设备内置时间源卡，时间源卡与整机为同一厂商、同一品牌。 二、性能要求： SM2时间戳签发≥15080次/秒，SM2时间戳验证≥8421次/秒。 三、功能要求 1、产品支持时间戳签发，验证时间戳，支持NTP协议，支持第三方CA证书，支持CDMA、GPS、北斗卫星授时； ▲2、支持SM1/SM2/SM3/SM4/SM7/SM9/ZUC国产密码算法；支持ECC/RSA1024/RSA2048	时间戳服务器	1套	**我司完全响应，情况如下：** 一、硬件规格配置： 1、标准2U，国产多核处理器，16G内存，480G企业级固态硬盘，2个千兆网口（支持扩展光口），时间源卡，触摸液晶屏，冗余电源； ▲2、内置密码卡与设备产品为同一厂商，并已提供密码卡商用密码产品认证证书； ▲3、设备内置时间源卡，时间源卡与整机为同一厂商、同一品牌。已提供著作权证明材料。 二、性能配置： **SM2时间戳签发：15430次/秒，SM2时间戳验证：8550次/秒。** 四、功能配置 1、产品支持时间戳签发，验证时间戳，支持NTP协议，支持第三方CA证书，支持CDMA、GPS、北斗卫星授时； ▲2、支持SM1/SM2/SM3/SM4/SM7/SM9/ZUC国产密码算法；支持ECC/RSA1024/RSA2048/RSA4096/SHA256/SHA384/SHA512/AES/3DES等国际通用算法；支持	正偏离

			/RSA4096/SHA256/SHA384/SHA512/AES/3DES 等国际通用算法；支持 kyber、Dilithium、SPHINCS+等国际标准抗量子算法；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 3、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等； 4、提供时间戳的签发和验证功能；支持验证时间戳信息的有效性、签名证书的有效性等内容； 5、提供获取时间戳信息功能，支持获取时间戳的时间、数据信息、消息摘要算法等； 6、时间设置支持 NTP、SNTP 方式，支持时间源卡方式，时间源卡可从 BD、GPS 以及 4G 信号方式同步时间。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 7、内置权威时间			kyber 、 Dilithium 、 SPHINCS+等国际标准抗量子算法；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 3、支持信创环境部署，包括国产化芯片平台、操作系统、数据库等； 4、提供时间戳的签发和验证功能；支持验证时间戳信息的有效性、签名证书的有效性等内容； 5、提供获取时间戳信息功能，支持获取时间戳的时间、数据信息、消息摘要算法等； 6、时间设置支持 NTP、SNTP 方式，支持时间源卡方式，时间源卡可从 BD、GPS 以及 4G 信号方式同步时间。（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 7、内置权威时间源卡，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检测，时间源卡精度小于 1us（已提供国家授时中心检测证明材料）；◆ 8、支持可信时间发布功能； 9、支持时间戳证书管	

			源卡，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检测，时间源卡精度小于 1us（提供国家授时中心检测证明材料）； 8、支持时间发布功能； 9、支持时间戳证书管理功能，实现时间戳证书的申请，导入，查看，导出等操作；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 10、支持时间戳检索功能，对已签发的时间戳进行查看、查找、删除、销毁；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 11、支持时间戳归档，将已签发时间戳进行归档整理；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 12、具有日志审计功能，支持第三方			理功能，实现时间戳证书的申请，导入，查看，导出等操作；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 10、支持时间戳检索功能，对已签发的时间戳进行查看、查找、删除、销毁；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 11、支持时间戳归档，将已签发时间戳进行归档整理；（提供由 CNAS 或 CMA 认证的第三方检测机构出具的测试报告的复印件并加盖供应商公章）； 12、具有日志审计功能，支持第三方 SYSLOG 日志服务器； 13、支持双机热备、负载均衡； ▲14、网络协议：支持 IPV6，已提供 IPv6 Ready Logo 认证证书； 15、防止产品存在中、高风险漏洞，具有信息技术产品安全测试证书； 16、客户端提供 API 接口，包括 C 接口、C#接口、Java 接口，支持定制接口开发。标准 2U 机架式服务器；工业触摸液晶屏。	

			SYSLOG 日志服务器； 13、支持双机热备、负载均衡； ▲14、网络协议：支持 IPV6，提供 IPv6 Ready Logo 认证证书； 15、防止[illegible]存在中、高风险漏洞，须具有信息技术产品安全测试证书； 16、客户端提供 API 接口，包括 C 接口、C#接口、Java 接口，支持定制接口开发。标准 2U 机架式服务器：工业触摸液晶屏。 四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0033《时间戳接口规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）			四、具有国家密码管理局商用密码产品认证证书；符合国家密码管理局 GM/T 0033《时间戳接口规范》和 GM/T 0028《密码模块安全技术要求》第二级要求。（在响应文件中提供有效的证书复印件加盖单位公章）	
11	SDK 接口（商用密码）	1 项	1、密码设备对医院应用系统做接口改造服务； 2、实施项目经理需具备电子信息专业高级职称证书及防爆电气设备安装、检修、维护技术培训证书； 3、实施人员至少	SDK 接口（商用密码）	1 项	**我司完全响应，情况如下：** 1、我方提供密码设备对医院应用系统做接口改造服务； 2、本项目中，我方提供的实施项目经理具备电子信息专业高级职称证书及防爆电气设备安装、检修、维护技术培训证书；	无偏离

	应用业务流程和开发流程设计服务）		有一人省市级密码管理局公示商用密码应用专家(官方网站截图证明及密码管理局公示的官方网站链接)提供有效证明文件复印件加盖单位公章。	应用业务流程和开发流程设计服务）		3、本项目中，我方提供的实施人员有一人具有省市级密码管理局公示商用密码应用专家(官方网站截图证明及密码管理局公示的官方网站链接)已提供有效证明文件复印件加盖单位公章。	
12	系统调用接口服务（系统密码应用开发改造服务	1项	医院业务系统为满足三级密码评测需要做业务流程改造适应密码设备的应用。包括不限于（HIS、EMR、集成平台、数据中心、PACS、LIS、B超、心电、内镜等系统，以医院等保备案系统为准）。	系统调用接口服务（系统密码应用开发改造服务	1项	**我司完全响应，情况如下：** 我方配合医院业务系统为满足三级密码评测做业务流程改造适应密码设备的应用。包括不限于（HIS、EMR、集成平台、数据中心、PACS、LIS、B超、心电、内镜等系统，以医院等保备案系统为准）。	无偏离

	）			）			
13	CA证书（个人数字证书）	1200张	第三方CA机构颁发的个人数字证书。	CA证书（个人数字证书）	1套	**我司完全响应，情况如下：** 第三方CA机构颁发的个人数字证书。	无偏离
14	国产门禁系统（国密电子门禁系统）	1套	一、功能要求 1、系统包含门禁管理系统、门禁日志审计系统和密钥管理系统等软件系统； 2、门禁用户身份鉴别：使用用户CPU卡和国密门禁读卡器，采用基于SM1/SM4的对称加解密技术，实现用户身份鉴别； 3、门禁日志记录完整性保护：采用基于SM3的HMAC技术，实现日志记录的完整性保护； 4、密钥注入和发卡设备物理分离：支持二者物理分离，采用密钥注入器进行密钥注入，采用发卡器进行发卡。 二、具有国家密码管理局颁发的商密认证证	国产门禁系统（国密电子门禁系统）	1套	**我司完全响应，情况如下：** 一、功能配置 1、系统包含门禁管理系统、门禁日志审计系统和密钥管理系统等软件系统； 2、门禁用户身份鉴别：使PU用用户C卡和国密门禁读卡器，采用基于SM1/SM4的对称加解密技术，实现用户身份鉴别； 3、门禁日志记录完整性保护：采用基于SM3的HMAC技术，实现日志记录的完整性保护； 4、密钥注入和发卡设备物理分离：支持二者物理分离，采用密钥注入器进行密钥注入，采用发卡器进行发卡。 **5、门禁日志记录篡改报警提示：支持门禁日志记录篡改报警提示。** **6、在密钥分散过程**	正偏离

			书。（在响应文件中提供有效的证书复印件加盖单位公章）			**中，支持国密算法配置，具有技术先进性。** 二、具有国家密码管理局颁发的商密认证证书。（在响应文件中提供有效的证书复印件加盖单位公章）	
15	国产监控系统（国密视频监控系统）	1套	一、功能要求 1、音像记录数据机密性保护：使用国密摄像机和国密NVR，采用基于SM4的对称加解密技术，实现音像记录数据的机密性保护； 2、音像记录数据完整性保护：使用国密NVR以及PCI-E密码卡（配合视频加密系统软件），采用基于SM3的HMAC技术，实现音像记录数据的完整性保护。 二、具有国家密码管理局颁发的商密认证证书。（在响应文件中提供有效的证书复印件加盖单位公章）	国产监控系统（国密视频监控系统）	1套	**我司完全响应，情况如下：** 一、功能配置 1、音像记录数据机密性保护：使用国密摄像机和国密NVR，采用基于SM4的对称加解密技术，实现音像记录数据的机密性保护； 2、音像记录数据完整性保护：使用国密NVR以及PCI-E密码卡(配合视频加密系统软件)，采用基于SM3的HMAC技术，实现音像记录数据的完整性保护。 **3、支持密评取证，支持通过网络抓包的方式对签名字段进行签名验证；** **4、支持视频记录篡改报警提示，具有技术先进性。** 二、具有国家密码管理局颁发的商密认证证书。（在响应文件中提供有效的证书复印件加盖单位公章）	正偏离
16	商用密	1次	依据《中华人民共和国密码法》、《中华人民共和国网络安全	商用密	1次	**我司完全响应，情况如下：** 依据《中华人民共和国密码法》、《中华人民共	无偏离

	码应用安全性评估服务		法》、《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）、《信息系统密码测评要求》（试行）等国家行业现行有效的标准、规范对被测系统进行商用密码应用安全性评估，信息系统的《密码应用安全性评估报告》须取得“基本符合”或以上评估结论，并完成密码应用方案商用密码应用安全性评估报告和被测系统商用密码应用安全性评估报告在密码管理局密评的备案工作。	码应用安全性评估服务		和国网络安全法》、《信息安全技术信息系统密码应用基本要求》（GB/T 39786-2021）、《信息系统密码测评要求》（试行）等国家行业现行有效的标准、规范对被测系统进行商用密码应用安全性评估，信息系统的《密码应用安全性评估报告》须取得“基本符合”或以上评估结论，并完成密码应用方案商用密码应用安全性评估报告和被测系统商用密码应用安全性评估报告在密码管理局密评的备案工作。	
17	商用密码应用咨询服务（密码应用方案	1次	根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，系统达到第三级密码应用基本要求，针对被测系统从方案制定和评审、终端密码改造、国密安全通道改造、设备层密码改造、应用和数据安全密码改造及密码应用管理体系制度编制服务等。供应商所选择的	商用密码应用咨询服务（密码应用方案	1次	**我司完全响应，情况如下：** 根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，系统达到第三级密码应用基本要求，针对被测系统从方案制定和评审、终端密码改造、国密安全通道改造、设备层密码改造、应用和数据安全密码改造及密码应用管理体系制度编制服务等。供应商所选择的密评机构须具备有效的《商用密码检测机构资质证书》，且业	无偏离

	评测）		密评机构须具备有效的《商用密码检测机构资质证书》，且业务范围为“商用密码应用安全性评估”，[须在国家密码管理局公告（第53号）公布的“商用密码检测机构(商用密码应用安全性评估业务)目录中”可查询]。 ▲1、为满足本项目测评要求，供应商所选择的密评机构投入本项目密码测评工具，支持SM2/SM9椭圆曲线点压缩计算。支持SM9密钥生成、签名验签、加解密、密钥封装功能。支持解析APDU流量包并提取签名值随机数，并自动进行验签及签名攻击。需进行视频演示。 ▲2、支持哈希算法猜测功能。支持Attach和Detach签名验签，P7签名值分析功能。支持PRF运算、KDF运算、TLCP密钥生成、SM2加密	评测）		务范围为“商用密码应用安全性评估”，[须在国家密码管理局公告（第53号）公布的“商用密码检测机构(商用密码应用安全性评估业务)目录中”可查询]。 ▲1、为满足本项目测评要求，我方所选择的密评机构投入本项目密码测评工具，支持SM2/SM9椭圆曲线点压缩计算。支持SM9密钥生成、签名验签、加解密、密钥封装功能。支持解析APDU流量包并提取签名值随机数，并自动进行验签及签名攻击。提供视频演示。 ▲2、支持哈希算法猜测功能。支持Attach和Detach签名验签，P7签名值分析功能。支持PRF运算、KDF运算、TLCP密钥生成、SM2加密-K碰撞功能。支持对称密码算法工作模式检测功能。提供视频演示。 ▲3、为满足本项目测评要求，我方所选择的密评机构投入本项目自主研发的密码测评工具，已包含密码资源监测系统、	

			-K 碰撞功能。支持对称密码算法工作模式检测功能。需进行视频演示。 ▲3、为满足本项目测评要求，供应商所选择的密评机构投入本项目自主研发的密码测评工具，至少包含密码资源监测系统、商用密码检测软件、密码应用业务管理平台字样的测评工具，需提供相关包含以上全部字样的测评工具证明材料的复印件并加盖公章或提交承诺函所用的测评工具符合要求（承诺函格式自拟） 4、供应商所选择的密评机构配备的密码测评技术工程师需同时具备持有国家密码管理局颁发的商用密码应用安全性评估从业人员考核证书，并具备 CCSK 云计算安全知识认证、网络安全管理员证书。需提供相关包含以上全部证书证明材料的复印			商用密码检测软件、密码应用业务管理平台字样的测评工具，已提供承诺函，并承诺所用的测评工具符合要求。 4、我方所选择的密评机构配备的密码测评技术工程师同时具备持有国家密码管理局颁发的商用密码应用安全性评估从业人员考核证书，并具备 CCSK 云计算安全知识认证、网络安全管理员证书。我方已提供承诺函，承诺配备的密码测评技术工程师符合要求。	

			件并加盖供应商公章或提交承诺函配备的密码测评技术工程师符合要求（承诺函格式自拟）				

注：

1. 说明：应对照谈判文件“第三章”中“货物需求一览表”的采购清单及技术参数条款逐条作出明确响应，并作出偏离说明。

2. 供应商应根据自身的承诺，对照谈判文件要求，在“偏离说明”中注明“正偏离”、“负偏离”或者“无偏离”。既不属于“正偏离”也不属于“负偏离”即为“无偏离”。当响应文件的技术参数低于竞争性谈判采购文件要求时，竞标人应当如实写明“负偏离”，否则视为虚假应标

3. 表格内容均需按要求填写并盖章，不得留空，否则按竞标无效处理。

4. 如果采购需求为小于、小于等于、大于或大于等于某个数值标准时，响应文件承诺不得直接复制采购需求，响应文件承诺内容应当写明竞标货物具体参数的具体数值，否则按竞标无效处理。如该采购需求属于不能明确具体数值的，采购人应在此采购需求的数值后标注◆号，对标注◆号的采购需求不适用上述“竞标无效”条款。

5. 如技术偏离表中的竞标响应与佐证材料不一致的，以佐证材料为准。

6. 负偏离超过允许偏离的项数竞标无效。

供应商名称（电子签章）：确信信息股份有限公司

日期：2026年1月30日

6、售后服务承诺

	系统）				术股份有限公司		能参数详见-货物需求偏离表
16	商用密码应用安全性评估服务	1次	无	无	长沙云创信安科技有限公司	无	完成密码应用方案商用密码应用安全性评估报告和被测系统商用密码应用安全性评估报告在密码管理局密评的备案工作。
17	商用密码应用咨询服务（密码应用方案评测）	1次	无	无	长沙云创信安科技有限公司	无	目标系统达到第三级密码应用基本要求，针对被测系统从方案制定和评审、终端密码改造、国密安全通道改造、设备层密码改造、应用和数据安全密码改造及密码应用管理体系制度编制服务等

备注：

以上性能配置清单中“货物名称、数量及单位、品牌、规格型号、制造商、原产地、参数性能、指标及配置”必须如实填写完整，品牌、规格型号没有则填无，填写有缺漏的，响应文件作无效处理。货物名称、数量及单位、品牌必须与“货物需求偏离表”一致，否则响应文件作无效处理。

供应商名称（电子签章）：确信信息股份有限公司

日期：2026年1月5日

九、售后服务承诺

我司承诺：

1、质量保证期为1年（自交货并验收合格之日起计）。

2、故障响应时间：供应商（确信信息股份有限公司）接到故障通知后在1小时内到达采

购人指定现场。

3、售后技术服务要求：

1）故障响应时间：我司接到故障通知后需在30分钟内做出响应（电话），在24小时内派工程师到现场进行故障解除，如48小时内无法排除故障的，必须提供不低于故障产品规格型号和档次的备用产品供用户使用，直至故障产品修复，保证系统恢复正常运行。

2）在保修期内由我司负责保修，排除故障，无偿提供非操作不当造成的部件、配件的更换，我司从在其指定地点收到故障产品之日起7天内将修理后的产品或替换产品运至最终用户现场。因操作不当或外部原因损坏，造成部件的更换，应由采购人承担有关费用。保修期内，所有维修服务均为上门服务，由此产生的费用均不再收取。

3）我方向采购人承诺终身优惠提供配件和维修。

4）我方免费培训采购人维护人员，保证维护人员能进行日常运行维护工作，提供用户操作手册和维修手册；并能熟练地排除故障、管理设备、分析故障等。

5）如需升级软件，免费升级软件。

确信信息股份有限公司

2024年1月5日

附表A:售后服务机构情况表（按此格式自制）

序号	机构名称	机构性质	注册地址	货物技术人员数量	联系电话
1	确信信息股份有限公司	股份有限公司	山东省济南市高新区孙村街道科嘉路粤浦科技济南科创中心8号楼	20	0531-88113379
2	天津光电安辰信息技术股份有限公司	股份有限公司	天津开发区信环西路19号5号楼5703室(存在	34	022-88165539

			多址信息）		
3	北京海泰方圆科技股份有限公司	股份有限公司	北京市海淀区上地九街9号9号6层611号	4	400-601-9696
4	长沙云创信安科技有限公司	有限责任公司	长沙高新开发区麓谷大道658号湖南软件信息港12栋202-205	3	137-8729-5333

注：关于项目涉及的所有售后服务机构均在本表注明，包括供应商本单位和符合条件的第三方货物机构；

附表B：售后服务人员情况表（按此格式自制）

序号	类别	姓名	性别	年龄	学历	专业	职称	本项目中的职责	响应时间	到达现场时间
1	总协调人	唐子元	男	34	本科	信息管理与信息系统	无	总协调人	7*24小时	按照合同要求
2	售后人员	刘存政	男	33	本科	计算机科学与技术	无	售后工程师	7*24小时	按照合同要求
3	售后人员	王缠国	男	34	本科	计算机科学与技术	无	售后工程师	7*24小时	按照合同要求

供应商名称（电子签章）：确信信息股份有限公司

日期：2026年1月5日