

珠海市公共资源交易中心 2024-2025 年度 “数字政府”政务云服务租赁项目方案

珠海市公共资源交易中心

一、项目提出的背景、项目建设的意义及必要性

（一）项目背景

珠海市公共资源交易服务平台系统目前部署在“数字政府”政务云珠海市分节点机房中，通过购买政务云资源服务的形式进行建设，需要按年购买服务。

（二）建设意义与必要性

1. 优化政府服务效率：

可以通过租用政务云资源，集中管理相关政务信息系统，提高系统之间的信息共享和协同工作能力；简化业务流程，提升数据处理和存储的效率，进而加快服务的提供速度。

2. 节约成本：

通过租用云服务，无需大规模投资于本地硬件和软件基础设施，这样可以大幅降低政府的资本支出和运营成本。此外，政务云服务可以根据实际需求进行弹性扩展，根据实际业务量进行动态调整，从而避免了资源浪费。

3. 提升数据安全性：

政务云平台具备先进的安全措施和技术，能够保障政府数据的安全性和隐私。

4. 增强应对突发事件的能力：

在突发事件或自然灾害等紧急情况下，政务云平台可以

提供必要的公共服务支撑，确保服务不受影响，确保政务活动的连续性。

5. 合规性和法规遵循：

通过政务云平台提供的等保、商用密码服务，政府信息系统可以更好地遵守国家和地方的法律法规，确保政务活动合法合规。同时，云平台的数据存储和处理符合国家和国际标准，有利于提高政府数据的可信度。

二、项目建设现状分析

珠海市公共资源交易中心信息化系统由应用系统服务器、数据库服务器等部分组成，通过政务外网将各业务系统映射至互联网，为各交易相关主体提供公共资源交易相关业务。系统整体于 2020 年迁移至“数字政府”政务云珠海市分节点机房中（珠海市政府香华路珠海信息大厦 6 楼政务云机房），截至目前运行状况良好。

为确保系统能持续稳定运行，根据系统运行需要，按周期租用“数字政府”政务云资源服务，具体云服务需包括虚拟机服务、裸金属服务、文件存储服务、数据备份服务、数据库审计服务、漏洞扫描服务、国密堡垒机服务、防火墙服务、商用密码服务-加解密服务、商用密码服务-签名验签服务、密钥管理服务、VPN 服务及软件服务。

三、项目数据资源规范情况

此项目为租赁和维护项目，不涉及此部分内容。

四、项目建设目标

本项目建设目标为租用“数字政府”政务云资源服务，为珠海市公共资源交易中心系统提供基础云资源、安全资源等服务，主要建设内容如下：

- ◆ 52 台虚拟云主机租用；
- ◆ 2 台裸金属服务器（含 4T 裸金属配套块存储）租用；
- ◆ 19T 文件存储租用；
- ◆ 面向虚拟云主机的数据备份服务，拟采购 42.8T 备份空间，主要分为（虚拟云主机快照备份、文件备份及数据库备份）；
- ◆ 4 个数据库实例的数据库审计服务；
- ◆ 珠海市公共资源交易中心 52 台虚拟云主机，全年共计 12 次的主机漏洞扫描服务；
- ◆ 平台国密堡垒机服务；
- ◆ 网络防火墙服务；
- ◆ WAF 服务；

- ◆ 商用密码服务-加解密服务；
- ◆ 商用密码服务-签名验签服务；
- ◆ 商用密码服务-密钥管理服务；
- ◆ 商用密码服务-VPN 服务；
- ◆ 软件服务-数据库服务；
- ◆ 软件服务-中间件服务。

本次政务云服务的租赁周期为 12 个月。

五、项目建设主要内容

（一）云服务内容及要求

1.1. 虚拟机服务要求

市公共资源交易中心所需虚拟云主机服务主要包含两部分，包含 246vcpu、720G 内存、35656G 磁盘，详细配置要求如下：

需求 1：

序号	所属业务	CPU(核)	内存(G)	磁盘 (G)
1	珠海市公共资源交易管理系统	4	8	400
2	珠海市公共资源交易管理系统	4	16	600
3	珠海市公共资源区块链	2	32	500
4	珠海市公共资源交易管理系统	8	16	300
5	珠海市公共资源交易管理系统	4	4	600
6	珠海市公共资源交易管理系统	8	16	300
7	珠海市公共资源交易管理系统	8	16	300

8	珠海市公共资源交易管理系统	2	2	300
9	珠海市公共资源交易管理系统	4	8	400
10	珠海市公共资源交易管理系统	4	8	200
11	珠海市公共资源交易管理系统	4	8	200
12	珠海市公共资源交易管理系统	4	8	3000
13	珠海市公共资源交易管理系统	8	8	200
14	珠海市公共资源区块链	8	16	3148
15	珠海市公共资源交易管理系统	4	4	500
16	珠海公共资源链资信	2	16	600
17	珠海公共资源链资信	2	16	600
18	珠海公共资源链资信	4	8	600
19	珠海公共资源链资信	4	32	600
20	珠海市公共资源交易管理系统	8	32	1100
21	珠海市公共资源交易管理系统	8	16	800
22	珠海市公共资源交易管理系统	4	8	1200
23	珠海公共资源链资信	4	16	1100
24	珠海市公共资源交易管理系统	4	8	400
25	珠海市公共资源交易管理系统	4	32	500
26	珠海市公共资源交易管理系统	12	32	200
27	珠海市公共资源区块链	8	32	800
28	珠海市公共资源交易管理系统	8	16	600
29	珠海市公共资源交易管理系统	4	16	600
30	珠海市公共资源交易管理系统	4	8	300
31	珠海市公共资源交易管理系统	4	8	300
32	珠海市公共资源交易管理系统	4	8	300
33	珠海市公共资源交易管理系统	4	8	300
34	珠海市公共资源交易管理系统	4	8	600

35	珠海市公共资源交易管理系统	4	8	300
36	珠海市公共资源交易管理系统	4	8	300
37	珠海市公共资源交易管理系统	4	6	600
38	珠海市公共资源交易管理系统	4	6	600
39	珠海市公共资源交易管理系统	4	12	4248
40	珠海市公共资源交易管理系统	4	8	600
41	珠海市公共资源交易管理系统	4	8	300
42	珠海公共资源链资信	8	16	600
43	珠海市公共资源交易管理系统	2	2	2560
44	珠海市政府投资工程项目信息化预警平台	4	16	300
45	珠海市政府投资工程项目信息化预警平台	4	8	500
46	珠海市政府投资工程项目信息化预警平台	4	16	300
47	珠海市政府投资工程项目信息化预警平台	4	16	500
合计		226	620	34156

需求 2:

序号	所属业务	CPU(核)	内存(G)	磁盘(G)	备注
1	应用服务器虚拟主机	4	20	300	国产化虚拟主机
2	应用服务器虚拟主机	4	20	300	国产化虚拟主机
3	数据库服务器虚拟主机	4	20	300	国产化虚拟主机
4	数据库服务器虚拟主机	4	20	300	国产化虚拟主机
5	中转机虚拟服务器	4	20	300	国产化虚拟主机
合计		20	100	1500	

1.2. 裸金属服务要求

需配备两台裸金属资源，具体配置要求如下：

序号	所属业务	服务名称	数量
1	珠海市公共资源交易管理系统	计算型（2 颗 E5-2650 V4（2 路 10 核），256G 内存，2*900G SAS 硬盘、HBA 卡、万兆网卡）	1 台
2	珠海市公共资源交易管理系统	计算型（2 颗 E5-2650 V4（2 路 10 核），256G 内存，2*900G SAS 硬盘、HBA 卡、万兆网卡）	1 台
3	珠海市公共资源交易管理系统	块存储服务：普通 IO 云硬盘（适用于大容量、读写速率中等、事务性处理较少的应用场景）	4T

1.3. 文件存储存储要求

需配置 19T 的文件存储服务，确保珠海市公共资源交易中心信息化系统正常使用。

1.4. 数据备份服务要求

依据 2023 年度政务云资源池实际稳定使用量，在提高政务云整体利用率的基础上，进行备份资源池扩容，扩容后备份资源池占用空间为 42.8T。因此本次项目需要配备 42.8T 的备份空间，预防系统故障或数据丢失风险。

数据备份的服务对象为珠海市公共资源交易中心各系统的虚拟机资源，备份服务范围包括虚拟云主机快照备份、文件备份及数据库备份。所有虚拟机每月提供 1 个全量备份及每天增量备份，保留 30 天；数据库每月提供 4 个全备及每天增备，保留 180 天。

1.5. 数据库审计服务要求

提供 4 个数据库实例的月度分析审计报表，报表内容包

括数据库风险趋势、客户端 IP 分布、数据库账号分布、规则命中等内容。

1.6. 漏洞扫描服务要求

珠海市公共资源交易中心共 52 台虚拟云主机，对以上虚拟云主机每月提供一次主机漏洞扫描服务，全年提供共计 12 次主机漏洞扫描服务。根据用户需求，每月对主机进行安全扫描，及时发现安全漏洞风险。该服务的漏洞库需要定期更新，确保可以检测出最新的安全漏洞。扫描任务完成后，需要及时向珠海市公共资源交易中心提供安全漏洞扫描和整改建议报告。

1.7. 平台国密堡垒机服务要求

政务云服务平台需向交易中心提供平台 VPN 服务连接平台国密堡垒机，并能为交易中心提供统一的身份管理和资源访问控制、自动化的批量常规操作，提高运维效率。交易中心只有平台国密堡垒机的使用权，无管理权限，无需自助对身份和资源进行关联，也无需对运维操作行为进行自助审计。

1.8. 网络防火墙服务要求

网络防火墙服务能提供流量访问控制，可控制 VPC 与网

间流量的互访，调用方式如下：申请防火墙策略后，由云平台防火墙管理员关联对应 VPC，按需配置 ACL 策略满足租户的安全策略需求。

1.9. WAF 服务要求

对 HTTP/HTTPS 应用防护,包含 SQL 注入防护、XXS、CSRF、文件包含攻击、目录遍历攻击、信息泄露攻击等 OWASPTOP10 的应用攻击。交易中心根据应用系统应用层访问流量大小选择 WAF 所需的安全防护能力。

1.10. 商用密码服务-加解密服务要求

为政务信息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。

1.11. 商用密码服务-签名验签服务要求

基于数字签名、验证签名技术，为政务信息系统提供应用级数字签名、验证签名等服务。

1.12. 软件服务-数据库服务要求

提供达梦数据库 1 套。

1.13. 商用密码服务-密钥管理服务要求

根据密码接入规范和标准管理协议，为政务信息系统提供密钥生成、存储、更新、备份、恢复及归档等密钥全生命周期管理。

1.14. 商用密码服务-VPN 服务要求

提供 VPN 服务,用于远程业务系统访问，支持远程接入政务云数据中心网络。

1.15. 软件服务-中间件服务要求

提供国产化中间件（东方通）1 套。

（二）安全机制及管理手段

本次云服务租赁项目拟采用“数字政府”政务云为项目提供服务，要求云服务商建立安全应急处置协调机制、指挥调度机制和通报制度，具备安全统一管理、漏洞扫描等安全管理手段，同时需要建立以下机制：

2.1 业务或系统平台数据异常应急恢复

2.1.1 故障发现

由用户业务侧检验数据按需发起或由运维人员在网络监控平台发现告警等手段及时通知用户，当故障后系统出现数据丢失的情况，云服务租赁提供商需及时检查备份情况选择调用本地备份或者同城备份进行数据恢复。

2.1.2 排查和应急处理步骤

云服务商根据平台监报告警以及用户业务反馈情况，得到用户微信或邮件确认才可以启动恢复流程，利用云平台的备份恢复服务，恢复对应虚拟或数据库到指定时间点并验证数据情况，解决时长视用户数据量所决定，需确保用户数据恢复完整。

2.2 保障服务

遵循“先抢通，后抢修”的原则，在较短时间内尽可能抢通业务，减少业务受影响的范围，缩短业务受阻的历时。

云服务商需成立系统突发事件处置工作组，负责处置和协调全市重要会议、节假日期间突发事件，承担系统巡检、技术支持、二线专家保障、IDC 现场值班人员保障等工作的保障。

2.2.1 基础运维服务保障机制

- 设备线路问题的日常检测和故障抢修等工作。
- 使用“数字政府”政务云基础监控软件和云资源管理平台监控软件，实时收集资源部署调度模块报告的资源状态、日志、告警信息；实时监测物理服务器的 CPU、内存、I/O、磁盘利用率和状态，查看物理服务器、虚拟机、网络设备、存储设备、系统软件主动发出的各种告警信息，根据不同告警信息发起故障处理流程。
- 对故障进行分析、定位、修复。
- 根据期间的特殊需求，配合用户进行资源开通及网络策略放通等。
- 按季度提交虚拟云主机及裸金属服务器使用率报表，该报表信息主要包括 CPU、内存、磁盘利用率和状态。
- 服务期间，根据网络安全重保等活动需求，配合提供网络设备相关系统日志及告警信息以及相关技术咨询。

2.2.2 二线专家保障

在基础运营服务团队遇到突发情况或疑难问题时，将安排维护专家提供远程或现场支撑。二线专家小组主要由云平台核心设备商、机房运营商的技术支撑及值班人员组成。

2.2.3 IDC 现场值班人员保障

负责“数字政府”政务云机房基础设施维护，实行机房7×24小时值班制度，工作职责包括：

- 设备及链路的日常巡检，每日两次。
- 故障发生时进行初步排查，并将现场情况及时反馈至基础运营服务团队。
- 重大事件发生时，基础运营服务团队必须到达现场，因为特殊原因（如疫情、天气灾害等）无法及时到达，IDC 值班人员提供远程环境。

2.2.4 应急事件发现机制

2.2.4.1 告警信息上报

云服务商主要设备及第三方软件当遇到严重告警时，运维人员需要为决策者提供及时、直观的告警信息。

2.2.4.2 日常监控

云服务商运维人员通过云管平台、网络监控系统等工具，需要实时对“数字政府”政务云内所有设备及第三方软件进行日常监控，为业务侧提供及时、精确的状态信息参考，从而有利于快速对故障进行定位处理。

2.2.4.3 常规应急处理

硬件故障、云平台故障、存储故障、大规模网络安全事件、网络故障等，云服务商应当通过远程方式进行判断或修复。

2.2.4.4 应急处置方式

应急事件发生后，云服务商运维人员初步判断为该事件无法通过远程方式进行判断或修复时，应于1个小时内到达现场进行处理。

2.2.4.5 特殊情况应急处理

重大事件发生时，云服务商专业运维人员必须到达现场，如因为特殊原因（如疫情、天气灾害等）无法及时到达时，机房值班人员可以通过远程环境进行处置。

六、本项目自主可控和网络与数据安全防护能力建设情况

本项目建设需求的情况下，采用数字政府政务云服务器资源，满足加强相关等保要求，国产密码算法使用要求，落实安全责任制度等，保证数据安全性，提升平台安全，如遭到侵害不会造成严重后果。

（一）符合等级保护要求

依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术网络安全等级保护测评要求》（GB/T 28448-2019）的网络安全等级保护（三级）工作要求，云服务商在服务当年应完成当年政务云平台网络安全等级保护（三级）的测评工作，并提供相关测评报告予以支撑。

（二）国产密码算法使用要求

云服务商需依据《信息系统密码应用基本要求》采取相应保护措施，按照 GB/T39786-2021《信息安全技术信息系

统密码应用基本要求》的第三级别要求，在服务当年应完成当年政务云平台密码应用安全性评估工作，提供相关测评报告予以支撑。

七、项目预算

参照广东省财政厅、广东省政务服务数据管理局关于修订省级政务信息化服务预算编制标准基础设施服务分册的通知(粤财行〔2021〕77号)、《省级政务信息化服务预算编制标准规范和标准安全服务分册》的通知(粤财行〔2023〕44号)要求，本次项目预计投入人民币陆拾贰万肆仟捌佰元整(¥624,800.00)含税费。

八、项目建设和工期及进度安排

项目服务期 12 个月。

九、经济和社会效益分析

(一) 经济效益分析

基于政务云的资源共享模式，可以有效降低硬件和软件投资，并减少相关维护和管理成本。此外，基于云端的服务还能减轻财政压力，提高工作效率，进而提升公共资源交易

服务能力。

（二）社会效益分析

通过租用政务云资源进行建设，实现了信息共享和业务协同，简化了操作流程，提高了工作效率，增强了民众和企业办理业务的便捷程度。总的来说，有助于提升公共资源交易服务的质量和效率，增强民众的满意度。

十、验收要求及标准

本项目为政务云服务租赁项目，项目验收须符合珠海市政府采购信息化项目管理的相关办法，通过珠海市政府服务数据管理局安排的验收等。