甲方合同编号：

乙方合同编号：SMXXY20260700031

三门峡市县一体化新型智慧城市建设（一期）延续项目A包合同

甲方（采购方）：三门峡市行政审批和政务信息管理局

乙方（服务方）：三门峡崤云信息服务股份有限公司

二〇二六年七月

甲方（采购方）：三门峡市行政审批和政务信息管理局

地址：河南省三门峡市湖滨区金谷路与广场北路交叉口西 50 米

项目联系人：彭振东

电话：13839820651

电子邮箱：zsjxmglk@163.com

乙方（服务方）：三门峡崤云信息服务股份有限公司

地址： 河南省三门峡市五原西路传媒大厦 11 楼

项目联系人：王玉卿

电话：15516291799

电子邮箱：wangyuqing@smxxy.cn

鉴于甲方购买乙方提供的三门峡市县一体化新型智慧城市建设（一期）延续项目A包服务，双方根据《中华人民共和国民法典》及其他有关法律法规的规定，经过甲乙双方协商一致，达成如下合同，以资共同信守。

第1条　合同标的

1.1　乙方根据本合同约定和甲方要求提供“三门峡市县一体化新型智慧城市建设（一期）延续项目A包”（以下简称“本项目”）政务云平台服务。

1.2　本合同服务内容包含计算服务、存储服务、备份服务、网络服务、基础软件服务、机柜服务、容器服务、云数据库服务、云中间件服务、安全服务、密码服务。服务要求见单一来源采购文件，服务内容和单价见附件1《服务目录》。

1.3　本项目服务范围为市本级、义马市、渑池县、湖滨区、陕州区、灵宝市、卢氏县、城乡一体化示范区、经济开发区、现代服务业开发区。

1.4　本合同的合作模式采用乙方投资、建设，甲方购买服务。乙方投入的所有软、硬件的所有权属于乙方，甲方在合同期限内仅享有使用权；在甲方使用过程中产生的所有数据归甲方所有。

第2条　合同期限

本合同服务期限为自合同签订之日起3年。

第3条　合同金额和计费方式

3.1　本合同含税上限价为￥64,153,486.44元（大写：人民币陆仟肆佰壹拾伍万叁仟肆佰捌拾陆元肆角肆分）。

3.2　本合同采用据实结算的方式计取服务费，单价见附件1《服务目录》。

3.3　甲乙双方应于每季度结束后30日内，核对该季度的服务清单，并盖章确认（一式两份，各执一份）。所有服务清单将作为后续绩效评价和合同费用结算的依据。

3.4　本合同总金额包含了甲方就乙方履行本合同所需支付的全部服务费用，除双方另有书面约定外，甲方不应向乙方另行支付任何费用。

3.5　当月15日（含）之前开通（或变更）的资源按整月核算费用；当月15日之后开通（或变更）的资源，当月不计费，自次月1日起开始计费。

第4条　绩效评价和支付方式

4.1合同签订后，由甲方聘请第三方机构每满一年对乙方的服务进行一次绩效评价，以绩效评价结果作为合同款项支付的依据。

4.2　绩效评价时间和支付方式约定如下：

（1）2027年8月31日前，甲方应完成第一年度的项目绩效评价，并根据绩效评价结果和服务清单向乙方支付第一年度服务费。

（2）2028年8月31日前，甲方应完成第二年度的项目绩效评价，并根据绩效评价结果和服务清单向乙方支付第二年度服务费。

（3）2029年8月31日前，甲方应完成第三年度的项目绩效评价，并根据绩效评价结果和服务清单向乙方支付第三年度服务费。

4.3　甲方每次付款前，乙方应按前述要求开具合规发票，具体开票时间以甲方

实际付款节点为准。

4.4　甲方开票信息如下，甲方如需变更开票信息，应提前十日书面通知乙方：

甲方名称：三门峡市行政审批和政务信息管理局

纳税人识别号：11411200MB1851405M

开户行：建设银行股份有限公司三门峡分行财政大厦支行

账号：41050169864608000355

4.5　乙方结算账户信息如下，乙方如需变更账户，应提前十日书面通知甲方：

乙方名称：三门峡崤云信息服务股份有限公司

开户行：建设银行股份有限公司三门峡分行财政大厦支行

账号：41050169864600000093

第5条　甲方的权利和义务

5.1　甲方在合同期限内，必须遵守《中华人民共和国网络安全法》《中华人民共和国计算机信息网络国际联网管理暂行规定》《互联网信息服务管理办法》等法律法规或相关规定，不得存在任何违法违规行为，不得侵犯乙方以及任何第三方的合法权益。

5.2、甲方有权要求乙方按照本项目单一来源采购文件及乙方提交的响应文件内容，提供项目服务。

5.3　甲方对在本合同履行期间，通过乙方提供的服务所产生、收集、处理、存储的全部数据（包括但不限于政务信息、业务数据、用户资料、统计报表、分析结果）享有所有权。

5.4　甲方应支持、协助乙方做好项目的相关工作，为乙方在合同履行过程中与相关政府部门及其他第三方的沟通、协调提供必要的协助。

5.5　甲方应向乙方提供开展服务所需的资料、系统访问权限及其他支持。

5.6　甲方在合同期内，如发现乙方存在服务质量问题，有权下达整改通知书，并要求乙方限期整改。乙方未落实整改要求或整改后仍不能满足本合同要求的，甲方有权终止本合同，并要求乙方承担由此给甲方造成的所有直接损失。

5.7　乙方未按要求落实重大安全事件处置责任、处置不及时或处置不当的，甲方有权责令乙方限期整改，并视情节采取扣减费用、暂停服务等措施。因乙方原因造成政务信息系统中断、数据泄露、资源重大浪费等损失的，甲方有权依法追究乙方的法律责任，并由乙方承担因此给甲方造成的所有直接损失。特别约定：因本合同第10条约定情形造成的除外。

5.8　甲方应按照合同约定组织项目绩效评价，并应在约定期限内完成付款。

第6条　乙方的权利和义务

6.1　乙方应按照本项目单一来源采购文件、响应文件及本合同约定，向甲方提供三门峡市县一体化新型智慧城市建设（一期）延续项目A包服务，并按照《服务目录》（附件一）的报价标准收取费用。

6.2　乙方提供的服务应符合国家网络安全等级保护要求及商用密码应用安全性评估要求，且应每年取得等保备案证明或由具备资质的第三方测评机构出具的合规测评报告。

6.3　合同期内，乙方在收到甲方的书面整改通知后,应当针对存在的问题进行及时分析并以书面形式予以回复,并在甲方指定期限内完成整改。

6.4　乙方保证其交付的服务成果不侵犯第三方合法权益。若因乙方原因导致服务成果被认定侵权，乙方应承担甲方因此遭受的所有直接损失。

6.5　乙方应采取符合国家及行业标准的技术措施和管理制度，保障甲方数据的保密性、完整性及可用性，防止数据泄露、损毁、丢失或被未授权访问。乙方应按照《网络安全等级保护基本要求》落实安全防护措施。

6.6　甲方组织项目绩效评价时，乙方应予以配合，按要求提供评价所需的资料、数据及说明。

6.7　本合同到期或终止后30个工作日内（豁免期），乙方应通知并配合甲方完成数据迁移或备份。豁免期满，若甲方未完成数据迁移或备份，经双方书面确认后，乙方可销毁数据。

6.8　为保障本合同项下服务的稳定性与连续性，乙方可根据需要自行采购或配置相关软硬件设备及设施。前述资产的所有权归乙方所有，甲方仅在本合同有效期内享有使用该等资产所提供服务的权利。如合同终止或解除，乙方有权取回或处置前述资产。

6.9　如政府审计部门或其委托的第三方审计单位需对涉及本合同的事项进行审计，乙方应当按照政府审计有关法律法规和政策要求，支持、协助审计部门或其委托的审计单位开展工作。

第7条　知识产权

7.1　本合同生效时已经存在并为各方合法拥有或使用的技术、资料和信息，其知识产权和其他权益仍归原权利人所有。

7.2　乙方及其工作人员在为甲方提供服务期间所产生的合法原创知识产权归乙方所有。

7.3　甲方对在本合同履行期间向乙方提供的业务数据、政务信息及其他资料，保留甲方原有的所有权及知识产权,本合同的履行不视为上述权利转移给乙方。

7.4　双方确认，乙方利用甲方数据进行分析、处理所形成的分析结果、统计报表、可视化展示，其数据内容归甲方所有，但乙方实现上述成果所使用的软件工具、

算法模型、技术方法归乙方所有。

7.5　乙方保证其在本合同项下向甲方提供的服务（不包括甲方提供的数据、资料、第三方软件及开源组件）不侵犯第三方的知识产权。若服务被生效法律文书认定侵犯第三方知识产权，并因此涉入诉讼、仲裁或其他司法程序，乙方应就诉讼策略及其他事宜向甲方提供充分的支持与协助，并承担甲方因此而产生的所有直接损失；如有生效的法律文书禁止甲方继续使用相关服务或要求甲方向第三人支付使用费，乙方应采取相应的补救措施，保障相应服务正常运行，并赔偿由此给甲方造成的所有直接损失。

7.6　甲方知悉可能的侵权主张后,应立即书面通知乙方,由乙方全权处理。未经乙方同意,甲方不得自行与第三方和解或承认侵权。

7.7　甲方应对其使用的、非由乙方提供的第三方产品的合法性、合规性、安全性及知识产权事宜自行承担责任。甲方保证其使用（包括授权乙方进行操作）第三方产品的行为，均已获得相关权利人的完整、有效的授权，且该等使用不会侵犯任何第三方的合法权益（包括但不限于知识产权、商业秘密等）。

7.8　因甲方自行使用第三方产品所引发的任何纠纷、索赔、诉讼或行政处罚（包括但不限于知识产权侵权、数据安全、隐私泄露等），均由甲方独立负责解决并承担由此产生的全部费用。若因此导致乙方遭受任何损失（包括但不限于赔偿款、罚款、律师费、诉讼费等），甲方应予以全额赔偿。

第 8 条　保密

8.1　本合同拥有信息的一方（“提供方”）根据本合同向另一方（“接收方”）提供的信息，包括但不限于技术性信息、商业性信息、文件、程序、计划、技术、图表、模型、参数、数据、标准、专有技术、业务或业务运作方法以及其他专有信息，本合同履行过程中形成的所有信息、数据、资料、阶段性成果和最终成果，本合同的条款和与本合同有关的其他商业信息和技术信息(以下统称“保密信息”)，只能由接收方及其人员为本合同目的而使用。除本合同另有规定外，对于提供方提供的任何保密信息，未经提供方的书面同意，接收方及其知悉保密信息的人员均不得直接或间接地以任何方式提供、披露或转让给任何第三方，或许可第三方使用，或以保密信息为任何第三方提供任何意见或建议。

8.2　提供方向接收方提供或披露的保密信息，仅可由接收方为执行本合同需要披露给指定的雇员，并且仅在为执行本合同所需的范围内进行该等披露。但是，接收方在采取一切合理的预防措施之前，不得向其雇员披露任何保密信息。该等预防措施包括但不限于告知该等雇员将要披露信息的保密性质，要求该等雇员做出至少与本合同保密义务一样严格的保密承诺等，以防止该等雇员为个人利益使用保密信息或向任何第三方做出未经授权的披露。接收方雇员违反保密义务的，视为接收方违反保密义

务。

8.3　接收方的律师、会计师、承包商和顾问为提供专业协助而需要了解保密信息时，接收方可向其披露保密信息，但是，接收方应要求上述人员签订保密协议或按照有关职业道德标准履行保密义务。

8.4　如相关政府部门或监管机构要求接收方披露任何保密信息，接收方可在该政府部门或机构要求的范围内做出披露而无需承担本合同项下的责任。但前提是，接收方应立即将需披露的信息书面通知提供方，以便提供方采取必要的保护措施，且该等通知应尽可能在信息披露前做出，并且接收方应尽商业上合理的努力确保该等被披露的信息获得有关政府机关或机构的保密待遇。

8.5　在任何情形下，本条所规定的保密义务应永久持续有效。

8.6　当本合同解除或终止时，接收方应立即停止使用且不得许可第三方使用提供方的保密信息。同时，接收方应按照提供方的书面要求，将提供方提供的保密信息退还提供方或予以删除或销毁，不得以任何形式留存。

第 9 条　违约责任

9.1　任何一方不履行本合同约定的义务或履行义务不符合本合同约定的，视为违约；违约方应停止违约行为，并按守约方的要求继续履行、采取补救措施或赔偿损失。乙方提供的服务不能满足本项目单一来源采购文件的服务要求的，视为乙方违约。

9.2　如乙方未能按本合同约定向甲方提供服务，则每逾期一日，应按当期应付服务费用的万分之三向甲方支付逾期违约金。逾期超过三十日，甲方有权单方解除本合同，同时，乙方应向甲方支付当期应付服务费用的百分之十的违约金，违约金不足以弥补甲方的全部损失的，乙方还应予以赔偿。

9.3　如甲方未能按本合同约定向乙方支付费用，每逾期一日，应按当期应付服务费用的万分之三向乙方支付逾期违约金。逾期超过三十日，乙方有权单方解除本合同，并立即停止提供后续服务且不承担任何违约责任。同时，甲方应向乙方支付当期应付服务费用百分之十的违约金，违约金不足以弥补乙方的全部损失的，甲方还应予以赔偿。甲方未按合同约定的时间组织并完成绩效评价的，视为违约。

9.4　任何一方违反本合同所约定的保密义务，给对方造成负面影响或损失，违约方应按本合同总价的百分之二十支付违约金。如包括利润在内的实际损失超过该违约金，受损失一方还有权要求对方赔偿超过部分的损失。

9.5　除本合同另有约定或法律规定外，任何一方无权单方变更或解除本合同，合同变更、解除须经双方协商一致并签署书面协议。任何一方违反本条约定，应向守约方支付合同总金额百分之十的违约金。

第 10 条 不可抗力

10.1　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。

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） 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；

（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；

（3） 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三十日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。

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。

10.4 如果不可抗力事件的影响持续达三十日，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变更或终止。如在一方发出协商书面通知之日起十日内双方无法就此达成一致，双方可根据乙方服务时间结算已产生的费用，多余费用乙方应在七日内退还甲方指定账户；实际已履行待支付的费用，甲方应在七日内支付至乙方指定账户。经协商一致无异议结算后，任何一方均有权解除本合同而无需承担违约责任。

第 11 条 通知与送达

11.1 根据本合同需要发出的全部通知，均须采取书面形式，以专人递送、传真、电子邮件、特快专递或挂号信件发出。特快专递或挂号信件的交寄日以邮戳为准。上述书面通知均须标明合同对方为收件人。

11.2 上述书面通知按对方在本合同首页中所列的地址发出，并按本合同条款规定时间被视为已经送达。如双方中任何一方的地址有变更时，须在变更前十日以书面形式通知对方，因迟延通知而造成的损失，由延迟通知方承担责任。

11.3 双方将按如下规定确定通知被视为正式送达的日期：以专人递送的，接收人签收之日视为送达；以传真方式发出的，发件方发送后打印出的发送确认单所示时间视为送达；以电子邮件方式发出的，电子邮件到达接收方指定电子邮箱的时间视为送达；以特快专递形式发出的,以实际签收日期为送达日期,若对方拒收的,发往本市内的,发出后第 3 日视为送达,发往国内其他地区的,发出后第 3 日视为送达;以挂号信件方式发出的,以实际签收日期为送达日期,若对方拒收的,发往本市内的,邮寄后第 7 日视为送达;发往国内其他地区的,邮寄后第 15 日视为送达。

第 12 条 法律适用和争议解决

12.1　双方就本合同的解释和履行发生的任何争议，应通过友好协商解决。协商不成的，应提交三门峡仲裁委员会，按照申请仲裁时该会现行有效的仲裁规则进行仲裁。仲裁地点在三门峡。仲裁裁决是终局的，对双方均有约束力。

12.2　争议解决过程中，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。

12.3　本合同全部或部分无效的，本条（即第 12 条法律适用和争议解决）依然有效。

第 13 条 合同变更、解除

13.1　变更、解除的事由

13.1.1 若本合同的继续履行将损害国家利益和社会公共利益，则双方均有权书面通知对方要求变更、解除本合同或针对本合同项下服务另行签署其他书面合同。

13.1.2 非乙方原因导致本合同在双方约定的期限内无法完全履行或在履行过程中出现双方无法预见的困难，导致合同目的难以实现的，双方可经协商决定变更或解除本合同。

13.2　除本合同另有约定或法律规定外，任何一方无权单方变更或解除本合同，合同变更、解除须经双方协商一致并签署书面协议。

13.3　特别约定：乙方具备平台个性化开发能力，可根据甲方业务发展需要提供新增功能、界面改版、业务流程变更、新增数据接口、第三方系统对接等定制开发服务。定制开发服务不包含在本合同服务范围内，若甲方提出相关需求，双方应根据开发工作量及技术难度协商一致，另行签订委托开发合同或补充协议。

第 14 条 其他

14.1　本合同由双方法定代表人（负责人）或授权代表签字并加盖公章或合同专用章后生效。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。

14.2　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，须由双方以书面作出并经双方签署后方为有效。补充协议与本合同具有同等法律效力，补充协议与本合同存在不一致之处的，以补充协议为准。

14.3　本合同一式六份，双方各执三份，具有相同法律效力。

14.4　本合同附件是本合同不可分割的部分，若附件与合同正文冲突，以本合同正文为准。

附件 1：《服务目录》

附件 2：《技术服务规范书》

（以下无正文）

（本页无正文，为《三门峡市县一体化新型智慧城市建设（一期）延续项目A包合同》的签署页）

甲　　方（盖章）：三门峡市行政审批和政务信息管理局

负责人或授权代表（签字）：

日　　期：2026.1.22

乙　　方（盖章）：三门峡崤云信息服务股份有限公司

法定代表人或授权代表（签字）：

日　　期：2026.1.22

附件 1：

服务目录

服务类别	规格		报价（元/月）
1.计算服务			
云主机服务	两核	2GB	76
		4GB	125
		8GB	154
	四核	4GB	220
		8GB	250
		16GB	310
	八核	8GB	440
		16GB	500
		32GB	630
		64GB	880
	十六核	16GB	889
		32GB	1000
		64GB	1200
		128GB	1510
		256GB	2410
	三十二核	32GB	1760
		64GB	2010
		128GB	2310
		256GB	2920
		512GB	4980
	核（vCPU）	1 核	30
	内存（G）	1GB	8
高性能物理机	CPU>=2 路 6 核，内存>=64G,本地硬盘>=600G		1020
	CPU>=2 路 8 核，内存>=256G,本地硬盘>=600G		1132
	CPU>=2 路 10 核，内存>=320G,本地硬盘>=600G		1244
	CPU>=2 路 10 核，内存>=256G,本地硬盘>=6TB		1346
	CPU>=2 路 10 核，内存>=256G,本地硬盘>=6TB，SSD 硬盘>=1.92TB		1384
	CPU>=2 路 10 核,内存>=256G,本地硬盘>=33.2TB,SSD 硬盘>=1.92TB		1889
	CPU>=2 路 14 核，内存>=320G，本地硬盘>=600G		1469
	CPU>=4 路 10 核，内存>=256G，本地硬盘>=600G		2047
	CPU>=4 路 14 核，内存>=320G，本地硬盘>=600G		2393
	CPU>=8 路 10 核，内存>=512G，本地硬盘>=600G		3554
	CPU>=8 路 14 核，内存>=512G，本地硬盘>=600G		4550
	CPU>=8 路 16 核，内存>=512G，本地硬盘>=600G		5000

国产化高性能物理机		2 路 32 核 CPU，256G 内存，2 块 480GSATASSD 硬盘（系统盘），一张 2 端口万兆网卡（含光模块）		1972
		2 路 48 核 CPU，256G 内存，2 块 480GSATASSD 硬盘（系统盘），一张 2 端口万兆网卡（含光模块）		2325
		2 路 64 核 CPU，256G 内存，2 块 480GSATASSD 硬盘（系统盘），一张 2 端口万兆网卡（含光模块）		2676
高性能物理机可选配件		32G 内存	1 块	64
		1TB SAS 硬盘	1 块	31
		1TB SATA 硬盘	1 块	16
		1TB SATA SSD 硬盘	1 块	58
		1TB NVME SSD 硬盘	1 块	167
		HBA 卡	1 块	117
		万兆网卡（含模块）	1 块	78
AI 加速卡		不低于 16G 显存，峰值算力不低于 96TOPSFP16	1 块	700
		不低于 24G 显存，峰值算力不低于 96TOPSFP16	1 块	1246
		不低于 48G 显存，峰值算力不低于 128TOPSFP16	1 块	2449
数据库一体机		数据库计算资源（实例）	1 核 8GB	912
			2 核 16GB	1744
			4 核 32GB	3487
			6 核 48GB	5232
			8 核 64GB	6976
			10 核 80GB	8720
		数据库存储	1GB	0.56
2.存储与备份服务				
存储	块存储（普通）	IOPS≥3000	1TB	149
	块存储（高效）	IOPS≥10000	1TB	330
	对象存储（低频）	IOPS≥500	1TB	78
	对象存储（普通）	IOPS≥1000	1TB	109
	文件存储（普通）	IOPS≥1000	1TB	109
	文件存储（高效）	IOPS≥10000	1TB	330
备份	本地虚拟机/文件备份服务	1TB		126
	本地数据备份服务	1TB		126

3.网络服务			
负载均衡	最大连接数 10000	1 实例	50
4.基础软件服务			
操作系统软件	1 套		82
数据库软件	1 套		784
Web 中间件软件	1 套		340
5.机柜服务			
机柜空间服务	机柜空间（1U）	1U	225
整机柜服务	单机柜租赁（4KW）	个	3600
	单机柜租赁（5KW）	个	4500
	单机柜租赁（6KW）	个	5400
6.容器服务			
容器服务	容器服务，不包含计算资源	1 节点	141
7.云数据库服务			
关系型数据库	两核	4GB	455
	四核	8GB	980
	八核	16GB	1998
	十六核	32GB	4210
		64GB	5432
	三十二核	64GB	8670
		128GB	11640
	存储空间	GB	0.31
缓存数据库	4GB		289
	8GB		591
	16GB		1189
	32GB		2311
	64GB		4689
	128GB		9340
	存储空间	GB	0.31
分布式数据库	四核	16GB	987
		32GB	1092
	八核	32GB	1897
		64GB	2190
	十六核	64GB	3657
		128GB	4620
	三十二核	128GB	9450
		256GB	12120
	存储空间	GB	0.31
8.云中间件服务			
分布式中间件服务、微服务	两核	8GB	461
	四核	16GB	884
	八核	32GB	1532
	十六核	64GB	2876

9.安全服务				
安全服务	入侵检测服务	为云上系统提供南北向的网络层入侵检测服务，支持漏洞攻击、蠕虫病毒、间谍软件、木马后门、溢出攻击、数据库攻击、暴力破解等的检测和防护,防护带宽≥50Mbps。	1IP	259
	WEB 应用防火墙服务	为云上 Web 应用系统提供应用层安全防护服务，支持 SQL 注入、XSS 攻击、网页木马、WEBSHELL 等 Web 威胁防护，http/https 协议防护带宽≥50Mbps。	1IP	259
	漏洞扫描服务	漏洞扫描系统，对云主机系统进行漏洞扫描，输出检测报告，提供修复建议。	1IP	9
	网页防篡改服务	实时监测和保护站点内容安全，防止非法篡改网页，保护站点公众形象。	1IP	151
	堡垒机服务	提供运维安全管理与审计系统，支持主机管理、权限控制、运维审计等功能。	1IP	21
	主机杀毒服务	提供主机杀毒功能，对云主机进行全面的病毒扫描、检测、清除和防护。	1 客户端	16
	日志审计服务	提供日志审计系统，对租户云主机、应用、网络设备等操作日志审计，支持日志采集、日志存储、日志检索、日志分析、可视化统计等。	1 日志源	43
	数据库审计服务	提供数据库审计系统，对数据库的操作行为审计，对各类数据库访问行为进行解析、分析、记录。	1 实例	808
10.密码服务				
密码服务	密钥管理服务	为租户提供密钥生成、存储、更新、备份、恢复及归档等密钥全生命周期管理。性能规格：并发请求数≥100 次/秒，密钥存储量≥10000 个。	1 套	1429
	加解密服务	提供标准 API 接口，为业务系统提供应用级数据加解密、杂凑等密码运算服务，实现信息的机密性、完整性、真实性和不可否认性保护。性能规格：并发请求数≥128 次/秒，SM1 计算速率≥15Mbps，SM2 加密≥2300 次/秒，SM2 解密≥1000 次/秒，SM4 计算速率≥150Mbps。	1 系统	1303
	签名验签服务	基于数字签名、验证签名技术，为业务系统提供应用级数字签名、验证签名等服务。性能规格：并发请求数≥128 次/秒，SM1 计算速率≥15Mbps，SM2 加密≥2300 次/秒，SM2 解密≥1000 次/秒，SM4 计算速率≥150Mbps。	1 系统	1483
	SSL VPN 接入服务	面向运维侧为租户提供基于国密数字证书认证方式的安全接入服务，提供通信数据机密性/保密性和完整性保护功能，构建安全传输通道（只提供账户服务，不包含数字证书及 USBkey）。	1 账户	2.0
	IPSECVPN 服务	为租户提供通信数据机密性/保密性和完整性保护功能，构建安全传输通道。性能规格：吞吐率≥500Mbps，最大并发隧道数≥1000 个。	1 套	797

	时间戳服务	提供时间戳签发、时间戳响应、时间戳解析、时间戳和有效性等多种安全功能。用于实现数据时间认证与签名需求奠定坚实基础。性能规格：时间戳并发量≥100 个/秒，时间戳签发≥80 次/秒，时间戳验证≥150 次/秒。	1 系统	495
	安全认证服务	为业务系统提供基于国产 SM2、SM3、SM4、SM9 算法的数字证书身份认证、数据链路加密的代理服务。性能规格：最大用户数≥500，加密吞吐量≥500Mbps。	1 系统	1688
	协同签名服务	用于移动端、无介质 PC 端基于数字证书的身份认证、链路传输加密场景，在终端用证时提供签名证书密钥生成、密钥签名、密钥解密、密钥协同功能。性能规格：身份认证≥1000 次/秒，并发速率≥1000，数字签名≥2000 次/秒，并发数≥100。	1 套	1643
	数据库加密服务	提供数据库加密服务，实现对数据库关键字段或全库的数据进行加密保存，满足结构化数据的存储机密性及完整性要求。性能规格：SM4 的加密性能≥70Mbps，数据库操作性，损耗≤20%，加密性能≥5000QPS。	1 实例	1699
	文件加密服务	提供非结构化文件加密服务，保障用户数据安全对非结构化文件提供加密服务，保障用户数据安全。性能规格：文件读写操作性能损耗≤20%，文件加密速率≥400Mbps。	1 系统	1699

附件 2：

技术服务规范书

一、服务概述

本附件为三门峡市县一体化新型智慧城市建设（一期）延续项目 A 包合同的技术服务规范书，明确乙方向甲方提供的服务的核心要求，详细技术要求以单一来源采购文件为准。乙方提供的政务云平台应符合国家有关政务云建设的政策法规要求，满足网络安全等级保护三级相关技术标准。

二、服务内容的核心要求

（一）计算服务

乙方应向甲方提供弹性云主机（虚拟机）服务，支持按需分配计算资源，满足甲方各业务系统的运行需求。计算服务应满足以下要求：

1. 支持主流虚拟化技术，提供虚拟CPU（vCPU）及内存的弹性配置；
2. 支持云主机的扩容、快照、克隆及迁移功能；
3. 云主机支持国产操作系统（如麒麟、UOS等）及主流Linux、Windows操作系统；
4. 提供云主机资源使用情况的监控与统计功能；
5. 云主机网络隔离符合政务云安全要求，支持安全组策略配置；
6. 服务可用性不低于99.9%，年累计不可用时间不超过8.76小时；
7. 计算资源支持超融合或分离架构部署，满足甲方业务扩展需求。

（二）存储服务

乙方应提供云存储服务，包含块存储、对象存储和文件存储，支持甲方业务系统的数据持久化存储需求。存储服务应满足以下要求：

1. 块存储支持SSD和HDD两种磁盘类型，提供数据冗余保护机制；
2. 对象存储支持RESTful API接口，适用于非结构化数据的存储与访问；
3. 文件存储支持NFS/CIFS协议，可供多台云主机共享访问；
4. 存储扩容操作对运行业务系统无影响；
5. 提供存储容量实时监控告警，当使用率超过80%时自动触发告警；

附件 2：

技术服务规范书

一、服务概述

本附件为三门峡市县一体化新型智慧城市建设（一期）延续项目 A 包合同的技术服务规范书，明确乙方向甲方提供的服务的核心要求，详细技术要求以单一来源采购文件为准。乙方提供的政务云平台应符合国家有关政务云建设的政策法规要求，满足网络安全等级保护三级相关技术标准。

二、服务内容的核心要求

（一）计算服务

乙方应向甲方提供弹性云主机（虚拟机）服务，支持按需分配计算资源，满足甲方各业务系统的运行需求。计算服务应满足以下要求：

1. 支持主流虚拟化技术，提供虚拟CPU（vCPU）及内存的弹性配置；
2. 支持云主机的扩容、快照、克隆及迁移功能；
3. 云主机支持国产操作系统（如麒麟、UOS等）及主流Linux、Windows操作系统；
4. 提供云主机资源使用情况的监控与统计功能；
5. 云主机网络隔离符合政务云安全要求，支持安全组策略配置；
6. 服务可用性不低于99.9%，年累计不可用时间不超过8.76小时；
7. 计算资源支持超融合或分离架构部署，满足甲方业务扩展需求。

（二）存储服务

乙方应提供云存储服务，包含块存储、对象存储和文件存储，支持甲方业务系统的数据持久化存储需求。存储服务应满足以下要求：

1. 块存储支持SSD和HDD两种磁盘类型，提供数据冗余保护机制；
2. 对象存储支持RESTful API接口，适用于非结构化数据的存储与访问；
3. 文件存储支持NFS/CIFS协议，可供多台云主机共享访问；
4. 存储扩容操作对运行业务系统无影响；
5. 提供存储容量实时监控告警，当使用率超过80%时自动触发告警；

6. 数据存储可用性不低于99.99%。

（三）备份服务

乙方应提供完善的数据备份服务，保障甲方业务数据和系统数据的安全。备份服务应满足以下要求：

1. 支持云主机整机备份和数据库备份，备份策略可灵活定制；

2. 支持全量备份、增量备份的备份方式；

3. 备份数据与生产数据应实现物理隔离存储；

4. 定期进行备份数据的可用性验证和恢复演练。

（四）网络服务

乙方应提供政务云网络基础设施服务，包含云内网络和外部访问网络服务，确保甲方业务系统的网络通畅与安全。网络服务应满足以下要求：

1. 支持网络IP地址规划；

2. 提供弹性公网IP、负载均衡、NAT网关等网络功能；

3. 支持云内不同安全域间的访问控制策略配置；

4. 网络带宽按需分配，支持弹性扩容；

5. 提供网络流量监控和异常流量检测告警功能；

6. 政务云与电子政务外网的互联互通符合相关规范要求；

7. 核心网络设备冗余部署，网络服务可用性不低于99.9%。

（五）基础软件服务

乙方应为甲方业务系统运行提供必要的基础软件支撑服务，包括操作系统、中间件、数据库管理软件等基础软件的技术支持。基础软件服务应满足以下要求：

1. 提供操作系统软件，支持国产化操作系统；

2. 提供相关基础软件的版本升级和安全补丁更新服务；

3. 基础软件的部署配置符合安全加固基线要求；

4. 乙方负责基础软件的日常运维管理，配合甲方完成业务系统的基础软件需求对接。

（六）机柜服务

乙方应提供政务云机柜托管服务，为甲方自有设备提供标准化机柜空间及配套设施。机柜服务应满足以下要求：

1. 提供标准机柜，机柜间距符合数据中心标准规范；

2. 提供稳定的市电和UPS不间断电源保障；

3. 机房环境符合国标要求；

4. 数据中心具备完善的消防系统、防雷接地、门禁安保设施；

5. 提供24小时有人值守服务，外来人员进出机房须登记；

6. 提供机柜内电源分配单元及必要的线缆管理配件；

（七）容器服务

乙方应提供云容器服务，支持甲方业务系统的容器化部署和管理，提高应用交付效率和系统弹性。容器服务应满足以下要求：

1. 提供Kubernetes容器编排平台，支持容器的自动化部署、扩缩容和故障自愈；

2. 支持容器镜像仓库服务，提供镜像的安全扫描和访问控制；

3. 提供容器资源的监控、日志采集和告警功能；

4. 容器网络与存储符合政务云安全隔离要求；

5. 支持容器应用的滚动升级和回滚操作；

（八）云数据库服务

乙方应提供云数据库服务，支持关系型数据库和非关系型数据库，满足甲方业务系统多样化的数据存储与访问需求。云数据库服务应满足以下要求：

1. 支持主流关系型数据库及国产数据库；

2. 提供数据库主备高可用架构，故障时可进行自动切换；

3. 支持数据库的自动备份和定时备份，确保业务数据安全；

4. 支持数据库的弹性扩容，扩容操作对业务影响降至最低；

5. 提供数据库访问控制和安全审计功能；

6. 数据库服务可用性不低于99.95%。

（九）云中间件服务

乙方应提供云中间件服务，支撑甲方业务系统的分布式架构运行。云中间件服务应满足以下要求：

1. 提供消息队列服务（如Kafka、RabbitMQ等），支持高吞吐量消息处理；

2. 提供分布式缓存服务（如Redis），支持主从高可用配置；

3. 中间件服务具备高可用部署能力，关键组件双节点以上冗余；

4. 中间件版本更新和补丁升级不影响业务系统正常运行；

5. 中间件服务与政务云安全防护体系融合，支持数据传输加密。

（十）安全服务

乙方应提供政务云安全服务，从主机安全、网络安全、数据安全和安全运营等层面构建全面的安全防护体系，满足网络安全等级保护三级要求。安全服务应满足以下要求：

1. WEB应用防护服务。在政务云平台部署WEB应用防火墙（WAF），对Web应用系统进行安全防护，防止SQL注入、XSS跨站脚本、CSRF、Web Shell上传等常见Web攻击。支持防护规则的实时更新，提供攻击告警和日志记录功能。

2. 主机安全服务。提供云主机安全防护能力，包括病毒查杀、漏洞检测、基线核查、入侵检测、异常登录告警等功能。定期对云主机进行安全基线扫描，对发现的安全风险及时整改。

3. 网络入侵检测与防护服务。部署网络入侵检测系统，对政务云网络流量进行实时监测，识别并阻断DDoS攻击、扫描探测、漏洞利用等网络攻击行为。

4. 日志审计服务。提供统一日志审计服务，对云平台内网络设备、安全设备的日志进行集中采集、存储和分析，日志保留时间不少于6个月，满足合规审计要求。

5. 漏洞扫描服务。定期对政务云平台内的服务器、网络设备进行漏洞扫描，并跟踪漏洞整改情况。

6. 数据库审计服务。部署数据库审计系统，对云平台数据库的访问行为进行全量审计，识别SQL注入攻击、违规操作等行为。

7. 安全态势感知。提供安全态势感知能力，对政务云整体安全状况进行综合评估，提供安全事件的关联分析和可视化展示，辅助甲方进行安全决策。

（十一）密码服务

乙方应提供符合国家密码管理相关法规和标准的密码服务，保障政务数据传输和存储的安全性。密码服务应满足以下要求：

1. 密码服务采用国家密码管理局认定的商用密码产品，支持国密算法；

2. 提供密钥管理服务，支持密钥的生成、存储、分发和销毁全生命周期管理；

3. 政务数据在传输过程中使用SSL/TLS加密，优先采用国密协议；

4. 重要数据的存储加密使用国密算法，密钥与数据分离存储；

三、技术服务保障

（一）服务团队要求

乙方应建立专职服务团队，负责政务云各项服务的日常运行维护工作。服务团队具体要求如下。如果提供人员不能满足项目实际需要，则需在接到甲方反馈后，第一时间替换相关人员，如两次替换仍不能满足项目需要，严重影响项目进度的，甲方有权追究乙方责任。同时，乙方须承诺提供7×24小时的投诉渠道，及时受理甲方对服务方面不满意的投诉意见。

序号	服务项目	服务说明
1	项目负责人	1名，负责统筹协调项目运维工作，5年以上信息化项目管理经验。
2	云平台运维工程师	2名，熟悉政务云平台运维管理，3年以上云平台运维经验。
3	安全工程师	1名，熟悉等保三级相关要求，负责安全事件响应和安全运营管理。
4	网络工程师	1名，负责政务云网络设施的运维管理。

（二）服务响应要求

1. 资源交付响应

乙方应于收到甲方书面政务云资源开通申请单后3个工作日内完成资源交付。若涉及资源释放、安全配置、密码重置或资源变更等，乙方需与使用部门另行商定具体交付时间，并在交付日前3个工作日内准备就绪。

2. 故障处理响应

乙方须建立完备的故障管理机制，并对各类故障的响应处理作出明确承诺。该机制应根据故障等级差异，分别设定相应的响应时长及故障恢复时限。

故障级别	响应时限	恢复时限	故障描述
一级（灾难）	5分钟内	2小时内	关键业务系统中断、云平台核心组件故障等影响业务正常运行的严重故障
二级（严重）	10分钟内	4小时内	部分服务性能严重下降、非核心组件故障等对业务有较大影响的故障
三级（较大）	20分钟内	8小时内	个别功能异常、性能轻微下降等对业务影响较小的故障
四级（一般）	30分钟内	2个工作日内	配置变更需求、技术咨询及使用问题等

（三）日常技术服务

乙方应提供以下日常技术服务，保障政务云平台的稳定运行：

1.提供7×24小时监控服务

乙方应提供全天候不间断的监控服务，通过监控平台对全部资源及服务进行全方位、多维度的实时监测。监控范围包括但不限于：云主机的CPU运行状态；块存储与对象存储的容量及健康状态；数据库的连接数、慢查询及主从同步延迟；中间件的消息积压及队列长度；网络带宽利用率、丢包率、链路通断情况；安全设备的告警及防护策略有效性等。监控系统应具备自动告警能力，对指标异常或服务中断情况能通过多渠道推送告警至相应服务人员，确保任何潜在风险或故障均能被及时发现、快速定位并启动处置流程，从而保障云平台的持续稳定运行和服务的可用性达标。

2.每日对机房进行巡检，每月编写机房巡检报告

乙方应在每个工作日对机房环境及基础设施开展不少于一次的现场例行巡检，巡检内容应涵盖但不限于：机柜供电状态、空调运行温度与湿度、设备运行指示灯及异常声响。巡检过程中如发现任何异常或潜在风险，须在当日内完成初步处置。同时，乙方应于每月前5个工作日内，汇总上月每日巡检记录及异常处置情况，编写机房巡检报告并报送甲方。

3.按季度提供云资源使用情况明细

按照合同约定，乙方应于每季度结束后次月向甲方提供上一季度的政务云资源使用情况明细。该明细须以电子表格形式交付，内容应完整覆盖本季度内所有已开通云资源的实际使用情况。

4.提供变更管理服务，重要变更操作须制定变更方案。

乙方应建立规范的变更管理服务，对云平台运行过程中涉及的系统升级、配置调整、资源扩缩容、补丁部署、安全策略变更等所有可能影响服务可用性或数据完整性的操作实施统一管理。

5.节假日及重大活动保障期间加派服务人员。

乙方应在国家法定节假日（如元旦、春节、清明、劳动节、端午、中秋、国庆等）及甲方书面指定的重大活动保障期间（包括但不限于重要政务会议、网络安全攻防演练、关键业务高峰期等），启动专项人员保障机制。保障期间，乙方须确保加派人员到位，并保障二线技术专家团队远程待命，所有人员须在告警发生5分钟内响应。因

[illegible]的保障导致的服务中断，甲方有权依据合同追究相应责任。

6. 提供全方位技术支持服务。

乙方应为甲方提供多种技术支持方式，包括但不限于热线电话支持、远程接入支持、现场技术支持等，并对甲方所提交的问题进行解答，提供相关建议；对未能彻底解决的问题应进行跟踪、反馈并及时处理。热线电话提供7×24小时问题答疑服务，及时解答使用中技术疑问，热线响应时间不超过30分钟；以远程接入方式对甲方系统问题进行检查、诊断和分析。乙方工程师仅在得到甲方许可的情况下方可访问甲方系统，并且乙方应确保所访问系统的安全，同时保证数据完整性；按照甲方要求，及时指派工程师提供现场支持服务。工程师必须在服务完成，并得到甲方确认后方可离开现场。

（四）保密要求

乙方参与本项目的所有人员须严格遵守保密规定，未经甲方书面授权，不得以任何形式对外泄露甲方的业务数据、系统架构及相关技术资料。乙方在合同期满后，应将在提供服务过程中获取的甲方数据及相关资料全部归还或销毁，不得留存。

四、服务质量与考核

甲方对乙方提供的服务实施绩效评价，评价结果作为服务费用支付的重要依据。具体评价指标应基于本附件及主合同约定制定；未另行约定的，以单一来源采购文件和响应文件作为评价标准。

五、其他要求

乙方提供的各项服务应严格遵守国家及地方有关政务信息化、网络安全和数据安全的法律法规，包括但不限于《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国》《政务信息资源共享管理暂行办法》等。

乙方在服务期内如需对云平台进行重大架构调整或服务方案变更，应提前书面告知甲方，经甲方确认后方可实施，并确保变更过程中甲方业务系统的连续性不受影响。

自费单位的政务云资源服务费用由其自行承担，计费标准应参照本合同服务价格目录。乙方需确保自费单位的服务质量与甲方标准一致并接受甲方的监督与检查。