合浦县人民医院商用密码应用改造
采购合同

项目名称：合浦县人民医院商用密码应用改造

项目编号：BHZC2025-J3-210016-YXGC

甲 方：合浦县人民医院

乙 方：中国移动通信集团广西有限公司北海分公司

2025年04月25日，（合浦县人民医院）以（竞争性谈判方式）对（合浦县人民医院商用密码应用改造）项目进行了采购。经（广西延信工程项目管理有限公司抽取专家小组）评定，（中国移动通信集团广西有限公司北海分公司）为该项目成交供应商。现于成交通知书发出之日起25个日历内，按照采购文件确定的事项签订本合同。

根据《中华人民共和国民法典》《中华人民共和国政府采购法》等相关法律法规之规定，按照平等、自愿、公平和诚实信用的原则，经（合浦县人民医院）（以下简称：甲方）和（中国移动通信集团广西有限公司北海分公司）（以下简称：乙方）协商一致，约定以下合同条款，以兹共同遵守、全面履行。

1.1 合同组成部分

下列文件为本合同的组成部分，并构成一个整体，需综合解释、相互补充。如果下列文件内容出现不一致的情形，那么在保证按照采购文件确定的事项的前提下，组成本合同的多个文件的优先适用顺序如下：

1.1.1 本合同及其补充合同、变更协议；

1.1.2 中标或者成交通知书；

1.1.3 投标或者响应文件（含澄清或者说明文件）；

1.1.4 采购文件（含澄清或者修改文件）；

1.1.5 其他相关采购文件。

1.2 标的

1.2.1 服务内容： 详见附件2【商务、服务（技术）响应、偏离情况说明表】，同时免费提供云电脑AI秘书服务；

1.2.2 服务标准：详见附件1【售后服务承诺书】，附件2【商务、服务（技术）响应、偏离情况说明表】；

1.3 价款

1.3.1 总价合同，本合同总价（含税）为：￥1708000 元（人民币大写： 壹佰柒拾万零捌仟元整）。

分项价格

序号	服务内容	数量	单位	金额（元）	税率	说明
1	服务器密码机	1	台	169300	13%	设备型号：奇安信网神 QuickHSM-HS1000
2	国密安全密码应用平台	2	套	721000	6%	

3	VPN 安全网关	1	台	244100	13%	设备型号：奇安信网神 SJJ19116
4	密码应用技术服务	1	项	162000	6%	
5	国密堡垒机改造	1	项	92000	6%	
6	日志审计升级服务	1	项	25000	6%	
7	堡垒机升级服务	1	项	28000	6%	
8	威胁感知系统升级服务	1	项	82000	6%	
9	内网终端安全升级服务	1	项	113600	6%	
10	防火墙板卡扩容	2	项	71000	6%	
合计				1708000		
合计，大写：壹佰柒拾万零捌仟元整						

1.4 履约保证金

本项目不设履约保证金

1.5 付款方式

分期付款：

第一期，签订合同后，支付合同金额的30%预付款，即512400元，大写：伍拾壹万贰仟肆佰元整；

第二期，待全部货物供货完成并安装调试完毕，经双方验收合格后，双方签署验收合格表后，由甲方向乙方支付剩余70%合同款，即1195600元，大写：壹佰壹拾玖万伍仟陆佰元整。

1.6 资金支付

1.6.1 甲方应严格履行合同，及时组织验收，验收合格后及时将合同款支付完毕。对于满足合同约定支付条件的，甲方自收到等额发票后将资金支付到合同约定的乙方账户，有条件的甲方可以即时支付。甲方不得以机构变动、人员更替、政策调整、单位放假等为由延迟付款。

1.6.2 资金支付的方式：对公转账。

1.6.3 甲方开票信息

甲方名称：【合浦县人民医院】

纳税人识别号:【450521498818888】

地址、电话:【广西合浦县廉州镇定海北路95号7797106990】

开户行:【中国建设银行股份有限公司合浦支行】

银行账号：【622357494213】

1.6.4 乙方发票、收款账户信息

乙方发票信息：

乙方名称：【中国移动通信集团广西有限公司北海分公司 】

国税纳税人识别号：【914505007114671332】

户名：【 中国移动通信集团广西有限公司北海分公司】

开户行：【 中国工商银行股份有限公司南宁市琅东支行】

银行账号：【9558852102001169516 】

公司地址：【北海市北海大道212号 】

乙方收款账户信息：

甲方名称：【中国移动通信集团广西有限公司北海分公司】

国税纳税人识别号：【914505007114671332】

账户名：【中国移动通信集团广西有限公司合浦分公司】

开户行：【中国工商银行股份有限公司南宁市琅东支行】

账号：【9558852102001169532】

地址：【北海市北海大道212号】

1.7 履行期限 、地点和验收

服务期：验收合格之日起1年

服务交付时间及地点：采购人指定地点。

交付使用期：60个工作日内完成合浦县人民医院商用密码应用改造工作并交付使用。

验收：项目交付使用时我公司承诺向采购人提供规范完整的安装调试技术资料或测试报告或技术文档、验收报告等，以上资料均需提供电子和纸质文档。（验收标准已招标响应文件响应内容作为验收合格依据）

1.8 违约责任

1.8.1任何一方未履行本协议项下的任何一项条款均应被视为违约（该方为“违约方”）。在此情况下，守约方有权要求违约方继续履行、承担因自己的违约行为而给守约方造成的经

济损失或采取补救措施，本协议另有约定的除外。

1.8.2乙方未按本合同约定提供系统集成服务，或未按本合同约定提供符合要求的系统集成服务人员的，甲方有权要求乙方整改，并有权视情况要求乙方支付本合同总额5%至20%的违约金，同时，甲方有权视情况单方解除本合同。

1.8.3在服务过程中，如因乙方提供的货物或服务质量问题、乙方人员行为造成甲方网络中断、运行故障、数据丢失等事件，则该事件造成的损失（包括但不限于修复费用、中断期间营业损失等）由乙方承担。如营业收入因数据丢失或运行中断无法计算的，则按当日每小时平均话务量类推计算。

1.8.4乙方未按法律法规规定和本合同约定与乙方人员签订劳动合同、购买社会保险、提供劳保用品的，乙方应向甲方支付本合同总额【10】%的违约金。同时，甲方有权视情况单方解除本合同。

1.8.5乙方违反国家法律、法规、规章、政策等规定开具、提供发票的，乙方应自行承担相应法律责任，并承担如下违约责任：

（1）乙方应按甲方要求采取重新开具发票等补救措施；

（2）乙方应向甲方支付合同含税总价【10】% 的违约金；

1.8.6乙方提供的增值税专用发票没有通过税务部门认证，造成甲方不能抵扣的，乙方应按甲方要求采取重新开具发票等补救措施，同时乙方还应向甲方支付未通过认证发票中载明的税款金额作为违约金。

1.8.7乙方未按本合同约定开具、送达增值税专用发票的，情节严重的，包括但不限于出现乙方未按合同约定开具、送达发票次数达【2】次及以上的、乙方违约给甲方造成严重损失的、乙方违约致使合同无法继续履行、乙方未按甲方要求采取补救措施、支付违约金和赔偿等情况，甲方有权终止合同，乙方应赔偿甲方因此遭受的全部损失。

1.8.8合同履行过程中，发生下列情形之一的，甲方有权终止本合同，乙方应向甲方支付合同总额的【10】%作为违约金，违约金不足以弥补甲方所受损失的，乙方还应予以赔偿：

1.8.9.1因乙方原因导致甲方设备损坏、重大通信故障、系统信息丢失、人员伤亡等事故，甲方遭受重大损失的；

1.8.9.2乙方不遵照安全、消防等规定开展工作，造成人员伤亡或者安全、消防等责任事故的；

1.8.9.3乙方违反信息安全义务，给甲方造成重大损失或重大影响的；

1.8.9.4乙方按照本合同的约定应支付的逾期违约金数额达到最大限额的；

1.8.9.5因乙方的违约行为，给甲方造成重大损失或重大影响的；

1.8.10合同任何一方违反保密约定，故意、过错或过失泄密的，除应立即采取措施停止泄密行为，减小泄密造成的损失外，还应向保密信息拥有方支付合同总价【10】%的违约金。上述违约金不足以弥补保密信息拥有方所受损失的，泄密方还应予以赔偿。同时，保密信息拥有方还有权根据泄密造成损失的大小，单方解除本合同。

1.8.11乙方违反本合同知识产权条款，应当向甲方支付合同总价的【10】%作为违约金。乙方提供的服务或提交的技术成果侵犯第三方的知识产权和其他合法权益的，除应按照上述约定向甲方支付违约金外还应赔偿因此给甲方和第三方造成的损失。

1.8.12合同一方应在另一方发生违约行为后，以书面形式向违约方发出违约或解除合同的通知。该等通知中应详细列明对方违约的时间、违约行为、违约造成的损失和要求对方承担违约责任的主张。违约方可就此向发出方提出解释或质疑，双方应及时确认违约责任的承担。但此种确认并不影响双方按合同应履行的其他义务和应行使的其他权利及通过其他途径追究对方的违约责任等。

1.8.13乙方必须严格按照合同要求的项目技术指标和参数，对软件架构进行调整，确保实现解耦以及模块化，支撑硬件资源池化和云化，如乙方违反本项约定，甲方有权按合同总价【5】%要求乙方支付违约金，并有权不予上线、初验和终验，直至终止合同，因此造成的损失由乙方负责。

1.8.14在乙方提供服务的过程中，因乙方或乙方工作人员行为，造成甲方或者甲方人员或者任何第三方遭受人身伤害或财产损失的，均由乙方自行承担全部赔偿责任。

1.8.15乙方未经甲方书面许可，擅自将本合同项下部分或全部工作转交第三方进行的，甲方有权要求乙方支付本合同总价【10】%的违约金，同时，甲方还有权利视情况立即解除本合同。

1.8.16如因乙方违约行为侵害第三方合法权益的，乙方应负责处理并承担所有责任。因此给甲方造成损失的，乙方应承担赔偿责任。

1.8.17若本协议项下约定的各项违约金尚不足以补偿由此给甲方造成的全部损失的，乙方仍需在甲方全部损失范围内承担赔偿责任。

1.8.18本合同基于各种服务规范、考核管理办法所设立扣款等措施均视为对违约责任的补充约定，乙方对此无任何异议。

1.8.19本合同所称之损失包括实际损失和合同履行后可以获得的利益、诉讼或仲裁费等相关法律费用。

1.8.20乙方同一违约行为同时涉及本合同数个违约责任、或者同时涉及本合同违约责任条款其和基于本合同的考核、管理办法规定的，甲方有权选择其中责任较重之约定追究乙方违约责任。

1.10不可抗力

1.10.1本合同所指不可抗力，是指不能预见、不能避免并不能克服的客观情况。

1.10.2由于不可抗力事件，致使一方在履行其在本合同项下的义务过程中遇到障碍或延误，不能按约定的条款全部或部分履行其义务的，遇到不可抗力事件的一方（“受阻方”），只要满足下列所有条件，不应视为违反本合同：

1.10.2.1 受阻方不能全部或部分履行其义务，是由于不可抗力事件直接造成的，且在不可抗力发生前受阻方不存在迟延履行相关义务的情形。

1.10.2.2 受阻方已尽最大努力履行其义务并减少由于不可抗力事件给另一方造成的损失；及不可抗力事件发生时，受阻方立即通知了对方，并在不可抗力事件发生后的十五(15)天内提供有关该事件的公证文书和书面说明，书面说明中应包括对延迟履行或部分履行本合同的原因说明。

1.10.3不可抗力事件终止或被排除后，受阻方应继续履行本合同，并应尽快通知另一方。受阻方应可延长履行义务的时间，延长期应相当于不可抗力事件实际造成延误的时间。

1.10.4如果不可抗力事件的影响持续达三十（30）日或以上时，双方应根据该事件对本合同履行的影响程度协商对本合同的修改或终止。如在一方发出协商书面通知之日起十（10）日内双方无法就此达成一致，任何一方均有权解除本合同而无需承担违约责任。

1.11 法律适用和争议解决

1.11.1 本合同的成立、有效性、解释、履行、签署、修订和终止以及争议的解决均应适用中华人民共和国法律。

1.11.2 如果任何争议或权利要求起因于本合同或与本合同有关或与本合同的解释、违约、终止或效力有关，都应由双方通过友好协商解决。协商应在一方向另一方送达关于协商的书面要求后立即开始。

1.11.3 如果在一方提出协商要求后的十(10)天内，双方通过协商不能解决争议，则任何一方均有权向【甲方所在地】有管辖权的人民法院提起诉讼。

1.11.4 诉讼进行过程中，除双方有争议的部分外，本合同其他部分仍然有效，双方应继续

履行。

1.11.5 本合同全部或部分无效的，本条依然有效。

1.12 合同生效、终止及其他

1.12.1 除非法律规定或任何主管机关要求，或经由另一方书面同意（不应无理拒绝或拖延同意），任何一方不应对本合同或任何相关事项予以发布或公告。

17.2 除双方及其各自的继任人和允许的受让人以外，本合同不应向任何个人或实体赋予权利或救济。

1.12.3 本合同主体文本及其附件构成双方就本合同标的达成的完整协议，取代以前双方就本合同标的所达成的所有口头或书面的协议、协商、条款、意向书以及其他协议和文件。

1.12.4 未经合同另一方书面同意，一方不得转让本合同项下任何权利和义务。

1.12.5 本合同以中文签署，一式【4】份，双方各执【2】份，具有相同法律效力。

1.12.6 本合同中加入的各章、条、款、项的标题仅为方便阅读而设，不应对本合同的含义或解释有任何影响。

1.12.7一方未强制执行本合同的一条或若干条款，或未行使其在本合同项下的任何选择权或其他权利，或任何时候未要求另一方履行其在本合同中的任何义务，均不应被理解为该方放弃上述有关条款，或者以任何方式影响本合同的有效性或该方强制执行本合同各项条款的权利，也不应阻止该方在任何时候采取其原本有权采取的其他任何行动。

1.12.8 本合同的任何条款或规定，如被有权机构判定为无效或不可执行，不应影响本合同其他条款或规定的效力或可执行性，也不应影响该条款或规定在其他情形下的效力或可执行性。

1.12.9 本合同双方应各自承担其自身与本合同及本合同项下的交易有关的所有开支和费用（包括法律费用），本合同另有约定的除外。

1.12.10 双方确认，没有任何代理人、中间人或中介人直接或间接就本合同或本合同拟定的交易为任何一方行事，并且没有任何人基于任何一方做出的或代表任何一方做出的合同、安排而有权收取与本交易有关的任何代理费、中介费、中间人佣金或类似的佣金。

1.12.11 本合同未尽事宜，应由双方友好协商解决。如需对本合同及其附件作任何修改或补充，须由双方以书面做出方为有效。修改或补充文件与本合同有不一致的，以修改或补充文件为准。

1.12.12 本合同签署前，双方将分别向其他方提供其授权本合同签署人代表其签署本合同的

授权文件。

1.12.13 合同将保持其效力直至双方已完全履行合同项下的所有义务并且双方之间的所有付款和索赔已结清。

1.12.14 合同附件为本合同的组成部分，与本合同正文具有同等法律效力。若合同附件与合同正文有任何冲突，以合同正文为准。

1.12.15 本合同已由双方授权代表签字并加盖公司公章或合同专用章，自双方签署之日起生效；如双方签署日期不一致，自较迟的签署日起生效。

（以下无正文）

甲方：**【合浦县人民医院】**（盖章）

法定代表人/授权代表（签字或盖章）：_____

日期：【2025】年【 5 】月【 20 】日

乙方：**【中国移动通信集团广西有限公司北海分公司】**（盖章）

法定代表人/授权代表（签字或盖章）：_____

日期：【2025】年【 5 】月【 20 】日

附件1

售后服务承诺书

致：（合浦县人民医院）

我公司参加贵单位组织的 合浦县人民医院商用密码应用改造（项目编号：BHZC2025-J3-210016-YXGC ）项目招标活动。我司对本项目的维护郑重承诺如下：

我公司响应并承诺以下内容

1、合同签订时间：自中标通知书发出之日起 25 个日历日内签订合同。

2、交付时间：交付使用期：60 个工作日内完成合浦县人民医院商用密码应用改造工作并交付使用；如因我公司的原因不能在规定时间完成交付任务，我公司承担违约责任。

服务有效期：自项目验收通过之日起开始计算，服务期 1 年。

3、售后服务要求：

1.软件支持服务

我公司保证系统能够长期安全、可靠、高效运行，必须提供软件的现场安装服务和技术后援支持，为今后系统中软件提供长期的技术支持。技术支持的方式包括：电话技术支持服务，现场技术服务、定期巡查服务，技术升级服务等。

2.售后服务时间及方式

我公司免费提供每周 7 天,每天 24 小时不间断的电话支持服务，解答采购人在系统使用、维护过程中遇到的问题，将在 1 小时内作出响应，为最终用户提供 7x24 远程电话技术支持服务（客户经理:庞鲜明，电话:15907893991），并及时提出解决问题的建议和操作方法；定期回访、维护；

应急响应时间：在维保期内，系统出现紧急故障时，将在 1 小时内作出响应，为最终用户提供 7x24 远程电话技术支持服务（客户经理:庞鲜明，电话:15907893991），如远程无法解决，将安排售后工程师进行紧急现场服务，4 小时内到达用户现场，并配合用户快速解决问题。

响应方式：电子邮件和服务电话（详见附表）、远程登录：4 小时内到达用户现场，一般问题应在 12 小时内解决，重大问题或其它无法迅速解决的问题应在 1 天内解决，如经工程师诊断为硬件故障的，将在 8 小时内为用户提供备机服务；如为软件故障，将在 4 小时内解决。同时，我司承诺一个月提供 2 次定期回访以及对设备维护。

姓名	职务	联系方式	邮箱
杨书杰	项目经理	13657713235	yangshujie@qianxin.com
蓝吉帮	实施经理	18878714988	lanjibang@qianxin.com
黄贵仁	服务经理	13377116150	huangguiren@qianxin.com
何成	安全工程师	13557573136	hecheng@qianxin.com
何勇	安全工程师	13321718167	heyong@qianxin.com
周发	安全工程师	18775513446	zhoufa@qianxin.com

3.售后服务保障

我公司具有售后服务能力，具有能胜任本项目日常技术维护工作的技术人员，以保证对用户的快速服务响应，提供优质的售后服务。常驻机构（北海市北海大道212号，中国移动通信集团广西有限公司北海分公司；合浦县迎宾大道169号，中国移动通信集团广西有限公司合浦分公司）

4、报价要求：

我公司报价含以下部分，包括：货物及服务采购、标准附件、备品备件、专用工具、软件提供、辅料、耗材、运输、保管、设计、改造、施工、安装、调试、验收、培训等各种费用和售后服务、税金及咨询服务等费用全部包含。

5、培训要求：

我公司将派驻专业工程师负责对安全管理员进行技术培训。经过培训后，确保培训对象能够了解网络安全基础知识、安全及密码产品知识、安全防护体系，熟悉目前系统中产品的原理、部署，充分掌握维护系统、产品正常运行的技术知识，从而快捷的维护本次采购产品的日常运行，能够独立地对产品进行管理、维护，而不需产品技术人员在场指导，能够独立解决系统、产品使用中的一般故障，能根据网络等需求的变化，对产品配置进行调整，保证系统、产品长期的运行。

6、系统对接要求：

本次所提供的设备及服务内容需与合浦县人民医院智慧医疗信息系统、心电及电生理网络系统、影像诊断系统、电子病例系统实现为被保护对象，我公司将对整个项目及建设方案做全局规划，全面了解合浦县人民医院信息系统情况，如涉及对部分原系统进行升级改造的，相应费用全部包含在本次报价中。

7、验收要求：

项目交付使用时我公司承诺向采购人提供规范完整的安装调试技术资料或测试报告或技术文档、验收报告等，以上资料均需提供电子和纸质文档。

8、其他：

每季度上门检修、检测及维护，或经采购方同意进行电话询查，并为用户出具该季度的系统故障统计分析说明或安全检测报告，为用户的维护、管理和升级工作提供理由充分的参考依据。遇到重大服务时， 我司将派遣具有丰富经验的工程师到用户现场，为最终用户提供完善周到的本地化的驻场服务。

本项目不得转包、分包。

9、本地化专职服务经理

北海移动公司指定首席客户代表和客户代表负责项目终身维系，为客户正常使用移动业务提供全方位、优质服务。客户在使用中的业务变更、业务咨询等均可通过客户代表一站式受理完成。本项目专职客户经理电话：**庞鲜明 15907893991**

承诺人名称：中国移动通信集团广西有限公司北海分公司

日期：

附件2

商务、服务（技术）响应、偏离情况说明表

项目名称：合浦县人民医院商用密码应用改造

项目编号：BHZC2025-J3-210016-YXGC

序号	竞争性谈判文件要求	竞争性谈判响应文件具体响应	响应/偏离	说明
商务部分				
1	付款条件 分期付款：第一期，签订合同后，支付合同金额的30%预付款；第二期，待全部货物供货完成并安装调试完毕，经采购人验收合格后，由采购人向供应商支付剩余合同款。	响应付款条件 分期付款：第一期，签订合同后，支付合同金额的30%预付款；第二期，待全部货物供货完成并安装调试完毕，经采购人验收合格后，由采购人向供应商支付剩余合同款。	完全响应	同意竞争性谈判文件要求的分期付款条件。
2	服务期：1年	如我司中标，服务期：1年	完全响应	如我司中标，根据招标要求，提供一年服务。
3	服务交付时间及地点：采购人指定地点。	服务交付时间及地点：根据采购人指定地点服务。	完全响应	如我司中标，根据采购人指定地点提供服务并交付。
4	合同签订时间：自中标通知书发出之日起25个日历日内签订合同。	合同签订时间：如我司中标，则自中标通知书发出之日起25个日历日内签订合同。	完全响应	如我司中标，则自中标通知书发出之日起25个日历日内签订合同。
5	本章服务需求说明全部内容须逐条作出承诺及实质性响应，否则谈判无效。	我司对本章服务需求说明，皆逐条做出承诺及实质性响应。	完全响应	我司对本章服务需求说明，皆逐条做出承诺及实质性响应。
服务（技术）部分				

1	**服务器密码机，1 台。** **技术参数及性能（配置）要求：** 1.★2U 机箱，CPU≥4 核，内存≥16G，硬盘≥120G，千兆电口≥2 个，RJ45 串口≥1 个，USB 口≥2 个，冗余电源，提供 3 年原厂维保及升级服务。SM4 加解密性能≥850Mbps；SM3 杂凑性能≥400Mbps；SM2 密钥对生产性能≥16000 对/秒；SM2 签名性能≥12000 次/秒；MAC_SM4≥880Mbps；最大并发连接数≥5000； 2.采用国家密码管理局认可的 Hsn3 物理噪声源芯片生成真随机数，支持生成各类对称密钥（SM1、SM4、DES、AES 等）和非对称密钥（SM2、RSA1024/2048 等）； 3.密码运算：支持数据加密/解密、数字签名/验签、消息鉴别码的产生/验证、数字信封、密钥协商等类型的密码运算，并且支持多任务并发访问； 4.密钥管理：支持至少三层密钥结构，支持管理密钥、用户密钥、设备密钥、密钥加密密钥、会话密钥的管理，支持对称与非对称密钥的生成及管理； 5.★出于后期运维排障难度和排障周期考虑，密码设备与密码卡应为同一厂家（需提供相关截图证明）； 6.支持对称加密/解密功能，支持分组加密的四种模式：ECB、CBC、OFB、CFB 模式； 7.支持基于 RSA/SM2 算法的数字签名及验签功能，可以根据需要使用内部存储的私钥或外部私钥进行数字签名和验签； 8.支持通过设备内密码卡物理噪声源生成 1024/2048 位 RSA、256 位 SM2 密钥对，以及 128 位/256 位 KEK 密钥； 9.支持证书链管理功能，支持配置多个 CA 或者多级 CA，可同时配置多条证书链； 10.★密码机支持内部密钥的安全备份和恢复，保证系统的安全性和可靠性；同时支持主备多台设备间的密钥同步；（需提供相关截图证明）	**提供服务器密码机，1 台。** **技术参数及性能(配置)要求响应如下：** 1.★2U 机箱，CPU4 核，内存 16G，硬盘 120G，千兆电口 2 个，RJ45 串口≥1 个，USB 口 2 个，冗余电源，**提供 3 年原厂维保及升级服务**。SM4 加解密性能 850Mbps；SM3 杂凑性能 400Mbps；SM2 密钥对生产性能 16000 对/秒；SM2 签名性能 12000 次/秒；MAC_SM4880Mbps；最大并发连接数 5000； 2.采用国家密码管理局认可的 Hsn3 物理噪声源芯片生成真随机数，支持生成各类对称密钥（SM1、SM4、DES、AES 等）和非对称密钥（SM2、RSA1024/2048 等）； 3.密码运算：支持数据加密/解密、数字签名/验签、消息鉴别码的产生/验证、数字信封、密钥协商等类型的密码运算，并且支持多任务并发访问； 4.密钥管理：支持三层密钥结构，支持管理密钥、用户密钥、设备密钥、密钥加密密钥、会话密钥的管理，支持对称与非对称密钥的生成及管理； 5.★出于后期运维排障难度和排障周期考虑，密码设备与密码卡应为同一厂家（需提供相关截图证明）； 6.支持对称加密/解密功能，支持分组加密的四种模式：ECB、CBC、OFB、CFB 模式； 7.支持基于 RSA/SM2 算法的数字签名及验签功能，可以根据需要使用内部存储的私钥或外部私钥进行数字签名和验签； 8.支持通过设备内密码卡物理噪声源生成 1024/2048 位 RSA、256 位 SM2 密钥对，以及 128 位/256 位 KEK 密钥； 9.支持证书链管理功能，支持配置多个 CA 或者多级 CA，可同时配置多条证书链； 10.★密码机支持内部密钥的安全备份和恢复，保证系统的安全性和可靠性；同时支持主备多台设备间的密钥同步；（需提供相关截图证明） 11.操作人员通过智能密码钥匙实现身	完全响应	

	11.操作人员通过智能密码钥匙实现身份认证，操作终端与加密机之间建立SSL安全通道，保证设备管理操作的机密性、真实性和不可否认性； 12.★支持SNMP协议，SNMP服务开启后可通过SNMP服务监控密码机状态；（需提供相关截图证明） 13.★支持设备启动自检功能：包括随机数自检、算法自检、以及密钥完整性自检等；（需提供相关截图证明） 14.支持集群部署，或双机热备等情景，防止单点故障，提高加密机业务运算性能，进一步提高高可用以及多并发等性能。支持任意扩容的部署模式，可以便捷的从单机模式转换成主从模式、集群模式（解决单点故障和负载均衡问题）； 15.支持与同厂家密钥管理设备绑定，与密码机通过安全通道分发、启用、销毁对称/非对称密钥； ★本次采购服务器密码机与用户现网使用的堡垒机为同一品牌，以方便对接管理。	份认证，操作终端与加密机之间建立SSL安全通道，保证设备管理操作的机密性、真实性和不可否认性； 12.★支持SNMP协议，SNMP服务开启后可通过SNMP服务监控密码机状态；（需提供相关截图证明） 13.★支持设备启动自检功能：包括随机数自检、算法自检、以及密钥完整性自检等；（需提供相关截图证明） 14.支持集群部署，或双机热备等情景，防止单点故障，提高加密机业务运算性能，进一步提高高可用以及多并发等性能。支持任意扩容的部署模式，可以便捷的从单机模式转换成主从模式、集群模式（解决单点故障和负载均衡问题）； 15.支持与同厂家密钥管理设备绑定，与密码机通过安全通道分发、启用、销毁对称/非对称密钥； ★本次采购服务器密码机与用户现网使用的堡垒机为同一品牌，以方便对接管理。		
2	**国密安全密码应用平台，2套。** **技术参数及性能（配置）要求：** 1.规格要求：支持数据库实例不小于7个； 2.算法要求：支持国密SM4算法和国际DES/3DES/AES算法；支持国密SM3算法和国际MD5/SHA1/SHA256/SHA384/SHA512等算法；支持国密SM2和国际RSA(1024-2048)算法；支持基于SM4的FPE格式保留算法（FPE格式保留算法提供截图证明）； 3.备份与恢复：支持系统的各类密钥、应用数据等数据定期、手动备份，通过加密技术保护备份，使用数字证书认证恢复备份； 4.支持密码服务可视化、以大屏动态展示的方式清晰直观反馈出所有密码服务的运行状态、应用服务排名等运行信息； 5.★密钥轮转：支持密钥自动定期，将应用系统的对称密钥进行定期的自动	**提供国密安全密码应用平台，2套。** **技术参数及性能（配置）要求响应如下：** **1.规格要求：支持数据库实例7个；** 2.算法要求：支持国密SM4算法和国际DES/3DES/AES算法；支持国密SM3算法和国际MD5/SHA1/SHA256/SHA384/SHA512等算法；支持国密SM2和国际RSA(1024-2048)算法；支持基于SM4的FPE格式保留算法（FPE格式保留算法提供截图证明）； 3.提供备份与恢复：支持系统的各类密钥、应用数据等数据定期、手动备份，通过加密技术保护备份，使用数字证书认证恢复备份； 4.支持密码服务可视化、以大屏动态展示的方式清晰直观反馈出所有密码服务的运行状态、应用服务排名等运行信息； 5.★密钥轮转：支持密钥自动定期，将应用系统的对称密钥进行定期的自动更新，密钥ID不变的情况下，产生多	完全响应	

	更新，密钥 ID 不变的情况下，产生多个历史版本，自动的进行密码生命周期更换（提供截图证明） 6. 数据库支持：支持 MySQL / PostgreSQL / SQLServer / Oracle 等基于 SQL92 协议的数据库 7. 数据类型支持：支持使用国密算法 SM4 对 CHAR、VARCHAR2、VARCHAR、BLOB、JSON 等数据类型的加密； 8. 免改造加密：实现数据写入数据库时自动加密，从数据库中读取时自动解密；不影响管理员使用数据库提供的工具实现备份恢复和运维； 9. 历史存量明文批量加密：支持对数据库中历史的存量明文数据进行识别批量加密； 10. 完整性保护：使用国密算法的 MAC 运算对数据进行字段级的完整性保护； 11. 密码设备管理：支持纳管具备商密认证资质的不同厂商异构的密码设备（密码机、签名验签服务器、时间戳服务、云密码机等）实现利旧复用，支持对设备创建、停用、下架等生命周期管理； 12. 密码接口服务：提供数据加解密、签名验签、时间戳、HMAC、CMAC、摘要计算等密码服务能力，通过封装 SDK 接口调用； 13. 字段加密：支持基于国密算法 SM4 和国际算法 AES 进行字段级（列）的数据加密，可通过 web 管理页面自定义配置，可做到一字段一密钥，精细化密钥配提供可视化的策略管理控制台，管理员可以在控制台上配置数据库表内每个字段的加解密规则，保护敏感字段（如姓名、手机号等字段）； 14. ★密文检索：支持对密文数据进行模糊搜索（LIKE 通配符查询）；（提供截图证明） 15. 支持应用系统之间的密钥授权机制，应用系统不仅可以调用自己主密钥分散派生的工作密钥，亦可授权其他应用借用自己的工作密钥，从而达到管理数据加解密权限的控制效果；	个历史版本，自动的进行密码生命周期更换（提供截图证明） 6. 数据库支持：支持 MySQL / PostgreSQL / SQLServer / Oracle 等基于 SQL92 协议的数据库 7. 数据类型支持：支持使用国密算法 SM4 对 CHAR、VARCHAR2、VARCHAR、BLOB、JSON 等数据类型的加密； 8. 免改造加密：实现数据写入数据库时自动加密，从数据库中读取时自动解密；不影响管理员使用数据库提供的工具实现备份恢复和运维； 9. 历史存量明文批量加密：支持对数据库中历史的存量明文数据进行识别批量加密； 10. 提供完整性保护：使用国密算法的 MAC 运算对数据进行字段级的完整性保护； 11. 提供密码设备管理：支持纳管具备商密认证资质的不同厂商异构的密码设备（密码机、签名验签服务器、时间戳服务、云密码机等）实现利旧复用，支持对设备创建、停用、下架等生命周期管理； 12. 提供密码接口服务：提供数据加解密、签名验签、时间戳、HMAC、CMAC、摘要计算等密码服务能力，通过封装 SDK 接口调用； 13. 字段加密：支持基于国密算法 SM4 和国际算法 AES 进行字段级（列）的数据加密，可通过 web 管理页面自定义配置，可做到一字段一密钥，精细化密钥配提供可视化的策略管理控制台，管理员可以在控制台上配置数据库表内每个字段的加解密规则，保护敏感字段（如姓名、手机号等字段）； 14. ★密文检索：支持对密文数据进行模糊搜索（LIKE 通配符查询）；（提供截图证明） 15. 支持应用系统之间的密钥授权机制，应用系统不仅可以调用自己主密钥分散派生的工作密钥，亦可授权其他应用借用自己的工作密钥，从而达到管理数据加解密权限的控制效果；		

	16.支持对称和非对称密钥管理，对称密钥支持平台通过密钥分散应用主密钥生成，也支持外部导入；非对称密钥对平台默认生成，也支持外部导入； 支持对接具备商密认证资质的第三方密钥系统进行密钥管理；	16.支持对称和非对称密钥管理，对称密钥支持平台通过密钥分散应用主密钥生成，也支持外部导入；非对称密钥对平台默认生成，也支持外部导入； 支持对接具备商密认证资质的第三方密钥系统进行密钥管理；		
3	**VPN 安全网关，1 台。** **技术参数及性能（配置）要求：** 1.★标准 2U 设备，国密专用系统主机，交流电源，配置≥6 个 10/100/1000M 自适应电口，1 个接口扩展插槽，1TB 工业级硬盘，配置国密卡，1 个 RJ-45 串口；提供三年硬件质保； 2.★整机 SSL 加密吞吐量≥600Mbps，最大支持并发用户数≥5000;配置 1200 个 SSL VPN 授权用户数； 3.网络接口地址配置支持 IPv6 地址，网络路由地址配置支持 IPv6 地址，； 4.支持多链路接入、支持策略路由、支持链路聚合； 5.支持配置向导功能，用户能够按照配置向导一步一步的操作，向导结束用户能够完成账号建立、服务发布、正常访问； 6.支持 B/S 和 C/S 的应用支持单点登录（SSO），并提供加密认证功能；访问多个应用，只须输入一次密码，支持针对不同的访问资源设定不同的 SSO 用户名和密码； 7.支持虚拟门户功能，能够按照不同的用户组来定义不同的虚拟门户，不同的虚拟门户登录界面、访问地址均可以不同； 8.支持自动跳转功能，用户登录后自动弹出默认的应用界面；可自定义应用图标，可自行设置智能终端应用图标、PC 端应用图标； 9.支持国产化中标麒麟操作系统客户端 APP，在 Linux 系统平台下不依赖火狐浏览器，具备独立的 SSLVPN 客户端； 10.★支持与用户现网中使用的终端安全管理软件联动，可以检查终端安全软件进程，并根据是否安装来判断用户接入情况，并能自动弹出 IE 链接提示客	**提供 VPN 安全网关，1 台。** **技术参数及性能(配置)要求响应如下：** 1.★标准 2U 设备，国密专用系统主机，交流电源，**配置 6 个 10/100/1000M 自适应电口**，1 个接口扩展插槽，1TB 工业级硬盘，配置国密卡，1 个 RJ-45 串口；提供三年硬件质保； 2.**★整机 SSL 加密吞吐量 600Mbps，最大支持并发用户数 5000 户**；配置 1200 个 SSL VPN 授权用户数； 3.网络接口地址配置支持 IPv6 地址，网络路由地址配置支持 IPv6 地址，； 4.支持多链路接入、支持策略路由、支持链路聚合； 5.支持配置向导功能，用户能够按照配置向导一步一步的操作，向导结束用户能够完成账号建立、服务发布、正常访问； 6.支持 B/S 和 C/S 的应用支持单点登录（SSO），并提供加密认证功能；访问多个应用，只须输入一次密码，支持针对不同的访问资源设定不同的 SSO 用户名和密码； 7.支持虚拟门户功能，能够按照不同的用户组来定义不同的虚拟门户，不同的虚拟门户登录界面、访问地址均可以不同； 8.支持自动跳转功能，用户登录后自动弹出默认的应用界面；可自定义应用图标，可自行设置智能终端应用图标、PC 端应用图标； 9.支持国产化中标麒麟操作系统客户端 APP，在 Linux 系统平台下不依赖火狐浏览器，具备独立的 SSLVPN 客户端； 10.★支持与用户现网中使用的终端安全管理软件联动，可以检查终端安全软件进程，并根据是否安装来判断用户接入情况，并能自动弹出 IE 链接提示客	完全响应	

	户下载安装（提供界面功能截图）； 11.★设备支持单独对每个应用发布业务进行负载均衡，具有轮询、加权轮询、最少连接数、静态就近性、动态就近性等算法来实现（提供界面功能截图）； 12.认证方式支持本地认证、USBKey、短信认证、数据库认证、邮箱认证、证书认证、动态口令认证、LDAP 认证、windows AD 认证、RADIUS 认证，并且支持本地用户名密码、证书认证、第三方证书、LDAP、短信认证、邮箱认证之间的“与”的认证；可实现 USBKey 认证、LDAP 认证、硬件特征码等多种因子绑定认证； 13.支持网关能够支持证书透传功能，即将证书直接传递给业务系统，可以根据证书中的 O、OU、CN 作为访问控制项，提供用户对某个业务系统的访问控制权限； 14.支持用户长期不登录时自动锁定，被锁定后需要管理员才能解锁； 15.管理员可分为状态管理员，系统配置管理员，VPN 管理员，应用安全管理员，防火墙管理员，IPsec 管理员，日志管理员，系统维护管理员，创建管理员可以为其分配相应的管理员权限； 16.管理员通过国密浏览器采用国密证书+国密 key 登陆网设备进行设备管理、系统配置； 17.支持移动应用封装功能，客户上传移动应用 APP 进行封装、加固； 18.支持 LDAP 用户动态化和策略化，实现组织单元映射、属性映射，并支持成员组反向映射； 19.支持客户端安全性检查，可以检测客户端进程、文件、注册表、服务、模块、端口、mac 地址、系统补丁、操作系统等信息，并且能够检查用户是否安装杀毒软件和防火墙，判断杀毒软件病毒库是否过期，凡是不符合检查规则的，均不允许用户登录访问； 设备可支持远程应用发布功能，发布 C/S 应用客户端界面而非整个桌面进行发布。	户下载安装（提供界面功能截图）； 11.★设备支持单独对每个应用发布业务进行负载均衡，具有轮询、加权轮询、最少连接数、静态就近性、动态就近性等算法来实现（提供界面功能截图）； 12.认证方式支持本地认证、USBKey、短信认证、数据库认证、邮箱认证、证书认证、动态口令认证、LDAP 认证、windows AD 认证、RADIUS 认证，并且支持本地用户名密码、证书认证、第三方证书、LDAP、短信认证、邮箱认证之间的“与”的认证；可实现 USBKey 认证、LDAP 认证、硬件特征码等多种因子绑定认证； 13.支持网关能够支持证书透传功能，即将证书直接传递给业务系统，可以根据证书中的 O、OU、CN 作为访问控制项，提供用户对某个业务系统的访问控制权限； 14.支持用户长期不登录时自动锁定，被锁定后需要管理员才能解锁； 15.管理员可分为状态管理员，系统配置管理员，VPN 管理员，应用安全管理员，防火墙管理员，IPsec 管理员，日志管理员，系统维护管理员，创建管理员可以为其分配相应的管理员权限； 16.管理员通过国密浏览器采用国密证书+国密 key 登陆网设备进行设备管理、系统配置； 17.支持移动应用封装功能，客户上传移动应用 APP 进行封装、加固； 18.支持 LDAP 用户动态化和策略化，实现组织单元映射、属性映射，并支持成员组反向映射； 19.支持客户端安全性检查，可以检测客户端进程、文件、注册表、服务、模块、端口、mac 地址、系统补丁、操作系统等信息，并且能够检查用户是否安装杀毒软件和防火墙，判断杀毒软件病毒库是否过期，凡是不符合检查规则的，均不允许用户登录访问； 设备可支持远程应用发布功能，发布 C/S 应用客户端界面而非整个桌面进行发布。		

4	**密码应用技术服务，1 项。** **技术参数及性能（配置）要求：** 1. 提供密码应用（密评）方案设计咨询服务，内容包含但不限于：客户现状需求调研分析、针对用户系统密码保障体系建设提供密码应用方案，并保障密码应用方案通过第三方测评机构的密码应用安全性评估。 2. 提供密码应用保障体系建设服务，内容包含但不限于：依据目前密码应用方案建设，成立项目建设团队，主导整体密码体系建设，配合系统应用厂商、网络安全厂商及系统使用方，完成用户系统密码应用保障体系建设，并通过第三方密评机构的安全性评估。 3. 密码安全运营服务，内容包含但不限于：为用户、管理人员及系统运维工作人员提供密码产品、技术等专项培训，保障密码应用工作顺利开展；针对后期业务供对接实施方案、对接咨询、对接测试，对接培训服务等内容，保障业务系统通过商用密码应用安全评估；针对后期出现密码应用安全事件，协助使用单位进行排查及处理。保障用户系统密码体系安全、稳定运行。 4. ★业务系统密码应用服务，内容包含但不限于：针对已有的业务系统接入密码应用服务提供对接方案设计、对接咨询、对接测试，对接培训服务，并为各业务系统提供定制相应的密码服务接口，保证密码服务的有效应用。并可针对业务系统提供密码应用方案设计，满足商用密码应用安全性评估要求及项目备案、验收等国家政策要求。 5. 5G 无线信号源安全网关服务	**提供密码应用技术服务，1 项。** **技术参数及性能（配置）要求响应如下：** 1. 提供密码应用（密评）方案设计咨询服务，内容包含但不限于：客户现状需求调研分析、针对用户系统密码保障体系建设提供密码应用方案，并保障密码应用方案通过第三方测评机构的密码应用安全性评估。 2. 提供密码应用保障体系建设服务，内容包含但不限于：依据目前密码应用方案建设，成立项目建设团队，主导整体密码体系建设，配合系统应用厂商、网络安全厂商及系统使用方，完成用户系统密码应用保障体系建设，并通过第三方密评机构的安全性评估。 3. 密码安全运营服务，内容包含但不限于：为用户、管理人员及系统运维工作人员提供密码产品、技术等专项培训，保障密码应用工作顺利开展；针对后期业务供对接实施方案、对接咨询、对接测试，对接培训服务等内容，保障业务系统通过商用密码应用安全评估；针对后期出现密码应用安全事件，协助使用单位进行排查及处理。保障用户系统密码体系安全、稳定运行。 4. ★业务系统密码应用服务，内容包含但不限于：针对已有的业务系统接入密码应用服务提供对接方案设计、对接咨询、对接测试，对接培训服务，并为各业务系统提供定制相应的密码服务接口，保证密码服务的有效应用。并可针对业务系统提供密码应用方案设计，满足商用密码应用安全性评估要求及项目备案、验收等国家政策要求。 5. 提供密码应用及运维平板服务 6. 提供 5G 无线信号源安全网关服务	完全响应	
5	**国密堡垒机改造，1 项。** **技术参数及性能（配置）要求：** 1. ★主要基于用户现网中使用的堡垒机进行升级改造成国密堡垒机； 2. 改造完成后支持采用国密算法进行重要数据加解密，包括但不限于用户信息、资源账户等； 3. 改造完成后支持对日志信息和访问	**提供国密堡垒机改造，1 项。** **技术参数及性能（配置）要求响应如下：** 1. ★主要基于用户现网中使用的堡垒机进行升级改造成国密堡垒机； 2. 改造完成后支持采用国密算法进行重要数据加解密，包括但不限于用户信息、资源账户等； 3. 改造完成后支持对日志信息和访问	完全响应	

	控制信息进行完整性保护； 4.支持与本次采购的服务器密码机联动，以实现基于国密的数据完整性校验等功能； 支持使用智能密码钥匙进行认证登录，认证时使用专用的密码套件调用加密卡或加密机进行签名验签。	控制信息进行完整性保护； 4.支持与本次采购的服务器密码机联动，以实现基于国密的数据完整性校验等功能； 支持使用智能密码钥匙进行认证登录，认证时使用专用的密码套件调用加密卡或加密机进行签名验签。		
6	**日志审计升级服务，1项。** **技术参数及性能（配置）要求：** 1.★主要基于用户现网中使用的日志审计系统进行软件升级，提供1年服务；升级完成后具备以下功能及相关服务； 2.支持对各类网络设备、安全设备、工作站、存储设备、机房设备、其他设备、中间件、数据库、防病毒系统、服务器系统的日志、事件、告警等安全信息进行全面的审计； 3.支持通过Syslog、SNMP Trap、Netflow V5、JDBC、WMI、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能； 4.支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警； 5.★支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示（提供功能界面截图）； 6.支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证； 7.★支持日志范化策略，针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级，保证最佳范化策略匹配（提供功能界面截图）； 8.★支持对日志中的源和目的IP地址进行自动补全，补全IP地址的资产、国家、区域和城市等信息（提供功能界面截图）； 9.远程支持：提供免费的远程技术支持服务，服务内容包括：产品应用情况及使用问题的解决；相关售后文档(FAQ)	**提供日志审计升级服务，1项。** **技术参数及性能(配置)要求响应如下：** 1.★主要基于用户现网中使用的日志审计系统进行软件升级，提供1年服务；升级完成后具备以下功能及相关服务； 2.支持对各类网络设备、安全设备、工作站、存储设备、机房设备、其他设备、中间件、数据库、防病毒系统、服务器系统的日志、事件、告警等安全信息进行全面的审计； 3.支持通过Syslog、SNMP Trap、Netflow V5、JDBC、WMI、文件\文件夹读取、Kafka等多种方式完成各种日志的收集功能； 4.支持对资产日志进行过滤，设置允许接收和拒绝接收日志，并可以对资产设置一定时间范围内未收到事件后进行主动告警； 5.★支持对资产IP地址（含内网IP）的地理信息进行管理，设置单IP及IP段行政区及经纬度，支持地图显示（提供功能界面截图）； 6.支持对日志进行归一化处理并保留原始日志，方便用户对关键日志快速定位和事后取证； 7.★支持日志范化策略，针对匹配的多条范化策略，系统支持用户手工设置策略匹配优先级，保证最佳范化策略匹配（提供功能界面截图）； 8.★支持对日志中的源和目的IP地址进行自动补全，补全IP地址的资产、国家、区域和城市等信息（提供功能界面截图）； 9.远程支持：提供免费的远程技术支持服务，服务内容包括：产品应用情况及使用问题的解决；相关售后文档(FAQ)	完全响应	

	的提供；产品应用情况通告等； 应急响应：在维保期内，系统出现紧急故障时，将在 1 小时内作出响应，为最终用户提供 7×24 远程电话技术支持服务，如远程无法解决，将安排售后工程师进行紧急现场服务，4 小时内到达用户现场，并配合用户快速解决问题。	的提供；产品应用情况通告等； **应急响应：在维保期内，承诺系统出现紧急故障时，将在 1 小时内作出响应，为最终用户提供 7x24 远程电话技术支持服务（客户经理：庞鲜明，电话:15907893991），如远程无法解决，将安排售后工程师进行紧急现场服务，4 小时内到达用户现场，并配合用户快速解决问题。**		
7	**堡垒机升级服务，1 项** **技术参数及性能（配置）要求：** 1.★主要基于用户现网中使用的堡垒机系统进行软件升级，提供 1 年服务；升级完成后具备以下功能及相关服务； 2.支持用户多次登录失败将自动锁定账户或 IP，可配置解锁时长、到期自动解锁，也可以手动解锁； 3.支持资源申请，运维场景中，对特定的资源发出工单请求，管理员审批后，可以在指定时间段内运维操作该资源； 4.★支持用户水印功能，避免数据泄露无法追责（提供功能界面截图）； 5.支持基于消息等级、消息类型设置是否告警和告警方式； 6.支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云和 Ucloud 云平台的资源； 7.支持通过 Web 页面访问目标支持，包括 SSH、RDP、TELNET、VNC 和应用发布资源； 8.支持 SSH 客户端、FTP 客户端、SFTP 客户端访问目标资源；支持直接在 FTP、SFTP 客户端进行编码切换，支持 big5、GB18030 和 utf8 编码切换； 9.支持将运维资源列表导出成 xshell 和 SecureCRT 格式的配置，通过客户端快速访问资源； 10.★运维过程中支持会话协同，可邀请其他用户参与、协助操作（提供功能界面截图）； 11.支持不同的用户设置不同多因子方式认证，包括手机短信和手机令牌； 12.支持用户帐号和目标设备的部门分权，不同的用户和设备可以归属于不同	**提供堡垒机升级服务，1 项** **技术参数及性能(配置)要求响应如下：** 1.★主要基于用户现网中使用的堡垒机系统进行软件升级，提供 1 年服务；升级完成后具备以下功能及相关服务； 2.支持用户多次登录失败将自动锁定账户或 IP，可配置解锁时长、到期自动解锁，也可以手动解锁； 3.支持资源申请，运维场景中，对特定的资源发出工单请求，管理员审批后，可以在指定时间段内运维操作该资源； 4.★支持用户水印功能，避免数据泄露无法追责（提供功能界面截图）； 5.支持基于消息等级、消息类型设置是否告警和告警方式； 6.支持云主机资源批量添加，包括阿里云、百度云、华为云、腾讯云和 Ucloud 云平台的资源； 7.支持通过 Web 页面访问目标支持，包括 SSH、RDP、TELNET、VNC 和应用发布资源； 8.支持 SSH 客户端、FTP 客户端、SFTP 客户端访问目标资源；支持直接在 FTP、SFTP 客户端进行编码切换，支持 big5、GB18030 和 utf8 编码切换； 9.支持将运维资源列表导出成 xshell 和 SecureCRT 格式的配置，通过客户端快速访问资源； 10.★运维过程中支持会话协同，可邀请其他用户参与、协助操作（提供功能界面截图）； 11.支持不同的用户设置不同多因子方式认证，包括手机短信和手机令牌； 12.支持用户帐号和目标设备的部门分权，不同的用户和设备可以归属于不同	完全响应	

	的部门（子部门）； 13.支持用户的批量修改，包括重置密码、移动部门、更改角色、修改多因子配置、修改有效期、修改IP限制、修改MAC限制； 14.支持SSH、RDP、TELNET、VNC、FTP、SFTP协议主机，支持发布MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client类型的应用； 15.★内置常用的系统类型，包括Linux、Windows、H3C、Huawei、Cisco，无需安装任何客户端插件，使用H5即可直接运维相关资源（提供功能界面截图）； 16.支持查看改密日志，了解改密账户总数、改密成功数量、改密失败数量和未修改数量； 17.支持传统的putty、SecureCRT、MAC Terminal等工具，支持双人授权和多因子认证，运维资源可分页显示，并且可以根据名称、IP、标签等多种条件进行查找； 18.★支持工单权限申请，支持文件上传、文件下载、文件管理、剪切板权限的申请（提供功能界面截图）； 19.远程支持：提供免费的远程技术支持服务，服务内容包括：产品应用情况及使用问题的解决；相关售后文档(FAQ)的提供；产品应用情况通告等； **应急响应：在维保期内，系统出现紧急故障时，将在1小时内作出响应，为最终用户提供7×24远程电话技术支持服务，如远程无法解决，将安排售后工程师进行紧急现场服务，4小时内到达用户现场，并配合用户快速解决问题。**	的部门（子部门）； 13.支持用户的批量修改，包括重置密码、移动部门、更改角色、修改多因子配置、修改有效期、修改IP限制、修改MAC限制； 14.支持SSH、RDP、TELNET、VNC、FTP、SFTP协议主机，支持发布MySQL、SQL Server、Oracle、IE、Firefox、Chrome、VNC Client、SecBrowser、VSphere Client类型的应用； 15.★内置常用的系统类型，包括Linux、Windows、H3C、Huawei、Cisco，无需安装任何客户端插件，使用H5即可直接运维相关资源（提供功能界面截图）； 16.支持查看改密日志，了解改密账户总数、改密成功数量、改密失败数量和未修改数量； 17.支持传统的putty、SecureCRT、MAC Terminal等工具，支持双人授权和多因子认证，运维资源可分页显示，并且可以根据名称、IP、标签等多种条件进行查找； 18.★支持工单权限申请，支持文件上传、文件下载、文件管理、剪切板权限的申请（提供功能界面截图）； 19.远程支持：提供免费的远程技术支持服务，服务内容包括：产品应用情况及使用问题的解决；相关售后文档(FAQ)的提供；产品应用情况通告等； **应急响应：在维保期内，承诺系统出现紧急故障时，将在1小时内作出响应，为最终用户提供7x24 远程电话技术支持服务（客户经理：庞鲜明，电话:15907893991），如远程无法解决，将安排售后工程师进行紧急现场服务，4 小时内到达用户现场，并配合用户快速解决问题。**		
8	**威胁感知系统升级服务，1项。** **技术参数及性能（配置）要求：** 1.★主要基于用户现网中使用的威胁感知系统进行软件升级及硬件维保服务，提供1年服务；升级完成后具备以下功能及相关服务；	**提供威胁感知系统升级服务，1项。** **技术参数及性能(配置)要求响应如下：** 1.★主要基于用户现网中使用的威胁感知系统进行软件升级及硬件维保服务，提供1年服务；升级完成后具备以下功能及相关服务；	完全响应	

	2.支持定期接收云端提供的威胁情报，威胁情报支持在线和离线升级两种方式； 3.支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等； 4.支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk等）、压缩格式文件（RAR、ZIP、GZ、7Z等）、文档类型文件（word、excel、pdf、rtf、ppt等）； 5.支持常见数据库协议的识别或还原：DB2、Oracle、SQL Server、Sybase、MySQL、MongoDB、PostgreSQL等协议； 6.★威胁检测告警能够直接体现攻击结果即企图、成功、失陷等，同时支持威胁情报实时匹配检测和自定义威胁情报（提供功能界面截图）； 7.网络攻击支持的协议类型达到100种以上，网络攻击引擎支持多种DDoS检测：SYN FLOOD、NTP放大、DNS放大、CC拒绝服务攻击、Udpflood、http flood、Pingflood、Dnsreqflood、Dnsreplyflood、ACK_FLOOD、PSH_ACK_FLOOD、ACK_FIN_FLOOD等； 8.具备WEB攻击检测技术，检测类型包含SQL注入、跨站脚本攻击、文件写入、文件下载、文件上传、文件读取、文件包含、弱口令、权限许可和访问控制、配置不当/错误、目录遍历、默认配置不当、命令执行、敏感信息/重要文件泄露、逻辑/设计错误、跨站请求伪造、后门程序、非法授权访问/权限绕过、代码执行、URL跳转、系统/服务配置不当等等，告警事件能标记主机攻陷状态是否失陷； 9.支持语义分析检测，提升未知威胁检测能力； 10.★支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒	2.支持定期接收云端提供的威胁情报，威胁情报支持在线和离线升级两种方式； 3.支持常见协议识别并还原网络流量，用于取证分析、威胁发现，支持：http、dns、smtp、pop3、imap、webmail、DB2、Oracle、MySQL、sql server、Sybase、SMB、FTP、SNMP、telnet、nfs等； 4.支持对流量中出现文件传输行为进行发现和还原，并记录文件MD5发送至分析设备，如可执行文件（EXE、DLL、OCX、SYS、COM、apk等）、压缩格式文件（RAR、ZIP、GZ、7Z等）、文档类型文件（word、excel、pdf、rtf、ppt等）； 5.支持常见数据库协议的识别或还原：DB2、Oracle、SQL Server、Sybase、MySQL、MongoDB、PostgreSQL等协议； 6.★威胁检测告警能够直接体现攻击结果即企图、成功、失陷等，同时支持威胁情报实时匹配检测和自定义威胁情报（提供功能界面截图）； 7.网络攻击支持的协议类型达到100种以上，网络攻击引擎支持多种DDoS检测：SYN FLOOD、NTP放大、DNS放大、CC拒绝服务攻击、Udpflood、http flood、Pingflood、Dnsreqflood、Dnsreplyflood、ACK_FLOOD、PSH_ACK_FLOOD、ACK_FIN_FLOOD等； 8.具备WEB攻击检测技术，检测类型包含SQL注入、跨站脚本攻击、文件写入、文件下载、文件上传、文件读取、文件包含、弱口令、权限许可和访问控制、配置不当/错误、目录遍历、默认配置不当、命令执行、敏感信息/重要文件泄露、逻辑/设计错误、跨站请求伪造、后门程序、非法授权访问/权限绕过、代码执行、URL跳转、系统/服务配置不当等等，告警事件能标记主机攻陷状态是否失陷； 9.支持语义分析检测，提升未知威胁检测能力； 10.★支持基于威胁情报的威胁检测，检测类型包含APT事件、僵尸网络、勒		

	索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报（提供功能界面截图）； 11.★支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（提供功能界面截图）； 12.★支持与终端安全管理系统联动，实现恶意文件的查杀、被感染主机的网络隔离（提供功能界面截图）； 13.远程支持：提供免费的远程技术支持服务，服务内容包括：产品应用情况及使用问题的解决；相关售后文档(FAQ)的提供；产品应用情况通告等； 14.保修服务：产品在维保期内提供免费保修服务，系统发生故障后将提供快速维修或更换发生故障的产品等服务； 15.巡检服务：在维保期内，将定期提供上门检修、检测及维护，或经业务方同意进行电话询查等巡检服务； **应急响应：在维保期内，系统出现紧急故障时，将在 1 小时内作出响应，为最终用户提供 7×24 远程电话技术支持服务，如远程无法解决，将安排售后工程师进行紧急现场服务，4 小时内到达用户现场，并配合用户快速解决问题。**	索软件、流氓推广、窃密木马、网络蠕虫、远控木马、黑市工具、其他恶意软件，并可自定义威胁情报（提供功能界面截图）； 11.★支持与云端威胁情报中心联动，可对攻击 IP、C&C 域名和恶意样本 MD5 进行一键搜索，查看基本信息、相关样本、关联 URL、可视化分析、域名解析、注册信息、关联域名、数字证书等（提供功能界面截图）； 12.★支持与终端安全管理系统联动，实现恶意文件的查杀、被感染主机的网络隔离（提供功能界面截图）； 13.远程支持：提供免费的远程技术支持服务，服务内容包括：产品应用情况及使用问题的解决；相关售后文档(FAQ)的提供；产品应用情况通告等； 14.保修服务：产品在维保期内提供免费保修服务，系统发生故障后将提供快速维修或更换发生故障的产品等服务； 15.巡检服务：在维保期内，将定期提供上门检修、检测及维护，或经业务方同意进行电话询查等巡检服务； **应急响应：在维保期内，承诺系统出现紧急故障时，将在 1 小时内作出响应，为最终用户提供 7x24 远程电话技术支持服务（客户经理：庞鲜明，电话:15907893991），如远程无法解决，将安排售后工程师进行紧急现场服务，4 小时内到达用户现场，并配合用户快速解决问题。**		
9	**内网终端安全升级服务，1 项。** **技术参数及性能（配置）要求：** 1.★需要对用户内网中使用的终端安全管理系统延续版本升级及原厂售后维保服务，提供 1 年升级维保服务； 2.服务中包含 1000 个 Windows 客户端升级维保服务，14 个 Windows Server 服务器升级维保服务；升级后 PC 终端包含防病毒、补丁管理、运维管控及移动存储管理等功能；Windows Server 服务器端包含防病毒及补丁管理功能； 3.PC 终端升级后支持以下功能： 1）支持根据分组、计算机名称、IP 地	**提供内网终端安全升级服务，1 项。** **技术参数及性能(配置)要求响应如下：** 1.★需要对用户内网中使用的终端安全管理系统延续版本升级及原厂售后维保服务，提供 1 年升级维保服务； 2.服务中包含 1000 个 Windows 客户端升级维保服务，14 个 Windows Server 服务器升级维保服务；升级后 PC 终端包含防病毒、补丁管理、运维管控及移动存储管理等功能；Windows Server 服务器端包含防病毒及补丁管理功能； 3.PC 终端升级后支持以下功能： 1）支持根据分组、计算机名称、IP 地	完全响应	

	址、操作系统、在线状态等条件筛选终端进行管理，支持单点维护功能； 2）支持通过图形化展示终端部署统计、终端安全趋势、终端更新状态、终端程序版本、终端在线统计、病毒库版本分布、安全更新和重要补丁安全趋势等信息； 3）★客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新，支持设置不同终端类型设置和每批次观察时长（提供功能界面截图）； 4）支持终端“防退出”、“防卸载”密码保护，支持设置自我保护功能，防止客户端进程被恶意终止、注入、劫持； 5）支持病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本； 6）支持手动添加、导入、导出黑白名单，支持通过文件数字签名添加黑白名单管理； 7）支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小； 8）支持扫描资源占用设置，可设置不限制、均衡型、低资源等三种模式； 9）★支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护（提供功能界面截图）； 10）支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录； 11）支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁； 12）支持对Windows操作系统、IE、.NET Framework、Office、Adobe、硬件驱动更新等软件进行补丁修复，支持补丁类型和级别包括：安全更新、重要补丁、功能补丁、可选补丁等； 13）★支持灰度发布的漏洞修复策略，	址、操作系统、在线状态等条件筛选终端进行管理，支持单点维护功能； 2）支持通过图形化展示终端部署统计、终端安全趋势、终端更新状态、终端程序版本、终端在线统计、病毒库版本分布、安全更新和重要补丁安全趋势等信息； 3）★客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新，支持设置不同终端类型设置和每批次观察时长（提供功能界面截图）； 4）支持终端“防退出”、“防卸载”密码保护，支持设置自我保护功能，防止客户端进程被恶意终止、注入、劫持； 5）支持病毒防护概况：终端基础信息、病毒库版本、发现病毒数、未处理病毒数、最后查杀时间、文件防护状态、引擎使用状态、扩展病毒库版本； 6）支持手动添加、导入、导出黑白名单，支持通过文件数字签名添加黑白名单管理； 7）支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小； 8）支持扫描资源占用设置，可设置不限制、均衡型、低资源等三种模式； 9）★支持对进程防护、注册表防护、驱动防护、U盘安全防护、邮件防护、下载防护、IM防护、局域网文件防护、网页安全防护、勒索软件防护（提供功能界面截图）； 10）支持自动阻止远程登录行为，防护黑客远程爆破和拦截恶意的远程登录； 11）支持网络入侵拦截对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁； 12）支持对Windows操作系统、IE、.NET Framework、Office、Adobe、硬件驱动更新等软件进行补丁修复，支持补丁类型和级别包括：安全更新、重要补丁、功能补丁、可选补丁等； 13）★支持灰度发布的漏洞修复策略，		

	将全网终端划分为由小到大的多个批次，按批次逐步扩大允许更新的范围，自动化编排完成漏洞修复（提供功能界面截图）； 14）支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口、IP范围； 15）支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源，并支持通过设备名称、PID/VID、实例路径等多维度进行添加例外或加黑； 16）支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理； 4.Windows Server服务器端升级后支持以下功能： 1）支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描； 2）★客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新（提供功能界面截图）； 3）支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复； 4）支持对终端当扫描到感染型病毒、顽固木马时，扫描时不允许终端用户暂停或停止扫描任务； 5）病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件； 6）★支持灰度发布的漏洞修复策略，将全网终端划分为由小到大的多个批次，按批次逐步扩大允许更新的范围，自动化编排完成漏洞修复（提供功能界	将全网终端划分为由小到大的多个批次，按批次逐步扩大允许更新的范围，自动化编排完成漏洞修复（提供功能界面截图）； 14）支持主机防火墙功能，通过添加IP、域名规则、支持允许/拒绝规则、支持任意流向拦截和允许，支持TCP、UDP、TCP+UDP、ICMP、多播和组播，支持自定义端口、IP范围； 15）支持外设库管理，可统计终端外接的各种设备，包括厂商和设备类型、产品、数量、PID、VID和设备来源，并支持通过设备名称、PID/VID、实例路径等多维度进行添加例外或加黑； 16）支持对互联网出口地址探测，支持对违规的互联网出口进行发现、断开网络、终端锁屏、断网+锁屏处理； 4.Windows Server服务器端升级后支持以下功能： 1）支持对压缩包内的病毒扫描，支持多层压缩包的扫描，可自定义配置压缩包的扫描层数，至少大约10层模式下的扫描； 2）★客户端主程序、病毒库版本支持按分组和多批次进行灰度更新，保持在低风险中完成终端能力更新（提供功能界面截图）； 3）支持对Windows操作系统、IE、.NET Framework、Office、Adobe Flash Player、Adobe Acrobat和Adobe Acrobat Reader DC、硬件驱动更新等软件进行补丁修复； 4）支持对终端当扫描到感染型病毒、顽固木马时，扫描时不允许终端用户暂停或停止扫描任务； 5）病毒扫描支持扫描所有文件和仅扫描程序及文档文件设置，支持对压缩包文件设置最大扫描层数和大小，当发现压缩包内存在病毒时，还需继续扫描压缩包内其他文件； 6）★支持灰度发布的漏洞修复策略，将全网终端划分为由小到大的多个批次，按批次逐步扩大允许更新的范围，自动化编排完成漏洞修复（提供功能界		

	面截图）； 7）支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。 5.远程支持：提供免费的远程技术支持服务，服务内容包括：产品应用情况及使用问题的解决；相关售后文档(FAQ)的提供；产品应用情况通告等； 6.保修服务：产品在维保期内提供免费保修服务，系统发生故障后将提供快速维修或更换发生故障的产品等服务； 7.巡检服务：在维保期内，将定期提供上门检修、检测及维护，或经业务方同意进行电话询查等巡检服务； **应急响应：在维保期内，系统出现紧急故障时，将在1小时内作出响应，为最终用户提供7×24远程电话技术支持服务，如远程无法解决，将安排售后工程师进行紧急现场服务，4小时内到达用户现场，并配合用户快速解决问题。**	面截图）； 7）支持开启自动修复漏洞，包括开机时修复，并支持随机延迟执行、间隔修复和按时间段修复，可设置延迟时间、间隔修复时间和修复时间段。 5.远程支持：提供免费的远程技术支持服务，服务内容包括：产品应用情况及使用问题的解决；相关售后文档(FAQ)的提供；产品应用情况通告等； 6.保修服务：产品在维保期内提供免费保修服务，系统发生故障后将提供快速维修或更换发生故障的产品等服务； 7.巡检服务：在维保期内，将定期提供上门检修、检测及维护，或经业务方同意进行电话询查等巡检服务； **应急响应：在维保期内，系统出现紧急故障时，将在1小时内作出响应，为最终用户提供7x24 远程电话技术支持服务（客户经理：庞鲜明，电话:15907893991），如远程无法解决，将安排售后工程师进行紧急现场服务，4 小时内到达用户现场，并配合用户快速解决问题。**		
10	**防火墙板卡扩容，2项。** **技术参数及性能（配置）要求：** 1.4口万兆光口板卡（选配）：4个SFP+插槽；万兆多模光口模块*4，波长850nm，有效传输距离0.3km，LC接口。 2.满足兼容原有防火墙设备型号NSG5000-R-QW的接口扩容。	**防火墙板卡扩容，2项。** **技术参数及性能（配置）要求：** 1.4口万兆光口板卡（选配）：4个SFP+插槽；万兆多模光口模块*4，波长850nm，有效传输距离0.3km，LC接口。 2.满足兼容原有防火墙设备型号NSG5000-R-QW的接口扩容。	完全响应	

说明：1.应写明竞争性谈判响应文件对商务与服务技术要求的响应和偏离情况；

2.应对照竞争性谈判文件“第四部分 采购项目需求”，逐条说明所提供服务已对竞争性谈判文件的商务、服务、技术要求做出了实质性的响应，并申明与采购项目要求的响应和偏离。特别对有具体商务、服务、技术要求的，谈判供应商必须提供对应的详细应答。如果仅注明“符合”、“满足”或简单复制竞争性谈判文件要求，将导致谈判被拒绝。

中国移动通信集团广西有限公司北海分公司（公章）

年 月 日