德阳数字科创城（1-4 号地块）产业园区智慧化项目施工工程

招标文件

招标单位：德阳市数字科技城开发有限公司

项目名称：德阳数字科创城（1-4 号地块）产业园区智慧化项目施工工程

项目编号：SZKJ-ZB-2022-002

日　　期：2022 年 08 月

目录

第一章　招标公告

一、项目概况

项目名称：德阳数字科创城（1-4 号地块）产业园区智慧化项目施工工程

工程地址：项目用地位于德阳市旌阳区龙泉山脉中，紧邻东湖山公园。是规划生态智谷的核心位置。

工程范围：本次项目建设包括 1 号地块、2 号地块、3 号地块、4 号地块的智能化系统和平台以及对接管理服务运营平台等内容。

二、项目基本信息：

1. 工期要求：250 天。
2. 中标方式：最低价中标。
3. 预算金额：__￥250,815,600.00__元

序号	项目名称	最高限价（人民币元）
1	德阳数字科创城（1-4 号地块）产业园区智慧化项目施工工程	￥250,815,600.00

4. 本项目是否接受联合体投标：是
5. 本项目是否接受进口产品：否

三、投标人资格要求

1. 投标人具备有效的营业执照、税务登记证及组织机构代码副本（或具备有效的三证合一的营业执照）。
2. 法定代表人本人投标的，提供身份证原件的扫描件；法定代表人委托代理人投标的，提供法人授权委托书原件和委托代理人的身份证原件的扫描件。
3. 具有履行合同所必需的资质：电子与智能化工程专业承包贰级资质证书。
4. 项目经理必须具有相关执业资格。
5. 根据相关的规定，投标人三年内无重大质量安全事故及不良业绩和财务状况，对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的投标人，拒绝参与本项目投标。
6. 其它：法律、行政法规规定的其他要求。

四、招标文件的领取

招标文件的领取时间： 现场获取时间：2022 年 8 月 26 日到 2022 年 8 月 29 日 到 福建省泉州市丰泽区丰海路南威科技园 1 号楼 31 层 领取招标文件或自行至网站：http://www.wanshiholdings.com/下载；

五、投标文件的递交截止时间及投标时间

1. 投标文件递交的截止时间及投标时间： 截止日期：2022 年 8 月 30 日 12 时 00 分、开标日期：招标人自行组织开标
2. 投标文件递交的地点及开标地点： 福建省泉州市丰泽区丰海路南威科技园 1 号楼 31 层
3. 递交方式：文件密封好后，现场递交。逾期送达的或者未送达指定地点的投标文件，招标人不予受理。

六、联系方式

招标单位： 德阳市数字科技城开发有限公司

联系地址： 福建省泉州市丰泽区丰海路南威科技园 1 号楼 31 层

联 系 人： 黄经理

电　　话： 13592846815

电子邮件： 546134867@qq.com

第二章　投标须知

一、　投标须知前附表

栏号	编列内容	
1	招标人	德阳市数字科技城开发有限公司
2	工程说明	
	项目名称	德阳数字科创城（1-4 号地块）产业园区智慧化项目施工工程
	工程地址	项目用地位于德阳市旌阳区龙泉山脉中，紧邻东湖山公园。是规划生态智谷的核心位置。
	工程范围	本次项目建设包括 1 号地块、2 号地块、3 号地块、4 号地块的智能化系统和平台以及对接管理服务运营平台等内容。
	建设内容	本次招标范围为德阳数字科创城产业园区部分，建设内容及功能需结合项目实际需求及后期设计图纸为依据，规划设计内容包含但不限于以下系统。 1. 一码通享系统 2. 智能一卡通系统 3. 智慧指挥中心 4. 楼宇设备管理系统 5. 智慧能源监测系统 6. 多媒体信息发布系统 7. 智慧灯杆系统 8. 智能照明系统 9. 房屋安全动态监测系统 10. 公共播放服务系统 11. 保洁机器人 12. 智慧灌溉系统 13. 智慧井盖系统 14. 政务服务中心 15. 智慧党建系统 16. 多媒体会议系统 17. 智慧酒店 18. 智慧服务 19. 智能充电桩管理系统 20. 计算机网络系统 21. 智慧安防视频监控系统 22. 智能一卡通管理系统 23. 数字化出入控制系统 24. 智能梯控管理系统 25. 智慧停车管理系统

栏号	编列内容	
		26. 入侵报警系统 27. 安保巡检系统 28. 无线对讲系统 29. 综合布线系统 30. 通讯系统 31. 弱电机房 32. 安防分控中心 33. 智能化管网 34. 云计算中心 35. 数据中心
	招标方式	公开招标（接受联合体投标）
	承包方式	本工程自行承担上述承包范围内包人工、包机械、包材料、包工期、包质量、包安全文明的承包方式，即对工程承包范围内的一切工程内容负责，并且包含五年维护服务。
	质量标准	合格，符合行业相关规范
	工程报价方式	工程量清单计价（详见附件；工程量清单）
	投标最高限价	￥250,815,600.00
	其他	不得高于招标要求的最高限价，否则其投标作无效标处理。
	工期要求	详见”投标须知-总则第 3 条”
3	招标时间表	招标文件获取时间：2022 年 8 月 26 日至 2022 年 8 月 29 日
		现场踏勘时间：投标人自行前往
		招标答疑截止时间：2022 年 8 月 29 日
		投标截止时间：2022 年 8 月 30 日 12:00 前
		开标时间：招标人自行组织开标
4	招标文件售价	/
5	投标保证金	投标保证金:80 万元（现金、转账、承诺函等）
6	投标人资格要求	投标人必须具有电子与智能化工程专业承包贰级以上资质，项目经理必须具有相关执业资格，且现场施工项目经理必须是投标的项目经理，投标人三年内无重大质量安全事故及不良业绩和财务状况。
7	招标文件的澄清限期	投标人对招标文件中的疑问在招标文件发出 7 天内书面提出；招标人在不晚于投标截止日期前 7 天对收到的澄清文件的予以书面答复。
8	投标有效期	自投标截止日起算 90 日历天
9	投标文件份数及组成	投标文件一式三份（一正两副），投标文件组成；商务文件，技术文件，电子版(投标文件电子版及报价清单需提供报价清单 excel 版存放于 U 盘)，商务文件和技术文件分开制作、装订、密封。
10	投标递交地址	福建省泉州市丰泽区丰海路南威科技园 1 号楼 31 层
11	开标、评标办法	开标办法：最低价中标； 评标办法：不得高于投标最高限价且不应低于投标人的成本。
12	答疑联系人	黄经理：13592846815

二、 投标须知

（一）总 则

1、 招标范围及内容

本次项目建设包括 1 号地块、2 号地块、3 号地块、4 号地块的智能化系统和平台以及对接管理服务运营平台等内容。

2、 承包方式、计价方式、合同签订方式：

2.1 承包方式：本工程自行承担上述承包范围内包人工、包机械、包材料、包工期、包质量、包安全文明的承包方式，即对工程承包范围内的一切工程内容负责。

2.2 计价方式及合同签订方式：本次招标采用工程量清单计价方式，合同签订采用为固定单价合同。

3、 工期及维保

工期要求：250 天。

投标单位根据自身情况明确投标工期。投标人如承诺缩短工期，则其合理性应通过其施工组织设计中的具体措施体现。

维保要求：5 年

合同中约定的工程质保金，质保期届满（且项目无质量问题）后付清。

4、 工程质量标准

4.1 工程质量标准：合格。

4.2 特别说明：本招标工程质量必须符合中华人民共和国国家标准，如果本招标文件规定的标准高于国家标准，按较高标准执行。

4.3 工程规范以投标及施工期间国家、地区和行业颁布实施的规范、规程为准。价款不因 规范、规程的调整而调整。

5、 付款方式

按合同另行约定

6、 合格投标人

6.1 本投标通过资格预审并且符合以下要求的投标人：

6.1.1 投标人必须具有电子与智能化工程专业承包贰级以上资质，项目经理必须具有相关执业资格，且现场施工项目经理必须是投标的项目经理，投标人三年内无重大质量安全事故及不良业绩和财务状况。

（二）招标文件

7、 招标文件的组成

7.1 招标文件包括以下内容：投标须知、项目建设需求和技术要求、建设内容工程量清单、商务文件格式、技术文件格式。

7.2 除 7.1 内容外，招标人以书面形式发出的相对招标文件的澄清或修改内容，均为招标文件的组成部分，对招标人和投标人起约束作用。

7.3 投标人获取招标文件后，应仔细检查招标文件的所有内容，如有残缺等问题应在获得招标文件后 3 日内向招标人提出，否则，由此引起的损失由投标人自行承担。投标人同时应认真审阅招标文件中所有的事项、格式、条款和规范要求等，若投标人的投标文件没有按照招标文件要求提交全部资料，或投标文件没有对招标文件做出实质性响应，其风险由投标人自行承担，并根据有关条款规定，该投标有可能被拒绝。

8、 招标文件的澄清

8.1 投标人若对招标文件有任何疑问，应于按招标人要求时间向招标人提出澄清要求。

8.2 无论是招标人根据需要主动对招标文件进行必要的澄清，或是根据投标人的要求对招标文件做出澄清，招标人都将于投标截止时间前予以澄清，同时将澄清文件向所有获得招标文件的投标人发送。投标人在收到该澄清文件后应在当日内，以书面形式给予确认，该答复作为招标文件的组成部分，具有约束作用。

9、 招标文件的修改

9.1 招标文件发出后，在提交投标文件截止时间 7 日前，招标人可对招标文件进行必要的澄清或修改。

9.2 招标文件的修改将以邮箱形式发送给所有投标人，投标人应在收到该修改文件后 24 小时内以书面形式发送给予确认。招标文件的修改内容作为招标文件的组成部分，具有约束作用。

9.3 招标文件的澄清、修改、补充等内容均以邮箱形式明确的内容为准。当招标文件、招标文件的澄清、修改、补充等在同一内容的表述上不一致时，以最后发出的书面文件为准。

9.4 为使投标人在编制投标文件时有充分的时间对招标文件的澄清、内容进行研究，招标人将酌情延长提交投标文件的截止时间，具体时间将在招标文件的修改、补充通知中予以明确。

（三） 投标文件的编制

10、 投标文件的语言及度量衡单位

10.1 投标文件和投标有关的所有文件均应使用汉语。

10.2 工程规范另有规定外，招标文件使用的度量衡单位，均采用中华人民共和国法定计量单

位。

11、 投标文件的组成

11.1 投标文件由商务文件和技术文件二部分组成。

11.2 商务文件主要包括如下内容：（详见第五章“商务文件格式”）

11.2.1 投标函；

11.2.2 法定代表人身份证明书；

11.2.3 授权委托书；

11.2.4 报价汇总表；

11.2.5 工程量报价清单；

11.2.6 投标人应提交的资格证明材料

11.2.7 投标报价需要的其他资料（若有）；

11.3 技术文件主要包括如下内容：（详见第六章“技术文件格式”）

11.3.1 技术文件内容承诺；

11.3.2 技术偏离表；

12、 投标文件格式

12.1.投标文件包括本须知中规定的内容，投标人提交的投标文件应当使用招标文件所提供的投标文件全部格式（表格可以按照同样的格式扩展）。

13、 投标报价

13.1 本工程采用工程量清单报价，投标人应充分考虑施工期间各类建材的市场风险和政策性风险，中标人的综合单价为固定单价。中标的综合单价除招标文件约定可调范围外不再调整。

13.2 工程量清单是依据招标内容、技术要求及有关的技术规范和施工现场实际情况进行编制的。

13.3 要求各投标人必须使用清单报价。

13.4 投标报价为投标人在投标文件中提出的各项支付金额的总和。

13.5 投标报价的内容

13.5.1 投标人的投标报价，应是应根据本招标书阐明的招标范围、工期及质量要求、合同条件，现场踏勘情况及答疑情况，根据招标人提供的工程量清单进行投标报价，不得以任何理由重复，作为投标人计算单价和总价的依据。

13.5.2 投标人可先到工地踏勘以充分了解工程现场位置、情况、道路、储存空间、装卸限制及任何其他足以影响承包价的情况，任何因忽视或误解工地情况而导致的索赔或工期延长申请将不被批准。

13.5.4 工程量清单中的分部分项工程量清单是指，为完成拟建工程实体工程项目数量的清单，投标人根据招标人给出的分部分项工程量清单项目，报出综合单价和合价，综合单价是指完

成工程量清单中一个规定计量单位项目所需的人工费、材料费、机械使用费和综合费（指管理费和利润，其中应包括了风险费）。

13.5.5 工程量清单中的措施项目清单（若有）是指，为完成工程项目施工，发生于施工前、施工过程中的技术、生活、安全等方面的非实体项目的清单。施工组织措施费及施工技术措施费等应根据施工图、各项技术规范要求、施工现场实际情况、企业自身特点进行投标报价，结算时单价措施费项目单价不得调整、总价措施费项目费率不得调整。

13.5.6 规费、安全施工费和税金。

13.5.6.1 投标人投标报价时，规费按照投标单位规费证取费计入。

13.5.6.2 投标人投标报价时，规费为不可竞争费。

13.5.6.3 本工程税金由投标人按相关规定计算。

13.6.投标报价编制的要求

13.6.1 投标报价应是招标文件工程量清单全部工作内容的价格体现，投标人不得低于成本报价。

13.6.2 工程量清单中的每一个项目，投标人都应填入综合单价和合价，对于没有填入综合单价或合价的项目，其费用应视为已包括在工程量清单的其他项目综合单价或合价中，承包人必须按发包人和监理工程师的指令完成工程量清单中未填入综合单价或合价的项目的工作内容，但不能得到结算与支付。

13.6.3 投标报价由投标人自主确定，投标报价应由投标人根据工程量清单、施工现场实际情况，结合投标人自身的技术及管理水平、经营状况、机械设备及制定的施工方案和招标文件的要求，确定报价。

13.6.4 投标报价中的单价和合价全部采用人民币表示。若单价与合价不一致时，以单价为准，并由评标委员会根据调整后的投标总价进行评定，若投标人拒绝澄清和补正评标委员会修正后的投标总价的，则该投标报价为无效报价，不进行商务标的评审。

13.6.5 投标报价中所报材料必须满足施工图设计的要求和国家相关施工及验收技术规范中对材料选用等级要求及招标文件规定材料的要求，保证材料质量。

13.6.6 投标人的投标报价明显低于其他投标报价时，如果投标人不能提供有关材料证明该报价可以按照招标文件规定的质量标准和工期完成招标工程，评标委员会将认定该投标人以低于成本价竞标，并作废标处理。投标人在编制投标报价时，应认真准备证明文件，在评标委员会要求澄清时，必须在 60 分钟内提供，否则评标委员会应当认定该投标人以低于成本价竞标，并作废标处理。

13.6.7 投标人的投标报价不得低于成本报价，否则其投标报价为无效报价。如果投标人的投标报价被怀疑低于其企业成本的，投标人应出具该投标价属不低于本企业成本的有效证明文件

（包括材料的价格、劳务费的价格等有效证明文件），供评标委员会评定其投标的有效性。前述文件应由投标文件签署人签署并加盖投标人公章。

13.6.11 投标人投标总价应是所有清单报价的单位工程费汇总，不允许采用汇总后优惠、打折的形式，否则其投标报价无效作废标处理。

13.6.12 本工程的任何间歇期间不另行付给停窝工费，不付给机械设备间歇后再次施工的进出场费，其发生的费用投标人在投标报价时自行斟酌考虑。

13.6.13 工程量计算原则：依据 (GB50500-2013)《建设工程量清单计价规范》计算规则。

14、 特别说明

14.1 投标报价采用综合单价方式，投标人所填写的单价和合价在合同实施期间不因市场变化因素而变动。

14.2 材料暂估价：无。

14.3 甲供材、设备：无。

14.4 招标人直接发包的项目：无

14.5 若由于招标范围变更或设计变更引起的新的工程量清单项目，其结算方式按以下方式计算：

14.5.1 投标报价中已有适用于此工程项目的综合单价，按已有的综合单价计算。

14.5.2 投标报价中只有类似于此工程项目的综合单价，可参照类似的综合单价计算。

14.5.3 投标报价中没有适用于或类似于此工程项目的综合单价，由承包人编制综合单价给发包人认可后确定。

14.6 变更洽商（签证）的调整范围：略

14.7 变更洽商（签证）的计价办法：如中标清单中已有相同子目或相近子目,按中标综合单价执行；如中标清单中无此项综合单价，由中标人提出，招标人予以确认。其中材料价执行中标报价，如中标报价中无相同材料单价则执行洽商实施时的市场价（价格须经招标人认可）。：

14.8 措施项目中的安全文明施工费必须按国家或省级、行业建设主管部门的规定计算，不得作为竞争性费用。

14.9 在本次招标范围内，除招标人分包或供货的材料设备外，图纸范围内施工材料、设备全部由投标人自行采购并安装，要求所用材料（设备）必须能够满足设计及国家规范规定的合格材料，投标时主要材料、设备需提供厂家品牌及单价。经评标确定的子目综合单价、主要材料、设备品牌及其单价、人工单价、费率以明细清单表的形式列入工程施工合同内，作为施工及编制合同总价的依据，签订补充协议或结算时不再调整。如施工过程中设计及招标人更换树种，由此产生的差价在工程结算时调整，差值只计取规定税金，不再计取其他任何费用。

14.10 本次招标中，中标单位的所填报的人工、材料、机械等价格，一经招标人接受，在合同的履行中不再调整。

15、 投标货币

15.1.本工程投标报价采用的币种为人民币。

16、 投标有效期

16.1.投标有效期见按招标文件规定的期限，在此期限内，凡符合本招标文件要求的投标文件均保持有效。

16.2.在特殊情况下，招标人在投标有效期内，可以根据需要以书面形式向投标人提出延长投标有效期的要求，对此要求投标人须以书面形式予以答复。投标人可以拒绝招标人的这种要求，而不被没收投标保证金。同意延长投标有效期的投标人既不能要求也不能允许修改其投标文件，但需要相应的延长投标担保的有效期限，在延长的投标有效期内，本须知第 22 条关于投标保证金的退还与没收的规定仍然适用。

17、 投标保证金

投标保证金在招标结束且招标人确定中标人后，招标人向未中标的投标人一次性无息退还投标保证金，中标人的投标保证金自动转成履行合同的履约保证金。

18、 投标文件的份数和签署

18.1 投标人应按本须知前附表中规定的份数提交投标文件。

18.2 投标文件的正本和副本均需打印，字迹应清晰易于辨认，并应在每一份投标文件封面的上清楚注明“正本”或“副本”。正本和副本如有不一致之处，以正本为准。

18.3 投标文件封面、投标函均应加盖投标人印章，并经法定代表人或其委托代理人签字或盖章。由委托代理人签字或盖章的投标文件中须同时提交投标文件授权委托书。投标文件授权委托书格式、签字、盖章及内容均应符合要求，否则投标文件授权委托书无效。招标文件规定盖章的地方，投标人应在投标文件的相应地方盖单位公司章。

18.4 除投标人对错处做必要修改外，全套投标文件应无涂改或行间插字和增删，如有修改必须由签署投标文件的人进行签字并加盖投标人印章。

（四） 投标文件的递交

19、 投标文件的装订、密封和标记

19.1.投标文件均应密封。

19.2.投标文件的装订要求：A4 纸、打印（或印刷）、清晰、工整、美观；所有投标文件均须左侧装订，装订须牢固不易拆散和换页，不得采用活页方式装订，可双面打印。

19.3.投标人应将商务文件和技术文件分别密封，并在密封袋上清楚地标明文件类型并标明 “正

本”或“副本”。投标的报价文件清单与投标文件需采用 U 盘存储并封装随招标文件一起提交。

19.4.为方便开标，投标人应投标文件单独密封，并在信封上标明文件名称，然后再装入投标文件密封袋中。文件密封袋上均应：

19.4.1 在投标文件密封袋上均应标注但不限于：

项目名称：
项目编号 ：
投标人名称：
投标人地址：
于　　年　月　日　时（北京时间）前不得启封

19.4.2 密封面加盖投标人公章和法定代表人或其委托代理人的印章或签字。

19.4.3 如果投标文件没有按本招标文件的规定装订和加写标记及密封，招标人将不承担投标文件提前开封的责任。对由此造成的提前开封的投标文件将予以拒绝，并退还给投标人。

20、 投标文件的提交

20.1 投标人应按本须知前附表中规定地点，于截止时间前提交投标文件。

21、 投标文件提交的截止时间

21.1 投标文件的截止时间见本须知前附表中规定。

21.2 招标人可按本须知中规定以修改补充通知的方式，酌情延长提交投标文件的截止时间。在此情况下，投标人的所有权利和义务以及投标人受制约的截止时间，均以延长后新的投标截止时间为准。

21.2.1 到投标截止时间止，招标人收到的投标文件少于 3 个的，招标人将依法重新组织招标。

22、 迟交的投标文件

22.1 在本须知中规定的投标截止时间以后收到的投标文件，将被招标人拒绝并原封退回给投标人。

23、 投标文件的补充、修改与撤回

23.1 投标人在提交投标文件以后，在规定的投标截止时间之前，可以以书面形式补充修改或撤回已提交的投标文件，并以书面形式通知招标人。补充、修改的内容为投标文件的组成部分。

23.2 在投标截止时间之后，投标人不得补充、修改投标文件。

24、 资格审查材料的更新

24.1 投标人在提交投标文件时，如资格审查申请材料中内容发生重大变化，投标人须对其更新，以证明其仍能满足资格标准，并且所提供的材料是经过确认的。如果在评标时投标人已经

不能达到资格标准，其投标将被拒绝。

25、 投标保证金的缴纳

25.1 投标保证金请于（2022 年 8 月 30 日 12:00）之前汇入我司账号，并同时将支付信息截图发至我司邮箱，凭缴费银行回执单到福建省泉州市丰泽区丰海路南威科技园 1 号楼 31 层领取收据。凡未按我司规定时间缴纳投标保证金投标单位视为弃标。

25.2 采用现金方式的投标人请于（2022 年 8 月 30 日 12:00）之前将投标文件及现金送至我司，检查无误后领取收据。

投标保证金缴纳账号信息：

名称	德阳市数字科技城开发有限公司
单位地址	四川省德阳市旌阳区钻石广场 3 楼 B3
电话号码	
开户银行	中国工商银行股份有限公司德阳东大街支行
银行账号	2305363109100114630

（五） 开 标

25、 开标

25.1 发包人自行组织开标；

26、 投标文件的有效性

26.1 经评标委员会进行评审后,投标文件出现下列情形之一的，应作为无效投标文件，不得进入评标；

26.2 投标文件未按照本须知中要求装订、密封和标记的；

26.3 投标文件的关键内容字迹模糊、无法辨认的；

26.4 投标文件未按照招标文件的要求提供投标保证金的；

（六） 评 标

27、 评标委员会

27.1 评标委员会由招标人代表组成，负责评标活动。

28、 评标过程的保密

28.1 开标后，直至授予中标人合同为止，凡属于对投标文件的审查、澄清、评价和比较有关的资料以及候选人的推荐情况，与评标有关的其他任何情况均严格保密。

28.2 在投标文件的评审和比较、中标候选人推荐以及授予合同的过程中，投标人向招标人和评标委员会施加影响的任何行为，都将会导致其投标被拒绝。

28.3 中标人确定后，招标人不对未中标人就评标过程以及未能中标原因作出任何解释。未中标人不得向评标委员会组成人员和其他有关人员索问评标过程的情况和材料。

29、 投标文件的澄清

29.1 为有助于投标文件的审查、评价和比较、评标委员会可以以书面形式或澄清会的形式要求投标人对投标文件含义不明确的内容作必要的澄清或说明。在采用书面形式的情况下，投标人应采用书面形式进行澄清或说明；在采用澄清会形式的情况下，投标人应在澄清或说明的会议记录上签字认可。

29.2 澄清或说明不得超出投标文件的范围或改变投标文件的实质性内容。根据本须知第 31 条规定，凡属于评标委员会在评标中发现的计算错误并进行核实的修改不在此列。

30、 投标文件的初步评审

30.1 评标时，评标委员会将首先评定每份投标文件是否在实质上响应了招标文件的要求。所谓实质上响应，是指投标文件应与招标文件的所有实质性条款、条件和要求相符，无显著差异或保留，或者对合同中约定的招标人的权利和投标人的义务方面造成重大的限制，纠正这些显著差异或保留将会对其他实质上响应招标文件要求的投标文件的投标人的竞争地位产生不公正的影响。

30.2 如果投标文件实质上不响应招标文件的各项要求，评标委员会将予以拒绝，并且不允许投标人通过修改和撤消其不符合要求的差异或保留，使之成为具有影响性的投标。

31、 投标文件计算错误的修正

31.1 评标委员会将对确定为实质上响应招标文件要求的投标文件进行校核，看其是否有计算或表达上的错误，修正错误的原则如下：

31.1.1 如果数字表示的金额和文字表示的金额不一致时，应以文字表示的金额为准；

31.1.2 当单价和数量的乘积与合价不一致时，以单价为准，除非评标委员会认为单价有明显的小数点错误，此时应以标出的合价为准，并修改单价。

31.2 按上述修正错误的原则及方法调整或修正投标文件的投标报价，投标人同意后，调整后的投标报价对投标人起约束作用。如果投标人不接受修正后的报价，则其投标将被拒绝并且其投标保证金也将没收。

32、 投标文件的评审、比较和否决

32.1 评标委员会将按照本须知中规定，仅对实质上响应招标文件要求的投标文件进行评审和比较。

32.2 在评审过程中，评标委员会可以以书面形式要求投标人就投标文件中含义不明确的内容进行书面说明并提供有关材料。

32.3 评标委员会依据本须知前附表中规定的评标标准和方法，对投标文件进行评审和比较，向招标人提出书面报告，并推荐合格的中标候选人。根据国家有关规定，招标人授权评标委员会直接确定排名第一的中标候选人为中标人。

32.4 评标方法和标准。

（七） 合同的授予

33、 合同的授予标准

33.1 本招标工程的施工合同将授予按本须知第 35 款所确定的中标人。

34、 招标人拒绝不合格投标的权力

34.1 招标人不承诺将合同授予报价最低的投标人。招标人在发出中标通知书前，有权依据评标委员会的评标报告拒绝不合格的投标，并对所采取的权利不作说明原因。

35、 中标通知书

35.1 中标人确定后，招标人将在投标有效期截止前，向中标人发出中标通知书。

35.2 招标人将在发出中标通知书的同时，通知所有未中标人。招标人对落标的投标人不作原因解释。

36、 合同协议书的签订（合同另行拟定）

36.1 招标人与中标人将于中标通知书发出 30 日内，按照招标文件和中标人的投标文件订立书面施工合同，招标人和中标人不得再行订立背离合同实质性内容的其他协议。

36.2 招标人如不按本投标须知第 36.5 款规定与中标人订立合同，或者招标人、中标人订立背离合同实质性内容的协议，应予改正。

36.3 中标人如不按本投标须知第 36.5 款规定与招标人订立合同，则招标人将废除授标，投标保证金不予退还，给招标人造成的损失超过投标保证金数额的，还应当对超过部分予以赔偿，同时依法承担相应法律责任。

36.4 中标人应当按照合同约定履行义务，完成中标项目施工，不得将中标项目施工转让（转包）给他人。中标单位必须选派富有经验、技术过硬、认真负责的技术人员和管理人员组成的施工队伍。施工期间未经招标人同意，不得调换招标书中所报的项目经理、技术人员、管理人员，

否则视为违约，招标人有权终止合同，并要求中标单位赔偿经济损失。

36.5 如果中标人未按规定与招标人签订合同，招标人可与其他投标人签订合同。

第三章　项目建设介绍和技术要求

一、　项目概况

项目名称：德阳数字科创城（1-4 号地块）产业园区智慧化项目施工工程

工程地址：项目用地位于德阳市旌阳区龙泉山脉中，紧邻东湖山公园。是规划生态智谷的核心位置。

工程范围：本次项目建设包括 1 号地块、2 号地块、3 号地块、4 号地块的智能化系统和平台以及对接管理服务运营平台等内容。

1、　工程建设目标

德阳数字科创城将被打造为以数字经济为主导产业的数字小镇。以产业、居住、生活为核心，引进专、精、特、新、单项冠军等数字经济瞪羚企业；引进独角兽企业、准独角兽企业、上市/准上市公司等数字经济龙头企业，形成数字经济产业集群，加快产业聚集和升级，打造一座低碳节能、科技智慧新城，带动数字产业升级发展变革。

德阳数字科创城的建设将在智能化建设的基础上，充分利用现有数据中台、AI 智能、平台、物联网、互联网等先进技术，建设一个以运营管理为核心，以信息化为主线，融合产业化、城市化、生态化的高端、开放的智慧新城。

德阳数字科创城建后，将形成以天府数谷、五大湖区公园建设为突破，全力推进凤翥湖数字小镇等一批重点项目规划建设，为成德绵经济区提供“都市田园新天地”，为城市居民创造“健康智慧新生活”，助力德阳建设西部数字经济重镇。同时，建设完成后的数字小镇将打造成为文旅景区、营造网红打卡地，为德阳市的城市空间做出最美好的贡献。

2、 项目实施标准及依据

规划纲要和政策依据

《四川省人民政府关于加快推进数字经济发展的指导意见》

《德阳市数字经济发展规划(2020- 2025 年)》

《德阳市“十四五”数字经济发展规划》

《德阳市新型智慧城市和大数据建设项目管理办法（试行）》

智慧城市相关国家标准

1.《面向智慧城市的物联网技术应用指南》GB/T 36620-2018

2.《智慧城市信息技术运营指南》GB/T 36621-2018

3.《智慧城市公共信息与服务支撑平台 第 1 部分：总体要求》GB/T 36622.1-2018

4.《智慧城市公共信息与服务支撑平台 第 2 部分：目录管理与服务要求》GB/T 36622.2-2018

5.《智慧城市数据融合 第 1 部分：概念模型》GB/T 36625.1-2018

6.《智慧城市数据融合 第 2 部分：数据编码规范》GB/T 36625.2-2018

7.《智慧城市评价模型及基础评价指标体系 第 4 部分：建设管理》GB/T 34680.4-2018

8.《智慧城市领域知识模型 核心概念模型》GB/T 36332-2018

9.《智慧城市 顶层设计指南》GB/T 36333-2018

10.《智慧城市软件服务预算管理规范》GB/T 36334-2018

11.《智慧城市 SOA 标准应用指南》GB/T 36445-2018

12.《智慧城市时空基础设施 评价指标体系》GB/T 35775-2017

13.《智慧城市时空基础设施 基本规定》GB/T 35776-2017

14.《智慧城市技术参考模型》GB/T 34678-2017

15.《智慧城市评价模型及基础评价指标体系 第 1 部分：总体框架及分项评价指标制定的要求》GB/T 34680.1-2017

16.《智慧城市评价模型及基础评价指标体系 第 3 部分：信息资源》GB/T 34680.3-2017

17.《新型智慧城市评价指标（2018 年）》

基础工程建设依据

本次项目规划设计参考以下国家及行业标准：

《智能建筑设计标准》GB/T 50314-2015

《智能建筑工程质量验收规范》GB 50339-2013

《建筑工程施工质量验收统一标准》GB 50300-2013

《建筑电气工程施工质量验收规范》GB 50303—2015

《智能建筑工程施工规范》GB/T 50606-2010

《安全防范视频监控联网系统信息传输交换控制技术要求》GB/T28181-2016

《视频显示系统工程技术规范》GB 50464-2008

《视频安防监控系统工程设计规范》GB 50395-2007

《入侵报警系统工程设计规范》GB 50394-2007

《出入口控制系统工程设计规范》GB 50396-2007

《建筑设计防火规范》GB 50016-2014

《厅堂扩声系统设计规范》GB 50371-2006

《会议电视系统工程设计规范》YD 5032-2018

《会议电视系统工程验收规范》YD 5033-2018

《现代设计工程集成技术的软件接口规范》GB/T 18726-2011

《民用建筑能耗标准》GB/T51161-2016

《电力装置的继电保护和自动装置设计规范》GB50062-2008

《工业建筑供暖通风与空气调节设计规范》GB50019-2015

《综合布线系统工程设计规范》GBT 50311-2016

《综合布线系统工程验收规范》GBT 50312-2016

《钢制电缆桥架工程技术规程》T/CECS 31-2017

《建筑物电子信息系统防雷技术规范》GB 50343-2012

《建筑物防雷设计规范》GB 50057-2010

《建筑设计防火规范》GB 50016-2014

民用建筑通信管理标准 EIA/TIA-428

民用建筑中有关通信接地标准 EIA/TIA-540

3、 总体定位

将信息技术服务业，大数据、区块链、互联网、人工智能等八大产业与德阳科创城深度融合，打造“迷你型的智慧城市”，提供全流程一站式服务，为产业发展助力，更为智慧人居生活全面护航，从而实现德阳数字科创城的产、城、人一体化。

德阳科创城，是德阳近年来少有的大型产城一体化项目，更是率先启动的重点数字产业项目，是实现其发展数字经济新使命，打造集科技、创新、人才、财富、生活于一体目标的强力引擎。以此及彼，互为关联，拥有无限价值和潜力的德阳数字科创城澎湃而来，将打造一座数字产业之城、科技智慧之城、低碳节能之城、人文自然之城、文旅休闲之城、活力商业之城，必将多维赋能天府数谷，助力德阳数字经济全面升级，推动德阳城市发展！

以四川省和德阳市推进“数字经济”发展总体要求为依托

2019 年，四川省人民政府发布《四川省人民政府关于加快推进数字经济发展的指导意见》，

文件中明确提出未来四川要以“数字产业化、产业数字化、数字化治理”为发展主线，明确数字经济发展目标是 2022 年全省数字经济总量超 2 万亿元。

围绕这个目标，未来四川将加快推进大数据产业集聚区和产业园建设，打造“成德绵眉泸雅”大数据产业集聚区，打造一批数字经济示范城市，因地制宜规划发展各具特色的数字经济发展集群。未来将在人工智能、5G 产业、电子信息基础产业、数字文创产业、智慧社会、智慧政务服务等各个领域深入发力，实现经济突破和城市更新。

德阳对外发布《德阳市数字经济发展规划(2020- 2025 年)》，明确提出把德阳建成“四川国家数字经济创新发展试验区、先行区和国内一流的工业互联网建设示范城市”，让数字科技成为德阳新的产业名片，“天府数谷”顺势而生。

以“三大中心”为总体定位，支撑天府数谷数字经济建设

德阳数字科创城作为天府数谷起步阶段重点打造项目，亦是天府数谷当前建设数字经济的重要动力引擎，其基于国家、城市产业发展战略的解读，以“德阳数字产业集群集聚中心”、“德阳数字产业人才交流中心”、“德阳数字产业金融创新中心”三大中心为总体定位，引进独角兽企业、准独角兽企业、上市公司、 准上市公司等数字经济龙头企业，形成数字经济产业集群。

以“科技园区+生态园区”为核心规划理念建设智慧科创城

在产业布局规划上，德阳数字科创城以“科技园区+生态园区”为核心规划理念，以软件与信息技术服务业、大数据、人工智能、工业互联网、区块链、物联网、数字制造、创新创造八大产业的组成，这与四川省未来“数字经济”发展的方向是一致的。

打造集科技、创新、人才、财富、生活于一体的数字产业新城

在德阳首创“一体化”全系智慧园区，在传统的智慧管理基础上，充分利用现有数据中台、Al 智能、云平台、物联网、互联网等先进技术，建设一个以运营管理为核心，以信息化为主线，打造一个融合产业化、城市化、生态化智慧新城。

4、 项目建设内容

本次招标范围为德阳数字科创城产业园区部分，建设内容及功能需结合项目实际需求及后期设计图纸为依据，规划设计内容包含但不限于以下系统。

1．一码通享系统

2．智能一卡通系统

3．智慧指挥中心

4．楼宇设备管理系统

5．智慧能源监测系统

6．多媒体信息发布系统

7．智慧灯杆系统

8．智能照明系统

9．房屋安全动态监测系统

10．公共播放服务系统

11．保洁机器人

12．智慧灌溉系统

13．智慧井盖系统

14．政务服务中心

15．智慧党建系统

16．多媒体会议系统

17．智慧酒店

18．智慧服务

19．智能充电桩管理系统

20．计算机网络系统

21．智慧安防视频监控系统

22．智能一卡通管理系统

23．数字化出入控制系统

24．智能梯控管理系统

25．智慧停车管理系统

26．入侵报警系统

27．安保巡检系统

28．无线对讲系统

29．综合布线系统

30．通讯系统

31．弱电机房

32．安防分控中心

33．智能化管网

34．云计算中心

35．数据中心

二、 项目技术需求描述

1、 德阳数字科创城业务需求

科创城属于复杂巨系统项目，项目不仅规模巨大，属巨系统范畴极广，而且元素或子系统种类繁多，本质各异，相互系统关系复杂多变，不同子系统之间又关联复杂，作用机制需要长期梳理及完善。在大数据、云计算、5G、AI 智能等科技技术指导与应用下，开发综合管理服务一体化平台，全面实现系统通、功能通、数据通、应用通，打造管理、服务、运营统一的智慧目标。新基建、智能化包含多个子系统，每个子系统既应用其本质功能，又作为物联网基础设施层中的来获取各类文字、图片、音视频、码、数据元等感知设备。新基建、智能化系统是建立在建筑楼宇的基础上，综合管理服务一体化平台是赋能到园区的运营上。

完善基础设施建设，提升共享协同能力

建设完成科创城统一的大数据中心,以地理信息为框架整合空间地理和自然资源、人口、法人、宏观经济数据，以空间信息、人口、法人等公用基础数据整合各领域的业务数据，形成信息资源整合与共享模式，为信息资源的整合提供统一框架，为信息资源的综合开发利用提供统一的数据资源体系。

实现科创城运营监管，提升科创城管理水平

全面提升科创城运行管理的智慧水平，通过管理创新方法转变科创城管理方式、进一步改进管理手段、创新管理模式、提升管理水平，实现科创城运行全面监督、统一指挥、综合分析，实现科创城规范化、智慧化管理目标，为决策层提供辅助决策和命令指挥，提升科创城运行质量。

升级平安城市建设，完善治安防控体系

配合国家“雪亮工程”，构建科创城视频联网平台，实现全面的视频监控，有重点有步骤地推进公共安全视频监控建设。以实战应用为核心，以视频监控规范建设为抓手，倾力打造一张覆盖全科创城的视频监控网，实现“科创城视频资源共享向全市各部门提供视频图像应用服务”的视频监控系统。

关注民生服务应用，提升居民幸福指数

智慧小区建设紧扣“以人为本”这条主线，以先进信息技术为手段，创新服务模式，拓宽服务渠道，完善服务体系，提高服务质量，实现公共服务均衡、优质、高效发展。通过着眼解决市民最关心、最直接、最现实的民生问题，倡导信息时代的品质生活，积极推动城市和谐社会的建设。

达成“最智慧的 2 平方公里”

通过计算、大数据、物联网、AI 等先进技术，来支撑科创城的管理模式创新、服务模式创新、运营模式创新、标准体系创新，来实现管理智慧化、服务智慧化、运营智慧化，智慧科创城。

最智慧的 2 平方公里主要体系在：智慧科创城管理精细化、服务人性化、应急指挥智慧化、环境保护物联化、公共服务便捷化、商业营销决策精细化等。

基于中台架构的大数据中心总体架构设计需求

按照总体设计、分步实施的思路，结合当前互联网环境数据中心发展趋势及中台化战略的理解，以德阳数字科创城数据共享与交换系统作为大数据中心项目的系统定位，对科创城城市级大数据中心总体架构进行初步规划设计，充分考虑当前主流的平台架构和中台理念，确定系统的初步总体架构、业务架构、数据架构、技术架构以及实施策略，对底层大数据平台的基础设施、软件产品进行选型，保障技术平台的先进性、合理性。

在总体规划设计的指导下，统一考虑大数据中心对网络、计算、存储等资源的需求，进行基于中台理念和平台架构的大数据基础平台搭建。大数据基础平台要求构建分布式的存储计算架构，提供资源池、运维管理、监控优化、容灾管理、安全管控等服务，满足大数据平台的底层资源需要。根据大数据软件产品组件的选型，对分布式数据仓库、数据接入组件、离线计算引擎、实时计算引擎、全文搜索引擎、大数据分析组件、数据挖掘组件等相关大数据产品进行安装部署，搭建企业分布式大数据基础环境。

其中，结合智慧科创城总体规划原则，本项目立足于构建开放的大数据中心基础架构，为未来逐步完善并构建功能完备的数据中心筑牢基础技术架构，项目涉及到的硬件类基础支撑环境暂考虑利用企业现有虚拟化平台资源，其它系统软件、大数据相关套件要满足上述大数据基础平台相关要求。

新基建提供融合创新服务平台的基础环境需求

“新基建”是面向智慧科创城高质量发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系，但不论是数字转型还是智能升级都建立在万物互联的基础上，而物联网正是实现万物互联的根本。

科创城物联网建设是互联网基础上延伸和扩展的网络，通过将科创城各种物品接入物联网，来实现智能化识别、定位、跟踪、监控和管理。物联网涉的技术种类较多，从感知技术到传输技术，再到数据挖掘及分析都是其涉及领域，这些技术也赋予物联网三种基础能力：基于感知技术的采集能力、依托于传输技术的连接能力，以及依托于数据分析技术的服务能力。

2、 功能需求分析

一体化平台功能需求

管理服务运营平台是将科创城运营商提供的各类服务、各类资源、各类信息等进行集中起来，并通过服务平台实现对外部公众以及内部企业进行科创城形象、政策、优势、招商流程等宣传展示；实现各类行政服务业务的统一申请办理；基础物业信息的在线查询、使用等；各类与生产和生活配套服务在线申请、结算及支付。最大程度满足入驻企业的服务需求、让入驻企业专注核心

业务，降低企业运营成本以及提高其办事效率，打造 24 小时无边界科创城服务网。

两个中心功能需求

管理服务运营中心（一屏统览）

服务管理运行中心是一个具备多项功能的综合性管理运行中心。设计内容包括八个功能中心：管理中心、指挥中心、决策中心、调度中心、服务中心、呼叫中心、运维中心和创新中心，每个中心都具备相应的功能，实现对科创城服务范围内所有的人、地、物、事、情、组织实现统一的管理、服务、运维，为指挥、决策、调度提供支持能力。同时支持呼叫、创新功能。

德阳数字科创城“一屏统览”项目应整合城区所有信息系统的数据资源，覆盖科创城运营管理各领域，凭借先进的人机交互方式，实现科创城内综合态势监测、综合安防监测、便捷通行监测、设施管理监测、能效管理监测、环境空间监测等多种功能，满足科创城日常管理、日常应急管理和同时处置突发事件的需求。

移动生活服务中心

通过接入政务缴费、教育、交通出行、停车、小区、城市信用、金融服务等公共服务与一城一码场景运营，围绕资金沉淀、用户获取与增值服务运营打造移动生活服务中心。将实现智慧科创城“五通”能力（即：业务通、数据通、证照通、支付通、便民服务通）。平台致力于为市民、企业提供政务、教育、医疗、社保、交通、住房等多方面便民服务，让企业和群众办事像“网购”一样方便。

应用系统需求

一网通办

通过对企业服务、资讯服务、业务服务、公共服务和数据服务的优化整合，以“一网通办”为核心理念，建设德阳科创城智慧政务服务中心、智慧服务一体化平台、智慧政务一体机等系统平台，打造全方位、全天候、全参与一键通平台，构建政府与企业，政府与个人，企业与企业之间的生态体系。

一网统管

将科创城内所有信息化系统、设备、数据全部接入“一网统管”，结合科创城房屋安全监测、智慧管廊系统、智慧小区、智慧物业、智慧养老、智慧楼宇、智慧灯杆、智慧能源、智能家居等综合服务项目，在系统接入、数据交互、设备协同等方面要实现深度融合，打造理念先进、管理科学、平战结合、全城一体的“一网统管”体系。

一码通享

一码通享应以科创城公民身份证号为根，以安全二维码为交互介质，通过码的多使用场景互通互认，实现一码通办、多码合一、园区生活、办事、出行只亮一张码。构建统一的科创城的数字身份标识，实现数据的结构化和在线化。

一码（刷码、刷脸）实现科创城无感通行，充分利用物联网、5G 、人工智能等新型基础设施，拓展二维码和人脸识别技术，应用在政务服务、交通出行、医药卫生、文化旅游、小区生活、商业消费等领域。以服务移动化为抓手，聚合认证、支付、管理等功能，实现政务服务、公共服务、社会服务的服务汇聚和服务融合，提供统一服务的移动化入口，构建市民和科创城互联互通的沟通体系，市民随时、随地可以畅享智慧生活的便利。打造“码上德阳”品牌，提升科创城治理现代化和为民服务便捷化水平。

一网协同

借助信云计算、大数据、物联网、5G 等信息化平台，整合科创城各方资源、系统、数据、设备，将科创城管委会、企业、服务机构之间进行机密联系，互联互动，将各方资源盘活，形成一个紧密联动的整体，促进产业链紧密合作、优化提升，从而实现整体价值放大。

以云计算、大数据中心、物联网为基础，建设智慧党建、智慧酒店、智能巡检、智慧办公、智慧生活、智慧物业、智慧出行等系统，整合数据资源，在数据统一与规范的基础上，实现信息互联互通、业务自由流转，从而为科创城的管理与服务提供一站式运作。

新基建功能需求

围绕智慧科创城创新示范建设，应推动“新网络”在科创城深度覆盖，建设 5G 基站，重点在各类重点区域逐步实现深度覆盖和功能性覆盖；推动“新设施”在科创城集中布局；推动“新平台”在科创城加快部署，应在城区内打造一批支撑集成电路、人工智能等产业应用的公共算力中心、数据中心；推动智能梯控管理系统、智慧停车管理系统、周界入侵预警系统等“新终端”在科创城广泛投放。

3、 数据资源中心需求

服务器托管需求

提供高等级数据中心机柜租赁服务。用户通过租用科创城机柜，托管自有设备，并按照科创城入驻企业自身业务特点进行私有部署。托管的设备可以和云服务，如云主机、云数据库等共同组建 IT 基础架构，构建混合云，支撑科创城客户业务稳定运行。

大数据存储需求

充分考虑目前存储系统现状及未来发展趋势，有效的将存储按照实际需求进行分类，采用组合对应的方法，充分照顾性能、容量、安全性、多协议融合、非结构化数据存储使用等方面，满足智慧科创城所产生图文声像集中存储要求。

针对用户的业务状况和发展趋势，建议采用以数据和存储为中心的系统结构，可以极大地保护投资，有效利用存储空间，降低管理费用，从而确保整体拥有成本最低。同时，降低管理难度，维护数据管理的统一性，提高了电子化数据管理的可靠性。数据的集中化管理，能够确保数据的一致性和完整性，保证电子化数据的可靠性。

数据双向获取需求

各个应用系统、新基建、智能化设备等功能区域在处理各自业务的过程中，为了提高办事效率、信息的准确度等，同时需要用到跨机构、跨层级、跨系统的信息，内网资源库建设需要满足数据双向获取的需求。

多种共享方式需求

实现信息共享首先就要先解决数据能够双向交换的问题，数据可以安全的传输到各内网各单位，同时内网各单位也可以按时的把数据安全的传输到内网资源库，所有过程不是人工的定期操作，而是由共享平台来实现安全高效的数据交换。

在内网各单位需要敏感保密数据的情况下，可以基于本地的数据，在内网资源库上根据对方的需要，提供一系列用户可交互的应用，如门户、核查、查询、比对、统计等应用系统，方便各接入单位的直接使用，这样既能解决数据不能直接交换出去的问题，又可以为各单位用户提供应用级的共享服务，同时加强了对数据共享的有效监管。

实现安全接入需求

在科创城内网网络安全、系统安全、物理环境安全和安全管理设施等安全环境下，实现系统建设和运行安全。通过自身的用户管理、角色授权、身份认证等功能实现细粒度授权和认证，与通过安全应用支撑系统实现的粗粒度授权和认证相结合，实现完整的应用系统权限控制，判定用户对系统、模块、功能、条目、数据的访问和操作权限，通过自身的数据备份与回复功能，为应用系统合理运行提供支持，通过自身的系统审计功能，记录用户所有操作活动，写入日志数据库，并为安全系统预留接口。

统一监管管理需求

本项目要突出平台的数据采集能力、数据治理能力、数据管理能力、共享发布能力和数据监控能力，进一步强化科创城的企业数据治理。同时，在完善并规范数据标准管理基础上，以元数据管理为核心、以数据质量管理为保障、以主数据管理为提升，积极构建数据治理体系，贯彻数据标准，完善数据质量管理，建立数据质量监控处理工作机制和技术平台，推进数据资产化管理。

统一数据规范需求

各应用系统所采用的运行平台、数据标准、数据库种类、数据库表信息格式、数据库管理层次结构模式、信息传输和交换格式及底层传输软件不尽一致，使不同系统之间的数据共享和交换存在较大困难，需要在信息资源平台上进行规范统一。

大数据智能分析需求

德阳科创城的数据资源遍及自然资源、公安、停车、市场、消费、人口、就业、卫生等各个方面，数据可能随着时间而变化（例如人口状态、产业状态），这种动态的信息变化，对于决策者来说，是非常重要的。智能系统是一种永远存在的社会性需求，对于科创城管理机构、德阳政

府机构，要数据智能，满足经营管理和决策能力。

4、 基础设施需求

云计算需求分析

建设科创城综合云计算服务中心，提供机房、服务器、存储、网络，备份等基础信息化服务支撑；建设物联网公共服务平台,提供 RFID、二维码等统一编码、统一认证和统一接入服务平台，以及专用物联网络建设；建设区域统一移动应用门户，实现统一身份认证、统一鉴权。

硬件设施需求分析

计算平台作为本项目应用服务平台，通过计算技术整合科创城新增计算资源，提高计算资源利用率，为各功能区新建的信息系统提供基础设施服务、平台服务、在线软件服务的需求。这些信息系统一般是基于三层体系架构，如网站、业务管理系统等，需要配置 Web 服务器、数据库服务器、区域存储网络，并需要保障其高可用性、快速响应性和安全性，并支持不同组织、部门间信息资源共享、业务协同。这部分需求，既包括基于内外网，又包括基于互联网的。因此，在硬件上的主要需求是配置应用系统及平台管理所需的服务器、存储设备、网络设备等。

软件系统需求分析

除了需要配置一定数量的服务器、存储设备、网络设备和安全防护设备外，还需要配备相关的系统软件，包括：

1)每台物理服务器和虚拟服务器的操作系统：主要是 Linux、Windows 等服务器操作系统。

2)虚拟化软件：基于 VMWARE、KVM、XEN 等虚拟化套件，以实现服务器和存储资源的虚拟化，建立可伸缩、可扩展的资源池；对于新购置设备，需要进行虚拟化套件的安装调试；而对于旧设备的整合，需要在迁移原有应用的基础上，实行物理服务器集中托管，安装调试虚拟化套件。

3)大型数据库管理系统：主流数据库管理系统，如 Oracle、SQLServer、MySQL 等；

4)计算管理平台：包括用户管理、资源管理、网络管理、统计报表、账单、监控等管理功能。并提供用户服务功能的实现以及与其他系统的相关接口。运营维护管理层还需要向管理人员和用户提供人机互操作功能（如门户或工作台），为管理人员对系统的管理提供入口，并为用户申请、使用和查询各类资源提供入口。

集成需求分析

在德阳数字科创城建设标准的指导下，以公司集成平台标准为基础，执行统一标准，按照统一平台、统一数据库、统一网络的要求，实现各应用模块的门户集成、数据集成和业务集成。要严格遵从整体技术规范，通过公司集成平台与“一网统管”、“一网通办”、“一码通享”、“一网协同”、新基建等公司或行业相关拟建的智能化系统和管理系统，建立完善的集成策略并落地实施，避免信息系统各自为政，相互无法互通互联、无法实现信息共享，从而避免“信息孤岛”情况的出现。

网络部署需求分析

安全系统需求分析

为了应对计算环境下的流量模型变化，安全防护体系的部署需要朝着高性能的方向调整。安全设备必然要具备对高密度的 10GE 甚至 100G 接口的处理能力。同时，考虑到计算环境的业务永续性，设备的部署必须要考虑到高可靠性的支持，诸如双机热备、配置同步、电源风扇的冗余、链路捆绑聚合、硬件 BYPASS 等特性。建设以虚拟化为技术支撑的安全防护体系，根据不同用户的需求，提供个性化的存储计算及应用资源的合理分配，利用虚拟化实例间的逻辑隔离实现不同用户之间的数据安全。服务器区安全方面，所有物理服务器全部配置相应的防火墙规则，禁止不用的端口访问，同时在虚拟机模板系统中，只打开最小可用端口（如 ssh、http、https 等），以保证初始系统的安全性。建立应用节点准入规范，保证应用节点自身的安全防护，避免内发生交叉传输。安全管理方面，则以技术管控为主，管理制度为辅，双管齐下。

界面需求分析

在决策分析及各种数据统计分析中应该支持图形化的分析及查看功能，如饼图、柱状图、线图等。

系统操作界面框架应支持左边是功能树，右边是功能窗口的操作界面。

每一个功能窗口的基本按钮（如新增、修改、保存、删除、帮助、打印、退出等）应该统一放在窗口上部的工具条中。

对于可选择信息项的输入应支持模糊匹配或弹出式帮助窗口帮助输入。

用户界面应简明清晰、易操作，易于使用和推广，符合不同层次人员的操作需求。

系统性能需求

德阳数字科创城项目是一个大型的信息化系统的常规性能要求，其主要性能需求如下：

响应时间:系统在正常情况和极限负载条件下，能够处理不断增加的访问请求，具体有良好的性能扩展能力。对用户查询的响应控制在合理范围内。

维护速度:系统维护是比较占用资源的操作，要求数据集、装入的时间安排合理，不影响用户日常使用，同时有较好响应。

数据存储性能:对数据存储要采用较先进的技术，重点考虑存储方法（文件系统/DBMS）、存储速度、查询统计速度等，合理地使用索引等文件组织的方法。

系统恢复性能:对异常情况出现后的系统恢复问题，包括对系统运行平台的恢复以及数据的恢复，要采用较先进的技术，在保证数据恢复正确的前提下让系统得以正常的运行和操作，不影响日常的办公工作。

应用性能需求

科创城软硬件系统的性能应满足业务处理流程的要求，稳定、可靠、实用，人机界面友好，

输入输出便捷，查询功能简单明了。

（1）提供丰富的功能和业务组件，保证灵活扩展，相关组件相互调用简单易用。

（2）服务接口：系统采用 Web Service 的形式提供数据服务，遵循 OGC 规范的 WMS/WFS 标准。

（3）系统运维管理操作简便，平台监控时效性高，对低质量服务和恶意访问及时提示管理员，并能有效、方便地进行控制和管理。

系统响应需求

平台系统、智能硬件、交互系统等应具备负载均衡能力，以保证多用户并发访问时的系统的可靠性和系统性能不受到严重影响，具体性能要求如下：

（1）系统应实现 7×24 小时的连续运行，平均年故障时间(MTBF)≤5 天，平均故障修复时间(MTTR)≤24 小时；

（2）在多人（10000 人以上）同时使用的情况下系统需运行流畅、稳定；网络和本地查询响应速度小于 5 秒；矢量数据浏览刷新速度在 7 秒以内，影像栅格数据刷新速度小于 5 秒；

（3）单次操作，资源搜索响应时间在 2 秒以内；基于图片引擎地图浏览平滑、不留白；

（4）数据库管理系统操作简便；数据库管理系统可移植性强，配置步骤少；地图图片裁剪效率 20 张/秒（256*256）；

数据准确需求

实时数据、共享数据、交互数据等数据的加载、存储、计算、统计和制表制图等功能必须准确。空间数据的存取准确、无信息遗失，在确保信息安全的情况下，空间数据的显示应体现正确的空间位置关系和拓扑关系。

系统容量需求

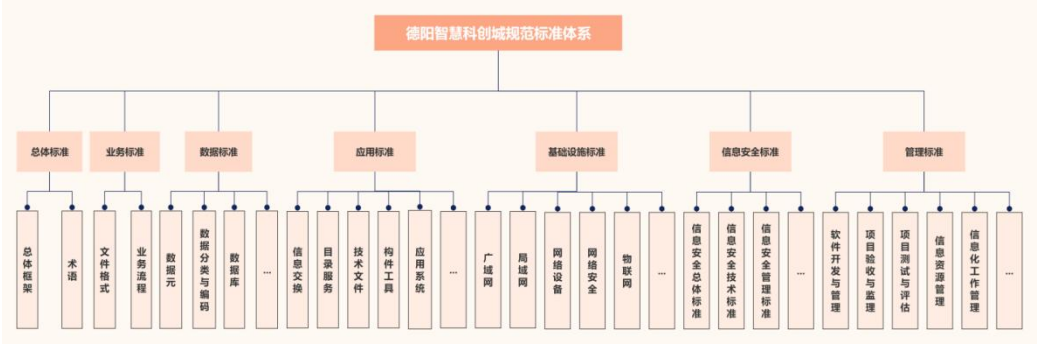
软硬件系统要求采用主流大中型数据库系统，对数据库记录数的增长没有限制，数据管理容量支持 PB 级容量，并且保证大容量数据库的可操作性。

查询速度需求

由于科创城项目涉及数据量大，格式不一，而且数量的增量非常迅速，对于关系数据库和空间数据的查询能力及算法是一个非常严竣的挑战。需设计出合理的数据库结构和查询算法，以保证查询的响应速度并不随记录数的增长而急速下降。

5、 其他需求分析

规范标准的制定



（1）标准规范体系需求

应编制总体标准、业务标准、数据标准、应用标准、基础设施标准、信息安全标准、管理标准等规范体系。

（2）运维管理体系需求

应结合科创城内规划情况和信息化系统建设的具体情况，设计并持续优化运维管理体系的建设，通过自主维护的方式对加强信息系统正常运行保障。

（3）安全保障体系需求

应积极推进标准化建设工作落实，建立健全标准体系，全力构建人防、物防、技防“三位一体”安全保障体系，辅以相应的考核和培训增效。

软件开发技术要求

1)基于 B/S 模式开发,浏览器端兼容 IE 6、IE 7、IE 8、FireFox、Chrome 等主流浏览器；

2)参考基于 XML 数据接口技术；

3)数据库系统采用 Oracle、sqlserver、MySQL 数据库软件；

4)应用系统服务器操作系统采用 windows Server\Linux 操作系统。

三、 总体设计要求

1、 总体设计原则

德阳数字科创城规划原则

统筹规划，分步推进。在政府的统筹指导下，对新型智慧城市标杆建设进行体系规划，顶层设计，集约建设。统筹考虑各行政层级、各部门、各项目之间的衔接匹配，急用先建，分阶段推进实施，通过迭代演进促进新型智慧城市标杆建设持续深入。

以人为本，需求导向。坚持以人为本，突出为民、便民、惠民，让广大居民享受到高效、便捷、绿色的新型智慧城市生活。统筹考虑经济社会各领域的发展需求，确定建设目标、主要任务和重点项目，全面推进新型智慧城市建设与城市改革发展的深度融合。

资源整合，创新引领。打通信息壁垒，加快数据融合和信息共享，推进跨部门、跨领域的业务协同。鼓励技术创新、模式创新、业态创新和制度创新，以创新促应用，以应用带产业，形成智慧应用和产业提升、城市发展之间良性互动的智慧城市建设格局。

重点突破，示范带动。围绕城市发展的特色优势、产业升级的战略重点、群众对公共服务的迫切要求，找准突破口，率先建设，推进技术与业务融合，提升城市运行效率和管理服务水平。支持重点区域先行先试，加快重点领域、重点项目的示范建设，通过试点示范，形成辐射带动效应。

科学规范，确保安全。坚持技术发展与安全并重，加强信息安全战略筹划，建立健全网络安全标准体系，落实网络安全责任制。加大依法管理网络和保护个人信息的力度，加强要害信息系统和关键信息基础设施保护，积极防御，综合防范，确保网络和信息安全可控。

建筑智能化系统规划原则

1）先进性

采用网络化与人性化管理设计，集成化和数字化的主流产品为核心设备，智能一体化的总体设计与实施。

2）完整性

考虑智慧化系统完整性。设备齐全、功能完善、各子系统协调工作、综合管理。

同时考虑智慧化系统的规划设计与整体科创城的规划定位要一致。

3）实用性

智慧化系统内容符合智慧科创城的实际业务需要，在全面考虑系统先进性的同时也要考虑系统实用性。系统设计时，充分考虑各类产品的性能价格比，对关键性的产品应以性能的先进性为主要考虑因素，以提高系统的整体水平，对非关键性产品则以实用性为主。

4）可扩展性

智慧化系统所应用的技术不断发展，用户需求也在不断变化，因此智慧化系统设计与实施应充分考虑到将来扩展的需要，采用模块化结构系统扩展容易。

5）安全性

智慧化系统中的所有设备及配件，要求可靠运转的同时，符合国家和地方标准的安全标准，并可在特殊环境下有效工作。在系统设计中，既考虑信息资源的充分共享，更要注意信息的保护和隔离。在线路设计上利用网络实时在线检测，具有故障报警提示分析功能；网络对外出入口处，充分考虑网络信息数据安全性。

6）实时性

智慧化系统中的各子系统应确保可靠、实时，并保持每天 24 小时连续工作。

7）集散性

智慧化系统设计应实现集散控制。既能分别独自使用，又能集中控制和互通信息。

8）开放性

为了满足系统所选用的技术和设备的协同运行能力、系统投资的长期效应以及系统功能不断

扩展的需求，必须追求系统的开放性。本系统设计中各子系统均提供了标准化和开放性的接口协议，保证了各子系统之间的网络化与集成化实现。

9）可靠性

系统的整体结构及其关键部件均考虑采用容错技术，使系统具有足够的冗余和备份能力，并在关键设备设有备品和备件，确保系统运行的可靠性。

10）易维护性

我们采取先进实用的技术，实现简约化的管理和维护的指导思想，以设备功能模块化，系统控制分级化为原则，为用户提供即强大又容易控制的系统硬件、软件管理功能，也便于故障诊断和日常维护。智慧化系统繁杂，运行过程中的维护是极为重要的，尽量做到简单易操作。系统的运转尽量做到给电后即可启动工作，平日免维修。维护过程中无需使用过多的专用维护工具。

2、 总体设计思路

德阳数字科创城承载的业务丰富多样，通过高度抽象概括，德阳数字科创城的蓝图框架将明确智慧科创城的愿景和建设思路，为后期建设提供指引。

德阳数字科创城蓝图框架，由愿景驱动、以核心价值为指引、以关键能力为保障、以领先基础设施为依托。愿景决定了科创城建设的理想和方向；核心价值导向科创城建设的最终目的，以终为始；关键能力为保障，确保愿景顺利落地；技术底座作为基础，保证整个蓝图得以实现。

3、 总体设计目标

德阳数字科创城项目以打造新型智慧城市为出发点，是以为企业服务全程全时、城市治理高效有序、数据开放共融共享、经济发展绿色开源、网络空间安全清朗为主要目标，通过体系规划、信息主导、改革创新，推进新一代信息技术与城市现代化深度融合、迭代演进，实现城市与城市的协调发展。

德阳数字科创城项目涵盖基础设施、城市管理、社会民生，将重点围绕核心领域选择重点进行智慧化建设，加强基础设施建设，全面可视化园区运行状态,系统融合、业务协同、创新应用，数据分析辅助决策，业务和运营模式整合升级，实现安全的信息处理和信息资源整合，为城市各类人群提供细分的精准服务。同时,构建城市规划与监管体系，保障城市高效、安全、稳定运行。其中包括：

（1）提高资源整合能力： 统一的展示平台和资源共享平台，充分降低科创城运营成本，提高工作效率，加强各类创新以及管理能力，使管理者、企业、用户形成一个紧密联系的整体，盘活科创城内各个方面的资源，获得高效、协同、互动、整体的效益，为科创城铸就一套超强的软实力。

（2）提升数据整合能力： 建设科创城综合管理平台，对各职能系统进行集中监视、控制和数据管理，通过数据处理分析，最大限度地发挥各个子系统之间的关联与协同，在顶层生成综合

职能系统特性的应用，在同一个操作平台上通过统一界面管理实现。

（3）增强管理能力： 建立统一的管理平台，进一步提升科创城内部的管理能力和服务水平；建立企业动态档案，为企业及管委会的管理和决策提供科学依据；实现信息可视化管理、环境能耗的远程管理、综合安防多维防范、基础设施设备可视化运维。

（4）促进科创城经济与环境协调发展： 通过搭建统一的服务平台，提升科创城对各类资源的利用效率。在运营管理、生产中的应用，将有助于有效规避市场风险，增强企业的竞争力。通过对企业排放的监测、监控以及节能改造，实现可循环、低排放、可持续的生产方式，促进科创城经济和环境协调发展。

（5）提升创新能力： 运用现代信息技术，降低成本，提升效率，扩大服务的覆盖面和受益面，同时，物联网、云计算等技术的应用促进科创城信息化建设，打造高科技、智能园区，提升科创城层次和服务水平。

（6）提高基础设施运行保障能力：科创城通过智慧技术的应用，能够实现基础设施在生命周期内的高可用性、高效率、高负荷、高安全性和高可靠性的运转。对于基础设施政策的损耗和可能的故障，能够做到提前预警、实时监控、自动反馈，实现园区基础设施高效实用，个性管理。

4、 总体规划目标

德阳数字科创城项目整体规划目标主要分为四类，包括政府使用规划、入住企业规划、科创城区规划和个体用户规划。主要包含：

政府使用规划：以善政、便民、营商的阳光服务为宗旨，作为试点建设，打造德阳数字城标杆。

入住企业规划：通过专、精、特、新的企业扶持政策着手，配套具有吸引力的环境基础设施，打造及孵化科技产业新生态。

科创城区规划：以人和企业为中心，实现精准的企业招商和人才引进，让政策精准服务、沟通有的放矢、管理高效全面、营销突破限制，创造聚集性强的、上下游联系紧密的、政企良性循环互动的高产能创新区。

个体用户规划：集吃、住、行、办公一体，打造居民住的舒心、用的放心、吃的安心、玩的顺心、学的开心、做的称心的新型城市综合区，让群众在科创城内就可以便捷获得基础生活保障、有效获取个人快速发展、多样获取娱乐休闲方式。

四、 详细功能设计

1、 一网通办

建设目标

通过智能化新基建为政务服务中心，包含所有政务服务、所有缴费、行政事业、所有政府为市民提供的服务以及园区公共服务提供支撑，要做到一网通办、异地通办，全网通办、移动办理。

并且通过在园区和小区设立智慧政务终端一体机，将该服务延伸到市民身边。

建设指南

（1）“网上办”、“掌上办”事项业务。

（2）园区个人、企业、商户等用户实现一窗或一平台受理。

（3）具有申请、受理、审批、监管等属性的管理系统要实现系统互通、数据互通、流程互通等。

（4）针对个人、企业、商户等用户的服务平台要实现服务系统/设备前置、服务数据互通、便捷缴费等智慧服务。

（5）要满足用户在科创城智慧生活方面体会到办理各类事项一网通、各种智能化系统和设备提供办理服务人性化、小区生活实现线上和线下办理事项的便捷。

2、 一网统管

建设目标

按照德阳市城市管理标准来规划，以新基建为基础，实现一网统管、数据一网统管、创造新的服务模式、车网协同和前端的传感器、前端数据感知等所有的信息化系统，要做到从前端数据采集到数据汇总分析应用全流程全场景的一网统管。

建设指南

将科创城内所有信息化系统、设备、数据全部接入“一网统管”，结合科创城综合服务项目现状，在系统接入、数据交互、设备协同等方面要实现深度融合，打造理念先进、管理科学、平战结合、全城一体的“一网统管”体系。

建设内容

根据园区参与主体（管理人员等）、使用场景（管理、服务、运营、生活）和建设指南（功能）规划“一网统管”的建设内容：园区运维管理系统、园区安防管理系统、房屋安全监测、智慧管廊系统、智慧物业、智慧楼宇、智慧灯杆、智慧能源、企业服务等。

3、 一码通享

建设目标

一码通享应以科创城公民身份证号为根，以安全二维码为交互介质，通过码的多使用场景互通互认，实现一码通办、多码合一、园区生活、办事、出行只亮一张码。构建统一的科创城的数字身份标识，实现数据的结构化和在线化。智能化新基建系统为一码通享提供基础支撑。

建设指南

（1）一人一码：证照码、个人信息码、身份码、资源码、财富码，个人管理中心等。

（2）一城一码：通行码、支付码、企业码等。

（3）打通各类场景和实体卡片，实现一码畅享科创城工作、生活。

建设内容

以服务移动化为抓手，聚合认证、支付、管理等功能，实现政务服务、公共服务、社会服务的服务汇聚和服务融合，为统一服务的移动化入口，包含：移动 APP、智慧政务码、园区服务码、智慧交通码、智慧物业码等应用系统提供基础智能化支撑。

4、 一网协同

建设目标

借助信云计算、大数据、物联网、5G 等信息化平台，整合科创城各方资源、系统、数据、设备，将科创城政府机构、企业、服务机构之间进行机密联系，互联互动，将各方资源盘活，形成一个紧密联动的整体，促进产业链紧密合作、优化提升，从而实现整体价值放大。

建设指南

以云计算、大数据中心、物联网为基础，整合数据资源，在数据统一与规范的基础上，实现信息互联互通、业务自由流转，从而为科创城的管理与服务提供一站式运作。

建设内容

根据园区参与主体（业务人员、管理人员等）、使用场景（管理、服务、运营、生活）和建设指南（功能）规划“一网协同”的建设内容，为协同办公平台、管理系统协同-接口、服务流程协同-数据、智能化系统建设-参数、服务协同-用户、运营指标数据-分析等服务提供统一、安全、稳定的网络支撑。

5、 新基建

建设目标

新基建为本方案建设的主要目标，为智慧科创城提供了新型信息基础设施、融合基础设施以及创新基础设施，这些基础设施与智慧德阳的架构深度融合，做到从智慧德阳的感知层、传输层、计算存储层、数据与服务融合层以及智慧应用层全方位夯实智慧德阳的技术基础，助力智慧德阳建设升级。

建设指南

（1）围绕智慧科创城创新示范建设，应推动“新网络”在科创城深度覆盖，建设 5G 基站，重点在各类重点区域逐步实现深度覆盖和功能性覆盖。

（2）推动“新设施”在科创城集中布局。

（3）推动“新平台”在科创城加快部署，应在城区内打造一批支撑集成电路、人工智能等产业应用的公共算力中心、数据中心。

（4）推动“新终端”在科创城广泛投放。

建设内容

结合科创城内规划情况和信息化系统建设的具体情况，设计并持续优化运维管理体系的建设，

通过自主维护的方式对加强信息系统正常运行保障。

新型智能化设备建设包含：网络系统、视频监控系统、门禁管理系统、智能梯控管理系统、智慧停车管理系统、周界入侵预警系统等等。

6、 详细应用系统要求

1） 一码通享系统

一码通以公民身份证号为根，以安全二维码为交互介质，通过码的多使用场景互通互认，实现一码通办、多码合一、科创城生活、办事、出行只亮一张码。

构建统一的科创城的数字身份标识， 实现数据的结构化和在线化，数据的积累为城市综合治理提供有效决策。

使得一人一码作为德阳科创城的网络畅游实名化的“身份码”、公共服务高效化的“通行证”、社会治理精细化的“催化剂”、公民数据资产化的“金钥匙”。

一城一码

设计说明

一码（刷码、刷脸）通科创城、无感通行，充分利用物联网、5G 、人工智能等新型基础设施，拓展二维码和人脸识别技术，应用在服务、交通出行、医药卫生、文化旅游、小区生活、商业消费等领域。

以服务移动化为抓手，聚合认证、支付、管理等功能，实现服务、公共服务、社会服务的服务汇聚和服务融合， 提供统一服务的移动化入口，构建市民和科创城互联互通的沟通体系，市民随时、随地可以畅享智慧生活的便利。打造“码上德阳”品牌，提升科创城治理现代化和为民服务便捷化水平。

功能描述

2） 智能一卡通系统

设计说明

智能卡管理系统主要包括：门禁管理、梯控管理、消费管理等系统。以手机移动端或感应

IC 卡、人脸、二维码为媒介，通过计算机和通信技术为手段，将服务中心内的各项设施连接成为一个有机的整体，用户通过手机或一张卡便可完成通常的资金结算和某些控制操作，如用卡开启门禁，用卡就餐、会议、办公等各项活动。而不必像以往携带多把钥匙开门，去各个对应部门交费等繁杂的操作，减少现金交易等等。整个系统可根据需要对系统内的个体进行监控管理和决策，各局部系统和终端可自动将收集到的信息整理归纳，以供系统查询、汇总、统计、管理和决策。既满足各个职能部门管理的独立性，又保证整体管理的一致性。

智能卡系统建设包括：门禁管理系统、梯控管理系统和消费管理系统。

主要业务功能描述

详见门禁管理系统、梯控管理系统以及消费管理系统描述。

德阳数字科创城专属 APP

德阳数字科创城专属 APP 是一个移动办事（办公）平台，是科创城/小区的移动大厅、物业的移动办公平台，采用 SaaS 技术实现附加阿里的安全保障为企业、居民、物业提供交流平台。APP 的设计迎合了智能终端时代用户的需求，为传统后勤管理换上了智慧的外装，带给用户全新的体验。

德阳数字科创城专属 APP 将物业服务、信息通知、缴费、周边商铺、科创城活动、科创城圈子等诸多信息及服务整合在一部小小的手机里，为企业/居民带来便捷与实惠。对于物业服务公司而言，一方面可以提升物业服务质量，提高物业公告等信息覆盖率，另一方面，可以节约人力成本，还可通过商家模块，获取一定的经济效益。

3） 智慧指挥中心

设计说明

智慧指挥中心负责项目一期智能化系统数据展示、系统控制、安全保卫的重要工作，满足园区日常管理、日常应急管理和同时处置突发事件的需求；包括指挥大厅、会商室、值班室等区域，建设显示系统、音响与数字会议系统、控制系统、照明系统、供电系统、综合布线系统等。

指挥中心计划建设在园区 1 号楼，为更好地配合结构及装修专业的设计，指挥中心建设位置先做临时规划。后续待 4 号地图纸规划阶段具体设计指挥中心。

系统架构

主要业务功能描述

指挥中心是开展值守应急、园区运行监测、指挥会商的办公场所，以及支撑平台基础设备运维的场所，其建设应满足园区进行园区日常管理、日常应急管理和突发公共事件应急处置的需求。

指挥中心是由一系列独立的视、音频系统，以及对它们进行控制的集中控制系统和场所保障环境组成的安全的、智能化的指挥中心，包括显示系统、会议系统、音响系统、集中控制、智能灯光照明、综合布线、供电系统等。总体上应采用以集中控制为中心的网络化多媒体指挥环境的整体设计思想，通过综合布线设连接指挥大厅、值班室、会商室等相关的指挥场所，通过对各种音视频信号的集中交换与处理，并对各种大屏、矩阵、功放等多媒体设备进行必要的集成，实现本地、远程分散/集中的应急指挥应用对音视频的需要，从而达到实现网络化、一体化管理，智能化指挥管理环境的整体目标。

指挥中心示意图

按照功能划分，指挥中心建设应满足园区日常管理、日常应急管理和同时处置突发事件的需求；包括指挥大厅、会商室、值班室等区域，建设显示系统、音响与数字会议系统、控制系统、照明系统、供电系统、综合布线系统等。

指挥中心按照管理功能划分区域，设置不同专业的操作台空间。划分情况如下：

园区综合管理席：综合管理席负责园区日常事务管理，是整个园区各业务处置、调度、协调的统一对外窗口，通常由园区值班负责人列席此位置。

园区安保管理席：安保管理席负责园区内安全防范的管理，是园区安保、交通、火灾等对外联络的窗口以及指挥、调度的管理窗口，通常由园区安保人员列席此位置。

园区应急管理席：应急管理席负责园区应急事件的管理，是园区应急事件方案制定、协助联动各席位应急处突、联络政府应急部门的窗口，通常由安保部门或园区应急指挥部人员列席此位置。

园区养老管理席：养老管理席是负责园区老年人日常监护、日常服务的重要席位，该席位需要处理园区内老年人提供日常家政预约、购物代办、应急事件联络、老人身体健康监测等关键业务，是体现养老服务的重要对外窗口，养老管理席通常有物业管理部及医疗管理部人员共同列席。

园区工程管理席：工程管理席是负责园区能源监测及设备维护的重要席位，该席位负责对园区内的能源消耗、设备运行状态、维护、工单调度工作，该席位通常由工程部人员列席此位置。

4） 楼宇设备管理系统

设计说明

科创城规划设计智慧楼宇设备管理系统将完成对通风、给排水系统、变配电系统、电梯系统等设备或系统的监控管理，从而实现创造一个高效、节能、舒适、高性能价格比、温馨而安全的工作环境，提高管理水平，达到节约能源、节约人工成本的目的，有效降低设备运行费用，延长设备使用寿命。

实现建筑各种机电设备的自动控制和管理

排风机的程序启停自动控制，设备故障报警的自动接收，备用设备自动切换运行等。按管理者的需求，自动形成各种设备运行参数报表，或随时变更设备运行参数(如启停时间、控制参数等)。

降低建筑的营运成本

智慧楼宇设备管理系统只需在管理中心安排一至二名操作管理人员，即可承担对建筑内所有设备监控管理任务，从而可大大减少有关的管理人员及其日常开支。另外，由于楼宇自控管理系统其所具有的多种有效的能源管理方案，使得建筑在满足舒适性条件下，能耗可大大降低，从而进一步降低了建筑的日常营运支出，提高了建筑的效益，延长机电设备的使用寿命以及提高建筑

安全性。

智慧楼宇设备管理系统可以通过编程实现有关机电设备的平均使用时间，从而提高机电设备(各种水泵等)的使用寿命。由于本系统具有极强的系统联网功能，在特定的触发条件下，可以和消防报警系统、安保系统等其它智能化子系统实现跨系统的联动功能，使建筑的安全性管理更可靠。

采用“分散控制，集中监控”的集散型控制模式。分散控制，能够极大地提高系统的可靠性，降低系统布线的造价和复杂程度；集中监控又为系统的操作管理和维护带来巨大的方便性。

建筑设备监控系统分为二层：管理层、设备层。

在控制中心部署楼控中央管理服务器，对楼宇设备统一监控管理，从建筑设备监控系统各个子系统传送上来的数据在这里汇总和进行交换。从而可以向管理人员提供大楼内所有设备和功能子系统的实时状况，使操作员可以在一个计算机平台对整个科创城进行全面集中监控管理。

设备层是功能子系统主机、通讯处理机及智能化控制器。它们通过大楼内的局域网与管理层相连。选用的现场 DDC 设备通过网关连接至 TCP/IP 以太网，监控中心可在 TCP/IP 以太网任何节点上。楼控网络数据能够和以高速 TCP/IP 以太网相连，实现建筑群总控中心和各个分控中心形成一个合理的、高效的、可靠的网络结构。

主要业务功能描述

送排风控制系统

包括：排风机、送风机。

监视控制内容：

风机的启停控制，运行状态及故障报警、手/自动状态监测；

按时间程序控制风机的启停；

CO 浓度检测；

系统正常运行所必须的其他监测和控制；

给排水控制系统

包括：生活水泵、生活水箱、污水池、排污泵。

监视控制内容：

污水池水位、高位报警监测；

排污泵运行状态、故障报警监测；

系统正常运行所必需的其他监测和控制；

电梯、电扶梯系统

现有电梯系统群控预留 RS485 接口，BAS 系统对电梯运行状态及故障报警进行监测，电梯系统的紧急控制由消防系统完成。

5） 智慧能源监测系统

设计说明

根据科创城建筑物设备分布特点选择分布式控制系统，实现就地控制，集中管理，既提高系统的稳定性，减少系统管线的投资，实现最大限度的最优比。根据相关要求和功能对各个独立分系统进行优化设计。规划设计架构分为三层：服务管理层、通讯管理层、现场测控层。服务管理层部署在服务器端，通讯管理层和现场测控层放置计量现场，各智能仪表使用 RS485 总线或无线网络接入通讯管理机，通讯层采用星型结构，通讯管理机上传至服务管理层。

能源监测系统需要在智能仪表实现数据自动采集及传输，智能仪表由设计院水电、暖通专业统一进行规划设计。

能耗监测系统是对建筑用电、用水、雷击计数等各类能耗及数据进行集中监控管理的系统，通过能耗监测系统可实现能耗计费、移动服务、设备监控等功能，提高物业运营效率及节约人工成本。

规划设计建筑能源管理系统实现以下功能：

对建筑用电、用水进行计量；

可读取、打印用户每日数据和各种报表清单；

可实时对系统的运行状态进行检测，如发生断线等故障能自动报警；

可实现数据共享，与第三方系统对接。

主要业务功能描述

基础数据管理

可按功能区域管理、行政部门管理、能耗分类分项、行政区划管理和建筑楼宇管理等多维度建立建筑信息管理

建筑能耗总览

对各类能源消耗情况一目了然，对总能耗、耗电量、耗水量、耗冷量、耗热量等能源的数值

实时显示（当天累积值、当月累积值），可以显曲线趋势图、柱状对比图，可显示同比、环比相差值和相差的百分比

建筑能耗分析

建筑能耗分析 按照能源种类分为水、电、热等几类负荷进行计量，做到每类负荷逐时、逐日、逐月、逐年能耗累计、排序、分析。通过热图了解各区域的能耗分布情况，分析用能规律，并与年度指标进行对照。

建筑能耗分类分项分析

对建筑能耗分析（可以选择日数据、月数据、年数据分析），展示建筑能耗值、人均能耗值，单位建筑面积能耗值。

集中授权

可根据不同的应用角色分配相应的功能模块，系统使用更加安全。

运维服务

实时监测设备工作状态，设备故障时软件界面闪烁提示，也可通过短信发送通知管理员及时处理，避免资源浪费，系统自动生成故障日志便于查询。

权限管理

根据不同操作人员开放不同的权限来操作功能模块。

6） 多媒体信息发布系统

设计说明

在科创城各主要出入口、电梯厅、电梯轿厢、大堂部署信息发布屏，用于发布科创城或企业视频及文字信息，也可用于为企业进行广告投放，实现运营收益。

规划设计信息发布系统可设定单级或多级的树型组织管理、内容发布结构，方便系统统一管理、控制。系统可自主控制管理，可精确到定义播放内容的播放终端点、发布时间及发布周期。同时支持相同或不同发布点分别播放相同或不同的内容。提供的素材可以是视频、文字、图片、动画、数据信息、文档，也可以来自互联网、电视频道、网络直播等多种途径。系统采用异构设计模式，支持多种显示设备，包括液晶显示器（LCD）、网络触摸终端等，系统支持各类操作系统，方便并灵活扩展。

系统架构

主要业务功能描述

采用 B/S 架构设计，管理员可根据权限远程登软件端进行管理，不受 PC 端的限制，可方便移动办公。支持首页图形化实时显示所有设备的状态信息、播出计划、素材类型等统计信息，并可以在首页快捷进去主要操作页面，如素材管理、新建播出单，待审核播出单、及待审核素材等主要功能页面。

支持多个以上分屏区域，可以对各类信息实现分屏管理，各区域播放内容独立，客户可根据自己需要，可自定义分屏及组合模式，有更强的个性化。

提供基于模板的组合播出内容的编辑功能，系统可以实现后台可视化编辑和管理节目，所见即所得，可随时进行编辑和预览，操作简单，可立即修改、立即应用；

允许设置播出单中每个节目的播放顺序、时间、次数，设置图片类型节目的切换特效，设置字幕信息的字体、字号、颜色、滚动方式、滚动速度、透明度等信息；单个播出单可实现多个视频、图片的循环播放，且视频、图片的数量没有限制。

支持播出单向多个播放终端的批量下发，方便快捷；

可扩展高清视频直播服务，实现现场直播或电视节目转播功能；

后台具有监播功能，可实时监控播放设备的运行状态，检查当前播放内容，一旦发现异常，可随时切换内容或切断播出，保证更高安全性；

支持多播放器的大规模集中管理，平台对播放器的扩展没有上限，并支持分组、分区域的个性化管理；可远程配置每台播放器的属性和参数。

针对不同时段、不同场景的不同需要，可以选择多种播出模式：垫片播、立即播、定时播、

周期播等；

可扩展多级安全审核机制，为不同管理员分配不同的审核权限；

前端设备采用自动上线的方式在软件中增加播放终端设备；

提供计划策略的管理功能，可以自定义管理策略，对于规模化管理灵活方便，由服务器自动完成对播放器的日常管理，包括自动关机，开关音量等控制功能等；

提供用户管理功能，既可为用户分配不同软件功能模块的管理权限，也可为用户分配不同终端设备的管理权限；

支持对播出单的导入和导出，方便系统维护，也避免重复编辑，省时省力。

在临时网络不正常时，可通过 U 盘实现文件传输/日志导出/U 盘播放/U 盘素材文件导出。

可扩展外接电源控制模块，控制显示终端或其他设备的通断电，以达到节能环保，并可提前设置计划，实现无人值守。

可扩展视频同步播放功能，实现所有终端设备之间的视频播放同步功能。

在同一显示画面上，设计多个不同元素在特定的区域内播放，有效组合从而扩大多媒体信息同步发布容量、提高展现力、增加观赏性，这个过程就叫做播出单制作。播出单制作是由多个类别的元素结合固定模板或自定义模板而组成，并且可有多页等显示模式。

可任意定制某年、某月、某天或每天固定时段的发布任务。一个任务里面可以包括一个或者多个内容，可以细化到某个时间段播放指定的内容。

如果有特殊需要，可以立即插播，插播时不会影响主任务正常发布的有效期，待插播结束后，主任务会从播放垫片播内容。

内容之间的无缝链接，为系统提供了完美的展现能力。

针对单个发布点或多个发布点的任务可支持自由排出播放列表。

7） 智慧灯杆系统

设计说明

规划设计在科创城园区内部道路旁设置智慧灯杆系统，每个灯杆照度覆盖范围 35-50 米，灯杆设计间距 35-50 米，可根据实际景观照明情况布置灯杆数量，集成路灯照明控制、WIFI 覆盖系、视频监控、信息发布、公共广播、电动汽车充电、求助报警、智慧储能充电、无人车路设等应用。

灯杆样式需要根据科创城块整体景观绿化设计风格进行选择。实际配置功能及选型需要根据实际设计图纸及景观来定制。

系统架构

主要业务功能描述

智能照明

控制实现对路灯智能控制，调光，开关，电压，电流，功率，电量统计，故障告警，能耗分析，GIS 地图，策略控制，回路监测等。

视频监控

300 万高清球机，支持台 360 旋转，支持 1080P 高清，支持本地存储，支持 Smart 侦测：区域入侵侦测、越界侦测、音频异常侦测、移动侦测、视频遮挡侦测功能,支持 NVR，支持接入公安网，支持视频数据的后期分析（具体视实际行业应用）支持远程查看。

WIFI 热点

路灯内嵌 WIFI 基站，实现 WIFI 热点覆盖，双频通信 2.4G/5G 共存,并发接入 200 点，距离 70m，支持多种认证入网方式，支持运营系统.可扩展探针应用，人流量统计等多种应用。

电子广告屏幕

电子显示屏可以发布便捷信息（播报气象、环境等城市综合信息）或者用于广告运营，一旦出现紧急事故，可用于发布紧急信息；运用智能化的手段管理广告，控制不同时间段的广告内容，不同区域投放不同广告，增加广告效应。

环境监测

智慧路灯可搭载多种传感器（噪音传感器、空气污染检测器、温湿度传感器、亮度传感器等），

用于检测风向、风速、温湿度、降雨量、水位、PM2.5、PM10 和噪音等，实现对城市环境和气象的智能监测。

传感器拓展

可拓展接入：红外传感器、雷达、车流量监测传感器，RFID 通信。

广播系统

内置 30W 防水音柱，支持背景音乐，支持应急广播，支持定时和监控室麦克风轮询和对话。

微基站

灯杆可预留移动，联通，电信的通信基站做为中继覆盖。

一键呼叫

支持一键呼叫可与监控室直接对话。

智慧储能

智慧储能，在电价低的时候充电，电价高的时候供电功能。

无人车路设

在需要的路段整合无人车的车路协同设备（充电设备、全息感知交叉口前端设备、激光雷达、边缘多源融合计算终端等）。

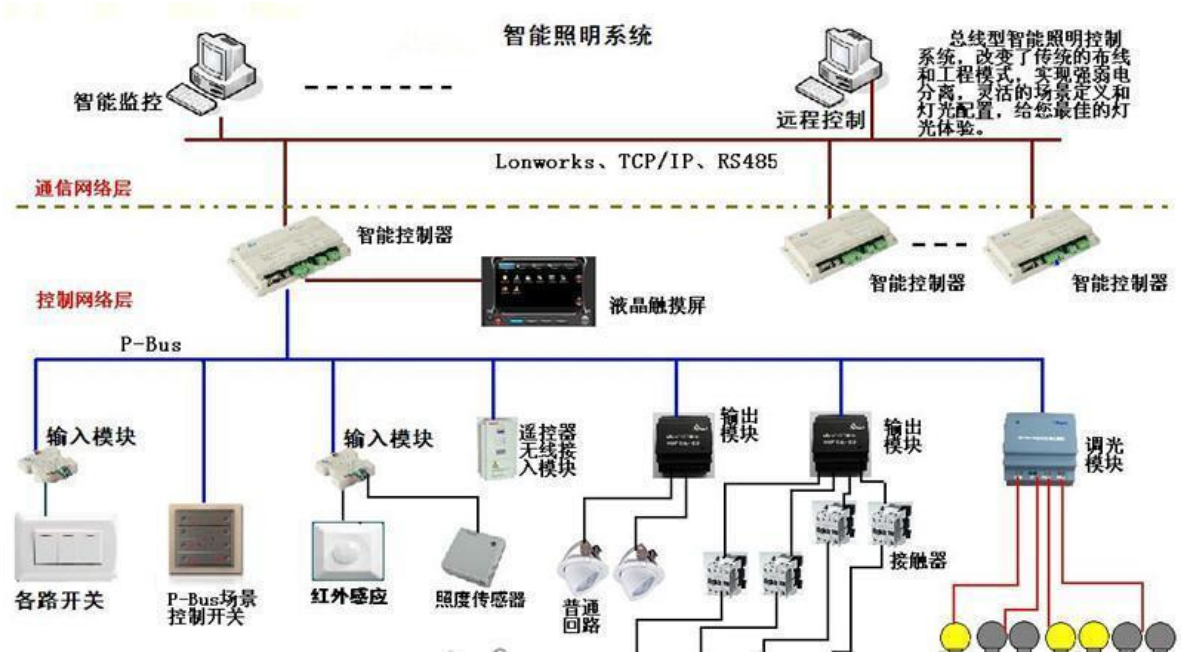
8） 智能照明系统

设计说明

规划设计科创城室外景观照明、室内照明设置智能照明系统，通过照明的智能控制，可实现最大程度电力能源的合理化利用与安排。减少不必要的能源浪费，通常项目对比可节约 20%-30%左右的电能。无论是评定绿色建筑 LEED 认证，还是评定 5A 建筑，其中公共环境建筑节能、室内光环境、信息服务与管理是重点考量项目。是区别于其他建筑的本质所在。

智能照明系统需要结合照明设计进行统一规划。

系统架构



主要业务功能描述

主动问询功能：监控中心可以主动问询每路路灯的开关状态、电流电压、电量等数据；

主动控制功能：监控中心可以随意开关任何一路路灯；

自动控制功能：现场按季节变化自动调节路灯开关时间，并按照开关路灯；

报警功能：通信中断、亮灯率过低、未按时开关等情况出现时，监控中心有报警显示；

显示功能：电子地图上显示每路路灯的开关状态及其它重要信息；

数据存储功能：现场监控设备和服务器上的数据库中存储历史记录；

数据查询功能：监控中心可以查询任意时间段每路路灯数据信息；

曲线报表功能：可以生成电流、电压、电能、亮灯率、开关时间的分析曲线和报表；

远程维护功能：监控设备中的采集和通信模块具备远程参数设置和维护功能；

每天可进行自动通、断电操作；可保证工作日、节假日按不同的时间自动通、断电；可对用电设备进行分区、分线路管理；

控制灯具的开/关和亮度，从而可以显著延长灯具的有效寿命，减少灯具更换次数，节约资源，减少有害气体污染环境。可以远程设置节点控制参数，实现节点的灵活控制。在后半夜车稀人少时，则控制路灯保持较低照度的照明。这样做主要优点就是在调光的同时，也大幅降低了电耗，节约用电，同时还可以延长灯源寿命。

9） 房屋安全动态检测系统

房屋安全动态监测系统平台设在中控室内，前端采集设备设计在各栋建筑物顶层安装三轴测振仪、三轴倾角仪、气像站传感设备、水准仪传感设备监测房屋沉降。该系统是对建筑中存在的

重大安全风险点进行实时自动化安全监测。

主要监测内容包括房屋沉降、房屋倾斜、房屋震动和气象数据等。系统采用无线自动组网、定期连续采样，实时数据上传与数据处理实时了解房屋的健康状态，帮助检测人员快速定位房屋主要危险源，及时对房屋安全性作出准确评估，预防事故的发生，避免人员伤亡，减轻经济损失

10）公共播放服务系统

设计说明

规划设计公共播放服务系统，系统设计分为室内及室外两部分，其中，在科创城各建筑物公共区域设置吸顶及壁挂式音箱，科创城室外区域在草地及灯杆出设置草地音箱及壁挂音箱，壁挂音箱可安装于智慧灯杆处。系统用于提供背景音乐播放、人工广播业务和强行插入灾害性事故的紧急广播，同时具有发布新闻和内部信息、发布作息信号等功能。

主要业务功能描述

可实现分区/全区播放背景音乐及业务广播；

背景音乐和紧急广播采用同一套系统设备和线路；

具有背景音乐、广播功放及扬声器故障自动检测功能；

消防等紧急情况下的联动报警功能。

11）保洁机器人

设计说明

本项目规划设计保洁机器人，用于部分商业、管理服务运营中心等区域的日常清扫，达到节省人工，计划清扫，时刻保持环境清洁等功效。

主要业务功能描述

扫拖一体，精准扫描，精准建图，自动充电，自动清洁，选区清洁，划区清洁，虚拟墙，拖地禁区。

12）智慧灌溉系统

设计说明

规划设计智慧灌溉系统，实现科创城块绿地喷灌养护的自动化、智能化的功能，智能喷灌系统是为实现现代农业所提倡的节水、节肥、省力、高效而研发出的一种自动化控制灌溉浇水系统。是集电子信息技术、远程测控网络技术、计算机控制技术及信息采集处理技术于一体，通过计算机通用化和模块化的设计程序，构筑供水流量、压力、土壤水分、作物生长信息、气象资料的自动监测控制系统，进行水、土环境因子的模拟优化，实现灌溉节水、作物生理、土壤湿度等技术控制指标的逼近控制，从而将农业高效节水的理论研究提高到现实的应用技术水平。滴灌智能控制系统实用性强，灌溉定时定量，适用范围广，功能强大。

智慧灌溉系统依托于景观绿化设计。

系统架构

主要业务功能描述

数据采集功能

可自动采集数据，处理温度、湿度、风速、雨量,光照等环境参数。

灌溉控制功能

具有自动灌溉、定时灌溉、周期灌溉、手动灌溉等多种模式，可根据需要灵活选用灌溉模式；可实现中控室控制，手机短信、现场遥控及现场手动等多种方式控制。

参数设置功能

系统可以对现场的温、湿度限值进行设置和修改；

系统可通过控制器或后台监控系统完成灌溉起始时间、停止时间、喷灌时间等参数设置。

显示功能

控制器上配有液晶屏，以中文菜单方式显示，现场采集数据显示在液晶屏上；

后台监控系统可配大屏幕显示器，图形、表格等多种形式动态显示整个灌溉区运行情况，准确、直观、明了。

报警功能

当灌溉系统出现故障。如水管破裂等，立即停止水泵运行，并报警。

通信功能

通过后台机查看、设置、修改参数；

采集数据上传后台机，供后台机进行数据处理和显示；

接收后台机发出的控制命令。

数据处理功能

后台机可完成用户提出的统计、贮存、查询等各种数据处理功能，并可打印用户要求的报表；

电磁阀门开启次数和时间统计；

通过电磁阀门的水流量统计；

系统故障次数统计，系统使用率统计。

13) 智慧井盖系统

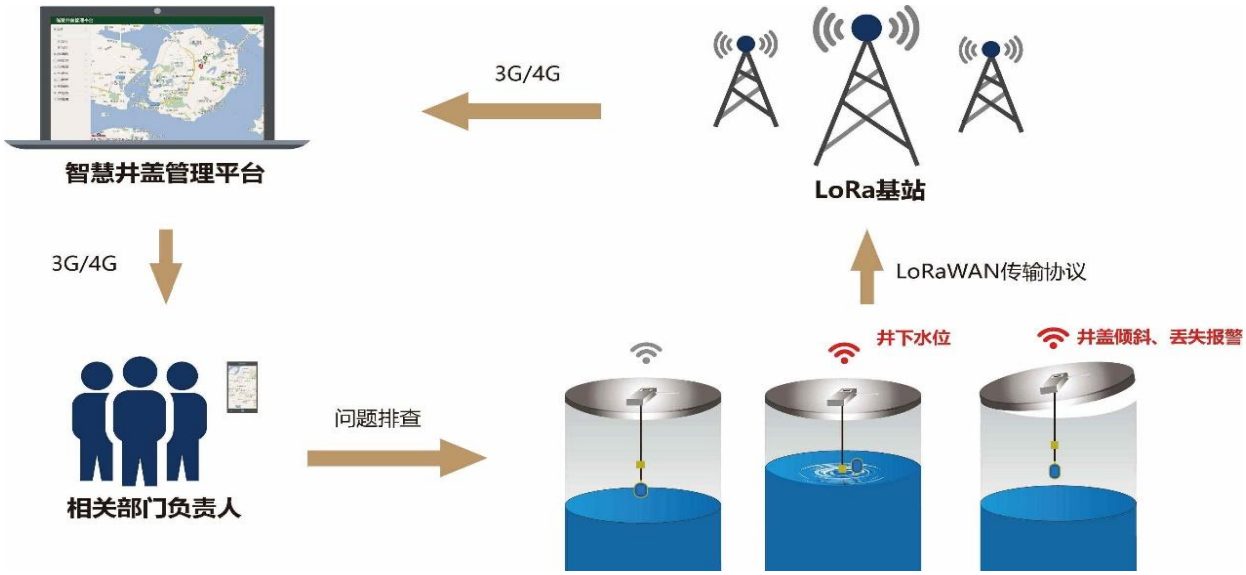
设计说明

为防止科创城内发生移动、偷盗井盖等违法行为时有发生，同时，为及时获得发现破损、损坏、丢失的井盖信息，及时进行修复，避免人员及财产损失，规划设计智慧井盖系统。

住建部于 2013 年 4 月提出了关于进一步加强城市窨井盖安全管理的通知，要求包括城市供水、排水、燃气、热力、房产（物业）、电力、电信、广播电视等部门，实行井盖的数字化管理，实现社会资源有效的监管，确保人民群众人身安全。虽然市政井盖的管理需求是非常明确的，但是，由于城市窨井盖数量庞大，管理部门即使是安排维护人员加强巡视，也无法完全保障窨井盖安全，无法实时有效的获得设备的信息，面对异常情况无法实现实时监控和快速高效的管理。为更好地保障公共设施安全，迫切需要采用新技术、新模式加强针对窨井盖的安全的管理。

智慧井盖系统设计依托于科创城室外管井设计。

系统架构



主要业务功能描述

井盖资产管理：对井盖的基本信息进行管理，包括井盖编号、经纬度、所在道路等。

实时定位监控：可实时监测科创城内井盖的各种状态信息，通过结合系统直观的科创城平面图，可实时查看井盖在所属区域内的位置和基本属性信息，并对区域内所属的井盖防盗进行统一指挥调度出警和工程维护。

采用 GIS 地理信息技术实现地理地图展示：在电子地图上显示井盖位置、基本信息、实时状态等，也可以通过文本形式展示井盖位置、基本信息、实时状态、历史状态记录等信息。

防盗监管：根据预先设定报警规则，对科创城井盖的异常情况进行防盗监管。安装在科创城井盖的智能井盖无线传感器，当井盖状态正常时，处于休眠状态，当井盖异常开启时，立即发出报警信号，通知相关负责部门采取措施。

报警联动：产生报警信息向报警中心报警后，同时还会向相关责任人和管理人员的手机等客户端发送报警信息。

鉴权设置：当工程人员需要对井盖和线路进行维护时，由控制中心经过判断合法性进行解防，或是经授权的工程人员手持终端设备或者监管中心可进行匹配解防，可以灵活设置井盖的维修时间。

数据分析：通过对系统中大量的数据进行深度挖掘，从不同角度、不同维度、不同需要等对各种数据进行重组、汇总及对比分析，挖掘出更有利于提升市政管理水平和效率的有价值数据。

14）政务服务中心

设计说明

随着“简政放权、放管结合、优化服务”深化行政体制改革、按照“职能在区街梳理、资源在片区整合、力量在科创城集中、服务在邻里提升”的思路，需要与当地相关部门对接，落实服务下沉的审批事项；按照“一个场地、一套资料、一支队伍”的标准推行服务硬件标准化工程。

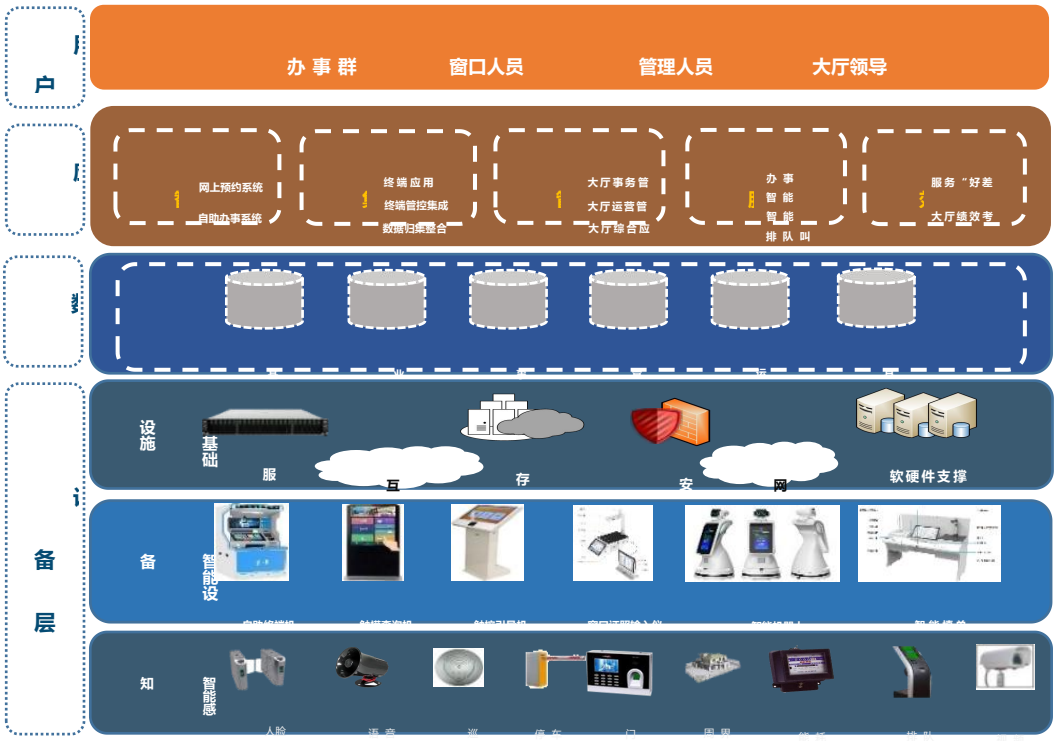
设置多个全科窗口。充分利用信息化、平台化、自助化、便捷化的服务理念。建设网上预约、

排队叫号、自助查询、自助办事、智能导办、智能 AI、智能填单等系统，实现“一次申请受理、材料内部传递、部门并联审批、全程一次办结”的便企服务目标。实现服务大厅的可视化、规范化、智能化管理，确保服务“优质、高效、有序、规范”。

整体架构

网上预约系统

网上预约系统支持通过微信公众号、服务网、手机 APP、自助查询终端等多渠道预约，方便



办事群众合理安排自有时间进行业务办理，实现来者能办、优先办，缩短办事群众办事时间。主要功能包括预约办件管理、预约配置管理、预约办事提醒设置、预约时间段设置、预约办理信息管理、预约事项属性配置等功能。智能导办服务系统

智能导办服务系统以智能导办终端为载体，通过简单直观的交互为办事群众和企业提供智慧导办服务，提供导航指引或是咨询解惑。系统以二维或三维的方式模拟大厅实景，并实现各事项的场景式导办，引导群众和企业快速查找到办事窗口并完成事项办理。

自助查询服务系统

自助查询服务系统以触摸查询终端为载体，为前来办事群众提供自助查询服务，公众可通过智能引导系统查询到中心简介、组织架构、法律法规、通知公告、中心位置、热点事项等相关信息。为公众提供智能化自动引导服务，提升服务中心形象。

排队叫号服务系统

排队叫号系统以排队叫号终端为载体，集中控制窗口显示屏、排队信息显示屏，建立灵活的多级菜单进行取号排队，实现业务办理人员分流。系统除具备基础的排队叫号功能外，将更多的

与业务流程和业务系统进行融合，从智能信息采集、业务流程发、线上平台引流、二维码关联、业务联办、在线排号、预约取号、数据沉淀等方面用户提供更加完善的办事体验。

自助办事服务系统

自助办事服务系统以服务终端一体机设备为载体，以公众和企业的办理需求为出发点，以提供“24 小时自助服务”为设计理念，从而缓解传统大厅人流量大、等待时间过长、办公时间有限等问题，让市民可以轻松享受 24 小时自助式的各项贴心便民服务，真正体现便民利民。该设备具有办事指南查询、填表打印、网上办事、进度查询、办事预约、办事取号等应用，不用排队，不受工作时限限制，同时提供人脸识别、热敏打印、二代身份证读取、A4 纸打印、二维码扫描、高清摄像头、A4 幅面扫描、银联缴费接口等功能，结合计算机技术、多媒体技术、工业制造技术为公众提供人性化、现代化的帮助引导服务，全面提升服务水准和服务效率。

智能填单服务系统

智能填单服务系统以自助填单终端设备为载体,用 PDF 电子表单取代纸质表单,推动传统“纸质填表”方式向“电子填表”方式转变，实现无纸化办事，大大节约纸张；另外，电子表单可以方便地设置填写约束、提示和样表对照等，确保表单填写规范准确，还能直接利用已有数据自动填写，实现一次填表，多次复用，大大方便群众企业办事。

智能机器人服务系统

智能机器人是一款面向大型室内场景应用的智能服务机器人。基于领先的人工智能技术,“智能机器人”凭借自然化、情感化的语音交互，通过建立与业务系统的对接，能够为用户提供人性化服务。同时，智能机器人的应用，可增加智慧大厅的科技感，提升大厅的智慧化程度，系统主要具有多模式唤醒、语音交互、运动和避障、室内导航、屏幕触摸辅助、智能人脸检测与识别、货物递送等特性。

15) 智慧党建系统

设计说明

本次项目智慧党建系统规划设计分两部分，第一部分为建设现有党员学习室；第二部分为考虑可通过与当地政府合作办校或建设红色传承展馆，作为德阳党建学习培训基地，实现运营，产生盈利，此种运营思路即起到宣传德阳、争取更多肯定与支持的宣传窗口作用，又可带动科创城配套产业的经济收益（如酒店、文旅、购物等），同时增加了科创城的知名度。

拟建设内容

德阳市红色传承展馆

红色传承展馆面积不少于 2000 平米。党史结合德阳地区党史，从第一位党员、第一个党支部谈开去，展开一幅德阳地区在党的领导下，艰苦奋斗、甘于奉献的奋斗史。暨重新温习了中国共产党党史，又深刻了解了德阳地区的发展史，并对今天的德阳和明天的德阳充分了解。起到宣

传德阳、争取更多肯定与支持的宣传窗口。

主要业务功能描述

2021 年是中国共产党百年华诞。百年征途波澜壮阔，百年初心历久弥坚。中国站在“两个一百年”的历史交汇点，全面建设社会主义现代化国家新征程即将开启。

投资兴建红色研学项目已成为具有红色革命情怀企业家们的理想与企业发展的方向。

“八项规定”出台以来，各级党委政府严格控制与查处公费旅游的不法行为，但“红色研学游”成为了名正言顺的公费开支。城市级组织部可以完全支配党费收入，用以党校建设、红色教育开支。

四川德阳是一座历史悠久、红色旅游资源丰富的美丽古城。国立六中四分校旧址--范家大院、李调元故里--星光村、特级战斗英雄黄继光纪念馆、汉旺地震遗址公园、广汉向阳公社旧址等红色景区景点，完全可以构成德阳地区的一幅高举旗帜、勇担使命、笃实务本、 甘于奉献的革命历史画卷。

在德阳整个红色研学线路上可以看出，党员干部在参观学习完红色景点后，缺少一个总结思想、畅谈体会及休息、就餐的场所。因此，投资建设一个集学习、研讨、就餐、住宿的德阳市党员干部教育基地暨红色传承教育基地是一个社会效益、经济效益双丰收的投资行为。

16）多媒体会议系统

设计说明

多媒体会议系统是本次项目智能化系统的重要组成部分，配备的会议系统应能为与会者迅速、准确、直观地提供、发布和传输各种信息，提高领导决策的准确性和科学性，提高会议和工作的效率。会议系统设计的功能定位应立足目前最新技术，设计功能适度超前，充分结合网络、多媒体、智能控制等各方面的技术，构建一个智慧的会议、培训环境，为可能举行的各种高规格、高档次的培训、会议、讲座、教学等活动提供一个智能化、网络化的基础支撑平台。

系统架构

主要业务功能描述

系统要做到可方便快捷的管理所有视频、音频系统；

满足会议室各路信号源任意切换到各个高清显示设备播放需求；

保证音频扩音系统易操作、功能灵活，满足会议的不同功能要求；

计集中控制系统，使整套系统能够方便快捷的管理；

满足召开日常会议、多功能会议等要求；

满足会议室管理、会议预约、会议签到、信息发布等需求；

满足有外宾参加会议，实现同声传译功能需求；

满足会议录制存储需求；

满足投票选举功能需求；

满足会议室讨论、表决等的需要。

参会人员通过会议发言话筒讲话，通过音响系统把声音高保真、清晰的扩声，达到会议室开会声压级的标准和需求；

通过无纸化会议系统，实现无纸化会议，开会的内容和资料都是事先上传到无纸化终端上，开会时可以选择会议内容、会议纪要、视频点播、会议讨论等功能，具有高效办公、环保以及保密性强等特点；

保证全场有较高的语言清晰度，并能长时间提供足够的声压。扩声系统在正常运行时，各项指标均能达到国家行业标准中语言与音乐兼用的一级指标。

扬声器声音覆盖服务区内，声音与频响覆盖均匀；音箱的外形和安装位置不影响场地的整体风格。

全场各个位置无明显回音、颤动回声和声聚焦等音质缺陷。（但考虑到会场如在装修时没有

进行必要的吸声处理，所以必须要求在会议时进行必要的人工干预手段来弥补，如会议时尽量拉起窗帘，窗帘选用的布料厚度要求等）

设计多种系统保护措施，保证音响系统长期处于稳定可靠的工作状态和在意外情况 下有效迅速保护音箱和音响系统的设备不受破坏。

音箱采用一对一定阻传输方式，音箱与功放阻抗匹配，采用全频宽频音箱，还原出最佳的音质效果，保证音频扩音系统易操作、功能灵活，满足会议的不同功能要求；

数字会议系统采用手拉手方式连接，发言单元采用便携式手拉手安装，外形美观，安装灵活，使用非常方便，而且布线量非常的少，不影响整体的装修布局，音质效果一流，拾音距离可达到50-80CM；

会议讨论系统主机可设置“先进先出模式”、“普通模式”、“限制模式”“自由模式”、“申请模式”等工作模式使用更便捷。

17）智慧酒店系统

设计说明

本项目 8 号地块规划酒店用地。德阳数字科创城是德阳市新兴崛起的一个大规模的综合科创城，是市区政府重点规划区域。本项目位于东湖山公园东侧，有着优越的自然生态优势。结合着办公差旅与旅游住宿需求，若是倾尽全力打造出一个地标性的酒店，定会是一副繁荣昌盛的景象。

主要业务功能描述

酒店系统分为硬件建设及酒店管理系统。硬件部分为酒店管理提供基础支撑，酒店管理系统是提高酒店管理效率的平台。

硬件部分包含但不仅限于以系统：

综合布线系统；

网络系统；

安防系统；

一卡通系统；

停车场管理系统；

楼控系统；

酒店锁系统；

智能家居系统等。

程控交换系统

有线电视系统

视频点播

智能客控

酒店管理系统包含但不仅限于以下功能：

前台接待；

前台收银；

客房管家；

餐饮管理；

财务查询；

电话计费；

系统维护；

经理查询；

工程维修。

智慧资产

覆盖后勤资产档案、计划、采购、出入库、领用、 借用、调拨、租借、维修、盘点、耗材、检测等业务需求。 通过移动办公、RFID、物联网等技术实现智慧资 产全生命周期管理。

资产管理系统是通过对固定资产的形成、使用、维护、保养、消耗、清理报废等方面进行全方位的准确监管，记录资产每次的变更，结合资产使用状态表、资产变更明细表、资产统计表等报表，不仅可以有效的对公司的资产进行统计，还可以为资产的更新等提供科学依据，更可有效避免资产损失；

提供 RFID 资产管理解决，方便出入库操作，加强库存安全管理手段，通过 RFID 资产管理解决放哪，可实现资产射频盘点，大大提升企业资产盘点效率。

耗材管理实现从请领到结算的全流程在线管理，中间过程全程可查可追溯，支持高值耗材条码管理，同时支持配送单转换成条码快速出入库。耗材的批次、效期、灭菌信息全程追溯，可根据效期进行先到期先出策略。支持高值耗材在院状态追踪，使用信息全流程追溯。对权证的效期，耗材的库存，效期全流程监控提醒。

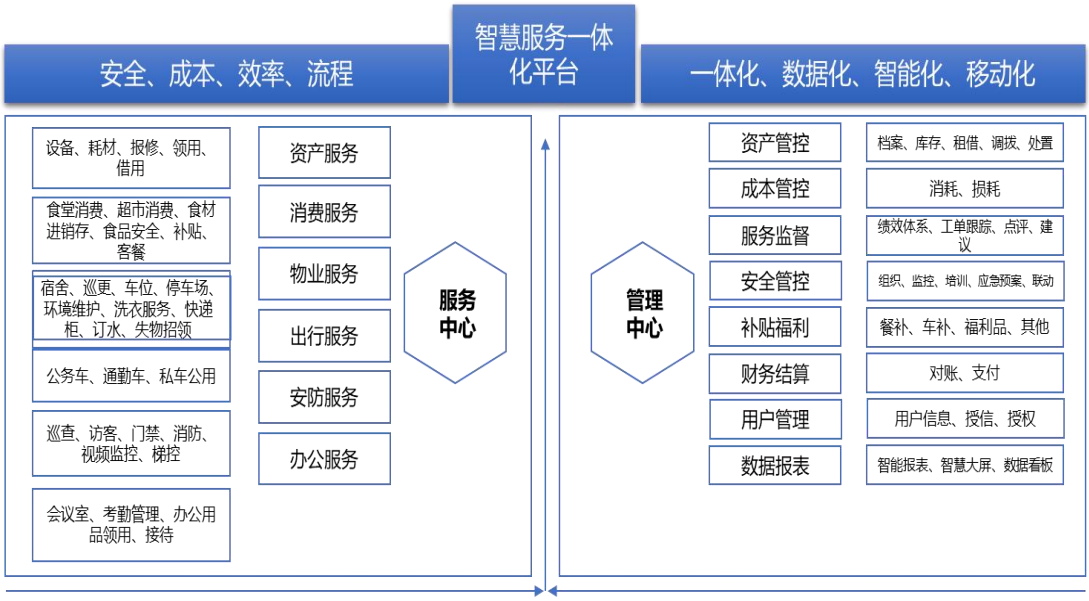
通过移动互联网实现随时随地报修、审核、派工、维修、完工、收费、验收、回访、评价等，利用互联网平台实现用户评价、维修质量、维修效率、维修工考核，物料管理等信息化、透明化，利用物联网、计算、大数据等，形成“互联网+报修”应用服务理念，建立适应互联网服务创新的后勤新模式，推动大数据在后勤管理中的应用创新，通过后勤大数据的挖掘和分析，科学合理配置资源，提高后勤服务效率和服务水平。

18）智慧服务

本项目规划设计智慧服务系统，智慧服务系统功能涉及资产、消费、物业、出行、安防、办公等六大业务板块。覆盖办公设备、公务车、通勤车、食堂、私车公用、会议室、报修、房屋、访客、互动平台、安全巡检、门禁授权、物资领用等场景，智慧服务帮助科创城后期管理及入驻

企业建设一体化、数据化、智能化、移动化的智慧服务平台，实现数据、流程、权限的统一管理，从而达到服务提升、效率高效、成本可控、安全有保障的目标为服务管理的智慧化升级提供工具。

系统架构



主要业务功能描述

智慧服务 APP

智慧服务 APP 是一个移动办事（办公）平台，是后勤服务的移动大厅、后勤管理的移动办公平台，采用 SaaS 技术实现的安全保障为企业提供后勤管理软件服务支撑。APP 的设计迎合了智能终端时代用户的需求，为传统后勤管理换上了智慧的外装，带给用户全新的体验，改变长久以来后勤就是扫扫地、开开车、修修东西的思维观念，让后勤也可以高大上。

APP 配合后端的各个业务模块实现全流程的无纸化办公，用户和后勤员工不在奔波于各种流程的人工审批，大大缩短了工作人员在途的时间提升服务效率。

智慧服务 APP 登陆后分为三个身份分别是：后勤管理、后勤服务、企业员工，每个身份登陆后将感受到截然不同的功能体验，同时他们却共享这同样的数据资源池。移动管理平台首页除企业需要发布的公告外，将各组织架构人员所常用的功能按钮在首页进行布局，常用功能一键直达针对管理者，将部门内重要数据以可视化的形式展现在管理员移动管理平台首页，重要数据实时查看，在保证所有功能便捷操作的前提下，最大程度提升各个角色的操作效率旨在做到“一键直达、只跑一次”。

1）智慧消费

涵盖食堂、超市、无人售卖、企业福利等多个消费场景。 借助全场景人脸消费方案及多种支付设备实现智慧 消费全面升级。 消费数据与进销存数据全面对接增加后勤管理深度。

（1）智慧食堂

通过人脸识别技术和信息化管理系统搭载不同智能硬件，打造便捷的食堂订餐及就餐模式，

实现档口、自选餐、自助餐、进销存等多模板管理，同时收集多维度数据分析助力后勤经营管理优化。系统轻松帮助客户实现精准配餐、提高就餐效率、降低运营成本、可控采购库存、提升用户体验、杜绝食安隐患等多种管理诉求。

档口菜谱点餐

主要实现的功能为收银+菜品+餐补+统计对账，管理员可以在后台编辑菜肴信息及价格并发布菜谱，食堂按照菜谱进行备餐，员工可以在就餐开始前通过手机 APP 或生活号、公众号选择自己喜欢的菜品进行预订，到就餐时间到食堂直接刷脸、扫码、刷卡便可以直接取餐，解决了食堂就餐高峰期排队拥堵的问题，除此之外，员工还可以在食堂终端进行现场点餐，结算人员可以在为员工点餐后点击结算，员工通过刷脸刷卡或扫码完成结算。

自选餐模式

主要实现的功能为收银+菜品+自选餐+餐补+统计对账，实现的场景为自助选餐结算，管理员可以在后台编辑菜肴信息及价格并发布菜谱，食堂按照菜谱进行备餐，根据菜品种类将不同菜品放到带有芯片的餐盘内，管理员将芯片定好价格。或者选用智能 AI 视觉结算台识别方式，对餐盘形状颜色识别、菜品识别。员工到达就餐食堂可自行选择个人喜欢的菜品，将盛菜的餐盘放到结算台后结算台会自动计算出所有餐盘的总价，通过刷脸、刷卡或扫码进行支付。此种方式的优势为无人值守，可极大地减少人力资源消耗。

自助餐模式

主要实现的功能为收银+自助餐+餐补+统计对账，实现的场景为自助就餐，分为有闸机模式和无闸机模式，用户可通过刷脸、刷卡、扫码等方式完成自动扣费，扣除已经设置好的固定金额。扣款成功后有闸机模式会打开通道放人员进入，无闸机模式根据情况可能需要安排人员值守。

（2）智慧超市

本模块依托人脸识别技术、智能化管理系统搭配智能硬件，实现企业超市的内部补贴消费、超市进销存管理、人脸识别消费、经营统计的目的，同时，智慧超市系统已经完成超 70 万常见商品条码的录入，大大减轻了企业新建超市管理系统初始化的难度，提升商品识别的准确度，从而帮助客户实现精准库存管理、经营分析、智能消费的管理需求

（3）无人售货

无人售货模块主要通过自动售货机+智能消费系统的联动效果，实现无人值守刷脸消费、自动出货、自动低库存预警的效果，通过信息化手段，大大提高员工日常消耗品购买效率，减轻企业售货人员成本

（4）福利商城

系统线上开通福利商城，企业可统一线上充值福利货币，通过一定兑换比例将福利积分下发至员工福利账户，员工可自行在福利商城兑换意向节日商品，既满足企业福利线上发放的管理目

的，也提升员工企业福利的满意程度，保障企业福利贴近人心

2）智慧出行

智慧通勤、智慧公车、智慧私车、智慧车辆档案。 全面覆盖企业出行管理诉求。

通过北斗定位、人脸认证、移动应用等技术方案为企业提供智能派车、智慧拼车、刷脸乘车、车辆监控、实时查询等解决方案。

（1）通勤车管理

通勤车（班车）智能管理系统，借助北斗定位/GPS、人脸识别、二维码、IC 卡等车载终端实时监控班车运营状态、汇总运营数据、多维度报表分析，并智能化收集站点信息，实现自动化排班条线，持续优化现有车辆配置方案等，不断提升企业通勤车管理水平及员工满意度。

（2）公车管理

智慧公车调度管理系统通过对车辆的档案、预约、调度、费用、油耗、监控等方面进行全面管理，对公车的使用进行实时人性化的管理，功能的设计，立足于企业对车辆管理的实际需求，为公务车管理“规范、高效、节约、透明，新的管理模式探索”提供了有力保障。

（3）私车公用

私车公用管理模块实现企事业单位私车公用时对车辆轨迹的有效监控，记录相关费用信息，且仅需手机 GPS 完成操作，在私车公用场景与保护员工隐私方面做到了协调，为有效降低相关费用报销成本提供可靠依据，提高用车满意度。

（4）车辆档案

车辆档案模块实现一车一档对车辆实现全生命周期管理，包括车辆的购入、年检、保养、保险、维修、驾驶员、安全检查、油料消耗、违章信息等相关数据的在线移动化管理，系统可通过车辆的基本档案信息在互联网寻找相关接口实现数据实时获取。

3）智慧物业

配套多种智能化设备，全面覆盖企业物业服务的各个方面包括：宿舍管理（申请）、环境管理、停车管理（授权）、快递收发、洗衣服务、图书借阅、物品寄存、内部物流、失物招领、订水、场地预约、工具借用等场景。

（1）宿舍管理

宿舍管理系统，实现对员工宿舍的数据化在线管理，实时在线审批入住、在线报修维护、物业水电等费用的智能化统计并推送，员工可一键申请入住，解放繁重的人力管理工作，提高效率，提高入住满意度，有效降低宿舍管理成本。

（2）便捷服务

便捷服务模块包括：洗衣服务、快递服务、订水服务、图书借阅、场馆预约能功能，系统借助终端设备及人脸数据实现全场景刷脸服务。

（3）停车场管理

实现企业对内部车辆的统一授权、外部车辆临时授权、计费车辆智能缴费、无牌车辆自动发卡、车牌识别、自动道闸的管理，系统还可实现实时统计停车场使用率、车位剩余个数等信息统计，为企业内部停车管理提供有效工具。

（4）环境管理

环境管理主要包括保洁管理、绿化管理、氛围管理三方面，保洁管理主要依靠任务工单系统进行保洁任务派发、监督，绿化管理应用智能灌溉设备以及通知中心功能，保障纸杯合理灌溉、修剪，氛围管理主要应用在企业节日、党建等景观布置以及音乐氛围管理场景，满足企业办公、生活、党建环境管理诉求

4）智慧办公

设计说明

智慧办公解决方案的提出是基于传统办公系统中环境、管理、安全、能源、共享等问题的出现。利用先进的技术、全面的方案、长效的产品，打造舒适高效、节能低耗、安全智能的智慧办公系统。

主要借助智能门锁、各种信息传感器、射频识别技术、红外感应器、激光扫描器等各种装置结合物联网技术为客户解决办公室、会议室、考勤、照明管理、能耗分析、环境质量监测等场景的智能化升级。

主要业务功能描述

会议室管理

会议管理系统支持 Web 网页、手机 APP、微信等多种预订方式；支持邮件、短信、微信等消息通知；支持各种 PAD、智能电视、一体机等终端设备展示。采用后勤帮智能会议管理系统，会议室预订和管理更简单、更轻松、更高效、更直观，可以帮您快速提高会议组织的效率，减少中间差错，同时，提高会议室资源利用率。

考勤管理

考勤管理系统支持企业自定义班次设计，排班灵活，通过人脸考勤机的部署，提升考勤真实性、有效性、便捷性；为员工提供移动端的请销假、出差、补卡、加班等常用考勤申请功能，方便企业考勤信息化管理，提升企业考勤精准度与实效性。

服务监督

服务监督系统主要从三个维度提升员工满意度和归属感，首先通过工单互动点评系统，使企业后勤每个工单都有反馈、有结果，再通过调查问卷主动调研后勤计划提升点以及隐患点，最后通过曝光台，让员工具有主动上报渠道，从而全面的监督后勤各项服务效果，提升员工满意度。

19）智能充电桩管理系统

在地下车库设置电动车充电桩。应用于电动车集中充电管理，通过统一管理、智能管控，避免因乱拉电线、充电过载等引发的火灾、触电危险。

应用功能：扫码充电、自动计费、充满自停、防火预警。

支付方式:微信、支付宝、刷 IC 卡三种付费方式。

20）计算机网络系统

设计说明

计算机网络系统分为三套网络:分别为内网、外网、设备网，三套网络物理隔离，确保各套网络的安全。

内网

内网主要由入住企业自行建设，运营商负责接入计算机网络设备、无线网络设备由入住企业自行购买。

外网

整个建筑共用一套互联网，包含无线网络、语音等在内，根据相关规范设置简单的网络安全即可。

设备网

整个建筑共用一套设备网，常规设计，设置简单的网络安全和监控设备即可。

主要业务功能描述

网络核心层

外网核心交换机位于中心机房，网络采用核心+汇聚+接入三层架构，主干采用万兆上行以太网的技术，实现 1000M 快速以太网技术到桌面。核心层设备作为网络的骨干，提供快速的数据交换和极高的永续性，从备份和负载分选用双核心。网络系统要求可靠性高、突发性强、实时性高、并发性强等。

汇聚层交换机

汇聚层交换机采用全万兆交换机，向上万兆连接到核心交换机，保障骨干链路高可靠性，向下万兆连接到接入交换机。

网络接入层

根据各楼层弱电间和信息点分布情况，每个楼层弱电间部署合适的接入交换机数量。接入层采用万兆交换机，实现千兆到桌面；上行通过万兆光链路连接汇聚交换机，接入层交换机提供 24/48 个千兆以太网电口。接入交换机支持快速检测链路的通断，并且支持端口下的检测环路功能，可防止端口下因个人私接 Hub 等设备形成的环路而导致网络故障的现象。

无线网络

在外网子系统中部署无线网络，实现科创城室外园区无线覆盖，园区部分楼宇办公室、走廊及公共区域采用放装 AP、人员密集区域、会议室采用高密度 AP，接入层交换机采用 POE 交换机连接 AP，同时提供无线智能网优、一键体检等特色功能，帮助无线实现快速部署、简便运维。部分楼宇设计无线网络，根据后期设计图纸及实际需求配置。

部署防火墙系统对外网出口和服务器区边界进行访问控制，根据业务需求，设置访问控制策略，定期进行安全策略的优化和维护。通过入侵防御系统，对网络入侵行为和网络层病毒进行检测和阻断，并进行告警。部署数据库审计系统实现对数据库访问行为的安全审计。部署日志审计系统实现对网络设备、安全设备、主机操作系统、中间件、数据库、应用系统在内的设备及系统的全面日志审计和分析。

设备网建设

设备网主要用于智能化各系统的数据通信的承载。按照核心-汇聚-接入三层部署方式，主干万兆光纤链路、千兆到前端，保证链路带宽和稳定性，接入端主要为监控摄像机、门禁以及各系统等设备，为正常数据的传输提供稳定的环境。各个弱电管理间部署满足日常需求的 24/48 口接入交换机作为智能化设备接入层。通过部署网闸实现与外网的安全隔离。

21）智慧安防视频监控系统

设计说明

规划设计全方位、多层次、内外保护的立体化的安全防范系统，视频监控系统主要通过前端摄像机对科创城内电梯前室、主要出入口、地下停车库和各进出口及和办公走廊等公共场所要害部位进行全天候监视、录像，便于及时了解和监视各个场所的动态情况，并及时进行有效的处理。

实际功能和需求根据后期图纸设计内容为准。

前端摄像机

摄像机配置要求：本次所有摄像机像素不得低于 200 万，在各楼层主要出入口、电梯厅、消防通道、工作人员通道设置人脸识别摄像机，其他公共区域全天 24 小时无死角监控。

防护要求：前端球机摄像机采用不低于 IP67 的防护等级设计，IP67 支持不透灰尘，无灰尘进入；防护强射水进入设备的水量不影响设备。护罩支持整体外罩，防摔防砸设计，防人为破坏的能力。

室内区域选型要求：根据不同区域选择不同类型的摄像机。

半球摄像机：主要设置在室内有吊顶的区域。

枪式摄像机：主要设置在地下室及楼梯处。

电梯摄像机：电梯轿厢内。

室外摄像机：主要出入口、园区干道等公共区域布置。

拾音器：服务窗口、业务窗口区域。

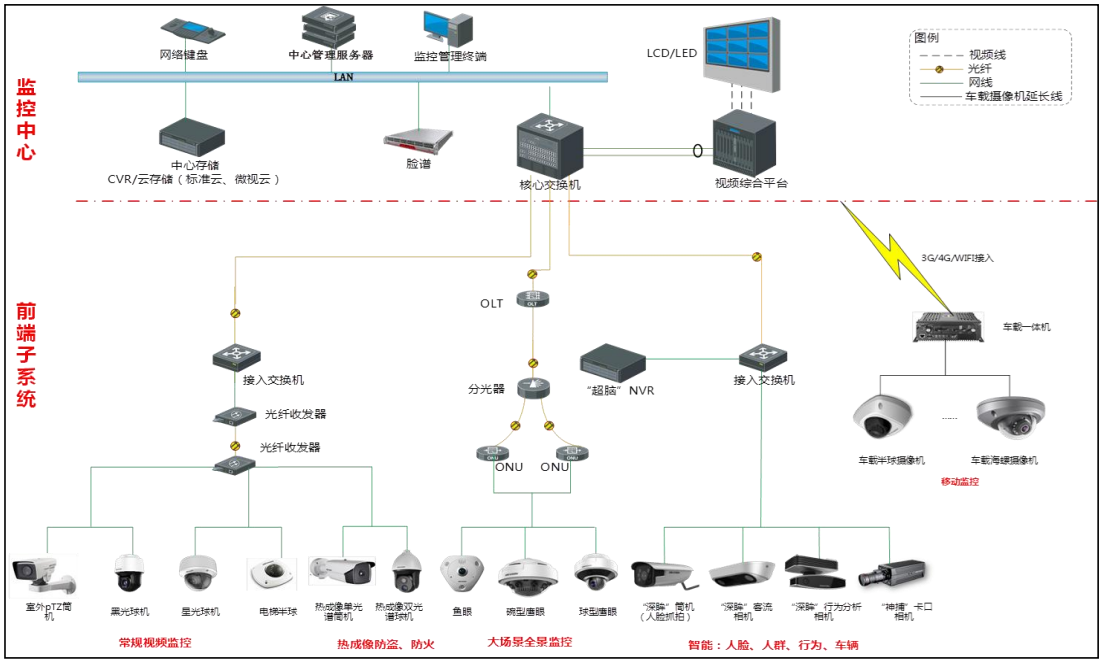
传输部分

一般来说，传输部分就是系统的图像信号通路，在某些系统中，除了要传输图像信号外，还需要传输声音信号、控制信号，故传输部分指所有要传输的信号形成的传输系统的总和。设计采用六类线传输视频信号，供电采用集中供电方式。

存储部分

采集的视频图像信息保存期限不得少于 90 日。本项目设计采用存储架构，由数据服务器和数据存储节点组成。数据服务器支持两台及以上形成集群，提供高可靠的元数据服务。数据存储节点提供高容量、高密度的存储介质和极高的 IO 能力，有效保障空间可扩展性和数据可靠性。

系统架构



系统示意图

主要业务功能描述

视频管理

视频管理服务器用于集中认证、注册、配置、控制、报警转发控制的专用信令服务器，可以实现完善的视频编解码设备网络管理功能，支持多台信令管理服务器相互协同工作组建多级多域的管理平台。支持对存储设备、存储资源和视频数据管理，支持对系统所有存储资源进行全方位的监控和管理，支持不间断的视频检索、回放等业务。网络存储系统，存储资源可以根据需求分布式部署并加以统一资源管理和调度，支持动态存储资源管理、在线部署，可以基于统一平台满足不同存储质量、容量和服务质量的需求，可以提供完善的备份和存储生命周期管理功能。

客户端可以提供友好方便的人机界面功能，包括监控对象的实时监视监听、查询、台控制、接警处理，通过解码进行将系统中视频图像统一上墙。

显示部分

监控中心：与科创城消防控制室共用。配置视频解码器把数字信号转为视频信号传输至拼接大屏上。

智能视频分析

结合本次项目的实际需求，将智能分析技术中的行为分析功能模块融合到了视频监控系统中，主要功能包含人员聚集检测、打架斗殴检测等行为分析功能。主要应用在公共区域走廊、业务区域、办公区域，当发生商业纠纷或业务纠纷的时候，有人员聚集、打架斗殴等异常情况发生时，前端摄像机通过将信息数据上传至监控中心智能分析管理服务器上，智能分析软件可通过预先设置好的行为规则进行判别，一旦系统确认为异常行为，系统可立即进行识别并报警。

22）智能一卡通管理系统

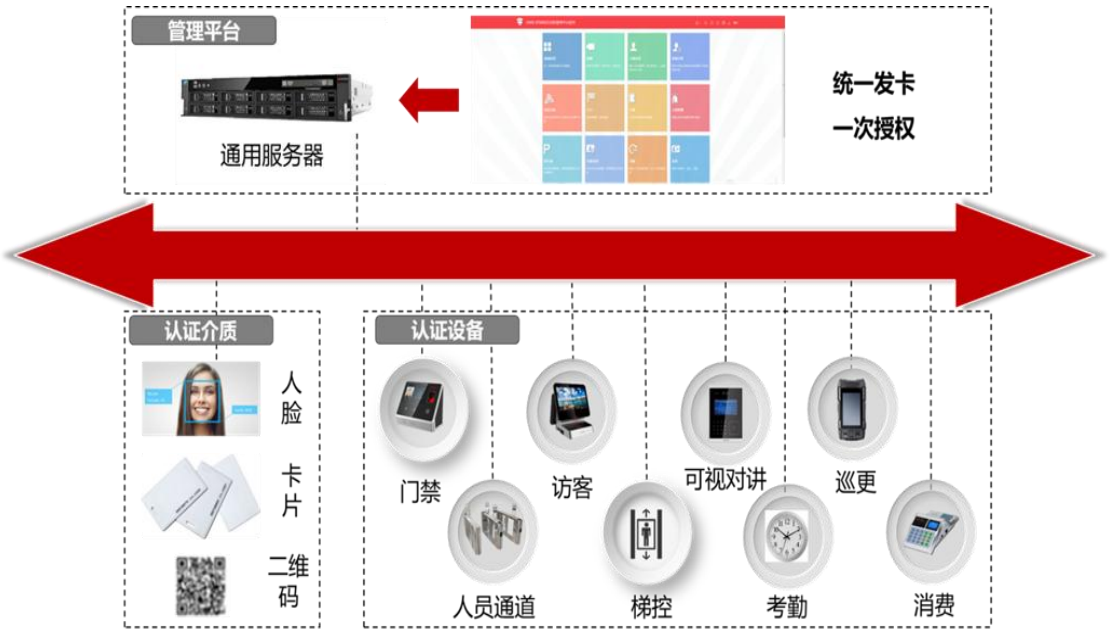
设计说明

一“卡”通包括卡片、人脸识别、二维码等介质，是用户在一卡通各子系统中完成身份认证的唯一凭证，为用户使用一卡通提供了全程的安全保障。同时借助先进的视频技术、射频技术、生物识别技术实现日常管理信息化和身份识别统一化，让管理更高效、让生活更便捷，让园区更安全。

一卡通应用系统包含：访客、人员通道、门禁、可视对讲、消费等，所有信息达到共享要求，通过管理平台将其整合成一个有机的整体。

智能卡管理系统主要包括：门禁管理、梯控管理、消费管理等系统。以手机移动端或感应 IC 卡和人脸为媒介，通过计算机和通信技术为手段，将服务中心内的各项设施连接成为一个有机的整体，用户通过手机或一张卡便可完成通常的资金结算和某些控制操作，如用卡开启门禁，用卡就餐、会议、办公等各项活动。而不必像以往携带多把钥匙开门，去各个对应部门交费等繁杂的操作，减少现金交易等等。整个系统可根据需要对系统内的个体进行监控管理和决策，各局部系统和终端可自动将收集到的信息整理归纳，以供系统查询、汇总、统计、管理和决策。既满足各个职能部门管理的独立性，又保证整体管理的一致性。

系统架构



系统示意图

主要业务功能描述

详见门禁管理系统、梯控管理系统以及消费管理系统描述。

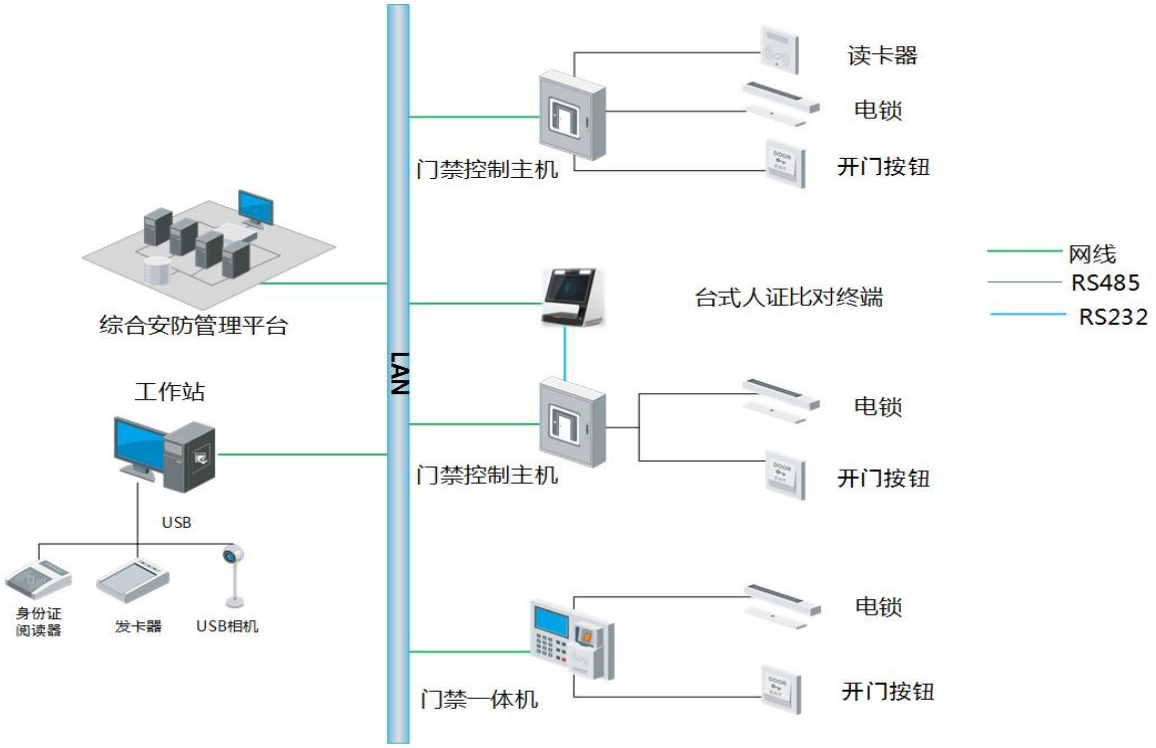
23）数字化出入控制系统

设计说明

在科创城各建筑物内出入口、办公室设置门禁管理系统，有效的控制人员的出入，并且记录所有出入的详细情况。具体包含发卡、出入授权、实时监控、出入查询及打印报表等。

控制机可以联网和脱机工作；TCP 网络多门系统可选择网络多门主机+单元控制。通过 TCP/IP 网络进行通讯，管理电脑可以指定 TCP/IP 网络中的任何一台；单元控制机根据使用场合实用型、标准型、增强型、国际型等可供选择使用；门禁的出入纪录可以做为考勤依据；门禁机同时也可兼做巡更，巡更人员刷卡时会纪录刷卡信息但不会开门。

系统架构



系统示意图

主要业务功能描述

对不同的人员设置不同的通行权限；

一天可设置四个时间段，可严格控制人员在每个时段的进出与否；

可以设定允许通行的时段在节假日及周末是否有效；

强行开门，超时未关门等自动报警；

多种信息记录：每次开门时间，开门卡、编号，报警原因、位置；

开门延时可调；

可脱机或联网使用；

可控制各种不同的电控锁。

安防联动：开门动作（包括非法闯入，门锁被破坏）时，启动联动监视系统，发出实时报警信息；

灯光等联动：当刷卡有效时，自动打开相应区域灯光等；

消防联动：当出现火警时，自动打开相应区域通道。

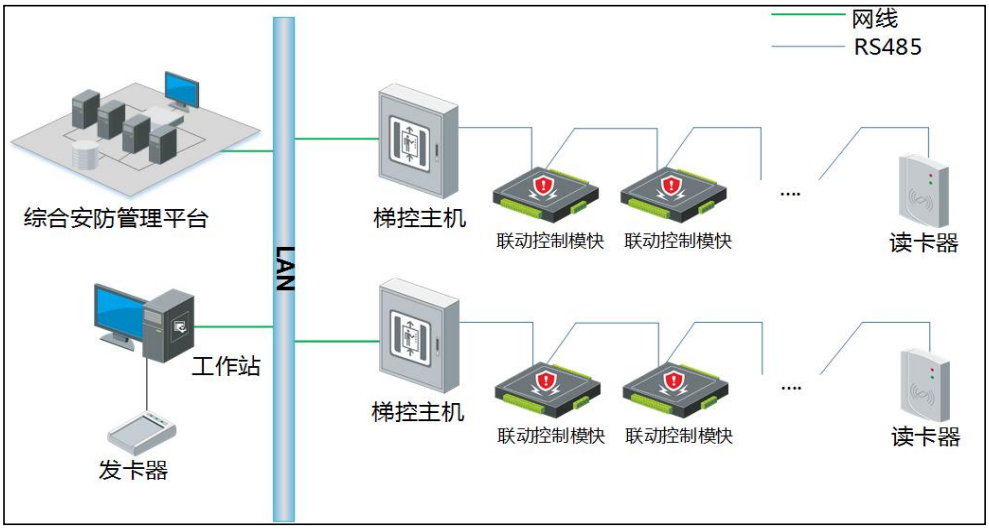
24）智能梯控管理系统

设计说明

在科创城电梯内设置梯控管理系统，使出入电梯的人员需要进行严格的权限认证，杜绝诸如恶意推销人员、无业人员等对物业内用户的骚扰。

针对没有卡片的访客，系统具备多种访客管理方式，可以通过发放临时卡片或住户召唤灵活、人性的实现访客乘梯的需求；针对实际情况，还可以设定在某电梯的自由运行时段，使人员无需刷卡即可乘坐电梯；对火警、匪警等特殊情况，也将自动做出反应措施，释放或关闭电梯的所有使用权限；同时对电梯的出入信息、状态等数据进行记录，使得电梯的使用都有据可寻。

系统架构



系统示意图

主要业务功能说明

电梯管理

电梯管理包括电梯基本资料的录入，电梯注册（包括服务器管理，电梯参数配置等），电梯网关参数远程配置，电梯上下线日志，电梯在线一览表，电梯维保记录，电梯年检管理，电梯终端管理等。

电梯基本资料管理

提供电梯信息的录入，比如电梯的使用单位，生产厂家，维保单位，型号，用途等。

电梯信息注册

注册电梯，提供电梯网关注册时的服务器地址（接入服务器，报警服务器等）以及电梯的业务信息，比如电梯的最底层，语音版还是视频版本，网络通信线路等。

电梯远程配置

对设备参数进行配置，比如：实时状态上传的周期，视频的分辨率、码率，视频显示信息等，也支持远程对设备软件进行升级，重启等。

电梯上下线日志管理

记录每台电梯的上下线情况，在这里可以看到电梯上下线历史、上线 IP 等信息。

电梯在线一览表

记录当前系统中所有电梯的实时状态。

电梯维保记录

针对维保单位在对电梯进行维保的时候，维保人员必须通过打卡或是其他方式告知监控中心，维保人员抵达现场并对该电梯进行了维保，中心平台会记录本次维保记录，并针对性的进行统计，比如电梯最近的维保时间，哪些电梯长时间未进行维保等。

电梯年检管理

记录电梯年检的功能，并推算出下次电梯年检的时间，针对到期要进行年检的电梯，进行提醒。

电梯终端管理

包含电梯流量统计、电梯自检管理等，电梯设备可以通过一段时间的状态，判断出各个设备的工作状态。

权限管理

乘梯人员需要在轿厢内进行刷卡，释放可达楼层的按键权限（没有被释放的按键时无效的），如果只有一个楼层权限则电梯直接到达，拥有多个楼层则需要手动按键。

25）智慧车辆管理系统

设计说明

车辆管理系统是一种高效快捷、公正准确、科学经济的停车场管理手段，是停车场对于车辆实行动态和静态管理的综合。其管理方式是在停车场的各出入口设置车牌识别设备及通道控制设备，对进出停车场的车辆进行科学、有序地管理与控制。

车辆管理系统是以一套完善的基于车牌及车型识别的收费系统作为车辆出入停车场凭证，通过出入口识别车牌号码及识别车型、车辆颜色来判断车辆出场的权限及车辆停放时间、所需缴纳的停车费，再结合多元支付系统（手机支付、无感支付、自助缴费机、中央缴费点，出口值守机器人）实现车辆不停车快速出入场。

停车管理系统

停车场系统设计理念是为停车场的管理提高管理质量和水平，最大程度减少出口人工干预，减少出口车辆收付款缴费时间，提高通行效率，避免现场收费手续导致的拥堵从而使停车场停车能够“进的去”、“出的来”。

在出入口设置进出车道，可采用无人收费管理，固定车辆自动放行，临时车辆通过场内自助缴费、手机支付或出入口值守机器人缴费；在后台管理中心建立一套后台服务管理系统，用于固定车辆信息管理及车辆进出场数据汇总、下发等功能。

设备主要包括相机道闸显示一体机、值守机器人、车辆检测线圈、出入口管理系统以及辅助设施等，实现数据采集、外设控制、数据上传及收费等功能。

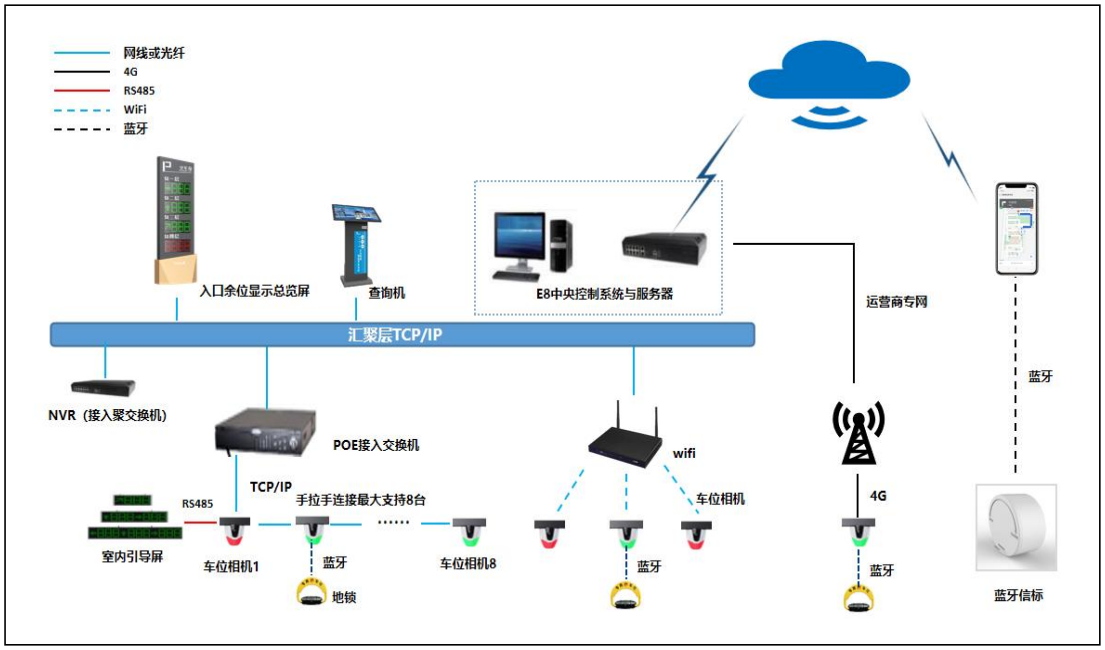
后台服务管理系统设备主要由系统服务器、交换机等设备组成，实现对车辆出入场数据、财务管理、各类数据查询、统计以及报表管理、人员管理等功能。

车位引导系统

在平面车位的正前上方安装前置一体式摄像机，用于检测车位停车状态，并控制自带的车位指示灯显示相应颜色。

车位摄像机自带指示灯，若检测车位停满车，则显示红灯。若检测车位还有空余车位，则显示绿灯，通过红、绿灯显示提示用户有无空余车位。

系统架构



主要业务功能描述

视频流识别技术高效、可靠，通过车牌识别可实现车辆快速进出。

搭配多种缴费方式，可有效分散车流，避免出场排队缴费。

管理软件全中文菜单式操作界面，操作简单、方便。

完善的财务管理功能，自动形成各种报表。

具有防抬杆、全卸荷、光电控制、带准确平衡系统的高品质挡车道闸。

高可靠性和适应性的数字式车辆检测系统

26）入侵报警系统

设计说明

规划设计在科创城园区内单体楼出入口、重要区域，如贵重物品存放室、财务室、核心机房、配电机房、泵房、控制室等设置防盗报警系统，有效防范外来入侵对关键设备设施及重要财务的盗窃与破坏。

在系统布防后，一旦有人进入警戒区域，双鉴探测器立即将警情传送至安装在安保中心内的报警控制器。在设防或不设防的时段，只要触动手动报警按钮，就会有报警信号传送到报警控制器。报警控制器在接到报警信号后，随即在相应显示区域发出声光报警，指示报警防区，实现二级报警，同时联动相应区域摄像机，进行实时录像。当警情得到确认后，值守人员可启动紧急按钮，由报警主机通过电话线将警情传至区域报警中心，实现报警。

主要业务功能描述

软件绘制电子地图

在地图上表示所有报警点，还可进行地图之间跳转，方便在大范围区域显示各级地图和所有的报警点。还可设置“电脑助理”功能，定时自动对各个报警子系统进行布撤防，减轻操作员的工作负担。

报警联动

通过报警联动模块，可自定义其驱动方式及动作方式：可由一些防区或子系统报警、未准备、布撤防、旁路等状态去驱动动作，通过指定串行口输出报警数据，与科创城内各视频监控摄像机实现联动。

布防后延时

如果布防时，操作人员尚未退出探测区域，报警控制器能够自动延时一段时间，等操作人员离开后布防才生效，这是报警控制器的外出布防延时功能。

防破坏

如果有人对线路和设备进行破坏，线路发生短路或断路、非法撬开情况时，报警控制器会发出报警，并能显示线路故障信息；任何一种情况发生，都会引起控制器报警。

布防与撤防

在正常工作时，工作及各类人员频繁出入探测器区域，整个系统处于撤防状态，报警控制器即使接到探测器发来的报警信号也不会发出报警。下班后，处于布防状态，如果有探测器的报警信号进来，就立即报警。系统可由保安人员手动布撤防，也可以通过定义时间窗，定时对系统进行自动布、撤防。

27）出入口控制

通过软件的设置，可以通过串口或其他方式把出入口系统的状态信息结合到本系统中，通过出入口系统的动作，实现自动布撤防的操作。比如，门禁系统中的门磁开关信号，可同时传递到报警系统中，作相应的数据分析、记录。

微机联网功能

系统具有通信联网功能，区域的报警信息送到控制中心，由控制中心的计算机来进行资料分析处理，并通过网络实现资源的共享及异地远程控制等多方面的功能，大大提高系统的自动化程

度。

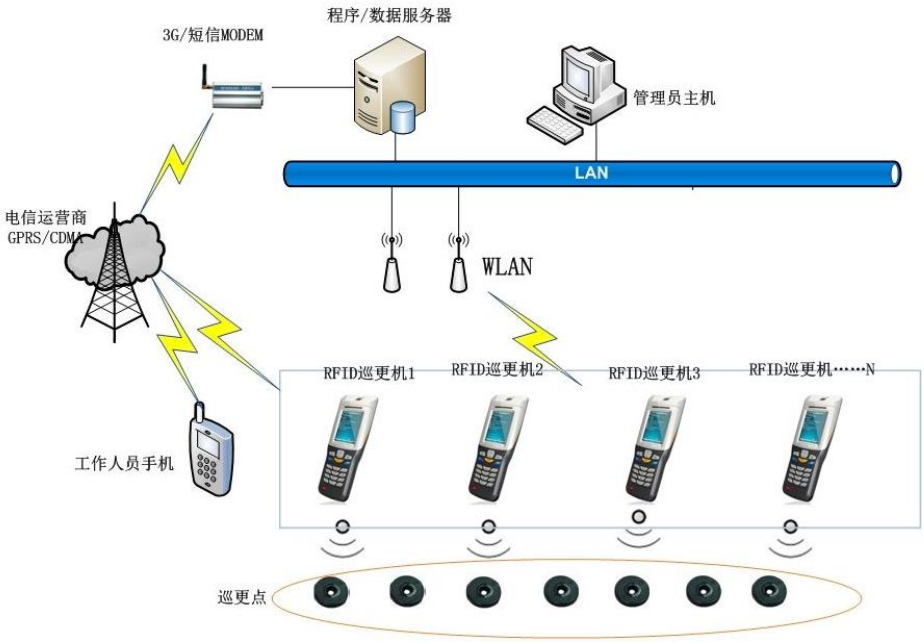
28）安保巡查系统

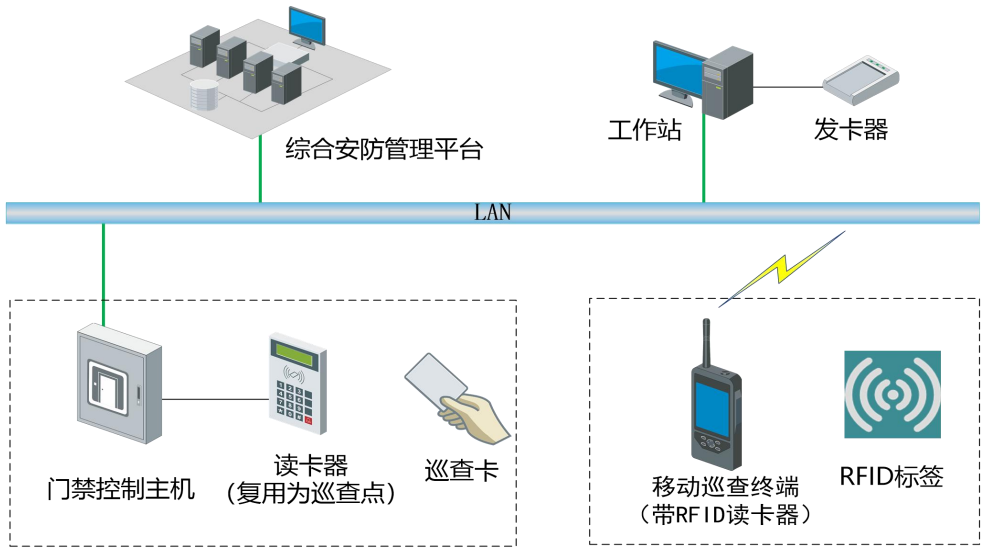
设计说明

在科创城安保巡逻设定路线上，设置电子巡更信息点（或门禁读卡器），为管理者提高各类巡逻巡检工作的规范化及科学管理水平。杜绝了对巡逻巡检人员无法科学、准确考核管理的现象，有效地保障了企业井然有序的工作流程，把巡逻人员管理工作落到了实处。把只限于特定时间、地点及人员的考勤范围通过系统的预先设定，可满足各种场合的特殊考勤，方便记录下工作人员到达巡更点的时间及状态信息。从而达到事半功倍的效果。

巡更管理系统采用 RFID 自动感应识别技术、计算机网络通信与数据处理技术、拍照技术，实现对巡逻人员的考核管理。将巡更点安装在指定的巡逻位置，巡逻人员手持巡更机到每一个巡更点采集信息后，自动记录巡逻人员所到位置的准确时间和位置名称。巡逻结束后通过传输底座将巡逻信息传输给计算机，就可以显示整个巡逻过程（如需要再由打印机打印，就形成一份完整的巡逻报告）。

系统架构





系统示意图

主要业务功能描述

计划：智能排班，可实现任何方式的排班计划，排班可修改。

查询：单条件及多条件组合查询，人员、线路、时间、漏检等情况。

统计：自动分析巡检巡更情况。

29）无线对讲系统

设计说明

无线对讲系统是现代化建筑管理中必不可少的通讯工具，它可以让各个部门内部和部门之间的工作人员随时随地进行联系，不受网络限制，也不需要交纳通话费用，不但极大地提高了工作效率，而且节省了通讯费用。可以起到一呼百应、高效联系的作用，在紧急或意外事件出现时可以及时对所有相关部门工作人员进行统一的调度和指挥，实现即时的处理，最大限度地减少可能造成的损失。因此无线对讲系统在日常管理和安全保卫中发挥着重要作用。

无线对讲系统由信源、多信道合路平台、室内外天线分布系统、数字对讲机等设备共同组成。

系统设计采用数字无线通讯系统，按讲通话，一呼百应。为了达到通信无盲区，克服建筑结构和环境对无线信号造成的阻挡和屏蔽，使信号能够覆盖地上建筑及地下停车场部分，需要采用数字中继转发基站，起到接力通讯的作用。数字中继基站是全双工工作方式，用户机是半双工方式。

主要业务功能描述

单呼

提供给用户私密呼叫的功能，即使呼叫双方并不在同一个通话组中也能通话。可以使两个对讲机之间进行一对一通信。

组呼

组呼是集群通信最基本的呼叫，它允许移动台与一组用户进行一对多的通话，移动台缺省是工作在组呼模式下，而且非常便于发起和接收组呼。

每个移动台可被编程多个通话组，用户可以很简单地选择进入一个通话组，也可以随时进入另一个通话组。一旦选择一个通话组，移动台不需任何动作，便可自动监听接收这个组的呼叫。要发起一个呼叫，用户仅需按下 PTT 即可讲话。

全呼

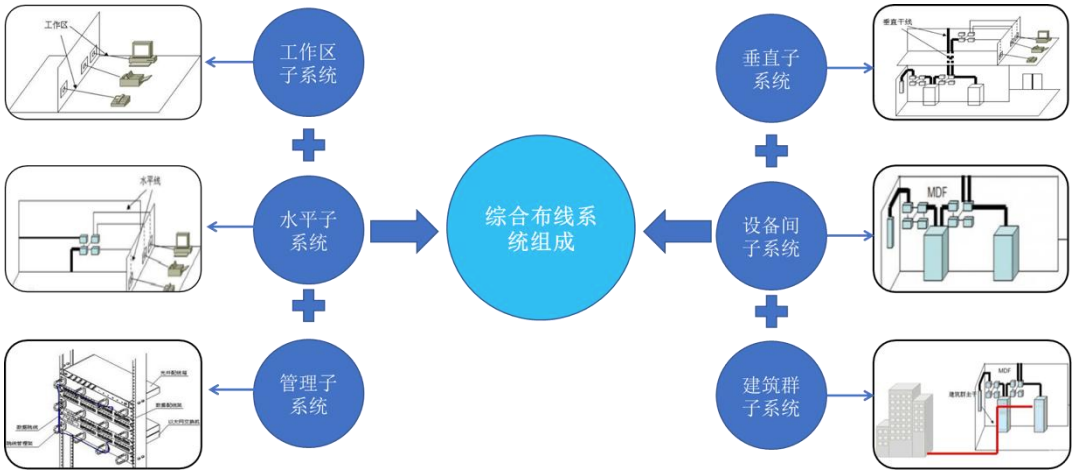
网络全呼允许对讲机呼叫网络里所有基站下的对讲机。

30）综合网络系统

设计说明

科创城综合网络规划设计 3 套网，即内网、外网、设备网，其中内网主要由入住企业自行建设，主要功能用于企业内部信息传输。外网主要由开发商进行规划建设，外网主干引至各楼建筑物配线间，由配线间引至各楼层，入住企业可根据需要选择外网端接。设备网主要由进行规划建设，用于为建筑智能化各系统等提供数据传输链路，为科创城的安保、出入、消费等提供通讯基础。

系统架构



系统示意图

31）通信系统

1）由运营商引入三合一网信号至电信机房，通过运营商设备将光纤引至各栋楼的弱电竖井分光器箱内（光纤由中标单位敷设），由分光器引至商户和办公户内弱电箱内。户内箱由弱电中标方提供，户内弱电箱设备由运营商和用户自备。

2）当电缆从建筑物外面进入建筑物时，应选用适配的信号线路浪涌保护器。

3）光纤到用户单元通信设施工程的设计必须满足多家电信业务经营者平等接入、用户单元

内的通信业务使用者可自由选择电信业务经营者的要求。

4）新建光纤到用户单元通信设施工程的地下通信管道、配线管网、电信间、设备间等通信设施，必须与建筑工程同步建设。

32）弱电机房

弱电机房建设要求按《电子信息系统机房设计规范》C 级标准设计。包括内容：机房环境要求、机房装修、机房照明、机房电气、机房防雷与接地、机房空调、消防与安全、机房环境监控。

（1）机房环境要求：主机房温度（开机时）18-28° C，主机房相对湿度（开机时）35%-75%，主机房温度（停机时）5-35° C，不得结露。不间断电源系统电池室温度 15-25° C.不得结露。

（2）机房装修:室内装修设计选用材料的燃烧性能除应符合本规范的规定外，尚应符合现行国家标准《建筑内部装修设计防火规范》的有关规定。机房室内装修，应选用气密性好、不起尘、易清洁、符合环保要求、在温湿度变化作用下变形小、具有表面静电耗散性能的材料。机房内墙壁和顶棚的装修应满足使用功能要求，表面应平整、光滑、不起尘、避免眩光，并应减少凹凸面。机房地面需要铺设防静电地板，活动地板的高度应根据电缆布线的空调送风要求确定高度。

（3）电气技术要求：供电电源应采用两回线路供电。需设置 UPS 不间断电源，不间断电源系统的供电时间满足信息存储要求，按总负载的 80%配备。不间断电源系统电池备用时间根据实际需要确定。电子信息设备供电电源质量要求稳态电压偏移范围（%）±5.

（4）机房照明：照明设计按照现行国家标准《建筑照明设计标准》的有关规定执行，主机房照度标准值为 500lx,辅助区照明标准值为 300lx.电子信息系统机房应设置通道疏散照明及疏散指示标志灯，主机房通道照明的照度值不应低于 5lx,其它区域通道疏散照明的照度值不应低于 0.5lx.

（5）机房静电防护：电子信息系统机房内所有设备的金属外壳、各类金属管道、金属线槽、建筑物金属结构等必须进行等电位联结并接地。

防雷与接地：

1）机房的防雷和接地设计，应满足人身安全及电子信息系统正常运行的要求，并应符合现行国家标准《建筑物防雷设计规范》和《建筑物电子信息系统防雷技术规范》的有关规定。

2）机房接地点由基建引入到机房，要求接地电阻值不大于 1 欧姆。

3）保护性接地和功能性接地宜共用一组接地装置，其接地电阻应按其中最小值确定。

4）采用 M 型或 SM 型混合型等电位联结方式时，机房应设置等电位联结网格，网格四周应设置等电位联结带，并应通过等电位联结导体将电位联结带就近与接地汇流排、各类金属管道、金属线槽、建筑物金属结构等进行连接。每台电子信息设备（机柜）应用用两根不同长度的等电位联结导体就近与等电位联结网格连接。

5）等电位联结网格应采用截面积不小于 25mm2 的铜带，并应在防静电活动地板下构成边长

为 0.6-3m 的矩形网络。

（6）机房空调：设置机房专用空调。

（7）消防与安防：机房内设置气体灭火。安全防范系统由视频安防监控系统、入侵报警系统和出入口控制系统组成，各系统之间应具备联动控制功能。

（8）环境和设备监控系统：设置空气质量温度、相对湿度监测，漏水检测报警，强制排水设备的运行状态，空调、新风、动力系统设备的运行状态、滤网压差监测。

33) 智能化管网

设计说明

智能化系统是现代建筑物内的综合系统工程，它与所有建筑物的机电设备如变配电、空调、照明等设施有密切关系，包括综合安防系统、综合布线系统、信息发布系统、机房系统等所有弱电系统。建筑智能化系统对建筑物来说是一个整体，每个弱电子系统都各有电缆管线，整个园区及建筑物内遍布着整个弱电系统的电缆布线。综合管路是智能建筑安装工程量最大的项重要工序，合理的弱电综合管路设计不仅会节省管槽及线缆材料，降低工程成本，也会减少施工工程量。

弱电管网设计包括室内水平桥架、室内垂直桥架、室内管线以及室外管网等。本次规划设计仅对室内管线提出规划设计要求，作为各子系统深化时，管网设计依据即参考，室内水平桥架、垂直桥架、室外管网由我方提出需求，由设计院统一进行规划设计。

主要业务功能描述

室内水平系统

水平管路主要为从水平桥架至各个系统终端所使用的管材，采用的材料视各个系统的不同而不同。综合布线系统水平线缆由桥架引出，穿 1-2 根 UTP6 线管材采用 JDG20，穿 3-4 根 UTP6 线的管材为 JDG25 到用户信息点；多媒体查询系统、信息发布系统管路均采用 JDG20 或 JDG25；LED 大屏显示系统采用 JDG25；安防系统采用 JDG20 或 JDG25。所有从引出管线在有吊顶处为吊顶内敷设，从吊顶内到信息插座的垂直管道采用暗敷方式。

本次设计采用 200*100 和 300*100 的水平桥架用于所有弱电线缆。详细规格见后期设计图纸。

室内垂直部分

本次设计中敷设 200*100 的垂直桥架用于所有弱电线缆。详细规格见后期设计图纸。

线管部分

线管部分主要为从水平桥架至各个系统终端所使用的管材。所有室内线管设计在有吊顶处为吊顶内敷设。本工程所有预埋管路地下层采用焊管，地面以上层面采用 JDG 材质穿线管，拟使用 16mm、20mm、25mm 两种规格的 JDG 管。在本系统管线部分的设计中，满足如下要求：

线管内线缆的填充率不超过 30%；

管线施工要求根据国家标准，确保电缆铺设的可能性，清除管内毛刺和垃圾，并在管内

留有穿线所需的引导钢丝；

为了确保穿线顺利，在电线管排放中根据建筑规范在管线分支、连接、转弯处设过线盒；

每根电缆的转弯半径要求为其电缆外径的 8-10 倍。因此，吊顶内桥架在转弯或分路处均设置 45°转角（例如：对于 200×100 的桥架，其 45 度转角边长为 200mm；对于 300×100 的桥架，其 45 度转角边长为 300mm）；

在管线转弯处不能拐死角，转弯半径>10cm；

水平线槽和竖井梯架连接处，及水平线槽和管线各连接处须配以相应规格的分支附件，不能断接，以保证线路路由的弯曲自如以及线路的安全；

为确保线路安全，使桥架有良好的接地端。金属桥架、金属软管均需整体连接，并在本楼层内接地（强电保护地）。接地线截面积不小于 6 平方毫米；

所有薄壁金属电线管均用导线连接，并与桥架连接。

室外部分

室外部分的作用是打通室外的路由管线，把智能化由室内引伸到室外，实现智能建筑整体化。详细规格见后期设计图纸。

34）云计算中心功能设计

中心定位

数字科创城（一期）云计算中心面向全区政务应用、公共服务提供基础服务，解决科创城区城市管理过程中数据计算、应用部署、视频分析智能分析、数据灾备方面的问题，综合提升智慧科创城大数据分析计算能力。

总体设计

本章节从云计算中心的设计原则和规范、云计算中心的特征、设计目标及规划内容进行阐述。

在信息技术高速发展的今天，信息的高度共享和数据的安全可靠是系统建设中优先考虑的问题。随着科创城区信息化工作的全面推进和信息基础设施水平的整体提高，数据规模和业务量快速增长，应用需求呈现多样化，对业务功能、系统关联、信息利用、数据质量、信息服务水平、信息化工作机制等提出了更高的要求和更深入的需求。

本次云计算中心建设方案以云计算为基础，整个方案体系主要分为三层架构，结构如下：

云资源池设计

网络资源池设计

云计算中心的网络设计采用二层扁平化架构，并采用分区建设方式,根据模块化的分区的方式，主要分为核心交换区、汇聚接入交换区、云安全访问控制区及云资源服务区。降低了网络设计的复杂度，同时提高网络可靠性和安全性。

计算资源池设计

服务器系统是整个科创城云数据中心的心脏，负责管理科创城区数据中心的基础信息、共享信息、各专业区域信息以及业务应用过程中发生的相关业务数据、以及数据管理的过程中产生的比对信息、整理信息、管理信息等，同时为各个分系统提供共享信息。

存储资源池设计

充分考虑目前存储系统现状及未来发展趋势，采用折中的方式，有效的将存储按照实际需求进行分类，采用组合对应的方法，充分照顾性能、容量、安全性、多协议融合、非结构化数据存储使用等方面，以数据和存储为中心必然对整个存储系统 I/O 有很高的要求，所以建议选用集中式、高性能、大容量、智能化的光纤存储区域网(Storage Area Network，简称 SAN)来构建新一代计算中心存储环境。

云管理平台设计

云管理平台架构

云计算中心管理平台作为平台管理员、用户同底层物理设备（服务器、存储、网络设备）通信的中间层，是整个云计算中心平台的核心。云管理平台主要分为三大部分功能，包括底层虚拟

化功能层、云资源和综合管理层、云平台门户管理界面层。

底层虚拟化层是科创城云管理平台的基础，主要功能是将物理资源（服务器、存储、网络设备等）虚拟化成虚拟资源池，可支持目前大部分主流的虚拟化组件，包括 VMvare、Xen、KVM 等；云资源和综合管理功能层是科创城云管理平台的核心，主要功能包括虚拟资源池的管理、资源计量计费、资源自动按需配置、资源监控、访问控制、业务全生命周期管理、应用服务器的管理、自助服务、虚拟网络隔离以及提供可扩展的 API 接口等；云平台门户管理层是云计算中心对外服务的门户，提供平台管理员及平台用户的访问入口。

云管理平台设计

云计算中心管理平台运行于数据中心虚拟化架构上，提供资源监控、管理与调度、资源使用流程审计等功能。协助数据中心管理员完成数据中心运维管理工作的同时，满足用户对资源的在线申请和使用要求。监控管理功能可以对硬件资源（服务器，存储和网络）进行实时监控和管理，对于系统异常情况可以实现实时告警。虚拟化功能可以实现虚拟资源的抽象化管理，以资源池的形式进行管理和资源分配，并对根据资源使用情况对资源进行动态调度。系统整体情况和资源使用情况可以通过个性化报表进行展现。通过本产品的资源自助式服务门户可以实现资源的按需获取，业务管理员根据自己的资源需要申请相应的资源，系统实现按量计费。

云资源使用流程设计

云资源的评估流程

本流程场景适用于科创城相关业务单位，向云计算中心提出项目的申请，由云计算中心对整体申请的基础资源进行综合评估，保障项目资源与业务软件的高耦合，保护投资的同时保障业务的稳定运行。

云资源评估流程：首先由申请单元发起流程，提出系统资源需求评估，由服务单元受理本次项目资源评估事项，启动评估，能够通过历史经验值对项目资源进行判断的，反馈给申请单元资源评估建议，如果历史经验无法做出合理评估判断，启动测试评估，随后给出资源评估建议到申请单元，申请单元根据此意见向管理单元提出项目审批。

云资源的申请流程

本流程场景适用于科创城区相关业务单位对云资源的申请，云资源管理单元对现有资源和业务资源的评估，分配相应资源，为业务系统提供服务。

云资源申请流程：由申请单元（科创城区）发起项目流程，向管理单元提出项目审批申请，如不能通过，则流程终止；如通过了评审，由服务单元，受理本次项目需求，启动云资源池的评估，如果资源池能够满足业务系统上线需求，创建资源；如资源不足，扩建资源池，在为用户创建资源池。由服务单元将资源交付给申请单元，申请单元部署系统，完成项目上线；服务单元负责基础设施的运行维护。

云资源的回收流程

本流程场景适用于科创城区相关业务单位对云资源的撤销申请，云资源管理单元对撤销申请进行综合评估，服务单元配合进行相关业务和数据备份，将数据打包迁出并释放资源。云资源回收流程：申请单元提出资源撤销申请，管理单元进行综合评估申请是否执行，针对同意的撤销申请，由服务单元进行已运行业务数据的整体备份和打包，数据交付给申请单元并签署确认单，资源撤销释放，纳入科创城云资源池。

云安全系统设计

数字科创城云计算中心的安全设计遵循国家信息安全等级保护相关要求，针对云计算中心科创城平台部分：办公区为等保一级，业务区为等保二级；针对云计算中心专网平台部分：办公区为等保二级，业务区、数据区为等保三级。

国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

云容灾备份系统设计

灾备设计原则

为了确保云计算中心应用系统的数据可靠性，需要提供的容灾备份及恢复能力，需要遵守如下设计原则：

可恢复性

数据备份的目的是恢复数据。如果一个集中式的备份系统无法完成备份功能，或者无法保证系统数据能在合理的时间内恢复，这个备份系统是毫无意义的。

稳定性

备份产品的主要目的是为生产系统提供一种数据保护的方法，所以其稳定性和可靠性是衡量产品的最重要方面之一。首先，备份软件应该与操作系统 100%完全兼容；其次，针对意外故障应该能够快速高效的进行数据恢复。

自动化

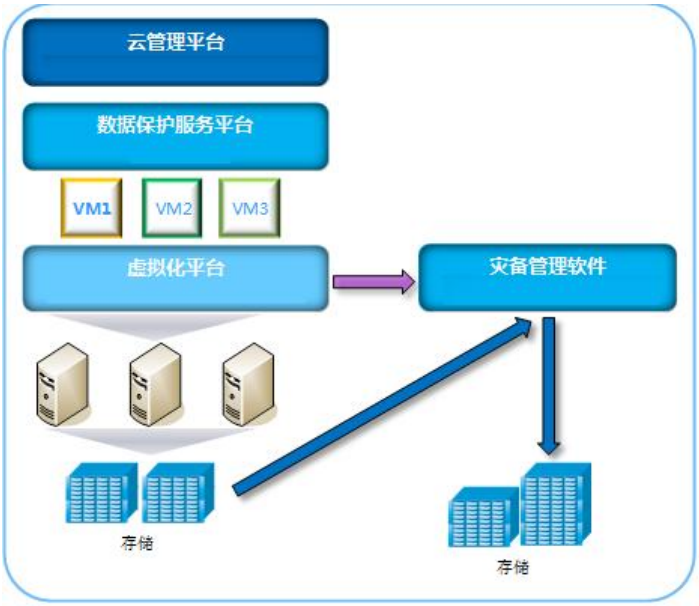
许多系统都会根据实际情况来确定何时进行备份，以及备份操作的时间窗口。为减少网络负担，备份应该选择夜间进行；系统管理员可能会由于深夜疲劳而频繁出错，这就会导致备份出现一些潜在故障；因此，时间表确定的自动备份必须在该方案中可用。在自动备份期间，若出现意外情况日志功能必须支持自动发出报警，DR（容灾）操作也同样必须自动进行。

实时性

一些关键业务需要 24 小时不间断运行，有一些文件可能仍然处于被使用的状态，那么在进行备份的时候，要采取措施，实时地查看文件大小、进行事务跟踪，以保证正确地备份系统中的

所有文件。

备份服务设计



备份方案的架构包括五个层面：云管理平台、数据保护服务平台、虚拟化平台、备份软件、备份存储。

备份服务管理流：管理平台按需根据租户的备份服务需求下发服务，数据保护服务根据服务指令进行备份服务的编排和调度，调用虚拟机平台集成的存储接口触发生产存储创建快照卷，调用备份接口触发备份软件执行快照卷的备份。

备份数据流：备份软件直接从生产存储读取快照卷的数据进行备份，将备份数据通过备份服务器写入备份存储。

远程备份设计

为了保证云计算中心的数据进一步的安全和可靠，可将业务数据备份至异地备份中心。

异地备份中心通过网络为各市提供备份空间，云计算中心在已有备份服务的基础上，将异地备份空间配置为远程备份系统的目标端。备份系统将需要本地备份的数据通过备份网络远程复制到异地备份资源池。

当本地业务数据出现问题时，可通过备份系统选择不同时段的备份副本通过备份网络远程复制回本地存储空间，实现业务数据的恢复。

应急指挥中心设计

以公共安全科技为核心，以资源整合为出发点，以信息技术为支撑的突发公共事件应急保障技术系统，是实施应急预案的信息技术工具；具备日常管理、风险分析、动态决策、综合协调、应急联动与总结评估等功能。

视频会商系统

视频会商系统应满足应急平台到各专业应急平台会议室进行双向交互视频会议功能， 在设

备选型上，从实际需要出发，以设备功能先进、稳定性为重，同时系统权衡性价比，在满足系统功能需求的基础上，达到系统功能先进、运行稳定、易于操作、升级维护方便、兼容性好、性价比高。

视频监控与图像接入系统

IP 网络技术的成熟，使得理论上可以在任何地方建立视频监控系统，并且可以实现远距离浏览监控图像，控制监控系统。IP 监控系统和图像接入以其高性能，高可伸缩性，高可用性，丰富的应用，即将成为未来监控和图像接入系统的主流。

IP 视频监控与图像接入系统作为一个开放、标准、高质量的网络视频监控基础平台，可通过开放内部协议接口、开放 SDK 接口，以应用需求为导向，提供完善的、统一的视频监控与图像接入解决方案。

视频监控和图像接入系统可提供多种基础业务功能及融合业务功能：

（1）基础业务功能

1）媒体播放业务：实时监控、点播回放、录像存储与播放、屏幕抓拍、本地下载。

2）远程控制业务：远程控制锁定、远程控制解锁、抢占远程控制、释放远程控制。

3）数字矩阵业务：可以通过轮切方案的配置，将有操作权限的摄像机视频输出任意监视器。

4）GIS 地图服务：进行 GIS 地图的各种操作。

（2）增值融合业务

1）与视频会商系统融合

视讯、监控系统通过数字方式无缝融合，可以任意调用监控图像到视频会议中供与会领导观看讨论，进行集体决策，形成一套完善应急联动方案，为领导快速、精确作出决策奠定良好基础。

2）与上层应用系统融合

可向增值应用合作伙伴（SVAP）提供中心平台的各种开发接口，包括通讯协议、API 函数、解码插件、SDK 开发包等各种方式，采用最灵活的方式共享集成监控平台的各种资源，开放接口可供应急指挥业务系统进行调用，业务系统通过 API 接口直接对监控系统图像进行调用和处理。

3）与其他监控系统兼容、互通

对于已部署模拟矩阵、DVR 等视频监控系统的场合，可以实现平滑扩容，可以通过多种方式，实现对视频监控系统的操作键盘/客户端，全局操控权限范围内的摄像机/云镜资源。

应急指挥场所

应急指挥场所包括应急指挥大厅、值班室、会商室等，应具有显示系统、智能控制系统和安全保障系统等。满足日常管理和处置两起突发公共事件应急的需要，提供 7×24 小时值守应急和指挥会商的基本条件。

（1）在应急指挥大厅、值班室、会商室等应急指挥场所设置显示系统。应能接入和显示计

算机、图像、视频会议和电视等多种来源的信号，应能支持 H.264 等 IP 视频流的接入和显示，满足日常值班、应急处置、指挥调度等业务的需要。

（2）智能控制系统实现图像接入、计算机显示、视频会议等音视频信号的切换、灯光分组开关、音响等环境控制。

安全运营服务设计

数字科创城合规体系

数字科创城组织规范

以信息安全等级保护标准为依据，结合科创城运营的需要，设计合理的组织体系，确定保证数字科创城网络安全运营所涉及的管理方、使用方、运营方、及用户的职责及定位。保障数字科创城网络信息安全管理合规，理清数字科创城网络安全运营职责。

数字科创城制度规范

以信息安全等级保护标准为依据，结合科创城运营的需要，设计贯穿业务系统全生命周期（系统设计、开发、发布、运维）各个方面完整的安全制度、操作流程及作业指导书。

数字科创城技术规范

以信息安全等级保护标准为依据，结合科创城网络安全事前防范、事中响应、事后处置的需求设计相关的安全技术体系，安全技术体系建设需满足等级保护的相关要求。

数字科创城网络安全运营平台

数字科创城网络安全运营保障平台的功能应支撑数字科创城信息安全保障工作的各主要工作环节，包括信息安全辅助决策、安全活动管理与管控、监控预警与合规管理、应急管理与风险分析等四个部分，各部分工作的主要功能应包含：

信息安全辅助决策

提供数字科创城信息安全状况的真实数据分析，便于管理者进行决策，并依据数字科创城的安全状况进行安全工作的组织和管理，使得数字科创城信息安全决策有据可依，信息安全工作易组织、易协调、易推动。

安全活动管理与管控

根据信息安全法规的要求，开展常态化的信息安全日常运维工作，并对信息安全工作进行跟着管理，使得信息安全运营工作规范化、有序化。

监控预警与合规管理

提供监控预警手段，及时发现并处置信息安全事件，依据国家法规要求，开展信息安全风险评估，等级保护等专项安全工作。

应急管理与风险分析

根据国家应急响应相关法规要求，建立系统的应急工作机制；提供信息多维度的、细粒度的

安全风险分析报表。

数字科创城网络安全运营

数字科创城网络安全运维

为持续保障智慧网络安全合规体系的正常运行，需配备网络安全管理及网络安全技术人员，负责数字科创城网络安全日常运营管理的相关工作。主要包含：安全制度的管理维护和落实、安全工作的监督和落实；安全设备的维护、巡检、日志分析，安全事件处理等。

数字科创城网络安全专项服务

为保障数字科创城各业务系统的安全稳定运行，及时发现数字科创城各业务系统存在的安全隐患，需定期开展风险评估、等级保护、渗透测试、安全扫描等专项工作，通过各专项工作及时发现存在的问题并提出解决方案。

智能监测平台设计

智能监测平台面向智慧科创城（一期）所有业务系统进行在线监测监管，提供运行环境监测、引擎监测、平台监测、节点监测、插件监测、服务实现监测。

运行环境监测

实现对运维环境的监控，主要包含操作系统、JVM、数据库、中间件等，并形成日志监控。

引擎监测

引擎监测可以用于运行和管理各个插件、管理各个节点。

平台监测

平台监测主要是对引擎基本信息、引擎运行信息、节点基本信息及插件基本信息进行展示，并支持对运行状态进行控制，对节点进行简单管理。

节点监测

节点运维主要是展示节点本身和运行在节点上的插件基本信息及其状态，支持对节点和插件的状态进行控制。

插件监测

插件监测主要是展示插件的基本信息、运行状态及插件上服务和服务实现的基本信息，并支持支插件的运行状态进行控制。

服务实现监测

服务实现监测运维用于展示实现的基本信息及实现的调用情况，并支持对服务实现的状态进行控制。

主要业务功能描述

水平子系统

水平布线子系统是整个布线系统的一部分，将干线子系统线路延伸到用户工作区。水平布线

子系统处在一个楼层上，并端接在信息插座或区域布线的中转点上。水平子系统的电缆数为六类 4 对 UTP（非屏蔽双绞线），支持大多数现代通信设备。

管理子系统

管理子系统由分散在各楼层的分配间组成，负责楼层信息点的配线管理，所有电缆光纤配线架需以整洁而且安全的方式安装并集成在独立的 19 英寸标准机柜内，并有足够空间应付将来增加的布线，机柜内须考虑网络设备的安装空间。

为保证语音、数据水平链路的互换，语音与数据水平链路端接到配线架上；语音主干链路大对数铜缆；数据主干链路采用万兆光缆。

按信息点数相应配置数据与语音跳线，并设置线缆管理器，语音跳线可根据语音大对数配线架的接口形式自由选择。

设备间子系统

光纤传输部分采用 24/48 口通用型机架式光纤配线架，并配备低损耗的 LC 接口的单模光纤耦合器。满足现场对光纤设备的管理与端接，采用模块化设计，根据实际需求选配光纤适配器。

语音传输部分采用语音配线架用于连接来自各管理间的 3 类 50 对大对数线缆，选择 100 对 110 配线架。数量配置能够将全部水平线缆和垂直主干线缆端接好为标准。

与管理间类似配置，在每个设备理间设置 42U 网络机柜进行管理。所有信息点位通过配线系统统一管理。配置 42U 的含 PDU 的机柜。

35）数据中心功能设计

数据中心将按照“稳妥推进、有序建设、保障安全”原则，加快数据中心建设和应用，构建智慧科创城模块化数据中心，减少建设投入，提高运行维护水平。

数据中心将按照“稳妥推进、有序建设、保障安全”原则，加快数据中心建设和应用，构建智慧科创城模块化数据中心，减少建设投入，提高运行维护水平。

设计思路

整体性机房工程内包括及多个专业，各个专业间存在千丝万缕的联系，必须从整体考虑、全局出发才能使各专业协调融会在一起。所有的系统设计应在建设时统一规划。

安全性采用高可靠性设计标准，为应用提供稳定可靠的基础环境和设计。对于各系统应采用高可靠性设计标准。应具备在现有条件下和规定时间内完成规定功能的能力；应具有长期可靠和稳定工作的能力；并具有合理的容余能力及灾难备份能力，为计算机应用系统的高可靠性目标要求提供匹配的基础环境设施条件。

应具有完整的安全策略和切实可靠的安全手段来保障计算机机房用户运行系统基础环境实施的安全从防火、防水、防盗、接地、防雷、防电磁干扰、降噪等方面采取有效措施，并考虑地面承重能力等特殊技术措施。

经济性 采用合理的冷气流管理、智能照明、EC 驱动、自动休眠轮巡等技术，全部使用国家认可的环保材料，设计方案要体现节能思想，保证工作人员工作环境的舒适性。

智能管理采用多系统、多地、多平台管理，各系统应具有较强的集中式管理加分布式实施的可管理性逻辑。便于工作人员对环境及放置的设备进行集中管理，便于维护、维修。

易用性各系统都必须具备灵活的系统扩容和升级能力。底座高度可调、机柜通道

框架式设计，快速安装，现场灵活可调。

先进性与实用性在满足可靠性前提下，采用先进、实用的技术、设备和材料。

总体设计

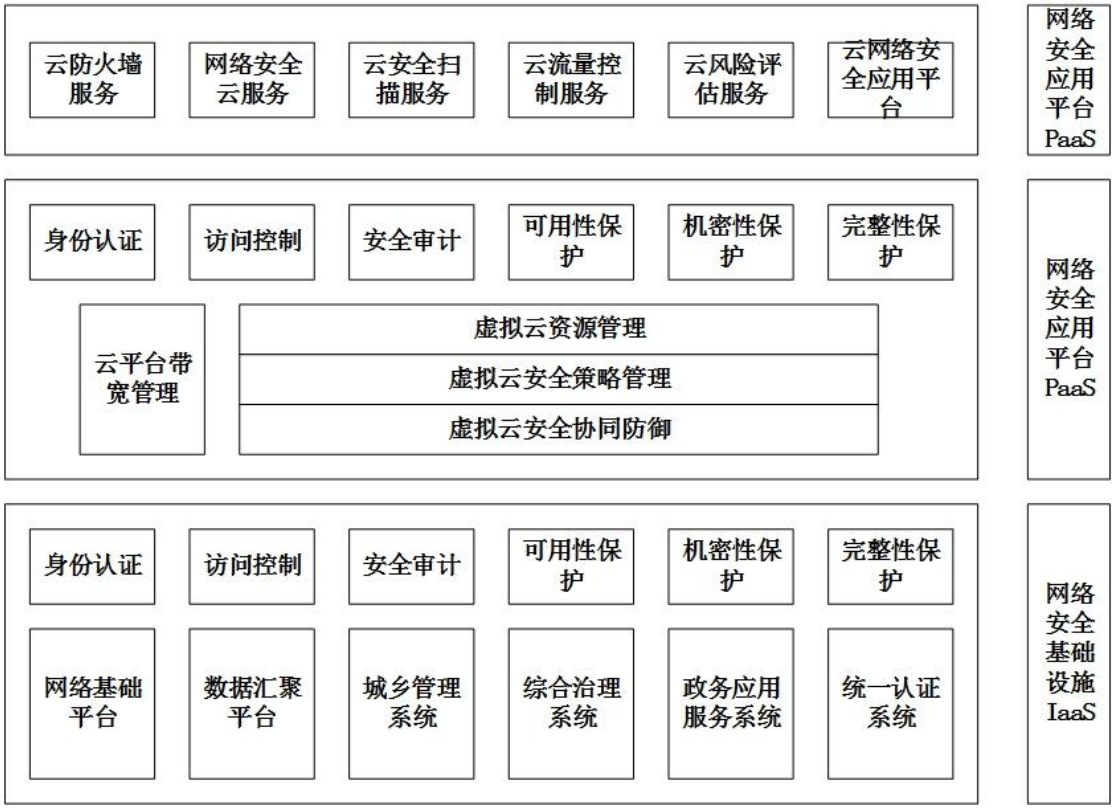
本次数据中心建设方案以计算中心建设标准为基础，整个方案体系主要分为三层架构，结构如下：

最底层为基础设施服务层（IaaS，Infrastructure as a Service,基础设施即服务），提供数据中心所需的基础设施；中间层为平台服务层（PaaS，Platform as a Service，平台即服务），主要提供数据中心的中间件平台；最上层为应用服务层（SaaS，Software as a Service，软件即服务），主要提供数据中心的相关业务应用。

计算服务基础架构通过对底层服务器硬件、存储、网络等资源实现虚拟化聚合部署，同时利用海量数据存储系统，配合计算管理平台，为科创城建设提供了一个功能完整的、标准开放的方便集成的 IaaS 服务层，这层提供的动态基础架构是整个数据中心服务的核心支撑层。资源池的规划参照行业现有的业务应用的资源需求进行逻辑划分，同时也必须兼顾未来业务发展的需要，为综合管理、服务和运营一体化平台提供支撑与数据保障。

总体安全架构

科创城数据中心安全设计基于信息安全等级保护三级设计，并依托计算平台建设，该平台的建设遵照信息系统等级保护三级要求建设。



智慧科创城项目依托计算平台建设，参考等级保护技术设计要求规范，从信息系统安全涉及角度，安全信息系统由安全应用支撑平台和在其上运行的应用软件系统两部分组成，而安全应用支撑平台又是由信息安全机制和信息安全基础技术支持来实现的，其中信息安全基础技术包括密码基础、系统安全技术、网络安全技术以及其他安全技术；这些基础提供了身份认证、访问控制、安全审计、可用性保护、机密性保护、完整性保护、监控、隔离、过滤等安全机制，用以形成覆盖计算环境、区域边界、通信网络的等级保护技术方案，同时通过引入多级互联机制以及安全管理中心，则构成了多级的安全信息系统。

网络安全设计

为进一步健全网络安全保障工作与信息安全监管工作机制，增强网络与信息安全监管应急协调能力，提升网络与信息安全突发事件应急处置水平，制订网络安全保障。

以构建网络安全保障为出发点，加强网络安全监管工作，坚持积极防御、综合防范的方针，全面提高安全防护能力。重点保障基础信息网络和重要信息系统安全，打造安全的网络环境，保障网络安全及信息化健康发展。

物理安全设计

本项目部署在模块化数据中心内。模块化数据中心依据《信息系统安全等级保护基本要求》对“物理和环境”的基本要求、GB50174－93《电子计算机机房设计规范》建设要求。符合信息系统安全等级保护相关要求。

数据资源共享

数据资源共享可以同时分享数据库中的数据资源，这也是数据库建立的最终目标，为的就是

能够实现资源利用率的最大化，在数据资源共享性的支持下，各平台不再收到系统程序的约束，能够自由的调用数据库中的共享资源,并且能够实现多套系统协同,在同一实现资源的同时利用。这样一来就能够保证各平台系统不会因为资源调度问题受到阻碍。

数据资源共享在一定程度上反映了信息化发展水平的高低。资源利用一直是重要的问题，数据库的资源共享可以解决有限的数据资源问题，为各平台协同进行数据信息交互，资源的直接利用能够有效的节省查询事件，减少重复性的问题，能够节约平台资源利用率，将资源利用可以投入到本身业务中。数据库资源的共享性能够实现资源的合理利用，保证数据资源的安全，提升效率。

计算环境安全设计

身份鉴别

身份鉴别可分为主机身份鉴别和应用身份鉴别两个方面：

（1）主机身份鉴别

提高主机系统安全性，保障各种应用的正常运行，对主机系统需要进行一系列的主机加固措施，包括：

对登录操作系统和应用系统的用户进行身份标识和鉴别，且保证用户名的唯一性。

根据基本要求配置用户名/口令；口令必须具备采用 3 种以上字符、长度不少于 8 位并定期更换；

启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。

远程管理时应启用 SSH 等管理方式，加密管理数据，防止被网络窃听。

对主机管理员登录进行双因素认证方式，采用 USB key+密码进行身份鉴别

（2）应用身份鉴别

为提高应用系统安全性需要进行一系列的应用加固措施，包括：

对登录用户进行身份标识和鉴别，且保证用户名的唯一性。

根据基本要求配置用户名/口令，必须具备一定的复杂度；口令必须具备采用 3 种以上字符、长度不少于 8 位并定期更换；

启用登陆失败处理功能，登陆失败后采取结束会话、限制非法登录次数和自动退出等措施。

应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

对于三级系统，要求对用户进行两种或两种以上组合的鉴别技术，因此可通过双因素认证（USB key+密码），采用 CA 认证系统的方式进行身份鉴别。

访问控制

三级系统一个重要要求是实现自主访问控制和强制访问控制。自主访问控制实现：在安全策

略控制范围内，使用户对自己创建的客体具有各种访问操作权限，并能将这些权限的部分或全部授予其他用户；自主访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级；自主访问操作应包括对客体的创建、读、写、修改和删除等。强制访问控制实现：在对安全管理员进行严格的身份鉴别和权限控制基础上，由安全管理员通过特定操作界面对主、客体进行安全标记；应按安全标记和强制访问控制规则，对确定主体访问客体的操作进行控制；强制访问控制主体的粒度应为用户级，客体的粒度应为文件或数据库表级。

由此主要控制的是对应用系统的文件等资源的访问，避免越权非法使用。采用的措施主要包括：

启用访问控制功能：制定严格的访问控制安全策略，根据策略控制用户对应用系统的访问，特别是文件操作、应用访问等，控制粒度主体为用户级、客体为文件或数据库表级。

权限控制：对于制定的访问控制规则要能清楚的覆盖资源访问相关的主体、客体及它们之间的操作。对于不同的用户授权原则是进行能够完成工作的最小化授权，避免授权范围过大，并在它们之间形成相互制约的关系。

账号管理：严格限制默认账户的访问权限，重命名默认账户，修改默认口令；及时删除多余的、过期的账户，避免共享账户的存在。

访问控制的实现主要采取对操作系统和应用系统进行安全加固和优化和部署内控运维管理系统达到以上要求。

系统安全审计

系统审计包含主机审计和应用审计两个层面：

主机审计

启用主机审计功能，或部署主机审计系统，实现对主机监控、审计和系统管理等功能。

监控功能包括服务监控、进程监控、硬件操作监控、文件系统监控、打印机监控、非法外联监控、计算机用户账号监控等。

审计功能包括文件操作审计、外挂设备操作审计、非法外联审计、IP 地址更改审计、服务与进程审计等。审计范围覆盖到服务器上的每个操作系统用户和数据库用户；内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等；保护审计记录，避免受到未预期的删除、修改或覆盖等。同时，根据记录的数据进行统计分析，生成详细的审计报表。

系统管理功能包括系统用户管理、主机监控代理状态监控、安全策略管理、主机监控代理升级管理、计算机注册管理、实时报警、历史信息查询、统计与报表等。

通过部署内控运维管理系统和安全管理平台，对用户操作行为、用户事件及系统状态加以监控、审计，范围覆盖到每个主机系统，从而把握主机系统的整体安全。

应用审计

应用层安全审计是对业务应用系统行为的审计，需要与应用系统紧密结合，此审计功能应与应用系统统一开发。

应用系统审计功能记录系统重要安全事件的日期、时间、发起者信息、类型、描述和结果等，并保护好审计结果，阻止非法删除、修改或覆盖审计记录。同时能够对记录数据进行统计、查询、分析及生成审计报表。

部署数据库审计系统和安全管理平台对用户行为、用户事件及系统状态加以审计，范围覆盖到每个用户，从而把握应用系统的整体安全。

入侵防范

针对入侵防范主要体现在主机及网络两个层面。

针对主机的入侵防范，可以从多个角度进行处理：

入侵防御系统 IPS 可以起到防范针对主机的入侵行为；

部署漏洞扫描系统进行网络、系统、应用、数据库安全性检测；

部署补丁管理系统，开启补丁分发功能模块及时进行系统补丁升级；

操作系统的安装遵循最小安装的原则，仅安装需要的组件和应用程序，关闭多余服务等；

另外根据系统类型进行其它安全配置的安全加固处理。

将入侵防御系统 IPS 部署在安全接入区域外部接入边界上，通过实时侦听网络访问数据流，当发现网络违规行为和未授权的网络访问时，能够根据系统安全策略做出反应，包括实时报警、阻断攻击或执行用户自定义的安全策略等。

入侵检测系统 IPS 可以部署在安全接入区域边界，监视并记录外网接入的所有访问行为和操作，有效防止非法操作和恶意攻击。同时，入侵检测系统 IPS 还可以形象地重现操作的过程，可帮助安全管理员发现网络安全的隐患。

需要说明的是，入侵检测系统 IPS 是对防火墙的非常有必要的附加而不仅仅是简单的补充。入侵检测系统 IPS 作为网络安全体系的第二道防线，对在防火墙系统阻断攻击失败时，可以最大限度地减少相应的损失。

主机恶意代码防范

各类恶意代码尤其是病毒、木马等对信息系统危害重大，病毒在爆发时将使路由器、交换机、防火墙等网关设备性能急速下降，并且占用整个网络带宽。

针对病毒的风险，我们建议重点是将病毒消灭或封堵在终端这个源头上，在所有服务器上部署网络防病毒系统，加强服务器的病毒防护能力并及时升级恶意代码软件版本以及恶意代码库。同时在安全管理平台中部署防病毒管理服务器，负责制定和主机防病毒策略和统一病毒库升级更新。

软件容错

软件容错的主要目的是提供足够的冗余信息和算法程序，使系统在实际运行时能够及时发现程序设计错误，采取补救措施，以提高软件可靠性，保证整个计算机系统的正常运行。因此在应用系统软件设计时要充分考虑软件容错设计，包括：

提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；

具备自保护功能，在故障发生时，应用系统应能够自动保存当前所有状态，确保系统能够进行恢复。

数据完整性与保密性

（1）数据完整性设计包括数据传输的完整性校验以及数据存储的完整性校验。

对于数据传输的完整性校验应由应用系统传输加密系统完成；

对于数据存储的完整性应由数据备份与恢复系统完成。

（2）数据保密性设计设计包括数据传输的完整性校验以及数据存储的完整性校验。

对于数据传输的保密性主要由应用系统完成，在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证，并对通信过程中的敏感信息字段进行加密。

对于数据存储保密性由应用软件加密系统完成。

备份与恢复

备份与恢复主要包含两方面内容，首先是指数据备份与恢复，另外一方面是关键网络设备、线路以及服务器等硬件设备的冗余。

资源控制

为保证安全接入区域应用系统正常的为用户提供服务，必须进行资源控制，否则会出现资源耗尽、服务质量下降甚至服务中断等后果。通过对应用系统进行开发或配置来达到控制的目标，包括：

会话自动结束：当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够及时检测并自动结束会话，释放资源；

会话限制：对应用系统的最大并发会话连接数进行限制，对一个时间段内可能的并发会话连接数进行限制，同时对单个帐户的多重并发会话进行限制，设定相关阈值，保证系统可用性。

登陆条件限制：通过设定终端接入方式、网络地址范围等条件限制终端登录。

超时锁定：根据安全策略设置登录终端的操作超时锁定。

用户可用资源阈值：限制单个用户对系统资源的最大或最小使用限度，保障正常合理的资源占用。

对重要服务器的资源进行监视，包括 CPU、硬盘、内存等。

对系统的服务水平降低到预先规定的最小值进行检测和报警。

提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

应用系统如具备上述功能则需要开启使用，若不具备则需进行相应的功能开发，且使用效果要达到以上要求。

客体安全重用

为实现客体的安全重用，及时清除剩余信息存储空间，应通过对操作系统及应用系统进行安全加固配置，使得操作系统和应用系统具备及时清除剩余信息的功能，从而保证用户的鉴别信息、文件、目录、记录等敏感信息所在的存储空间（内存、硬盘）被及时释放或再分配给其他用户前得到完全清除。

抗抵赖

解决系统抗抵赖特性最有效的方法就是采用 CA 认证系统实现。

边界访问控制

通过本项目的边界风险与需求分析，在网络层进行访问控制部署防火墙产品，可以对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。

智慧科创城项目连接互联网与外网，系统边界部署防火墙产品，能极大地提高内部网络的安全性，并通过过滤不安全的服务而降低风险。由于只有经过精心选择的应用协议才能通过防火墙，所以网络环境变得更安全。

边界完整性检查

边界完整性检查核心是要对内部网络中出现的内部用户未通过准许私自联到外部网络的行为进行检查，维护网络边界完整性，通过在交换机上进行 IP 和 MAC 绑定实现非法接入的安全防范。

边界入侵防范

防火墙起到了协议过滤的主要作用，根据安全策略在偏重在网络层判断数据包的合法流动。但面对越来越广泛的基于应用层内容的攻击行为，防火墙并不擅长处理应用层数据。

智慧科创城项目互联网与外网安全边界部署了防火墙，对每个安全域进行严格的访问控制。鉴于以上对防火墙核心作用的分析，需要其他具备检测新型的混合攻击和防护的能力的设备和防火墙配合，共同防御来自应用层到网络层的多种攻击类型，建立一整套的安全防护体系，进行多层次、多手段的检测和防护。WEB 防护系统和入侵防御系统（IPS）就是安全防护体系中重要的一环，它能够及时识别网络中发生的入侵行为并实时报警并且进行有效拦截防护。

将 IPS 串接在防火墙后面，数字科创城服务管理信息平台应用系统的前面，在防火墙进行访

问控制，保证了访问的合法性之后，IPS 动态的进行入侵行为的保护，对访问状态进行检测、对通信协议和应用协议进行检测、对内容进行深度的检测。阻断来自内部的数据攻击以及垃圾数据流的泛滥。

边界安全审计

安全接入区域边界部署了相应的安全设备负责进行区域边界的安全。对于流经安全接入边界的数据需要设置必要的审计机制，进行数据监视并记录各类操作，通过审计分析能够发现跨区域的安全威胁，实时地综合分析出网络中发生的安全事件。一般可采取开启边界安全设备的审计功能模块，根据审计策略进行数据的日志记录与审计。同时审计信息要通过安全管理平台进行统一集中管理，为安全管理中心提供必要的边界安全审计数据，利于管理中心进行全局管控。

网络安全隔离

系统出口除了接入电子外网，还需要与公安、卫生和计划生育、社会事业、市场监督管理等部门网络进行连接完成数据交互，因此，出口必须进行安全隔离。在市信息网络管理中心的业务系统出口部署安全隔离与信息交换系统，保障数据的隔离交换和信息安全。

安全隔离与信息交换系统，采用多主机隔离的体系结构和专用安全芯片设计的安全隔离与信息交换系统可以满足该要求，其内外网模块连接相应网络实现数据的收发及预处理等操作，数据迁移模块采用专用的硬件设计，在固化的硬件逻辑控制下，通过专有信道，采用私有协议实现与内外网模块进行数据交换，保证任意时刻内外网之间没有物理层和链路层以上的连接。一个网络上的数据只能以专用数据块方式静态地通过本设备进行“摆渡”，传送到与该网络物理隔离的另一个网络中。同时，集成了多种安全技术手段，采用强制安全策略，可扩展支持病毒查杀模块，对数据内容进行安全检测，保障数据安全、可靠地交换。

网络链路安全

网络结构安全

网络结构的安全是网络安全的前提和基础，对于数字科创城服务管理信息平台项目系统核心网络设备需要进行冗余部署，避免单点故障，并考虑业务处理能力的高峰数据流量，因此需要冗余空间满足业务高峰期需要；网络各个部分的带宽要保证接入网络和核心网络满足业务高峰期需要。

按照业务系统服务的重要次序定义带宽分配的优先级，在网络拥堵时优先保障重要业务服务器，合理规划路由，业务服务器之间建立安全路径绘制与当前运行情况相符的网络拓扑结构图；根据所涉及信息的重要程度等因素，划分不同的网段或 VLAN。

重要业务系统及数据的重要网段不能直接与外部系统连接，需要和其他网段隔离，单独划分安全区域。

网络安全审计

网络安全审计系统主要用于监视并记录网络中的各类操作，侦察系统中存在的现有和潜在的威胁，实时地综合分析出网络中发生的安全事件，包括各种外部事件和内部事件，通过《运维管理体要求》章节中的网络监控功能及启用网络设备日志审计，并纳入安全管理平台统一监控管理实现。

网络设备防护

为提高网络设备的自身安全性，保障各种网络应用的正常运行，对网络设备需要进行一系列的安全加固措施，包括：

对登录网络设备的用户进行身份鉴别，用户名必须唯一；

对网络设备的管理员登录地址进行限制；

身份鉴别信息具有不易被冒用的特点，口令设置需 3 种以上字符、长度不少于 8 位，并定期更换；

具有登录失败处理功能，失败后采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

启用 SSH 等管理方式，加密管理数据，防止被网络窃听。

同时需要部署内控运维管理系统对设备管理用户登录认证和审计，确保经过授权的管理员通过可靠路径才能登录设备进行管理操作，并对所有操作过程进行审计、控制、记录，避免授权用户非法操作或误操作，保证对网络设备进行管理维护的合法性。

通信完整性

信息的完整性设计包括信息传输的完整性校验以及信息存储的完整性校验。

对于信息传输和存储的完整性校验可以采用的技术包括校验码技术、消息鉴别码、密码校验函数、散列函数、数字签名等。

对于信息传输的完整性校验应由传输加密系统完成，对于信息存储的完整性校验应由应用系统和数据库系统完成。

通信保密性

应用层的通信保密性主要由应用系统完成。在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；并对通信过程中的敏感信息字段进行加密。

对于信息传输的通信保密性由应用系统和数据库系统传输加密系统完成。

网络可信接入

为保证网络边界的完整性，不仅需要进行非法外联行为，同时对非法接入进行监控与阻断，形成网络可信接入，共同维护边界完整性。可以将服务器的 IP 和 MAC 地址绑定，并禁止修改自身的 IP 和 MAC 地址。

资源池设计

网络资源池设计

数据中心的网络设计采用二层扁平化架构，并采用分区建设方式,根据模块化的分区的方式，主要分为核心交换区、汇聚接入交换区、安全访问控制区及资源服务区。降低了网络设计的复杂度，同时提高网络可靠性和安全性。

核心交换区设计

数据中心未来会部署大量的业务，将有大量的数据转发，所以对核心层设备的性能要求很高，在核心层设备部署两台计算数据中心核心交换机，采用网络虚拟化技术提高设备可靠性和性能。核心设备层设备支持网络虚拟化能力，包括：一虚多、多虚一、纵向虚拟化，支持 FCOE 等。负责整个计算平台上应用业务数据的高速交换。核心交换机间及与服务器接入交换机、管理区接入交换机、核心路由器间均采用万兆接口捆绑互联。

汇聚接入交换区设计

汇聚接入层网络通过多台数据中心接入层交换机使用虚拟堆叠技术构建，并通过跨设备链路聚合提供更高的数据传输带宽，具备更强的扩展性，以满足目前大数据处理传输及分布式处理节点间数据同步的带宽需求。同时，其毫秒级的故障收敛时间，为网络稳定运行提供高可靠保证。

安全访问控制区设计

此区域是逻辑区域，用于部署与互联网公有、广域网接入区进行数据交互的安全隔离设备，确保数据访问安全，包括设置网络隔离、防 DDOS 攻击设备、防火墙、IPS、端口安全检测等。保证物理网络安全性的同时，通过虚拟化技术，实现在虚拟化环境下数据访问的安全控制，此区域实现的功能：

1、DDOS 流量清洗：对进入数据中心的数据流量进行实时监控，及时发现包括 DOS 攻击在内的异常流量。在不影响正常业务的前提下，清洗掉异常流量。有效满足用户对数据中心运作连续性的要求。同时通过时间通告、分析报表等服务内容提升用户网络流量的可见性和安全状况的清晰性。

2、访问控制：利用防火墙实现数据中心的整体安全防护；同时为每个申请安全服务的租户提供独立的 VFW 服务，实现租户业务的隔离需求。

3、入侵防御：为数据中心内部提供了更坚固的安全保护机制。通过 IPS 的深度检测功能可以有效保护内部服务器避免受到病毒、蠕虫、程序漏洞等来自应用层的安全威胁。

计算资源池设计

服务器系统是整个数据中心的心脏，负责管理数据中心的基础信息、共享信息、各专业区域信息以及业务应用过程中发生的相关业务数据、以及数据管理的过程中产生的比对信息、整理信息、管理信息等，同时为各个分系统提供共享信息。

服务器资源池

服务器虚拟化计算资源池，服务器设备的选型主要看业务的应用类型，比如单一业务运行，占用资源比较大的时候，可以采用高端四路、八路服务器为该单一业务进行服务，保证业务的正常运行。对于资源占据不大的业务，则可以选用高端双路服务器进行资源整合，将其划入同一资源池为业务进行服务。

高端和低端服务器在性能上存在较大差异，如果划入统一资源池，会导致上面的应用体验到不同的性能指标。因此，应该采用统一档次，统一类型的 x86 服务器。单台物理服务器的计算能力最大化，以便于进行资源池资源动态分配，有别于传统的部门级和企业级服务器，建议选择性能更加强劲的 x86 四路服务器以上平台。目前主流四路多核服务器服务器，具备 40 个以上的计算核心和 80 个以上的逻辑核心，是传统单核服务器计算能力的 40 倍以上。

数据库是用来保存计算的最终结果的，所以核心数据库是整个信息系统的最重要组成部分。对于所有的数据库而言，除了记录正确的处理结果之外，它们都面临着四方面的挑战：如何提高处理速度，数据可用性、数据安全性和数据集可扩性。核心数据库采用数据库服务器 RAC 集群技术，能够最大限度提供数据库应用的处理速度，提供数据的可用性和安全性，并且提高数据库应用的可扩展性，便于以后业务扩展的平滑升级。

对于核心数据库集群的硬件平台支撑必须采用性能强劲，可靠性稳定性高的服务器设备。基于 X86 架构的四路、八路高端服务器作为核心数据库的应用载体，具有极高的性价比，能够提供强大的安全可靠的并行计算处理能力。

可以根据需求，在数据中心划分单独的智慧应用资源池。

服务器监控

服务器的管理手段：基于硬件的管理工具、网络操作系统的附加管理功能以及第三方的系统管理软件。

服务器管理软件是一套控制服务器工作运行、处理硬件、操作系统及应用软件等不同层级的软件管理及升级和系统的资源管理、性能维护和监控配置的程序。服务器管理软件是构建于工业标准之上，并具备易于使用的设计。通过网络有效拓展现有智慧科创城管理环境，使用丰富的安全性能来访问和管理物理分散的硬件设备。系统管理员可以观察远程系统硬件配置的细节，并监控关键部件如处理器、硬盘驱动器、内存的使用情况和性能表现。通过可选择的附加产品扩展服务器管理、部署和软件分发。所有这些工具与管理软件平滑集成，提供兼容的服务以及单点管理功能，同时发挥管理软件的监控、日程安排、告警、事件管理和群组管理功能。

利用服务器管理软件对服务器节点进行状态实时监控和资源管理，为系统管理员提供了一个统一的、集中的、可视化的和跨平台的管理工具。通过远程故障报警、拓扑管理等，极大的降低用户的管理成本，同时也提高了用户的管理效率，降低系统维护 TCO。

考虑到管理人员的方便运维，管理软件突出以下特点：

B/S 架构：提供 web 界面，通过浏览器远程控制；

跨平台监测：对 windows、Linux 等不同平台的服务器进行严惩监测；

灵活的告警：标准的 SNMP 告警功能，支持服务器的 CPU、内存、硬盘、I/O 性能、服务、进程资源等监测；支持标准的 IPMI 协议，在不依赖操作系统的情况下，对服务器的一年运行状态实时监测，包括 CPU 温度、风扇转速、机箱内部温度、电源状态等；

远程开关机：实现原厂开关机功能，方便管理员对设备进行管理；

弹性架构：管理员可根据被管理、被监控的设备数量和复杂程度，灵活的设置或定制管理软件；

安全可靠

操作便捷：部署快、实施快，操作简单、易用，无需特殊、专业培训；

丰富的报表、拓扑和日志功能：可提供长期内的监控历史情况，可根据记录数据快速生成报表、资产列表等；实现拓扑的分层、显实，了解设备安置及地理位置情况

存储资源池设计

存储资源池

充分考虑目前存储系统现状及未来发展趋势，采用折中的方式，有效的将存储按照实际需求进行分类，采用组合对应的方法，充分照顾性能、容量、安全性、多协议融合、非结构化数据存储使用等方面，方案设计如下：

针对用户的业务状况和发展趋势，建议采用以数据和存储为中心的系统结构，可以极大地保护投资，有效利用存储空间，降低管理费用，从而确保整体拥有成本最低。同时，降低管理难度，维护数据管理的统一性，提高了电子化数据管理的可靠性。数据的集中化管理，能够确保数据的一致性和完整性，保证电子化数据的可靠性。

以数据和存储为中心必然对整个存储系统 I/O 有很高的要求,所以建议选用集中式、高性能、大容量、智能化的光纤存储区域网(Storage Area Network，简称 SAN)来构建新一代数据中心存储环境。

采用以数据和存储为中心的 FC-SAN 解决方案，集中的解决了系统体系结构中对存储 I/O 性能和数据库应用共享的挑战，它的主要特点为：

（1）开放的标准，适合于服务器和存储设备之间的共享

SAN 标准最早就是为了多个服务器之间通过专用的高速网络来共享存储和更加有效地管理存储设备所设计，经过近十年的发展，已经成为非常完善的标准。各主流厂商均遵循开放的观念，保证各家设备之间的互连性。在物理连接上是采用已经成熟的光纤技术实现。由于规模比较大、各项应用和各种设备都比较多，使用户能迅速、方便地建立、整合和管理其多平台的存储环境，对其异构存储局域网拥有无限的扩展能力、管理能力和百分之一百的可用性。

（2）高性能的数据存取

SAN 采用的链路连接是通过光纤，光纤本身具有抗干扰能力强，传输距离长，传输速度快的特点，目前具有的速度是 8Gb/s。而且最关键的是，基于 SAN 架构，服务器和存储设备之间的协议是专为数据密集型存取所设计。

（3）具有高度的可扩充性

基于 SAN 架构的存储设备，本身具有可扩充性。而且一旦 SAN 架构构建以后，可以很容易增加存储设备，并且这些存储设备均可以作为一个整体来共享，它们可以作为一个卷或多个卷来共享。在 SAN 的架构下，存储是独立于应用的。

（4）具有无与伦比的可靠性

作为关键性应用中，设备的可靠性是必须考虑的。在 SAN 架构中，主机和光纤交换机，和存储设备之间的连接均是冗余的，冗余的通路带来的好处，在正常情况下，是带宽的扩充，实现自动负载均衡，如果某一通路出现问题，它又可以作为另一选择路径，保证系统的可用性。

为了保证虚拟化平台的高性能、高可用及动态资源平衡、可持续性、可扩展性等特性，建议服务器通过以光纤链路连接到存储阵列，阵列采用冗余的双控制器，以保障业务的连续性和稳定性。首先，存储资源池计算节点服务器通过两块 HBA 卡全冗余 8Gb 光纤交换机连接全光纤存储产品，实现从服务器到存储设备路径完全冗余，数据链路的高品质性能保障；其次，在保证物理链路连通的同时通过存储链路冗余软件来保证逻辑的冗余性；第三，依托虚拟化架构的优势，虚拟架构系统生产出来的虚拟机的封装文件都存放在 FC-SAN 存储阵列上。通过共享的 FC-SAN 存储架构，可以最大化的发挥虚拟架构的优势，在基于 FC-SAN 存储的 guestos（用户应用）可通过计算平台架构实现双机热备（HA）、容错（FT）、进行动态的资源管理和在线地迁移正在运行的虚拟机等功能，保证业务的可连续性和可扩展性。集中的基于虚拟机快照技术的 Lan-Free 的整合备份等，而且为容灾备份提供扩展性和打下基础。

（5）通过镜像和复制实现数据的冗余部署

通过 FC 存储特有的卷镜像复制软件，实现两台存储之间的镜像复制，保障数据的安全。生产环境中采用两台 FC 存储相互之间形成镜像关系，两台 FC 存储同时提供生产支持提供，分担整体压力负载，同时互为备份，一台存储故障，上面运行的数据会通过脚本切换到另一台存储，继续提供服务，保障业务连续性，提升服务效率。

（6）基于 SAN 的备份恢复、灾难恢复等多种解决方案

目前具有多种基于 SAN 架构的解决方案，比较典型的是包括远程容灾解决方案和零停机时间备份。它可以通过异地远程的两台阵列实现数据的同步，独立于操作系统和应用，一旦某地的系统出现问题，可以很快地切换到异地，保证系统的应用。数据的备份和恢复也是一个数据密集型访问的应用，如果基于 LAN，要占用企业内部大量的带宽，前台响应将极为缓慢，因此，在 SAN

的架构下，可以实现 LAN-free 的备份解决方案，Severless 的备份解决方案和零停机时间的备份解决方案。

（7）集中式管理

分布式的设备，包括主机系统、存储系统、交换机和光纤适配器等等，均可以可采用 B/S 架构软件平台，通过一个简单的管理平台从单点管理。

存储虚拟化是一种将存储系统的内部功能从应用、主机或者网络资源中抽象、隐藏或者隔离的技术，其目的是进行与应用和网络无关的存储或数据管理。虚拟化技术为底层资源的访问提供了简单、统一的接口，使用户不必关心底层系统的复杂实现。

对存储虚拟化而言，不同层次的虚拟化实现具有不同的目标：

存储设备层存储设备层的存储资源是最底层的物理设备，通过数据块存储地址的虚拟化，实现对存储内容的快速寻址。

块聚合层将存储设备层的物理存储设备虚拟化，通过合理的组织，将其构建为能被统一访问的物理资源池。

文件/记录层进一步对物理资源进行抽象，将其虚拟化为逻辑资源，并为上层应用使用。

存储池主要包含两个方面。

结构化数据部分：面向平台资源区提供核心数据服务，采用冗余方式进行配置，并同时提供 FC、iSCSI 等主机接口支持。通过 SAN 交换的模式进行连接。根据业务的实际数据存储需求，配置 SAS 盘达到大容量数据存储的要求，实际的磁盘容量配置可以根据整个信息系统的实际需要进行系统规划配置。

非结构化数据部分：此处考虑到其实际使用特性，可以采用分布式存储技术，利用大数据存储服务器进行存储整合，提供海量存储资源为大数据业务提供支撑。

存储管理与监控

传统的存储系统维护，需要一部实体电脑透过以太网或串口连接，下载系统的配置文件、日志等，才能进行后续的诊断和除错。

而高端存储系统本身都自带管理程序，可提供直观的图形用户界面。高端的存储设备，提供的管理程序都具备强大的管理功能，可实现有效的存储系统管理功能，并且支持多种数据应用功能。

这些管理程序一般具有以下特点：

（1）采用直观的图形管理窗口，可对磁盘存储系统实现全面、灵活的配置与管理；

（2）支持多种高级管理功能，包括：

具备在线式存储扩展功能，可以多种方式，对驱动器、逻辑卷等作数量与容量扩展，可根据需要，有效获得容量与性能提升。

具备在线式动态 RAID 级别迁移功能，可安全地改变卷组 RAID 级别。

具备卷分段动态调整，可以根据应用需要，改变特定卷的分段大小。

具备动态碎片整理功能，可对卷的存储做有效整理，合并卷内空闲容量，获得最优化的空间使用效能和存储效能。

具备非中断式的控制器固件升级功能。

直观的诊断和恢复程序提供了很重要的故障诊断帮助，它能对存储系统出现的问题进行诊断并确定出恰当的恢复步骤。

管理平台设计

管理平台架构

数据中心管理平台作为平台管理员、用户同底层物理设备（服务器、存储、网络设备）通信的中间层，是整个数据中心平台的核心。管理平台主要分为三大部分功能，包括底层虚拟化功能层、资源和综合管理层、平台门户管理界面层。

底层虚拟化层是管理平台的基础，主要功能是将物理资源（服务器、存储、网络设备等）虚拟化成虚拟资源池，可支持目前大部分主流的虚拟化组件，包括 VMvare、Xen、KVM 等；资源和综合管理功能层是管理平台的核心，主要功能包括虚拟资源池的管理、资源计量计费、资源自动按需配置、资源监控、访问控制、业务全生命周期管理、应用服务器的管理、自助服务、虚拟网络隔离以及提供可扩展的 API 接口等；平台门户管理层是数据中心对外服务的门户，提供平台管理员及平台用户的访问入口。

管理平台功能设计

数据中心管理平台运行于数据中心虚拟化架构上，提供资源监控、管理与调度、资源使用流程审计等功能。协助数据中心管理员完成数据中心运维管理工作的同时，满足用户对资源的在线申请和使用要求。监控管理功能可以对硬件资源（服务器，存储和网络）进行实时监控和管理，对于系统异常情况可以实现实时告警。虚拟化功能可以实现虚拟资源的抽象化管理，以资源池的形式进行管理和资源分配，并对根据资源使用情况对资源进行动态调度。系统整体情况和资源使用情况可以通过个性化报表进行展现。通过本产品的资源自助式服务门户可以实现资源的按需获取，业务管理员根据自己的资源需要申请相应的资源，系统实现按量计费。

平台门户

数据中心管理平台为用户和运维人员提供管理平台门户功能，用户和运维人员可通过门户使用计算平台的相关功能。

数据中心管理平台门户是管理平台提供给管理员和用户访问数据平台相关运营管理功能的人机操作界面和功能访问入口。在逻辑上，管理平台门户可以按照服务对象分为服务门户和管理门户，但在实际开发建设中，可使用统一的门户向管理人员和用户提供访问入口，通过角色定义

和权限控制来区分管理人员和用户。

服务门户

服务门户是为用户提供的自服务界面。

服务门户主要功能主要包括但不限于如下内容：

资源目录查询

用户资源实例管理（申请、查询、变更、终止等）

用户管理

用户资源监控管理

用户统计报表查询

管理门户

管理门户是为平台的管理人员和操作人员提供的操作界面和功能访问入口。

管理门户主要功能包括但不限于如下内容：

资源目录管理

资源管理

资源实例管理（创建、审核、查询、变更、终止等）

监控管理

用户管理

统计分析

资源管理

资源目录是数据中心管理平台向外发布的可用资源类别的列表。资源目录管理实现对管理平台中各种资源类别的增加、修改和删除等功能，并为运维人员提供资源设计、资源目录维护、资源目录状态管理、资源发布审批流程等功能。

资源目录管理主要包括但不限于如下内容：

设计并增加新的资源目录条目

对资源目录条目名称、描述等相关信息进行修改

删除资源目录条目

资源目录的内部审批流程管理

查询资源目录中的资源列表

基于资源目录，数据中心管理平台可对各种资源进行管理，主要的功能是管理各种资源的生命周期及资源配置逻辑。运维人员可以通过运营管理平台完成资源的创建，发布，激活，挂起以及删除等操作，并对这些过程完成相关审批的管理。

资源管理主要包括但不限于如下内容：

向资源目录条目中新增资源

设置资源的状态（创建，发布，挂起和下线）

修改资源的名称、描述等信息

查询资源的状态信息，资源状态包括资源分配状态（如待分配、已分配等）和资源运行状态（如启用、停用等）

将资源从资源目录中删除

提供资源分配、更改以及回收等操作的历史记录和查询功能

数据中心管理平台提供对各类资源的多维度统计功能，并以适当的方式输出统计报表。资源统计分析报表包括但不限于：

数据资源物理主机数量及占用状况

计算资源虚拟机运行数量

物理主机

CPU 速率及其利用率均值及峰值

内存容量及其利用率（去除 Cache 和 Buffer 占用）均值及峰值

磁盘容量及其利用率

磁盘 IO 吞吐量及利用率

网络流量统计。

虚拟机

CPU 速率及其利用率均值及峰值；

内存容量及其利用率（去除 Cache 和 Buffer 占用）均值及峰值；

磁盘容量及其利用率；

磁盘 IO 吞吐量及利用率；

网络流量统计。

基于 SAN 存储资源总容量及占用状况，已分配卷的总数，IO 吞吐量，各类磁盘的数量；

基于 NAS 的文件存储资源数量，各类磁盘数量，总存储容量及占用状况，IO 吞吐量；

支持对资源池管理平台输出的统计数据进行收集、存储（文件系统存储或数据库存储）、合并；

支持定制过滤器，支持接收/拒绝特定类型的统计数据；

报表应可以按照 HTML、XML、EXECL 等格式进行导出；

至少保存三个月的原始数据和一年的统计数据；

能够对五分钟以前的流量数据进行统计分析；

监控类报表必须能够灵活的定制，针对需要监控指标设立监控条件，统计时延必须控制在合

理范围之内，应该支持定制周期报表，定期自动采集生成所需报表；

访问控制

数据中心管理平台提供用户注册、用户权限更改、用户密码更改、用户删除等用户管理功能。注册用户在登录之后仅可在权限许可范围内进行系统操作或数据访问。

用户管理包括但不限于如下内容：

用户管理（包括用户注册、用户信息修改、用户状态修改、用户删除等）；

用户组管理（包括用户组的增、删、改）；

角色管理（包括角色的增、删、改）；

权限管理；

用户审计；

数据中心管理平台可以与现有的独立用户管理系统（如 LDAP、ActiveDirectory）集成，共同完成用户管理功能（此要求可选）。

资源池管理平台支持为用户提供不同强度的资源隔离功能，保障用户资源不被非法访问。为用户提供的资源隔离等级包括虚拟隔离、物理隔离和虚拟网络隔离等。用户在申请资源时可选择资源隔离等级。

资源自助门户是组织申请虚拟数据中心(vdc)、组织网络，组织用户申请 vApp 的入口。管理员或组织内用户通过在线提交资源表单申请，审批后即可在线获取到计算、存储、网络资源。通过虚拟机的控制台或者 RDP 可连接至虚拟机来部署、维护业务系统。

数据中心管理平台基于模块化的系统架构，针对不同用户，灵活组合各种功能模块以提供不同的功能。可选的或基于定制的用户 Portal，为不同的用户提供了丰富的系统访问体验。

数据中心服务门户与底层虚拟化平台协同工作，可以将基础架构作为服务提供给终端用户来使用，即 IaaS，包括了对 IaaS 使用流程的管理，资源生命周期的管理以及所提供的服务内容的管理。

IaaS 服务采用自服务的方式，服务的生命周期如下图：

IaaS 服务生命周期主要分成以下几个阶段：

1、服务模板定义，主要指准备环境，将各种合适的资源纳入到数据资源池，以虚拟 CPU、虚拟内存、虚拟磁盘空间、虚拟网络为颗粒度，准备标准的计算能力；

2、创建服务目录，主要指将数据资源标准化，按照服务的方式进行提供；

3、服务订阅，主要是指服务消费者申请数据能力和服务，或者更改某个已有的服务申请；

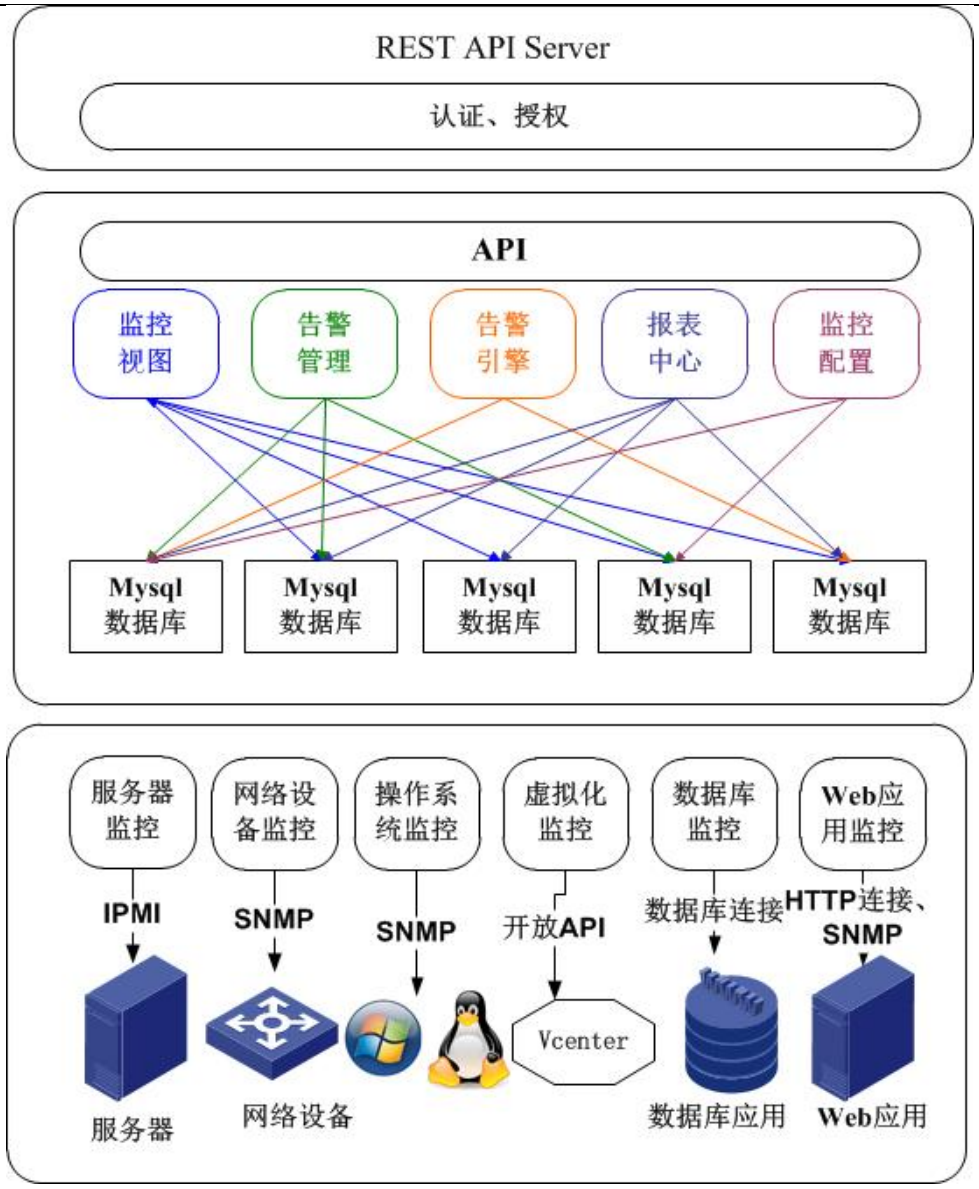
4、服务运行，服务运行期间需要保证服务质量；

5、服务终止，回资源以重新利用。

资源监控

资源池管理平台对平台中的各类设备及资源进行监控，提供对各类设备和资源的故障监控、性能监控、自动巡检等功能。系统提供最小粒度为 5 秒的关键性能实时监控，从而实时了解关键性能变化情况。

数据中心是众多的物理设备通过各种资源池化技术构成的数据资源池，为了满足各种各样业务应用对资源的需求，资源池应该可以提供物理数据资源和虚拟数据资源等不同形式的资源。而且 Hypervisor 本身也是一种物理数据资源，因此在实现对虚拟数据资源的管理基础上，还应该实现对物理数据资源的有效管理。



平台的监控子系统的核心功能是对服务器、网络设备、操作系统、数据库等各种资源进行监控，并根据监控信息进行灵活的告警通知。也可以根据用户需要按资源的类型、可用性和健康状况的统计和分析，提供各资源的趋势分析报告等。

监控功能通过插件扩展、性能优化等实现，最终可以将资源分解为各种类型的监测器，通过精确的监测各监测器全面监控各资源的状态、使用情况和详细数据信息。

监控子系统需要对以下几种资源进行监控：

监控服务器硬件的健康状况，包括 CPU、内存、风扇、电源、主板等的温度、电压、转速、功耗传感器信息；

监控路由器和交换机等网络设备，如设备端口流量、端口速率、系统资源等；

监控操作系统，包括 Windows 和 Linux 两种操作系统，监控其 CPU 负载、内存利用率、磁盘利用率、网络接口流量、系统进程、系统服务、TCP 端口情况和 ICMP 状态检测情况等；

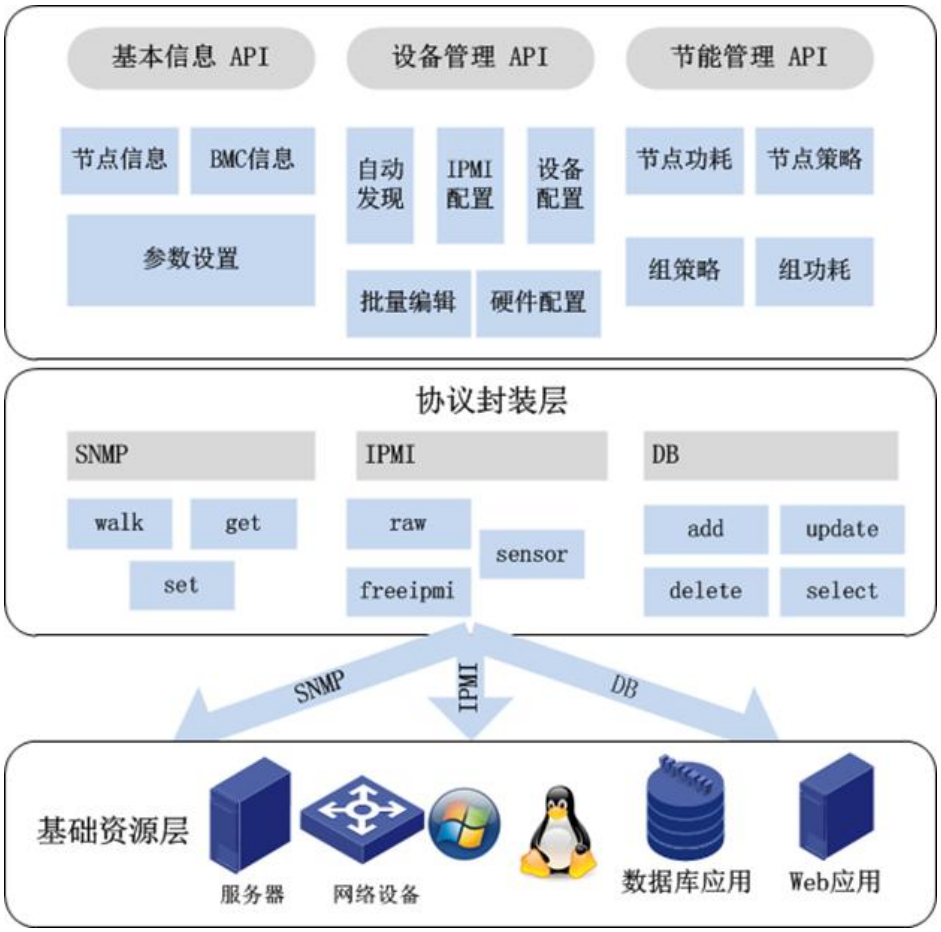
监控数据库应用，监控其表空间利用率、最大连接数等；

监控 Web 服务应用，包括 Apache、IIS 和 Tomcat 三种类型的 Web 应用，监控其并发连接数

量、资源使用情况等；

监控虚拟化资源，监控其 CPU 使用情况、内存使用情况、IO 读写状况、存储使用情况、vmfs、service 等

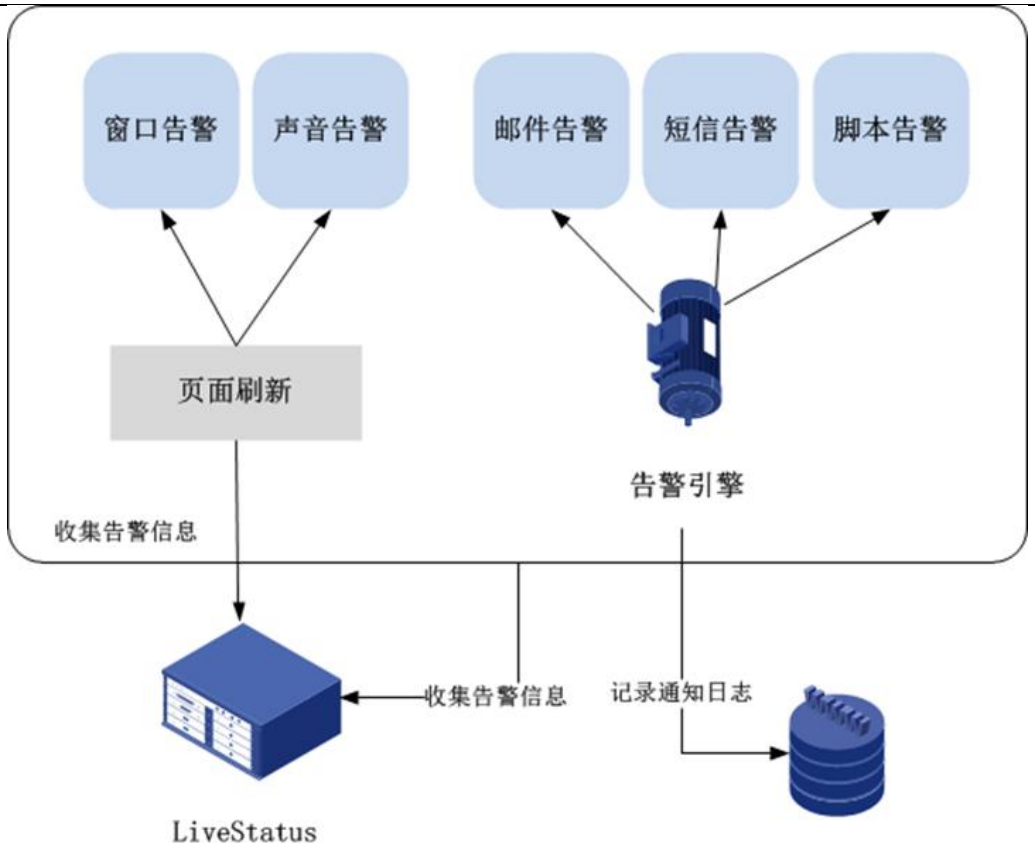
平台的管理子系统提供对设备资源池以及用户手动添加的物理设备的综合管理功能，在此基础上通过 SNMP 和 IPMI 协议实现强大的系统管理能力。本子系统包括基本信息、节能管理、电源管理、设备管理、拓扑图、日志六个模块，其中，节能管理、电源管理和拓扑图是三个最主要的功能，节能管理采用 NodeManager 技术实现对数据中心服务器的功耗控制，达到增大机架密度降低能耗的目地，电源管理实现对服务器的开关机、重启操作，拓扑图模块提供展现物理设备的拓扑状态。



异常告警管理

告警机制在底层物理资源出现问题时，系统自动通知相关人员，方便系统管理人员及时了解设备运行状态，维护问题设备。

系统监控可以实现通过资源的状态信息获取,实时、有效的资源信息更新以及资源的故障检测等技术实现物理资源，服务资源和虚拟机资源等状态信息的动态采集和获取，并按照合理的时间粒度更新,向用户或管理员提供实时的信息，以支持资源的有效控制与管理。



监控代理负责采集底层资源的各种信息，通过定时数据采集、数据请求以及配置模块完成对底层数据的监控，同时通过可扩展的资源信息模型提供对底层物理资源的描述，支持对信息模型描述文件动态扩展与更新。

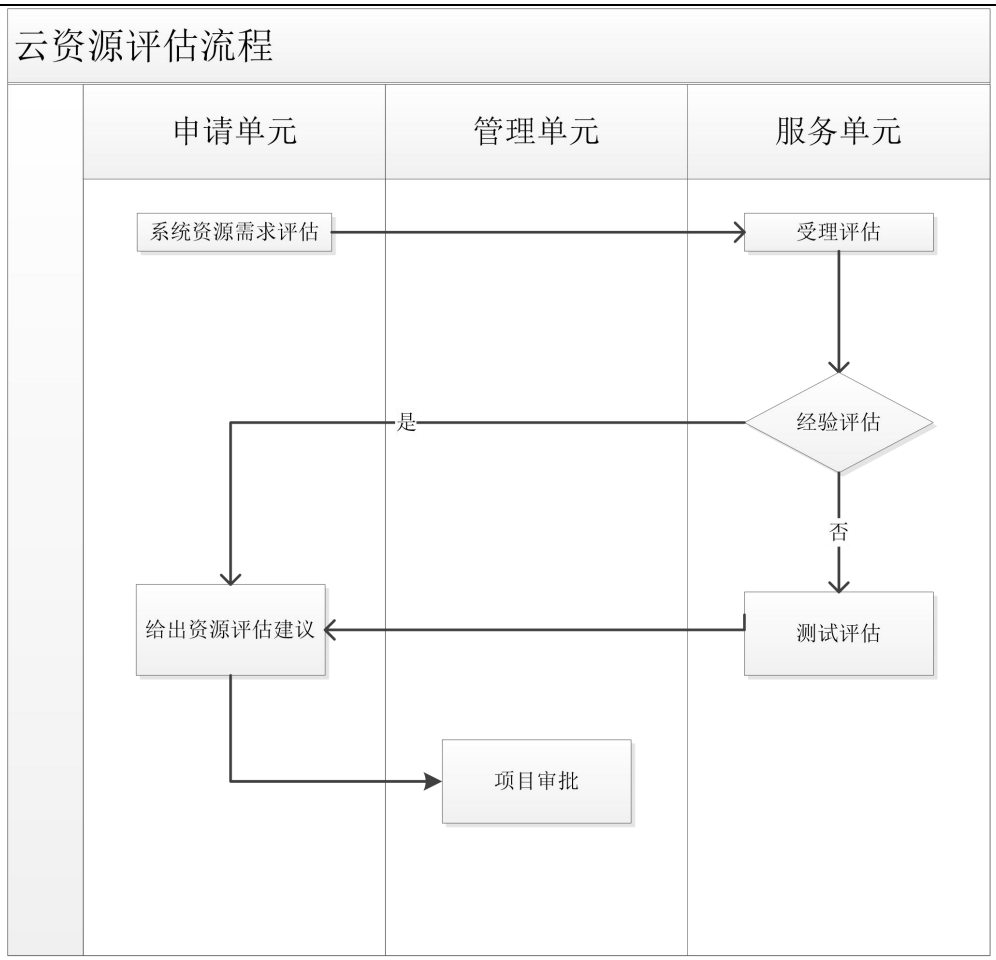
监控代理提供资源注册访问接口，实现对不同类型资源监控能力的动态部署、加载、运行以及更新支持。

支持多种方式（例如 Web 界面，邮件或者短消息）对用户、运维人员和运营人员进行资源状态、系统负载、故障和租赁费用等系统消息进行通知。

资源使用流程设计

资源的评估流程

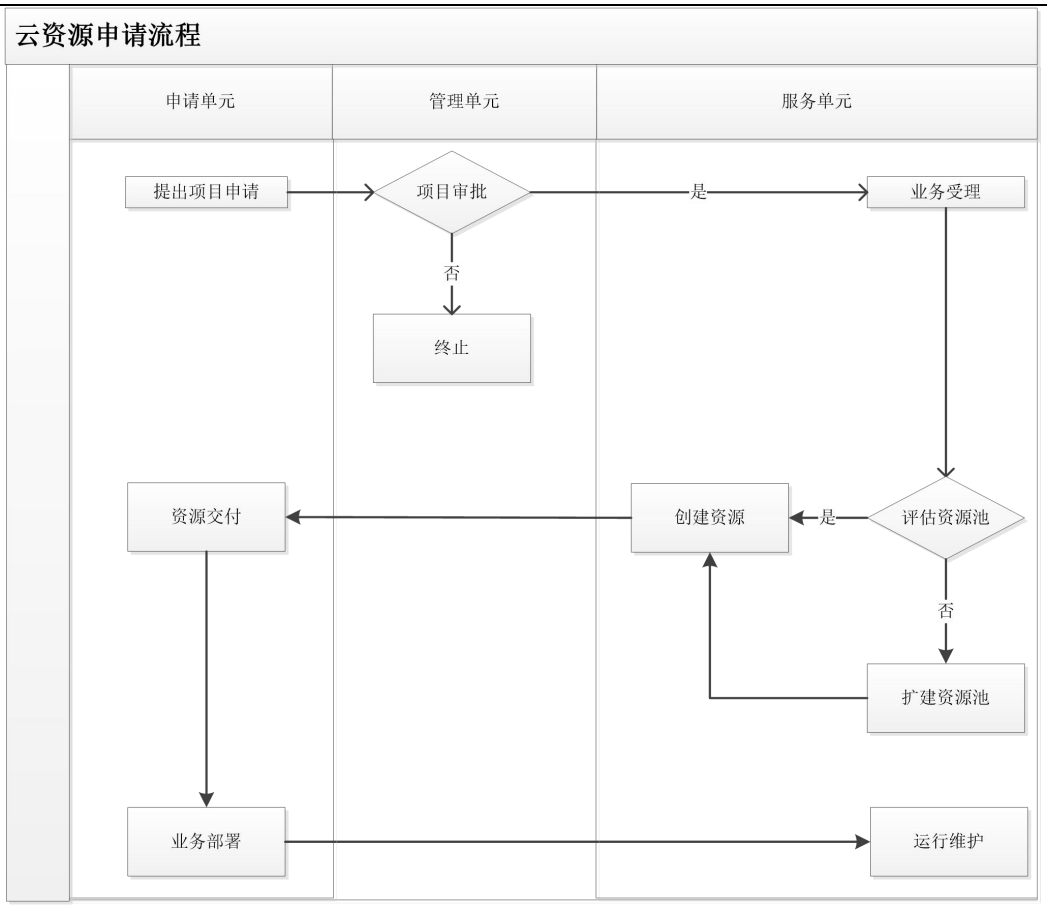
本流程场景适用于科创城相关业务单位，向数据中心提出项目的申请，由数据中心对整体申请的基础资源进行综合评估，保障项目资源与业务软件的高耦合，保护投资的同时保障业务的稳定运行。



资源评估流程：首先由申请单元发起流程，提出系统资源需求评估，由服务单元受理本次项目资源评估事项，启动评估，能够通过历史经验值对项目资源进行判断的，反馈给申请单元资源评估建议，如果历史经验无法做出合理评估判断，启动测试评估，随后给出资源评估建议到申请单元，申请单元根据此意见向管理单元提出项目审批。

资源的申请流程

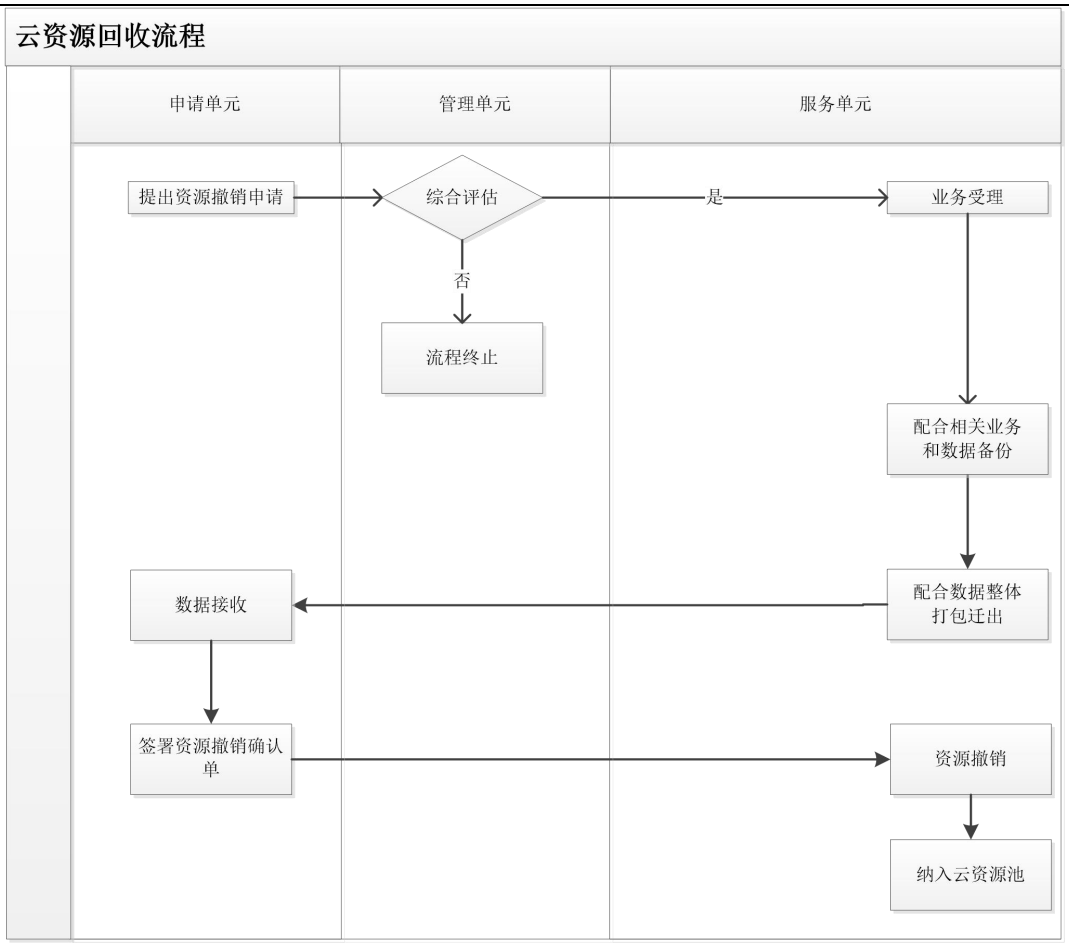
本流程场景适用于科创城城市相关业务单位对资源的申请，资源管理单元对现有资源和业务资源的评估，分配相应资源，为业务系统提供服务。



资源申请流程：由申请单元发起项目流程，向管理单元提出项目审批申请，如不能通过，则流程终止；如通过了评审，由服务单元，受理本次项目需求，启动资源池的评估，如果资源池能够满足业务系统上线需求，创建资源；如资源不足，扩建资源池，在为用户创建资源池。由服务单元将资源交付给申请单元，申请单元部署系统，完成项目上线；服务单元负责基础设施的运行维护。

资源的回收流程

本流程场景适用于科创城相关业务单位对资源的撤销申请，资源管理单元对撤销申请进行综合评估，服务单元配合进行相关业务和数据备份，将数据打包迁出并释放资源。



资源回收流程：申请单元提出资源撤销申请，管理单元进行综合评估申请是否执行，针对同意的撤销申请，由服务单元进行已运行业务数据的整体备份和打包，数据交付给申请单元并签署确认单，资源撤销释放，纳入资源池。

安全系统设计

数据中心安全风险分析

从“数据”的概念提出以来，关于其数据安全性的质疑就一直不曾平息，这里的安全性主要包括两个方面：一是自己的信息不会被泄露，避免造成不必要的损失，二是在需要时能够保证准确无误地获取这些信息。总结起来，用户在选择数据服务时主要关注的安全风险有以下几方面：

资源聚合技术的应用使得数据、存储、网络资源高度集中：用户数据存储、处理、网络传输等都与数据中心密切相关，如果发生故障造成的后果较传统数据中心更为严重。

虚拟化等技术的应用使得传统物理安全边界缺失：传统网络安全设施与防御机制在防护能力、响应速度等方面越来越难以满足日益复杂的安全防护要求，用户信息安全、用户信息隔离问题在共享物理资源环境下的保护需求更为迫切。

数据传输安全：通常情况下，数据中心保存有大量的私密数据，这些数据往往代表了核心竞争力，如财务信息、关键业务流程等等。在数据模式下，将数据通过网络传递到数据中心进行处理时，面临着几个方面的问题：一是如何确保数据在网络传输过程中严格加密不被窃取;二是如何保证数据中心在得到数据时不将绝密数据泄露出去;三是在数据中心处存储时。如何保证访问

用户经过严格的权限认证并且是合法的数据访问，并保证数据中心在任何时候都可以安全访问到自身的数据；

数据存储安全：数据中心的数据存储是非常重要的环节，其中包括数据的存储位置、数据的相互隔离、数据的灾难恢复等。在数据模式下，数据中心在高度整合的大容量存储空间上，开辟出一部分存储空间提供给数据中心使用。但用户并不清楚自己的数据被放置在哪台服务器上，甚至根本不了解这台服务器放置在哪个国家;数据中心在存储资源所在国是否会存在信息安全等问题，能否确保数据中心数据不被泄露;同时，在这种数据存储资源共享的环境下，即使采用了加密方式，数据中心是否能够保证数据之间的有限隔离;另外，即使数据中心用户了解数据存放的服务器的准确位置，同时对所托管数据进行备份，以防止出现重大事故时，用户的数据无法得到恢复；

数据审计安全：数据中心进行内部数据管理时，为了保证数据的准确性往往会引入第三方的认证机构进行审计或是认证。但是在数据环境下，数据中心如何存确保不对其他数据中心的数据数据带来风险的同时，又提供必要的信息支持.以便协助第三方机构对数据的产生进行安全性和准确性的审计，实现数据中心的合规性要求;另外，数据中心对数据中心的可持续性发展进行认证的过程中，如何确保数据中心既能提供有效的数据。

为了更好地消除这些潜在的安全风险，让更多用户享受到数据服务的优点，在选择数据服务时，一方面要根据自身的业务需要，关键业务模型可以选择建立数据模型进行保障;另一方面需要和城市建立规范的条款来规避风险，保证数据存储的安全性以及和其他灾备中心之间的加密隔离。

数据中心安全体系

安全设计标准

智慧科创城数据中心的安全设计遵循国家信息安全等级保护相关要求，针对数据中心平台部分：办公区为等保一级，业务区为等保二级；针对数据中心专网平台部分：办公区为等保二级，业务区、数据区为等保三级。

国家信息安全等级保护坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序和公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

安全设计原则

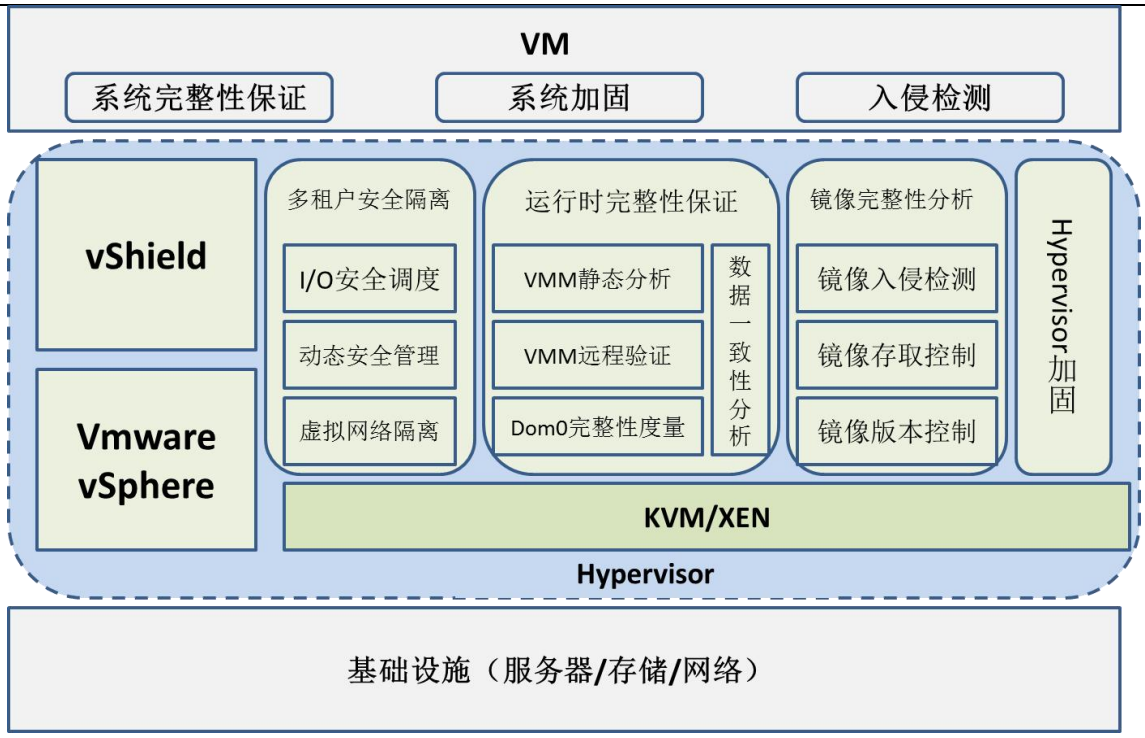
本次数据中心安全整体解决方案，应根据防范安全攻击的安全需求、需要达到的安全目标、对应安全机制所需的安全服务等因素，参照 SSE-CMM(″系统安全工程能力成熟模型″)和 ISO17799(信息安全管理标准)等国际标准，综合考虑可实施性、可管理性、可扩展性、综合完备性、系统均衡性等方面，还要包括影响系统安全的方面有物理安全、网络隔离技术、加密与认证、应用层面安全、网络反病毒、网络入侵检测和最小化原则等多种因素，它们是设计信息安全方案所必须考虑的，是制定信息安全方案的策略和技术实现的基础。数据中心安全设计将着重从以下原则是进行考虑：

原则：进不来、拿不走、打不开、抹不掉

安全技术体系

主机/服务器虚拟化安全

虚拟化安全涉及的层面比较多，包括虚拟机监控器（Hypervisor）、虚拟机、虚拟机监控器与虚拟机之间的通信、虚拟机之间的通信、虚拟机动态迁移、虚拟机镜像管理、虚拟机镜像完整性、虚拟机安全隔离等。数据环境中，虚拟化安全必须从系统的角度出发，建立完整的虚拟化安全体系才能有效解决虚拟化安全问题。因此，虚拟化安全首先建立如图所示的虚拟化安全方案框架如下，主要包括虚拟层 Hypervisor 的安全加固控制、虚拟化可信启动、强身份认证和虚拟机加固等模块。



虚拟化管理器安全控制通过各虚拟化接口库和虚拟机自省机制实现：

虚拟机：监控局域网环境中的虚拟机，获取虚拟机基本信息（虚拟机名称，虚拟化类型，所在主机，虚拟机配置信息，UUID）和动态信息（虚拟机 ID，CPU 占用，内存用量，运行时间，运行状态）；

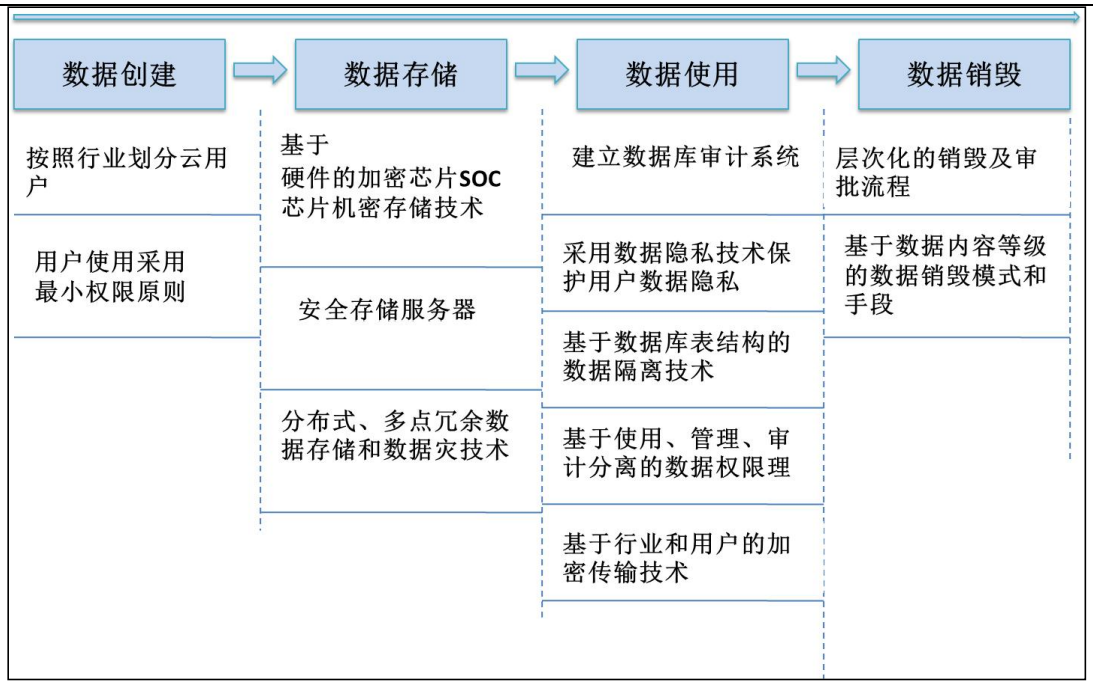
虚拟网络：监控局域网环境中的虚拟网络，获取虚拟网络基本信息（网络名称，IP 地址范围）和动态信息（输入输出流量等）；

存储监控：监控局域网环境中的存储，获取存储的基本信息（名称，总量）和动态信息（使用率）；

对虚拟机的生命周期进行管理，包括创建、启动、迁移、关机、终止等操作，并获取相关的虚拟机动态信息。

数据与信息保护

面对数据的数据安全问题，基于数据生命周期的管理策略，从数据的创建、存储、使用和销毁四个层面逐层解决环境下数据安全的问题，运用层面间内部互联，整体独立的安全思想保证数据安全，具体从如下方面提出了环境中数据安全保护措施：



（1）芯片级存储加密技术

数据存储上采用的是 SOC 芯片加密技术，是一款集成在主板上基于 I/O 的、实时性的加密手段，SOC 芯片加密技术因为集成在主板上，所以对数据机的性能损耗非常低。该方案支持国产加密算法，同时也可支持 256 位 AES 加密算法，具有高度的兼容性，支持最新的 ONFI 和 Toggle 协议。

SOC 芯片加密对用户是透明的，保证用户在数据处理过程中业务的连续性。SOC 芯片支持 TLCFlash 等，具有高度可定制化以满足更多的应用需求，保证数据存储的安全性。

（2）基于行业和用户的加密传输技术

为解决数据在网络信道上的传输安全，安全中心运用基于行业和用户的身份认证和加密传输技术保证数据传输安全，结合行业特点和安全需求主要的技术实现有如下方式：

用户身份认证：基于用户信息及应用内容的防火墙认证机制；基于 CA 芯片的 U 盾身份认证技术。

数据加密传输：基于行业特色和用户安全需求采用不同的安全防护措施，数据在网络上安全传输主要采用的技术手段是 VPN 和加密机，VPN 安全产品主要依据 IPSEc-VPN、SSL-VPN 两种技术，加密机采用的是自主研发的加密机，整体上保证数据传输安全。

（3）数据访问控制机制

建立了数据库管理员、数据库审计员和安全管理员，实行三权独立原则。严格的身份审查，赋予最小的管理权限；针对数据库管理人员结合需求进行分配权限。特殊权限采用密钥分开保管的原则。

建立了账号集中管理平台系统，集中管理用户、设备、系统账号；集中管理用户、系统账号的密码；集中配置账号密码策略、访问控制策略；集中管理所有用户操作记录；实现账号实现实

名制管理，定点登录。

（4）运用灵活的数据隔离技术

在面对不同的数据隔离技术，保证数据安全。主要的数据隔离技术有：

共享表架构技术：即所有的软件系统用户共享使用相同的数据库实例和相同的数据库表，共享表架构最大化地利用了单个数据库实例的存储能力，所以这种架构的硬件成本非常低廉，但对程序开发者来说，却增加了额外的复杂度。由于多个用户的数据共存于相同的数据库表内，因此需要额外的业务逻辑来隔离各个用户的数据。此外，这种架构实现灾难备份的成本也非常高，不但需要专门编写代码实现数据备份，而且在恢复数据时，需要对数据库表进行大量的删除和插入操作，一旦数据库表包含大量其他用户的数据，势必对系统性能和其他用户的体验带来巨大影响。

分离数据库架构技术：即每个软件系统用户单独拥有自己的数据库实例，相比于共享表架构，由于每个用户拥有单独的数据库实例，这种架构可以非常高效便捷地实现数据安全性和灾难备份，但是随之而来的缺点便是其硬件成本非常高昂。

分离表架构技术：软件系统用户共享相同的数据实例，但是每个用户单独拥有自己的由一系列数据库表组成的 Schema，分离表架构是一种折中的方案，在这种架构下，实现数据分离和灾难备份相对共享表架构更加容易一些，另一方面，它的硬件成本也较分离数据库架构低。

（5）数据访问安全审计

为保证在发生事故时，对系统和管理员行为进行追溯和事件回放，能够准确的定位发起某项行为的人员、时间、结果等信息，保证证据采集、证据保全、证据安全存储以及基于证据的审计的完整性和保密性。数据中心部署了世界领先安全审计产品，本产品具有如下功能优势：

可以对数据库操作进行审计支持诸如查询（Select）、插入（Insert）、删除（Delete）、创建（Create）等 SQL 命令以及存储过程的执行进行审计和分析；

可以对数据库的访问控制进行审计，审计对象分为基于操作者身份和数据库表操作的审计；

面向操作和应用的智能化分析，通过对 SQL 命令的截获、分析和还原，直观地显示出关键操作的结果，并可对多个操作进行并发跟踪和分析。

（6）数据隐私增强技术

在解决数绝隐私安全方面主要选择构建私有或者混合来实现弹性数据和数据隐私的均衡两种模式，

中数据隐私保护涉及数据生命周期的每一个阶段，将集中信息流控制(DIFC)和差分隐私保护技术融入中的数据生成与数据阶段，依据隐私保护系统 Airavat，防止 Mapreduce 数据过程中非授权的隐私数据泄露出去，并支持对数据结果的自动除密，在数据存储和使用阶段采用了基于客户端的隐私管理工具，提供以用户为中心的信任模型，帮助用户控制自己的敏感信息在端的存储和使用。

（7）剩余数据保护

数据信息在从产生到消亡的整个过程中，都必须进行数据安全性防护。数据销毁作为数据安全的最后一步，也是最重要的一步，在对数据销毁的过程中常常采用以下几种方式：

磁盘格式化：磁盘格式化分为磁盘普通格式化和磁盘快速格式化，磁盘快速格式化仅仅是清除文件分配表，使系统认为数据已经清除掉了，而实际上相应的数据还存在相应的扇区上。仍然可以通过软件的方式来恢复数据。磁盘普通格式化会将磁盘上的所有磁道扫描一遍，清除磁盘上的所有内容，相当于对数据进行一次覆盖。普通数据一般采用磁盘格式化方式。

数据清除软件：数据清除软件采用随机乱码的方式对文件所在的扇区、簇进行重复覆盖，敏感信息或秘密信息一般采用软件进行数据销毁。

消磁机：消磁机通过强磁场，来改变磁性存储介质的矫顽力，通过改变小磁体的方向来达到完全销毁的目的。经过消磁机消磁后的存储介质无法使用，机密以上的数据采用这种方式进行数据清除。

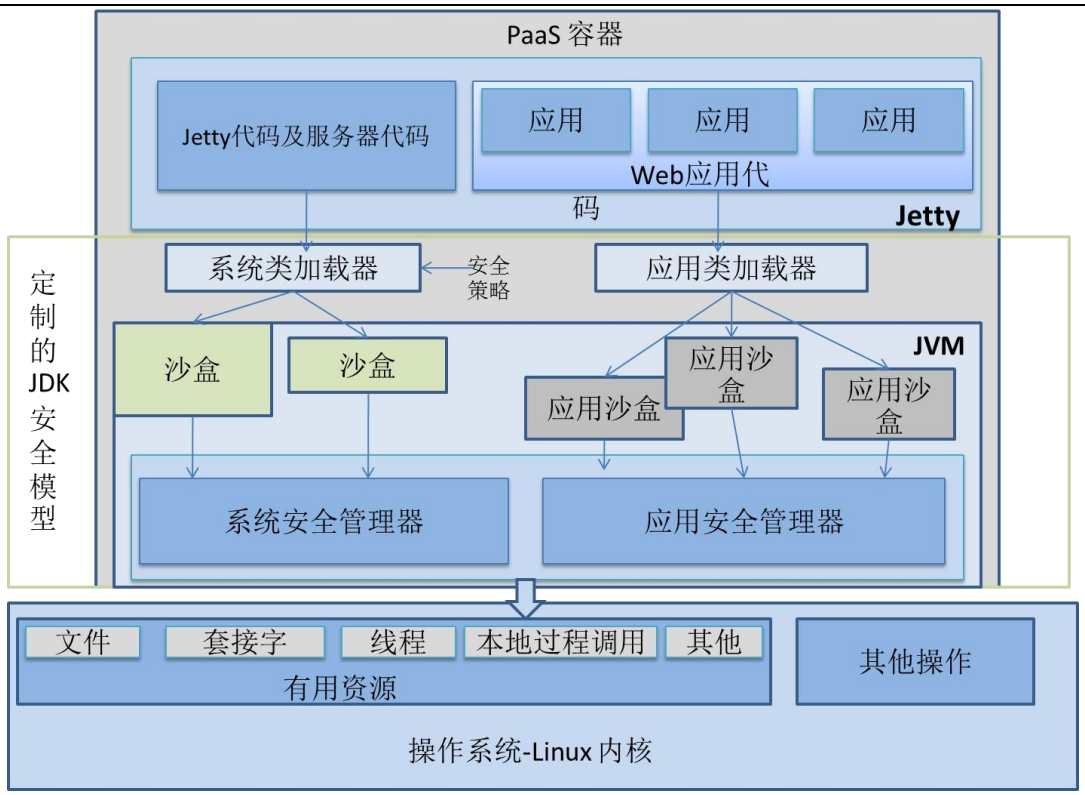
物理粉碎：使用硬盘物理粉碎机将硬盘盘片捣碎来达到销毁的目的，经过销毁后的硬盘彻底无法使用，绝密以上的数据采用物理粉碎的方式进行数据的销毁。

应用安全

多租户应用隔离

在 PaaS 层，提供基于基础设施（即 IaaS）上的软件、中间件和应用开发工具。不同的 PaaS 提供不同组合的服务，综合的 PaaS 是一个集开发、测试、部署、托管和应用维护为一体的集成运维环境，有的 PaaS 还提供源代码和版本控制等应用软件开发的过程管理。

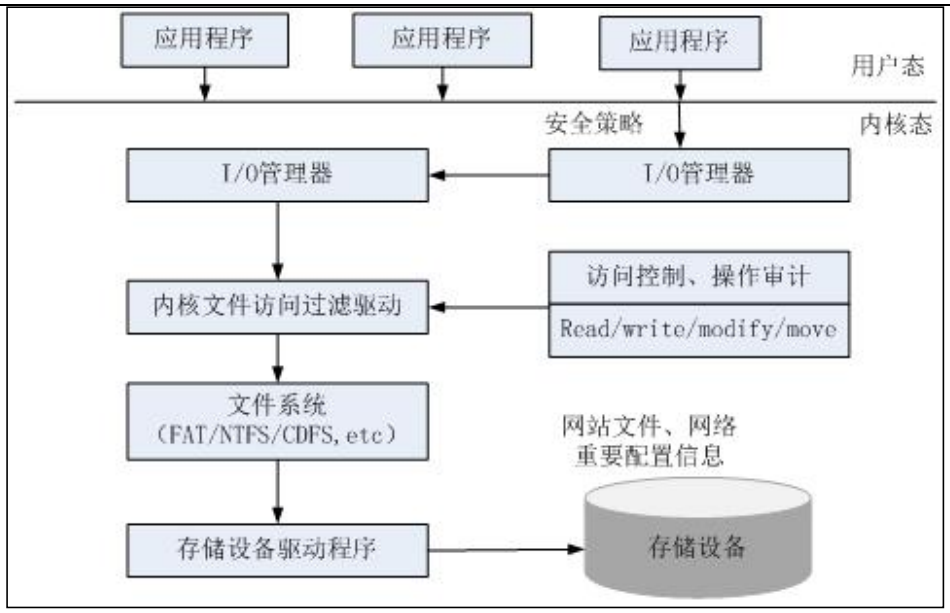
在多用户 PaaS 的服务模式中，最核心的安全原则就是多用户应用隔离。数据中心用户应确保自己的数据只能有自己的用户和应用程序访问。提供商维护 PaaS 平台运行引擎的安全，在多用户模式下必须提供“沙盒”架构，平台运行引擎的“沙盒”特性可以集中维护用户部署在 PaaS 平台上应用的保密性和完整性。服务提供商负责监控新的程序缺陷和漏洞，以避免这些缺陷和漏洞被用来攻击 PaaS 平台和打破“沙盒”架构。



针对 PaaS 平台的多用户特点，在 Java 沙盒模型的基础上进行扩展，提出如图所示的 PaaS 平台安全沙盒。在 PaaS 平台运行环境中，安全容器提供应用运行的受限的环境，即沙盒环境。沙盒环境实现应用运行时 5 个方面的访问控制：文件访问控制；网络访问控制；多线程控制；JNI 访问控制；System.exit()方法访问控制。如图所示，在 PaaS 平台运行环境中，安全容器在 Java 安全体系结构基础上进行扩展，实现了两套逻辑沙盒模型，在逻辑上把系统代码和应用代码分开处理，实现简化安全策略文件的配置，提高系统性能。

应用主动防御

通过核心内嵌技术，将篡改检测模块内嵌在 Web 服务引擎中，对每一个数据流出请求都进行完整性检查。对于数据流出请求中涉及到关键词、敏感词的，流出检测模块会及时的屏蔽，并报警和日志记录。



备份功能：将 Web 服务器中需要保护的网页文件加密备份到服务器，并将文件的基本信息记录到数据库中；

发布功能：通过发布工具，将待更新的文件传至发布服务器的备份目录中，Web 服务器自动同步更新；

检测功能：通过事件触发方式自动检测 Web 服务器，查看网页内容是否有变化；

恢复功能：发现文件有修改，包括图像改变或是文字变化，当检测到为非授权变化后，将删除该页面，并将正常页面解密上传至 Web 服务器；

自动报警功能：对篡改事件进行报警，通过邮件或页面消息通知管理员。

应用攻击防御

对于数据中 Web 应用安全而言，数据安全解决方案体现在如下几点：

Web 应用的安全建设需要贯穿到 Web 应用的生命周期中，进行分阶段的防护；

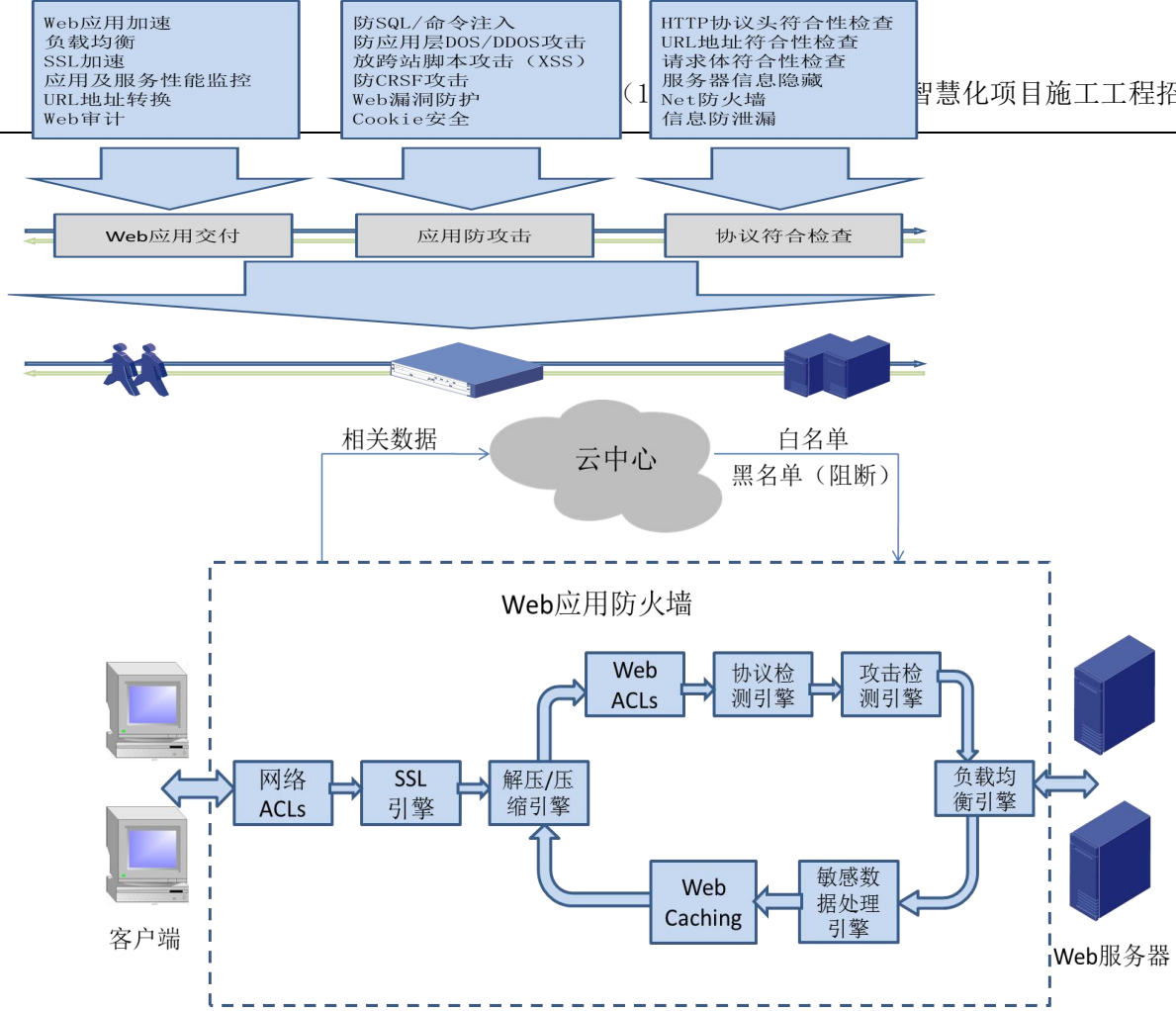
运行阶段，是需要重点进行防护的关键阶段，需要从事前主动防护（防患于未然），事中实时控制（攻防的关键），和事后处理（最后的防线）三个方面提供全面的防护；

部署必要的安全产品是安全防护的主导，需要和 Web 应用业务的特 性相结合；

安全服务是安全产品的必要补充。安全服务可以最大程度上减少运营商时间和管理成本，同时获得全天候监控服务。

加入数据中心安全计划，可实时获取互联网最新恶意攻击信息，第一时间防止潜在的恶意行为，将可疑的 URL 请求提交到数据中心安全中心，由的安全专家定制化安全策略；

通过数据中心，及时获取最新的互联网安全态势和安全预警。



Web 应用安全解决方案的支撑产品是 Web 应用防火墙，此产品是应用安全解决方案的具体实现，是结合多年应用安全的攻防理论和应急响应实践经验积累自主研发完成。Web 应用防火墙这一防御系统能够保护中 Web 服务器免受应用级入侵，它弥补了防火墙、IPS 这类安全设备对 Web 应用攻击防护能力不足的问题。解决方案从用户对功能、性能、易用性诉求点出发，对应用防火墙概括出三个方面，从基于流程的防护模型上来看，Web 应用防火墙具备事前预防、事中防护及事后补偿的综合能力。对最为核心的事中防护能力而言，作为一种专业的 Web 安全防护工具，基于对 HTTP/HTTPS 流量的双向解码和分析，可应对 HTTP/HTTPS 应用中的各类安全威胁，如 SQL 注入、XSS、跨站请求伪造攻击（CSRF）、Cookie 篡改以及应用层 DDoS 等，能有效解决网页篡改、网页挂马、敏感信息泄露等安全问题，充分保障 Web 应用的高可用性和可靠性。对于事中疏漏的攻击，可用事前的预发现和事后的弥补，形成环环相扣的动态安全防护。事前是用扫描方式主动检查网站，而事后的防篡改可以保证即使出现疏漏也让攻击的步伐止于此，不能进一步修改和损坏网站文件，对于要求高信誉和完整性的用户来说，这是尤为重要的环节。

容灾备份系统设计

计算数据中心业务涵盖系统多、类型复杂、关键性程度不一，因此对于恢复目标也有不同的要求，如针对核心关键的业务系统，要求 24 小时持续可用，即 RPO、RTO 以及 NRO 几乎为 0，针对一般性重要业务系统（和关键业务有关联度）平台则有一定的,RPO、RTO 和 NRO 的时间窗口。鉴于以上分析，根据恢复目标将业务的关键等级划分为两部分，分别为核心业务系统、一般业务

系统两个级别，根据不同级别分别有针对性的制定容灾备份方案。

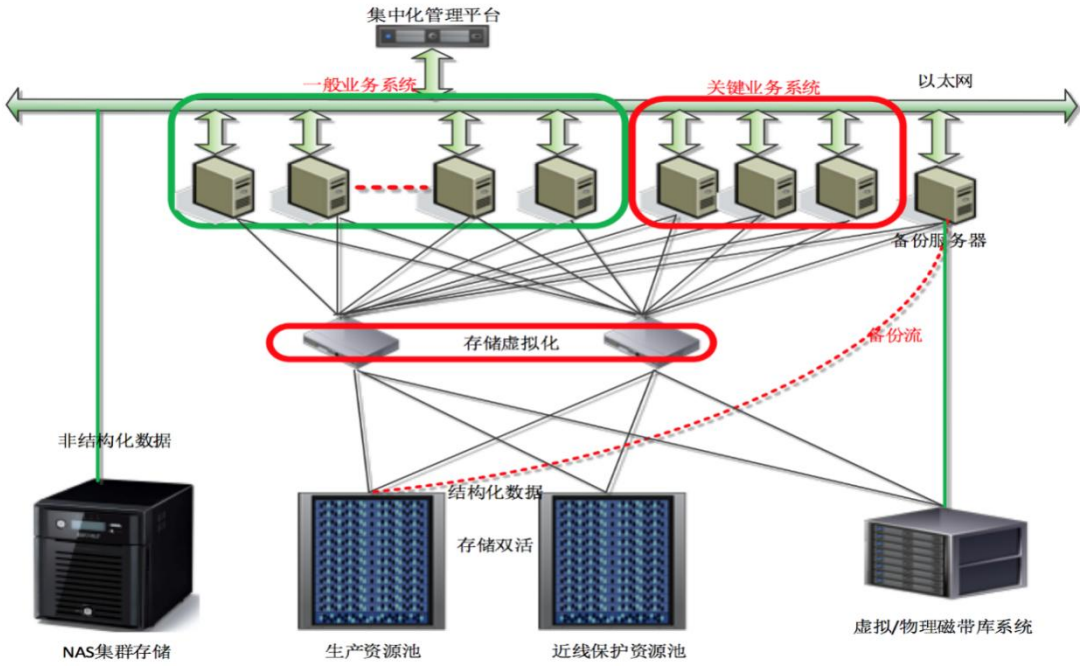
数据中心业务分析

计算数据中心业务涵盖系统多、类型复杂、关键性程度不一，因此对于恢复目标也有不同的要求，如针对核心关键的业务系统，要求 24 小时持续可用，即 RPO、RTO 以及 NRO 几乎为 0，针对一般性重要业务系统（和关键业务有关联度）平台则有一定的,RPO、RTO 和 NRO 的时间窗口。鉴于以上分析，根据恢复目标将业务的关键等级划分为两部分，分别为核心业务系统、一般业务系统两个级别，根据不同级别分别有针对性的制定容灾备份方案。

灾备技术实现

根据以上业务分级和恢复目标要求，针对核心业务系统，采用存储数据双活的方式来实现业务平台的持续可用；针对一般性重要业务平台，采用主流成熟的备份系统进行定时备份保护；针对一般业务系统可根据业务数据的重要度，采用定时备份或者不备份策略。

同时利用现有存储资源采用存储虚拟化平台来进行资源整合和管理，存储虚拟化平台本身的高级复制功能也是实现双活数据中心的重要技术手段，在实现关键业务系统灾备时，也是性价比较高的灾备方式。容灾备份设计拓扑规划如下：



◆ 针对关键业务系统，采用存储双活的方式保障关键业务的连续性，提升关键业务数据的可用性和可靠性，在任意一台 存储出现问题时，存储自动切换应用无感知。

◆ 针对一般系统，采用主流备份软件来实现基于时间策略的定时备份，来保证业务数据的可靠性和可恢复性要求。

平台灾备方案

数据备份及异地灾备

对于异地容灾的数据备份以及恢复，对于不一样的场景需求，用户可以灵活地选择不同级别

的容灾备份的方案。

集群间 HDFS 分布式文件系统的数据备份机制

（1）强一致性方案

对于重要敏感数据，数据从客户端写入 HDFS 中，同时向两个集群写入数据，当两个集群都完成写入后，再开始一下个文件的写入。基于强一致性的容灾方式对于集群的写入性能会受到外部网络的延时的影响，写入性能会显著下降，所以仅对重要敏感数据进行强一致性备份。在数据的备份基础上，保证关键业务在灾备集群上有足够的资源，提供持续的稳定服务。

（2）弱一致性方案

则是单位周期内（每小时、每天），基于 HDFS 的 distcp 机制，将写入的数据以增量备份的方式通过网络实现内容在异地机房的备份。基于弱一致性的容灾方式对于集群的运行效率几乎没有影响，数据备份也能得到保证，但是最后单位周期内写入的数据无法得到备份。

集群间 Hyperbase NewSQL 数据库的备份机制

在 Hyperbase NewSQL 数据库中的数据，利用 Hyperbase 的 Replication 机制，可以做到实时数据备份。数据写入的时候会通过 WAL（Write-Ahead Logging）机制在写入 Hyperbase 之前先写入日志，然后通过解析日志实时同步进入灾备集群 Hyperbase，从而做到实时数据备份。

数据容灾实现方案

在复制启动的时候，从集群会将自己的 ZooKeeper 地址注册给主集群。Master 通过从集群的 ZooKeeper 知道从集群有多少 RegionServer，并从中随机挑出 10%的 RegionServer 用于复制。由于不同的 Master 会挑选不同的 10%的机器，因此可以认为主集群的复制压力会大致均匀的分布到从集群的每台 RegionServer 上。

数据故障处理

数据完整性保障和方案选择

对于存储在 TDH 平台中的数据，通过统一的分布式存储 HDFS，将数据的访问和存储分布在大量服务器之中，在可靠地多备份存储的同时还能将访问分布在集群中的各个服务器之上，默认采用 3 份副本保证数据的可靠性。在发生磁盘故障或者任意节点宕机的情况下，不会导致服务以及业务的中断，并自动进行副本的复制恢复每个数据达到 3 副本的存储。

主集群异常及上层业务切换

上层业务应用前期已配置主从集群的访问信息（IP 地址、端口、访问权限等），当主集群的某个 RegionServer 宕机后，该集群中的其他的 RegionServer 会从 Zookeeper 上感知到这点，并接管该 RegionServer 的复制任务，将剩余的 HLog 数据复制到对应的从集群中。

从集群异常及上层业务切换

上层业务应用前期已配置主从集群的访问信息（IP 地址、端口、访问权限等），当从集群

中正在复制的 RegionServer 宕机后，主集群的 Master 会选择另外一个备选的 RegionServer 进行复制。

密码安全设计

为强化安全管理体系，突出商用密码的安全性，本次密码方案按照国家商用密码管理办公室制定的一系列密码标准，遵循国家密码管理局 2018 年 2 月 8 日发布的 GM/T0054-2018《信息系统密码应用基本要求》密码行业标准和 2019 年 1 月 17 日发布的《电子电子认证服务业务规则规划》(国密局字〔2018〕572 号)相关规定，采用国密算法进行设计，突出商用密码的安全性，按照国家商用密码管理办公室制定的一系列密码标准，采用 SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法（ZUC)等进行安全加固认证。

密码应用需求

在所有业务系统中，均需采用国密 SM 系列算法，包括：

为提高系统中核心数据的安全性，防止相关数据泄露。系统中需要对相关数据进行加密后以密文的形式存入数据库中，对数据传输过程中使用 HTTPS 技术强化保护，对机构之间以及使用人员进行强身份认证，从而加强数据安全性。其密码应用主要包括：

密码算法采用国密标准的国密 SM4 对称密码算法、SM2 国密非对称算法、SM3 国密摘要算法。

敏感数据入库后全程加密，结合“一次一密”策略，对数据库中记录数据进行加密，保障明文信息数据不泄密。

对关键记录内容进行防篡改校验，系统在数据使用过程中或定期进行篡改检查，及时发现被篡改的信息内容，保障信息有效性。

综合安全网关产品作为专业的通信保密应用交付设备，能够为用户的网站应用发布提供包括 3-7 层负载均衡、SSL VPN、IPSec VPN、PKI 就绪、数据优化加速等的全方位解决方案。可以帮助客户构建极高的安全性和稳定性极高的网络，保障客户业务连续性与安全性。综合安全网关全部基于国密算法实现，提升算法安全性。

机构之间构建身份认证系统，保障机构系统身份可识别，信息可以安全传递，主要通过签名服务器设备。用户在使用系统时，身份可识别，可基于 USBKEY、协同签名等形式。

设计原则

1）安全性原则

为保证密钥安全，采用了密钥分层保护和密钥分散保护机制。采用主传输密钥保护各业务应用密钥传输；根据业务密钥的应用将密钥分开保护存放，并对密钥应用的使用次数和使用权限进行限制。密钥的存储介质应为国家密码管理局批准的设备，禁止任何方式导出密钥。一旦密钥的使用次数达到设定的次数，密钥对应文件目录将禁止访问和使用。使用分散因子分散后的过程密钥进行身份认证和数据加解密保护。

按需分配原则

国产密码应用体系设计充分考虑密码资源的按需分配能力，密码资源是一个庞大的资源池，可以通过密码资源模板建立不同性能的密码计算资源，可以按需购买，密码资源可以像平台的计算资源一样按需计费。

可靠性原则

采用国家密码管理局批准的，质量可靠，能在长时间高负荷的使用场景下保持稳定性和高可靠性。

3）易维护原则

加密设备软硬件均提供自检功能，使用过程中能将维护的工作量降到最小。

4）可扩展性原则

在系统根据使用状况需要增加一些功能或者提高系统处理能力时，在满足系统安全需求的条件下，可较容易的通过分布式或其他方式提升系统的性能和多样性。

5）合规性依据

2011 年国家密码管理局下发了《关于做好公钥密码算法升级工作的通知》(国密局字【2011】50 号)

自 2011 年 3 月 1 日起，新研制的含有公钥密码算法的商用密码产品必须支持 SM2 椭圆曲线密码算法。已审批的商用密码产品应抓紧开展升级换代工作。

2011 年 3 月 1 日起，在建和拟建公钥密码基础设施电子认证系统和密钥管理系统应使用 SM2 椭圆曲线密码算法；

自 2011 年 7 月 1 日起，投入运行并使用公钥密码的信息系统，应使用 SM2 椭圆曲线密码算法。已投入运行并使用公钥密码的信息系统，应尽快进行系统升级，并使用 SM2 椭圆曲线密码算法。

《中华人民共和国电子签名法》于 2004 年 8 月 28 日通过，自 2005 年 4 月 1 日起施行，确立电子签名的法律效力，维护有关各方的合法权益而制定的法律。

2016 年 11 月 7 日发布《中华人民共和国网络安全法》是为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定的法律，自 2017 年 6 月 1 日起施行。

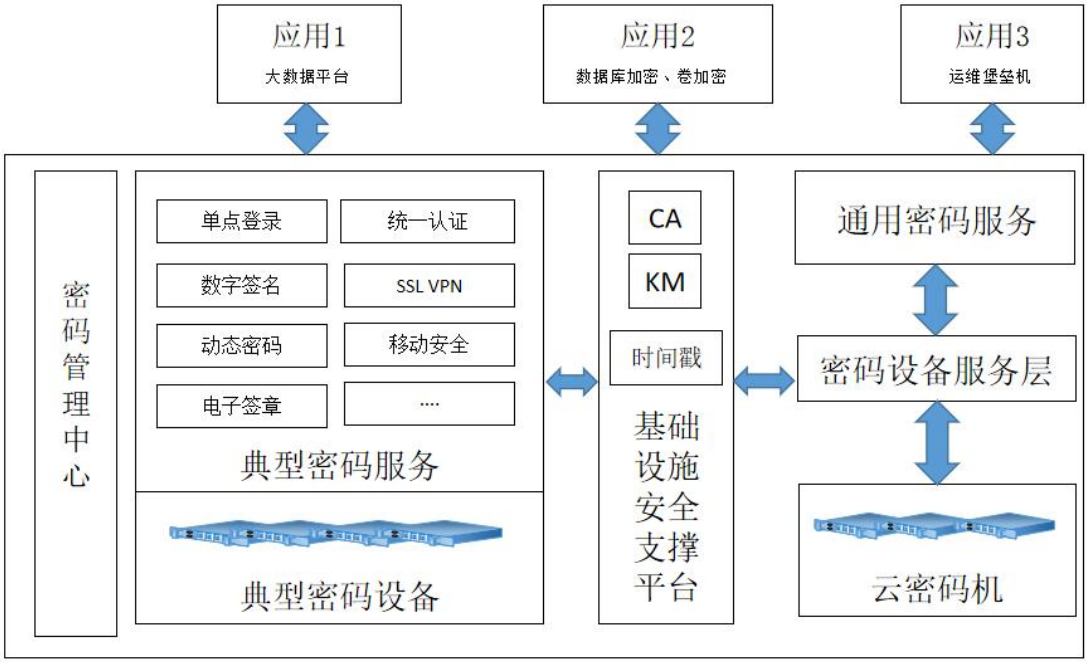
2018 年 2 月 8 日，国家密码管理局发布 GM/T0054-2018《信息系统密码应用基本要求》密码行业标准。针对信息系统等级保护级别的不同给出了不同的密码应用的基本要求。

国家密码管理局 2019 年 1 月 17 日发布的《电子电子认证服务业务规则规划》(国密局字〔2018〕572 号)相关规定，采用国密算法进行设计，突出商用密码的安全性，按照国家商用密码管理办公室制定的一系列密码标准，采用 SM1（SCB2）、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法

（ZUC)等进行安全加固认证。

2019 年 5 月《信息安全技术 网络安全等级保护要求》、《信息安全技术 网络安全等级保护测评要求》等核心标准正式发布。

密码平台总体架构



密码平台总体架构图

国产密码应用项目总体建设思路如图所示，密码服务平台的密码功能包含典型密码服务、通用密码服务、基础设施安全支撑平台、密码管理平台。

1）典型密码服务

密码服务硬件是支持高性能密码计算的专用密码设备，内置有支持虚拟化的密码卡，密码服务硬件上运行有密码管理平台，支持通过虚拟化的方式虚拟出多个典型密码服务。

典型密码服务使用密码卡虚拟化、网络虚拟化和主机虚拟化等技术，将物理密码资源层、密码设备服务层、通用密码服务层以及典型密码服务层从下至上封装为标准的典型密码服务，为平台租户提供安全可靠、部署敏捷的 PaaS 级密码服务。

每个典型密码服务拥有自己独享的密码卡、CPU、内存、网络等计算资源，并且不同的典型密码服务之间的资源是隔离的，在保证密钥安全的前提下同时提供性能保证。

PaaS 级典型密码服务包括单点登录服务、统一身份认证服务、数据签名服务、动态密码服务、电子签章服务、SSL VPN 服务、移动认证服务、SSL 加密服务等。PaaS 虚拟典型密码服务除了支持目前常用的典型密码服务外，可以通过密码服务平台导入密码资源模板方式扩展支持其他的典型密码服务。

2）通用密码服务

通用密码服务通过密码设备服务层调用物理密码服务层的密码机，实现卷加密、数据库加密、

应用系统调用 API 加密等方式下提供密码计算资源来实现数据加解密等服务

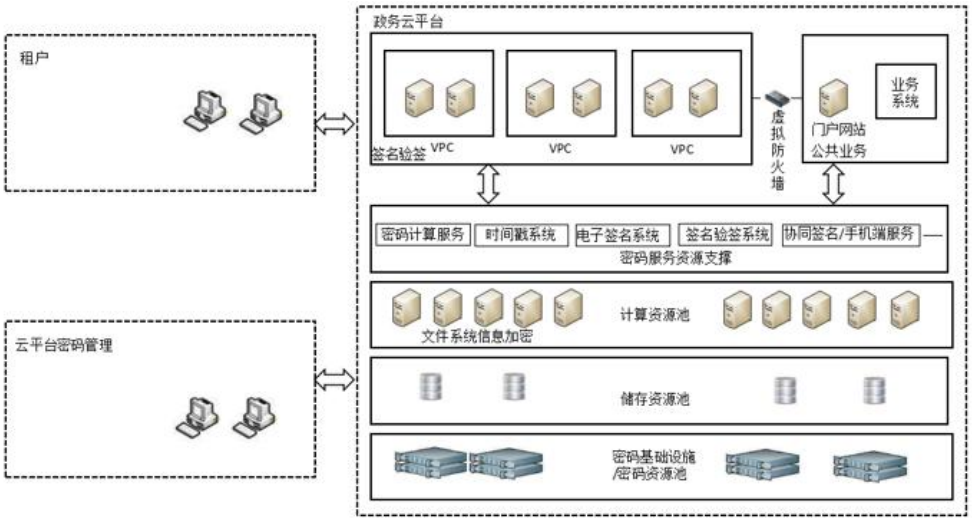
3）基础设施安全支撑平台

基础设施安全支撑平台包含 CA、KM 以及 TSA 等服务，通过密码设备服务层调用物理密码服务层的密码机实现数字证书的密钥管理和运算。

4）密码管理平台

密码管理平台以可视化界面为管理人员提供资源管理、服务管理、权限管理、运营监控等运维管理功能。管理人员可根据实际业务需求与数据流向以拖拽的方式定义密码服务业务拓扑、分配密码服务资源，简化密码应用部署工作。密码安全管理平台运营监控功能可监控密码服务硬件节点运行状况、独立密码应用服务运行状况、业务密码应用行为分析等。

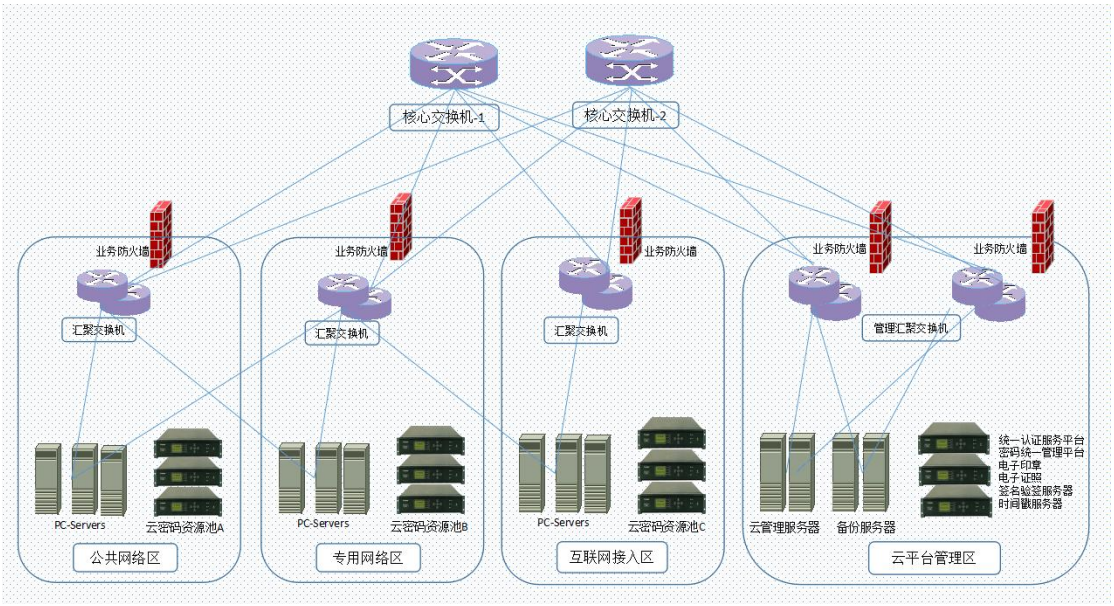
密码平台部署方式架构



密码平台部署架构图

密码平台设计说明

将密码资源池部署在公共网络区、互联网接入区、专用网络区，为其他密码服务以及业务应用系统提供加密服务。



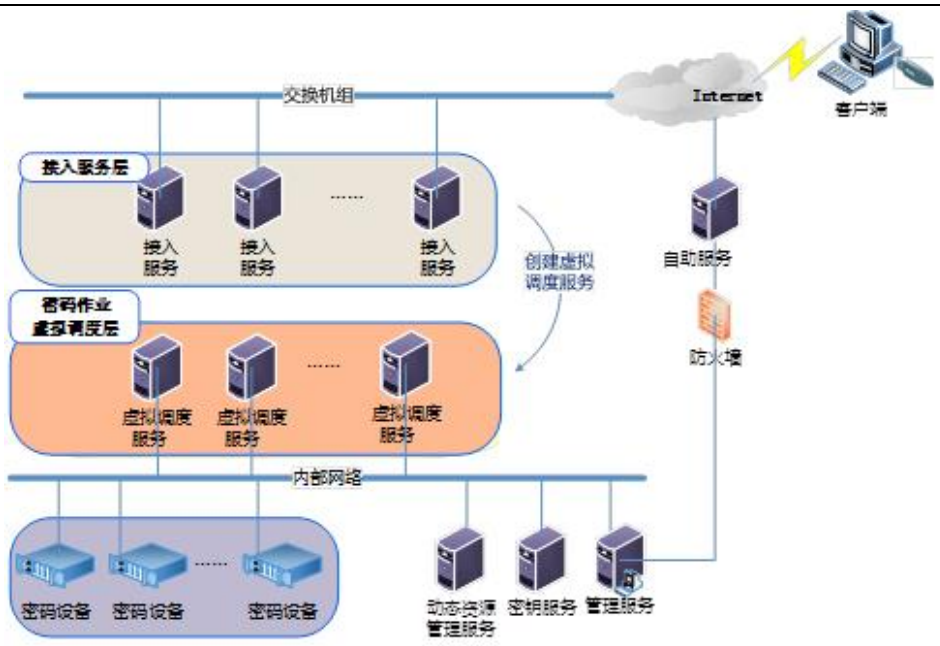
密码平台部署图

在公共网络区、互联网接入区、专用网络区分别部署密码资源池。密码资源池可运行多个虚拟密码机，并且每个虚拟密码机之间完全隔离。对密码服务使用者来说，每个用户可以各自管理各自的设备，独自生成并管理各自的密钥，每一台密码机都可以看作是一台独立的物理密码机。

密码管理平台部署在管理平台区域的虚拟服务器上。密码管理平台可以实现对平台中所有的密码资源的集中统一管理。运维人员通过密码管理平台可以查看所有密码设备的状态、所属密码资源池的虚拟密码机数量、虚拟密码机的运行状态。用户通过密码管理平台可以查看和管理自己租用的虚拟密码机。这种部署模式要求中管理区域的密码资源池和所有区域的密码资源池之间的网络要连通。

密码资源池

密码资源池可为用户数据提供密码运算资源实现数据加解密、签名验签、电子签证、时间戳、CA 等密码服务。密码资源池是主要由应用接口、用户自助平台、接入管理、系统管理、虚拟调度、动态资源管理、密码服务这七部分组成。如图所示：



密码资源池

平台可以部署在私有、信息中心的网络环境中，为私有、信息中心的各种应用系统提供密码服务。

应用系统只需提出需求，无需关心密码设备硬件配置，由虚拟调度系统从其管控的密码服务资源中为应用系统动态灵活的选择出最佳服务配置。系统能够支持上千的应用服务，并可根据用户需求，不断快速扩展服务能力，能对现有的密码设备和新的密码设备进行统一管理，并提供良好的状态、性能、用户等资源监控，实现了整合资源提升管理效率、减少开销提升资源利用率、专业管理加强安全服务能力和统一防护提高安全运维能力。

其主要功能如下：

1） 可以将密码设备进行统一管理，并将集成的密码设备的服务能力（如算法类型、性能和密钥空间）进行整合，形成统一的密码资源池，支持算法资源的实时动态分配，提升密码服务能力；

2） 平台可依据用户的实际需求，以秒级为单位，为每个用户即时量身定制细粒度的密码服务；

3） 平台支持上千用户同时共享有限的密码资源，达到对密码资源使用上的稳定可控和高效利用；

4） 平台可监控密码设备资源（如 CPU、内存、算法类型、性能和密钥空间）、用户虚拟密码服务和密钥使用情况，并进行可视化展示。

5） 平台支持国密 SM1、SM2、SM3、SM4 等国密算法。

客户价值

基于用户应用对网络通道进行加密保护，保证数据在网络传输过程中的机密性和完整性；

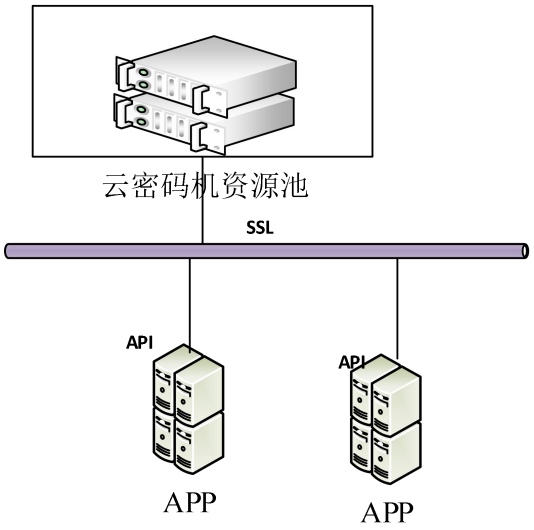
对敏感数据进行加密保护，保证数据在平台内的机密性和完整性；

对客户端、管理员等角色进行身份认证，同时对使用者操作数据进行签名验签，保证数据的抗抵赖性和身份唯一性；

密码资源灵活调配，后期增加密码功能和资源简单方便；

可为平台提供密码增值服务，为租户提供灵活的可租式增值密码服务。

加密服务



加密服务结构

通过密码资源池为用户分配密码资源后，密码资源池可以直接为各租户与平台本身提供相应的密码运算服务。通过配置用户 VPC 与密码资源池 VPC 网络打通，可以确保用户只可以访问到自己所分配的密码资源，实现不同用户的密码服务隔离。

密码子系统

由虚拟加密机、相应密码产品的 API 组成，对用户传输数据或者存储数据提供密钥加密、解密、签名、验签等运算功能。

对外提供接口

初始化接口：通过 API 初始化对接虚拟加密机；

加密接口：加密服务接口；

解密接口：解密服务接口；

签名接口：签名服务接口；

验签接口：验签服务接口；

服务断开接口：服务断开接口。

密码产品和密码服务

使用的密码产品包括虚拟密码机。

密码协议

全面支持国产密码算法，支持 SM2 数字签名算法、SM3 摘要算法、SM4 加解密算法，兼容 RSA1024/2048 算法。

密码应用工作流程

用户在密码管理平台管理界面上操作虚拟密码机创建相应的加解密服务；

用户在密码管理平台管理界面上操作虚拟密码机，在虚拟密码机内为创建的加解密服务产生密钥信息；

应用系统端部署配置加密服务的 API 接口，以便相应的应用系统通过 API 接口调用加解密服务；

应用系统通过部署的 API 接口调用虚拟密码机配置的加解密服务中的密钥进行数据加解密。

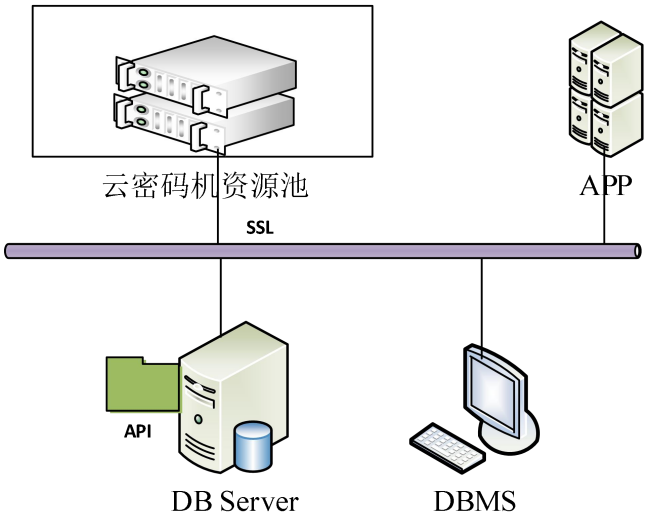
解密服务中的虚拟密码机采用用户的密钥对信息进加密或者解密服务，并将加密结果或者解密结果返回给应用系统；

应用系统得到加密结果或者解密结果，进行下一步的业务流程。

密钥管理

需要在虚拟密码机内生成用户密钥。密钥的生成和管理在用户密码管理平台界面上有最终用户进行操作。

数据加密服务



数据库加密结构

通过数据库加密组件，结合数据库 TDE 技术，在数据库底层完成加解密：通过加密数据库的物理文件实现静态数据安全保护，数据在写入存储之前，实时自动加密，并在存取器读取时进行解密。该方式对应用系统透明，数据库表加密和解密没有任何额外的编码及数据类型或模式修改。

密码子系统

由密码资源池和 API 开发包组成，对数据库提供密钥存储、加解密运算功能。

对外接口

初始化接口：通过 API 初始化对接虚拟加密机；

数据加密接口：数据加密服务接口；

数据解密接口：数据解密服务接口；

服务断开接口：数据加加密服务结束断开

密码产品和密码服务

使用的密码产品包括密码资源池，API 开发包；开发包部署在应用服务器上，为应用系统提供数据加解密服务。

密码协议

全面支持国产密码算法，支持 SM2 数字签名算法、SM3 摘要算法、SM4 加解密算法，兼容 RSA1024/2048 算法。

密码应用工作流程

以实现 mysql 数据库安全加密工作流程为例；

通过调用 API 初始化数据库加密系统；

配置 MySQL 数据库加密系统，部署安装 API 接口；

系统管理界面集成批量模板功能，设置原用户批量加密模板，设置生成新用户批量加密模板，设置其他需求加密模板；

备份数据库原用户数据，导入数据库用户信息，根据模板批量加密数据原用户数据；

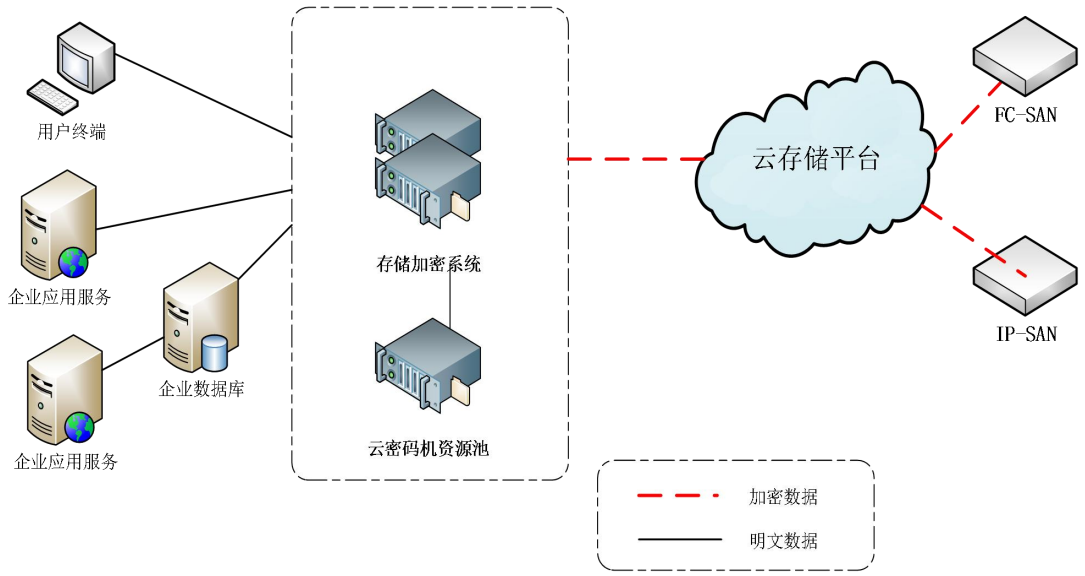
调用加密模板生成新数据库用户。

正常调用数据库相关命令。

密钥管理

主密钥在密码资源池内产生和存储，密钥的产生、销毁等由管理员操作密钥管理系统进行管理。

存储加密服务



存储加密结构

采用密码资源池对端存储盘阵提供磁盘级的加密服务，支持 FC-SAN 和 IP-SAN 两种存储架构。用户终端或应用服务器，通过密码资源池和端存储映射的加密磁盘，进行数据存放。通过该加密磁盘的数据将被自动加密，密文数据保存到端存储盘阵上。存取数据时的加解密过程，对用户和应用透明。

密码子系统

由密码资源池和 API 开发包组成，对存储数据提供密钥存储和加密、解密等运算功能。

对外接口

初始化接口：通过 API 初始化对接虚拟加密机；

存储加密接口：存储加密服务接口；

存储解密接口：存储解密服务接口；

服务断开接口：存储服务断开接口。

密码协议

全面支持国产密码算法，支持 SM2 数字签名算法、SM3 摘要算法、SM4 加解密算法，兼容 RSA1024/2048 算法。

密码应用工作流程

配置映射加密磁盘；

产生加密主密钥；

调用密钥对数据存储加密解密；

正常存储数据。

密钥管理

需要在密码资源池内生成主密钥，存储磁盘加密密钥。密钥的生成和管理在密码资源池的管理界面上进行操作。

签名验签服务

采用密码资源池对平台和其租户提供日志审计的签名验签服务。应用系统中操作数据行为动作将被自动签名，签名后的日志可通过验签行为提供时间、用户、行为和地址等日志报告。

密码子系统

由密码资源池和 API 开发包组成，对操作数据行为动作进行签名和验签过程。

对外接口

初始化接口：设置服务器连接、验证服务的访问权限

数据签名接口：为应用系统提供数据签名接口

签名验证接口：为应用系统提供签名数据的验证接口，并将签名数字证书信息解析返回给应用系统

PDF 签名接口：为应用系统提供 PDF 文件签名接口

PDF 验签接口：为应用系统提供 PDF 文件签名验证接口，并将签名数字证书信息解析返回给应用系统

数字信封接口：为应用系统提供数字信封接口服务。

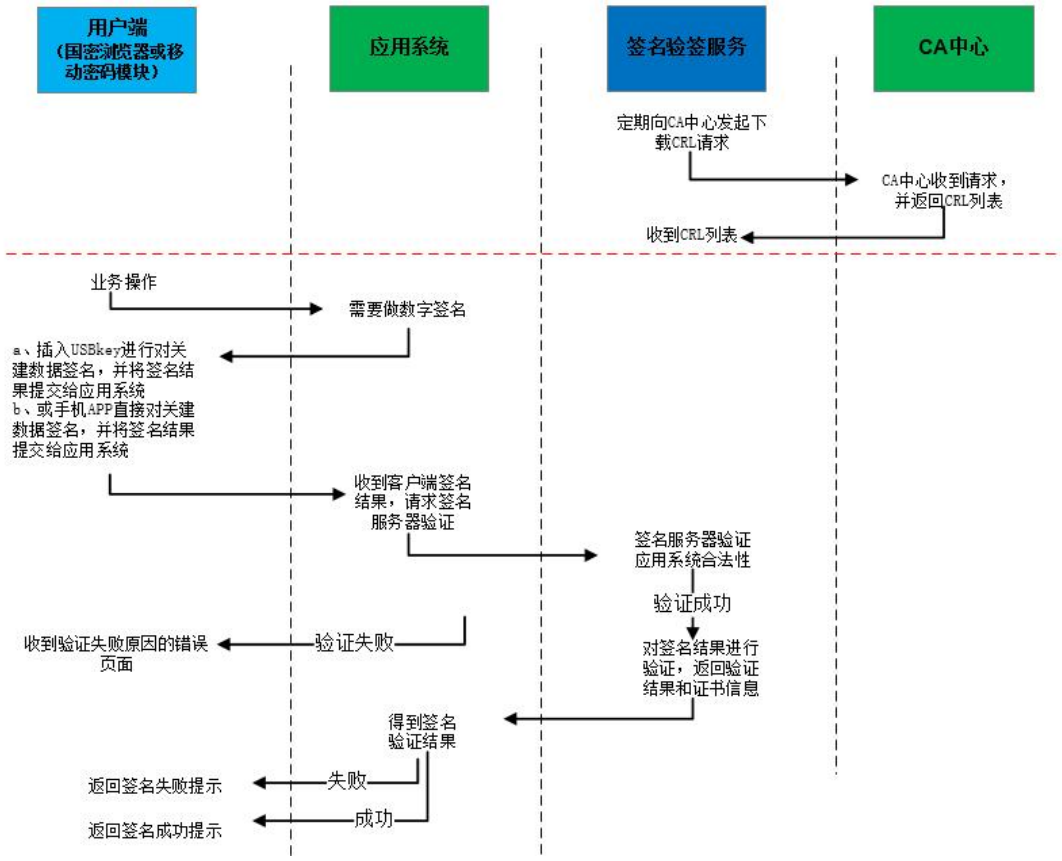
解数字信封接口：为应用系统提供解数字信封接口，并信封结果返回给应用系统

密码协议算法

全面支持国产密码算法，支持 SM2 数字签名算法、SM3 摘要算法、SM4 加解密算法，兼容 RSA1024/2048 算法。

密码应用工作流程

数据签名验签流程



签名验签工作流程

客户在应用系统中遇到需要签名的业务时，流程如下：

应用系统提示客户需要做数字签名，使用浏览器访问则提示插入 USBkey，若使用手机 APP 则直接弹出输入 PIN 码；

USBkey 插入后，则提示输入 PIN，输入 PIN 码后完成对关建数据的签名操作，并将签名结果提交给应系统；

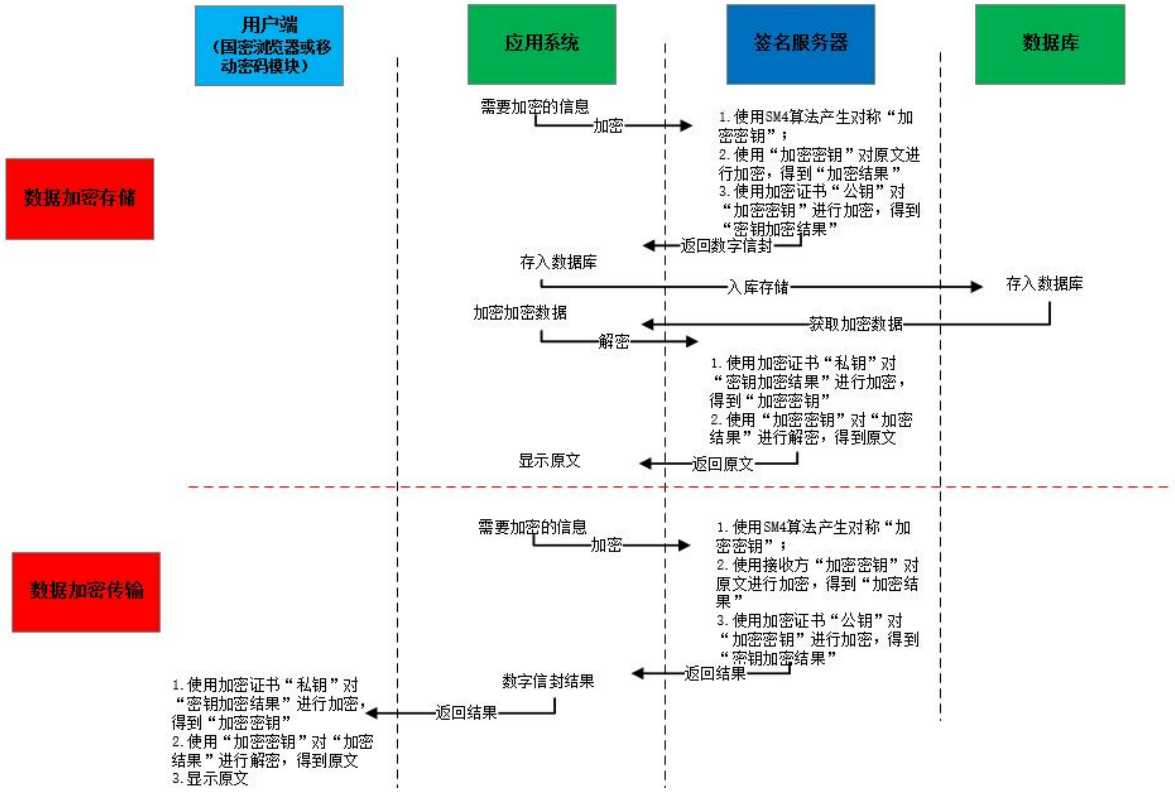
应用系统收到签名结果后，将请求签名验签服务器进行验签；

签名验签服务器收到验签服务器请求，先对客户端证书状态、有效期、信任体系进行验证，验证通过后在对签名结果进行验证，验证通过后将验证结果和证书信息返回给应用系统；

应用系统判断签名服务器返回的结果，成功则提示签名成功，失败则提示签名失败。

成功则业务结束。

加解密流程（数字信封）



数字信封工作流程

数据的加密存储流程：

应用系统将需要加密的数据发送给签名验签服务器；

签名验签服务器使用 SM4 算法产生对称密钥“加密密钥”，使用该密钥对原文进行加密，得到“加密结果；使用加密证书私钥对“加密密钥”进行加密，得到“密钥加密结果”，最终封装成数字信封返回给应用；

应用系统将保存如数据库。

数据的加密传输流程：

应用系统将需要加密的数据发送给签名验签服务器；

签名验签服务器使用 SM4 算法产生对称密钥“加密密钥”，使用该密钥对原文进行加密，得到“加密结果；使用接收方加密证书私钥对“加密密钥”进行加密，得到“密钥加密结果”，最终封装成数字信封返回给应用；

应用系统将数据信封发给用户。

用户收到之后，使用自己加密证书私钥对“密钥加密结果”进行解密，得到“加密密钥”，在使用“加密密钥”解密“加密结果”得到原文信息。

密钥管理

系统用户使用 USB Key 数字证书：

其中签名证书密钥对在 RA 签发数字证书时由 USB Key 加密芯片产生，签名证书私钥保存在加密芯片中，公钥通过 LDAP 系统发布。

其中加密证书密钥对由数字认证中心的密钥管理系统产生，并通过 RA 系统，将加密证书私钥写入 USB Key 芯片，公钥通过 LDAP 系统发布。

系统用户使用移动数字证书：

其中签名证书密钥对在 RA 签发数字证书时由移动密码模块产生，签名证书私钥离散不保存中，公钥通过 LDAP 系统发布。

其中加密证书密钥对由数字认证中心的密钥管理系统产生，并通过 RA 系统，将加密证书私钥在移动密码模块中加密保存，公钥通过 LDAP 系统发布。

签名验签服务器使用专用的加密卡存储数字证书：

通过签名验签服务器的数字证书管理功能，产生签名证书密钥对，并将证书请求文件发送给 RA 请求签发数字证书，RA 签发数字证书后导入签名验签服务器加密卡。

其中加密证书密钥对由数字认证中心的密钥管理系统产生，并通过 RA 系统签发的加密证书将私钥导入加密卡芯片，公钥通过 LDAP 系统发布。

传输加密与访问控制

采用综合安全网关，通过基于国产密码的加密技术在物理网络层之上建立虚拟网络层，各主机在接入网络后须经过身份认证方能接入虚拟网络层，并可根据其认证身份的不同将其划入不同的虚拟安全域中。

因其虚拟化的特性，该安全域可以通过软件技术自由定义其属性、权限，管控其按照最小权限原则访问相关系统和组件，同时数据传输将通过加密隧道进行保护。保障中心与业务人员之间信息的安全传递。

采用综合安全网关，通过基于国产密码的加密技术在不同平台之间建立 IPSec VPN 安全隧道，为平台间大量应用数据传输提供可靠的安全保障。

密码子系统

服务端有综合安全网关，客户端国密安全浏览器或者移动密码模块、IPSec 客户端。

对外接口

CRL 下载接口：连接 CA 中心的 CRL 发布服务地址，根据 CRL 发布策略，自动下载 CRL 文件；

安全认证接口：认证客户端数字证书是否有效，验证内容包括数字证书信任链、黑名单验证、证书有效期验证及公私钥匹配验证；

数字证书解析接口：对验证通过的数字证书，将数字证书解析后放在与应用系统约定的 header 或者 URL 等载体中，供应用系统使用。

支持协议算法

对称算法：SM4 算法（国密）、AES 算法、3DES 算法（国际）。

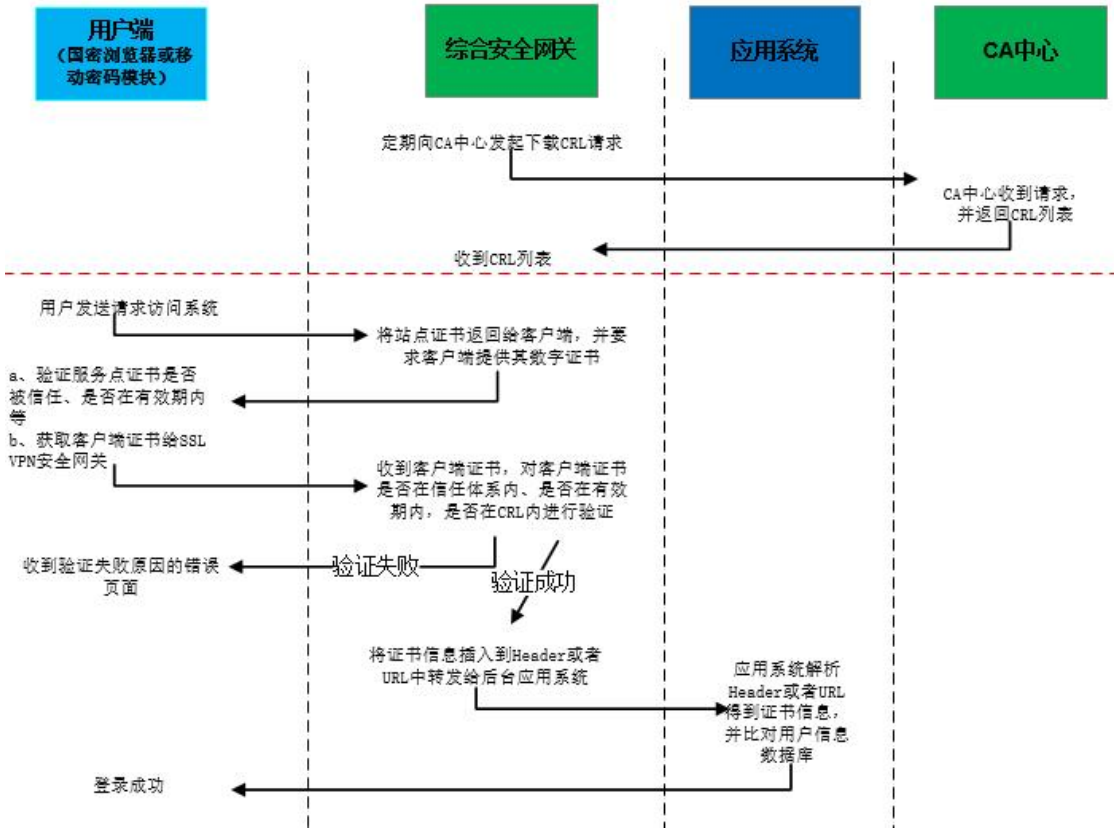
非对称算法：SM2 算法（国密）、RSA1024/2048/4096 算法（国际）

摘要算法：支持 SM3（国密）、SHA-1（国际）、SHA224（国际）、SHA256（国际）、SHA384（国际）、SHA512（国际）等算法。

密码产品和服务

采用综合网关和国密浏览器，产品分别遵循： GM/T0026-2014《SSL VPN 安全网关产品规范》和产品遵循：GM/T 0002-2012 《SM4 分组密码算法》（原 SMS4 分组密码算法）、GM/T 0003-2012 《SM2 椭圆曲线公钥密码算法》、GM/T 0004-2012 《SM3 密码杂凑算法》、GM/T 0024-2014 《SSL VPN 技术规范》。

密码工作流程



安全认证加密工作流程

用户启动浏览器，输入 SSL VPN 安全网关代理应用系统的网络地址或域名，或打开手机 APP 直接访问；

浏览器或移动密码模块将该访问请求发送至 SSL VPN 安全网关；

SSL VPN 安全网关发送站点证书给客户端同时要求客户端提交能够标识其身份信息的数字证书；

浏览器通过国密 SKF 接口调用 USBKEY,弹出 PIN 码框，信息对话框，用户输入 PIN 码完成 USBkey 的用户验证；手机 APP 通过移动密码模块获取证书，要求用户输入 PIN 码（可数字、手势、指纹等）；

浏览器或手机 APP 将用户证书信息提交至 SSL VPN 安全网关；

SSL VPN 安全网关验证客户端证书，验证失败返回响应的错误页面给客户端，验证成功则将证书信息插入到请求数据包的 Header 或者 URL 中，并转发给后台应用系统；

后台应用系统收到请求数据包后，解析 Header 或者 URL 中的证书信息，将证书信息与用户信息数据库中的证书信息进行比对验证，验证通过则返回登录成功。

密钥管理

系统用户使用 USB Key 数字证书：

其中签名证书密钥对在 RA 签发数字证书时由 USB Key 加密芯片产生，签名证书私钥保存在加密芯片中，公钥通过 LDAP 系统发布。

其中加密证书密钥对由数字认证中心的密钥管理系统产生，并通过 RA 系统，将加密证书私钥写入 USB Key 芯片，公钥通过 LDAP 系统发布。

系统用户使用移动数字证书：

其中签名证书密钥对在 RA 签发数字证书时由移动密码模块产生，签名证书私钥离散不保存中，公钥通过 LDAP 系统发布。

其中加密证书密钥对由数字认证中心的密钥管理系统产生，并通过 RA 系统，将加密证书私钥在移动密码模块中加密保存，公钥通过 LDAP 系统发布。

签名验签服务器使用专用的加密卡存储数字证书：

通过签名验签服务器的数字证书管理功能，产生签名证书密钥对，并将证书请求文件发送给 RA 请求签发数字证书，RA 签发数字证书后导入签名验签服务器加密卡。

其中加密证书密钥对由数字认证中心的密钥管理系统产生，并通过 RA 系统签发的加密证书将私钥导入加密卡芯片，公钥通过 LDAP 系统发布。

应用密钥管理服务

用户应用密钥管理基于密码资源池提供的安全管理机制实现安全管理和应用。

1）密钥管理：中用户应用密钥主要存储在用户从密码资源池租用的虚拟密码机中，并且用户之间的密钥由密码资源池的隔离策略保证安全隔离。用户通过自身的 USBKey、协同签名以及综合安全网关身份认证进行密钥的产生、存储、更新、销毁等操作。平台运维人员无权查看用户密钥信息，也获取不到用户的密钥。

2）密钥使用：用户使用应用密钥时，预先在密码统一管理平台生成独立应用凭证，通过该凭证与虚拟密码机建立 SSL 通道，安全的调用用户自己的密钥。

协同签名服务

协同签名服务主要是解决 USBkey 在移动终端（手机、平板等）使用兼容性差、使用不方便，将数字证书通过移动安全中间件密码模块内置到移动终端，并与服务端协调签名平台共同协同完成身份认证、数字签名/验签、数据加密解密、电子签章、动态密码等功能。

密码子系统

协同签名服务由服务端协同签名平台和移动安全中间件密码模块两部分组成。

支持协议算法

对称算法：SM4 算法（国密）、AES 算法、3DES 算法（国际）。

非对称算法：SM2 算法（国密）、RSA1024/2048/4096 算法（国际）

摘要算法：支持 SM3（国密）、SHA-1（国际）、SHA224（国际）、SHA256（国际）、SHA384（国际）、SHA512（国际）等算法。

对外接口

服务端协同签名平台提供的主要接口：

初始化连接接口：完成与系统建立连接；

用户注册接口：完成用户数字证书或这动态口令的申请；

签名验签接口：完成数据的签名和签名结果的验证；

动态口令验证接口：完成动态口令的验证；

二维码接口：二维码的产生和验证。

移动安全中间件密码模块提供的主要接口：

初始化连接接口：完成与系统建立连接；

用户注册接口：完成用户数字证书或这动态口令的申请；

签名接口：完成数据的数字签名；

动态口令计算：完成当前时间动态口令的验证；

证书管理接口：实现数字证书生命周期的管理；

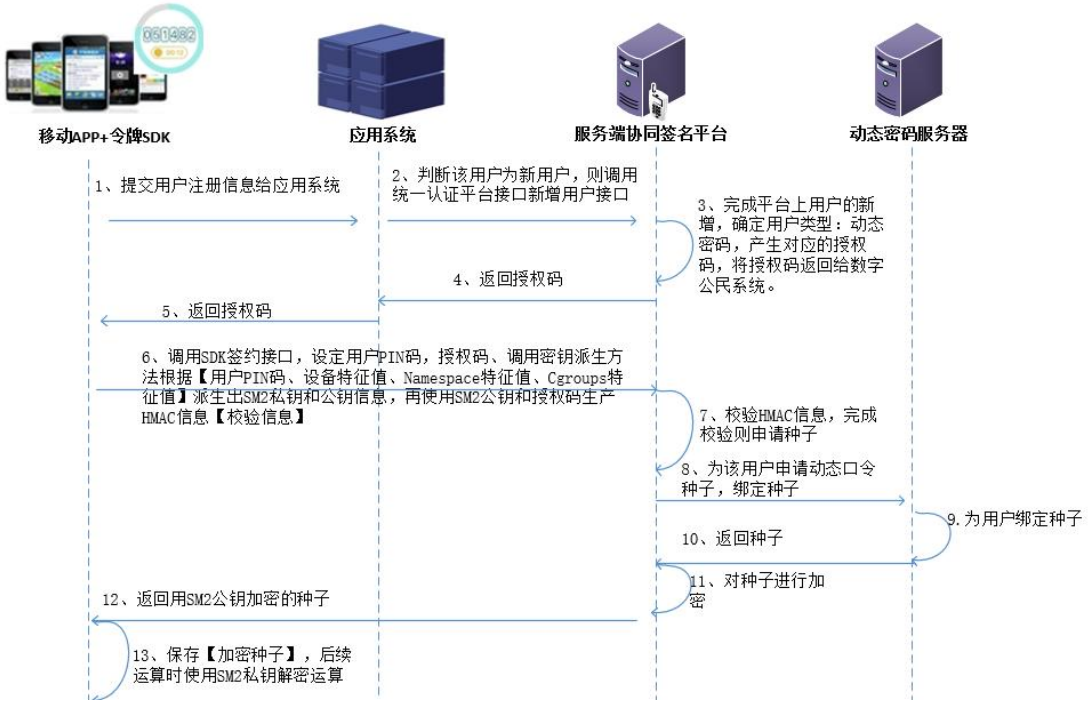
电子签章接口：完成电子签章；

二维码接口：支持二维码扫一扫功能。

密码工作流程

流程只介绍动态令牌系统种子的申请和数字证书的申请，口令的验证密码工作流程，数字签名的验证详见签名验签服务密码工作流程。

动态令牌种子申请工作流程如下图：



移动安全认证系统证动态令牌申请流程

提交用户注册信息给应用系统

判断该用户为新用户，则调用服务端协同签名平台接口新增用户接口

完成平台上用户的新增，确定用户类型：动态密码，产生对应的授权码，将授权码返回给应用系统。

返回授权码

返回授权码

调用 SDK 签约接口，设定用户 PIN 码，授权码、调用密钥派生方法根据【用户 PIN 码、设备特征值、Namespace 特征值、Cgroups 特征值】派生出 SM2 私钥和公钥信息，再使用 SM2 公钥和授权码生产 HMAC 信息【校验信息】

校验 HMAC 信息，完成校验则申请种子

为该用户申请动态口令种子，绑定种子

为用户绑定种子

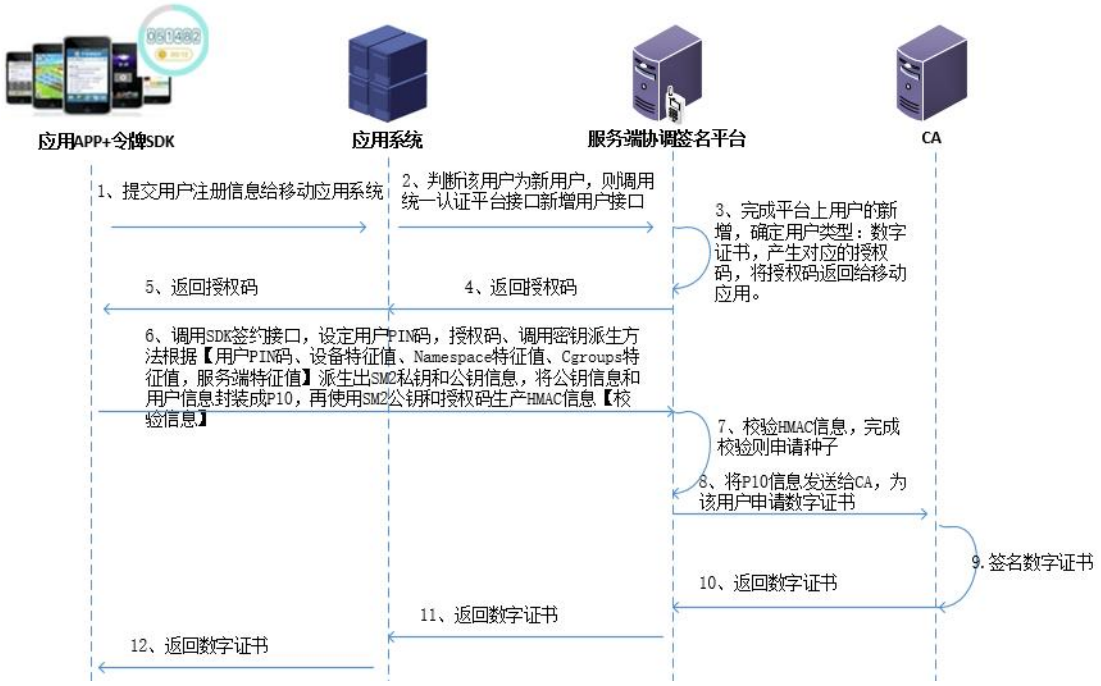
返回种子

对种子进行加密

返回用 SM2 公钥加密的种子

保存【加密种子】，后续运算时使用 SM2 私钥解密运算

软数字证书申请流程



移动安全认证系统证书申请流程

提交用户注册信息给移动应用系统

判断该用户为新用户，则调用服务端协同签名平台接口新增用户接口

完成平台上用户的新增，确定用户类型：数字证书，产生对应的授权码，将授权码返回给移动应用。

返回授权码

调用 SDK 签约接口，设定用户 PIN 码，授权码、调用密钥派生方法根据【用户 PIN 码、设备特征值、Namespace 特征值、Cgroups 特征值，服务端特征值】派生出 SM2 私钥和公钥信息，将公钥信息和用户信息封装成 P10，再使用 SM2 公钥和授权码生产 HMAC 信息【校验信息】

校验 HMAC 信息，完成校验则申请种子

将 P10 信息发送给 CA，为该用户申请数字证书

签名数字证书

密钥管理

协同签名服务密钥管理由移动安全中间件密码模块实现，一个用户的私钥由设备、服务端和用户信息等组成：

用户私钥设备分散片段由密钥管理算法采集设备硬件特征值(包含但不限于 MAC 地址、CPUinfo、IMEI 等)、设备系统特征值等信息，调用密钥派生函数派生得到。该私钥分散片段不保存，使用时由密钥管理算法自动采集派生参与计算。

用户私钥用户分散片段根据用户因子信息(用户 PIN 码、用户行为特征值等)、采集的设备硬件特征值(包含但不限于 MAC 地址、CPUinfo、IMEI 等)等信息调用密码派生函数派生。该私钥分散片段不保存，用户需要使用时采集用户因子临时派生参与计算。

用户私钥服务端片段由服务器生成和保存。在用户申请数字证书时，根据用户行为特征，生成随机数作为用户私钥服务端片段。用户需要使用该私钥分散片段参与计算时，由服务器根据用户行为特征分析结果确定该私钥分散片段是否参与运算，返回运算结果

时间戳服务

时间戳系统为数字签名提供可信的时间保障，能够为应用系统中关键操作的数字签名提供可信时间戳服务。

时间戳服务器能够直接为客户端电子签章、签名控件提供服务，也能够为应用系统、签名验签服务器提供服务。

密码子系统

数字时间戳服务子系统由时间戳服务器及相关服务接口构成。

对外接口

时间戳服务器对外的主要服务接口包括：

时间源连接接口：与国家授时中心连接，获取可信时间；

数字时间戳接口：提供时间戳服务，根据请求为数据制作数字时间戳

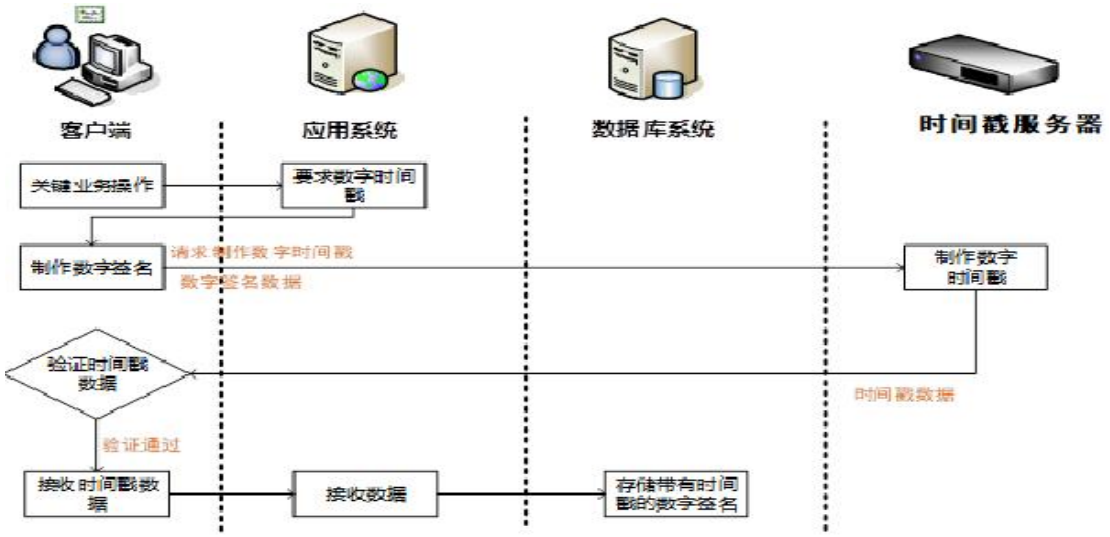
支持协议算法

时间戳服务器支持国产 SM2 数字签名算法、SM3 摘要算法。

密码工作流程

时间戳服务器应用流程如下图所示：

为客户端数字签名制作数字时间戳



时间戳工作流程

应用系统要求客户端提交带有时间戳的签名数据时：

用户登录应用系统，进行关键业务操作；

应用系统根据业务要求，要求客户端提交带有时间戳的数字签名；

客户端对关键业务数据制作数字签名，并向时间戳服务器发出对签名数据制作时间戳的请求；

时间戳服务器为签名数据加盖时间戳并数字签名，数据返回给客户端；

客户端验证时间戳数据，确认时间戳签名有效后将带有时间戳的签名数据发送到应用系统；

应用系统将带有时间戳的签名数据存入数据库。

密钥管理

时间戳服务器上部署第三方电子认证中心签发的时间戳服务机构数字证书，用来为时间戳数据制作数字签名。

时间戳服务器使用专用的加密卡存储数字证书：

通过时间戳服务器的数字证书管理功能，产生签名证书密钥对，并将证书请求文件发送给 RA 请求签发数字证书，RA 签发数字证书后导入安全认证网关加密卡。

其中加密证书密钥对由数字认证中心的密钥管理系统产生，并通过 RA 系统签发的加密证书将私钥导入加密卡芯片，公钥通过 LDAP 系统发布。

动态密码服务

动态令牌认证系统主要为应用系统、主机系统、运维审计系统提供动态密码身份认证服务。

密码子系统

动态密码服务包括服务端的动态密码服务系统、客户端为动态令牌、移动安全中间件、手机短信的形式。

对外接口

动态令牌认证系统主要为应用系统、主机系统、运维审计系统提供主要接口如下：

动态令牌管理接口：令牌生命周期管理、令牌与用户绑定等接口；

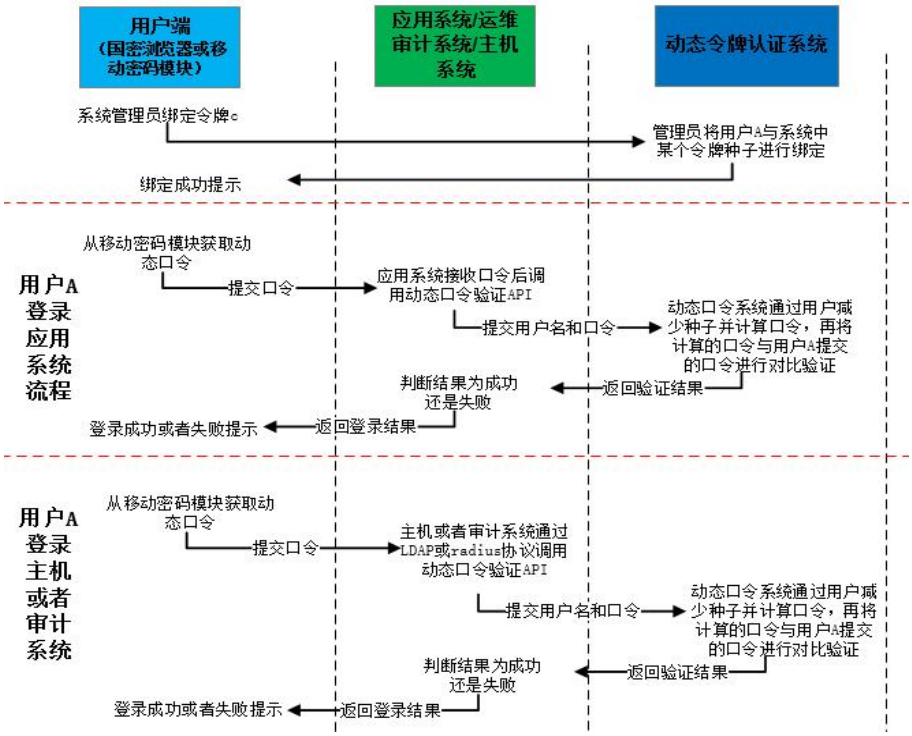
动态令牌验证接口：对于应用系统、主机系统或者运维审计系统提交的动态口令进行验证。

支持协议算法

摘要算法：支持 SM3（国密）、SHA-1（国际）、SHA256（国际）、SHA384（国际）、SHA512（国际）等算法。

密码工作流程

动态令牌认证系统与应用系统、主机系统或者运维审计系统结合的密码工作流程如下图：



动态令牌认证系统流程图

动态令牌认证系统管理员需要为用户绑定动态令牌系统内的种子文件。

与应用系统结合流程：

用户从移动密码模块获取当前时间的动态口令，提交给应用系统；

应用系统接收用户提交的动态口令，通过接口的形式调用动态令牌验证 API，将用户名和口令提交给动态令牌认证系统；

动态令牌认证系统结束到验证请求，使用用户名检索对应的种子文件，并计算当前时间上下浮动 5 分钟（验证策略可设置）对应的动态口令，再与用户提交的动态口令进行比对验证，返回验证结果给应用系统；

应用系统判断验证结果并告知用户。

与主机系统或运维审计系统等网络设备

用户从移动密码模块获取当前时间的动态口令，提交给应用系统；

应用系统接收用户提交的动态口令，通过 LDAP 或 RADIUS 协议形式调用动态令牌验证 API，将用户名和口令提交给动态令牌认证系统；

动态令牌认证系统结束到验证请求，使用用户名检索对应的种子文件，并计算当前时间上下浮动 5 分钟（验证策略可设置）对应的动态口令，再与用户提交的动态口令进行比对验证，返回验证结果给应用系统；

应用系统判断验证结果并告知用户。

密钥管理

动态密码中密钥有设备初始化产生，永不出设备。

第四章　建设内容工程量清单

一、 数据中心建设清单

序号	名称	功能及参数	单位	数量	单价	总价
网络系统						
1	核心路由器	支持包转发率≥2800Mpps，支持双引擎热备功能，配置 2 个引擎，配置 8 个万兆光口，24 个千兆电口。	2	台		
2	核心交换机	机框式交换机，支持≥16 业务槽位，包转发率≥190000Mpps，双引擎，支持网络虚拟化和设备虚拟化功能；支持 IPv6 静态路由、RIPng、OSPFv3、IS-ISv6、BGP4+；配置≥64 个万兆光口（SFP+），≥14 个 40G 光口，≥48 个千兆电口，配置单个 IP 和单个端口的流量控制功能；配置 4 个电源模块	2	台		
3	汇聚交换机	整机转发性能≥220Mpps，提供≥48 个千兆电口，≥4 个 SFP+万兆端口，配 4 个万兆模块	10	台		
4	服务器交换机	数据中心汇聚交换机，整机包转发率≥1000Mpps；提供≥48 个万兆 SFP+光接口，≥2 个 QSFP+接口；配备 2 个 40G QSFP+光模块	2	台		
5	SDN 控制器	支持 OpenFlow V1.0、V1.3。支持基于 OpenFlow 协议的 LLDP 的拓扑发现以及 SNMP 的 LLDP mib 读取，支持基于整网的物理设备人工构建出基于 GRE 隧道、Ipv4-over-Ipv6 隧道实现设备间互联的逻辑拓扑。支持网络设备管理、端口统计、流统计、端口状态管理。通过 WEB 界面以图形方式统一呈现平台信息、整网的流量状况、各链路质量状况、各条流在整个路径上的流量信息、选路状况，呈现基于隧道手动构建的网络拓扑。支持安全设备故障检测，并且自动 bypass 故障安全设备。为保证可用性，保留测试权利	2	台		
网络安全						
6	防火墙	≥30G 网络吞吐量，最大并发连接数≥1000 万，插板结构或者机架式结构，插板结构必须支持插入本次配置的核心交换机；支持虚拟防火墙功能：支持虚拟防火墙的创建、删除功能；可独立分配 CPU/内存等计算资源；虚拟防火墙可独立管理，独立保存配置；虚拟防火墙具备独立会话管理、NAT、路由等功能。配置 5 年病毒库升级服务	2	台		
7	入侵防御	≥30G 网络吞吐量，IPS 吞吐量≥10G，最大并发连接数≥1000 万，插板结构或者机架式结构，插板结构必须支持插入本次配置的核心交换机；5 年	2	台		

		IPS 特征库升级服务				
8	日志审计	支持被动采集方式，包括 SYSLOG、SNMP Trap、NetFlow 等；支持主动采集方式，包括 FTP/TFTP、JDBC\ODBC 等；支持自定义采集解析规则以兼容未适配日志；支持日志格式归一化；支持保留原始日志；支持通过情景数据丰富归一化日志；日志存储空间阈值告警；支持日志采集代理，采集代理支持 Windows、linux 操作系统、中间件如 TOMCAT 等、数据库如 Oracle 等；可对多厂家日志进行采集分析，日志存储不少于 180 天，支持 PDF、HTML、Excel 格式等多种报告导出。含硬件服务器	1	台		
9	网页防篡改	通过监测网页完整性的变化，通过对篡改行为的实时拦截或自动恢复被篡改的内容来实现对网页完整性的保护	1	套		
10	堡垒机	为了保障网络和数据不受来自外部和内部用户的入侵和破坏，运用各种技术手段监控和记录运维人员对网络内的服务器、网络设备、安全设备、数据库等设备的操作行为，从而实现集中报警、及时处理及审计定责。	1	台		
11	漏洞扫描系统	针对传统的操作系统、网络设备、防火墙、远程服务等系统层漏洞进行渗透性测试。测试系统补丁更新情况，网络设备漏洞情况，远程服务端口开放等情况进行综合评估，在黑客发现系统漏洞前期提供给客户安全隐患评估报告，提前进行漏洞修复，提前预防黑客攻击事件的发生。针对 SQL 注入、XSS 跨站脚本、信息泄露、网络爬虫、目录遍历等 Web 攻击方式进行模拟黑客渗透攻击评估	1	台		
12	数据库审计	支持将多个数据库 IP 绑定为一个业务系统，后期的数据分析如流量、用户数和操作行为等；支持 Oracle，Microsoft SQL Server，DB2，Sybase，Informix、MySQL、人大金仓(Kingbase)、达梦(DM)、Caché等，可以准确分析出这些数据库的协议；支持对多种不同类型和不同版本的数据库的同时审计	1	台		
13	上网行为管理	支持 10M/100M/1000M 自适应电接口数量≥8，支持千兆 SFP 光接口数量≥4，万兆接口总数≥4；网络吞吐量≥60Gbps，应用性能≥20Gbps，最大并发连接数≥1000 万，最大用户数≥50000；接口无路由/交换/LAN/WAN 等固化区分，均可作为二三层接口使用	1	台		
14	杀毒软件	100 客户端，50 个服务器端，五年升级服务	1	套		
15	云平台虚拟化安全	包括防病毒+防火墙+入侵防御+web 防护四项功能，提供单颗 CPU 五年使用授权，包括：7x24 远程电话支持服务、相应模块规则库升级、模块软件升级。	30	CPU		
16	安全态势感知系统	以大数据平台为基础，通过收集多元、异构的海量日志，利用关联分析、机器学习、威胁情报等技术，	1	套		

		帮助政企客户持续监测网络安全态势，实现从“被动防御”向“积极防御”的进阶，为安全管理者提供风险评估和应急响应的决策支撑，为安全运营人员提供威胁发现、调查分析及响应处置				
17	网络管理系统	50 个服务器授权，200 个虚拟化服务器授权，200 个网络节点授权	1	套		
国密建设						
18	数字签名服务器	为各种规模的企业和政府机构提供多种数字签名服务。包括 ttached/Detached/RAW 签名验签、数字信封加密/解密、签名二维码生成、PDF 电子签章、XMLSignature 等多种签名验签及数据加解密服务，支持 RSA 算法和国密算法。 签名：SM2：20KTPS；验签：SM2：15KTPS。	2	套		
19	HTTPS 国密应用网关	提高交易的 SSL 处理效率，为用户提供完善的用户数字证书与网上应用结合的机制。 SM2：3KTPS； 并发连接：500K，最大吞吐：2G。	2	套		
20	SSL VPN 系统	最大支持 3 万在线用户，默认用户数为 100，需要单独购买用户才可以使用。最多支持 128 个虚拟门户，默认提供 5 个虚拟门户授权。SSL 吞吐：2.5G	1	套		
21	移动统一认证安全管理平台	提供协同签名功能，并可加软件功能扩展模块以实现简单的证书颁发、签名验证和动态密码验证等功能； 最大支持 500 个用户，本次配置 300 个授权，协同签名 1600TPS，验证令牌 6000TPS。	1	套		
22	移动安全中间件	提供安卓和 IOS 的 SDK 或者 APP，提供数字证书管理、数字签名、电子签章等服务	1	套		
23	电子签章系统	为各种规模的企业和政府机构提供多种电子签章服务，提供基于数字证书的电子印章的制作、管理、签盖、验证和审计等功能。 最大支持 100 个印章，内置 50 个授权， 签章：SM2：签章 60TPS； 验章：SM2：100TPS。	1	套		
24	动态密码系统	系统具备动态密码种子生成、验证服务和服务管理三个子系统，产品提供多种终端形态支持，主要包括：时间型令牌，事件形令牌，多键令牌，手机软件、手机短信、二维矩阵等多种方式。最大支持 5000 用户，响应性能 500TPS	1	套		
25	应用交付系统	支持 L2-L7 的后台业务负载均衡；支持 Web 服务器负载均衡，App 服务器负载均衡；灵活的、可定制的应用分发策略，可根据不同业务提供 22 种负载均衡策略通过定义灵活多样的负载均衡策略，依据丰富的服务器负载均衡算法来实现真正的合理流量分配。 L4：新建：280K，并发：4M，最大吞吐：3.7G； L7：新建：1.2M，并发：690K，最大吞吐：3.7G	1	套		
26	时间戳服务器	时间戳服务器与国家授时中心时间同步，通过标准接口提供可信的标准时间，保障时间的真实性、完整性、不可抵赖性。用于电子印章应用系统。签发	1	套		

		效率 ≥1500 次/秒;验证效率≥1000 次/秒。				
27	服务器加密机	标准机架，2 个千兆网络接口；SM3 杂凑算法≥900Mbps；SM4 算法加解密速度：≥900Mbps；SM2 算法：生密钥≥56000 次/秒，签名速度≥56000 次/秒，验签速度≥41000 次/秒，加密速度≥28000 次/秒，解密速度≥46000 次/秒；密钥存储能力：SM2 签名密钥对≥500 对,SM2 加密密钥对≥500 对，数据加密密钥≥1024 个；对称密钥加/解密：提供国家标准的 SM1 算法和 SM4 算法，用于数据的加解密。	1	套		
28	服务器证书	用于表明服务器合法身份，每个网站一个证书，国密算法，三年有效	3	套		
29	数字证书	含存储介质：usb key	200	个		
主机存储系统						
30	虚拟化服务器	≤4U 机架式服务器,配置 4 个英特尔 12 核及以上，主频≥2.3Hz CPU；配置≥512GB 内存;配置≥2 块 600GB 10K SAS 热插拔硬盘；配置磁盘阵列卡≥1GB 缓存，支持 RAID0,1,5,6,10，带掉电保护；配置≥4*GE 以太电口卡，≥2*10GE 光口；配置≥2 块 16Gb 单端口 SFP+(含光模块)FC HBA 卡；冗余电源	10	台		
31	云管理服务器	2U 机架式服务器，配置 2 个英特尔 14 核及以上，主频≥2.2Hz CPU;配置≥256GB 内存;配置≥4.2TB SAS 硬盘,20TB SATA 硬盘，3.2TB SSD 硬盘；配置磁盘阵列卡≥1GB 缓存，支持 RAID0,1,5,6,10，带掉电保护；配置≥4*GE 以太电口卡；≥2*10GE 光口；配置≥2 块 16Gb 单端口(含光模块)HBA 卡；冗余电源	2	台		
32	磁盘阵列	双控制器,单控缓存≥64GB,单控提供≥2 个 16G FC 口；提供≥150TB 实际可使用容量，SSD、SAS 与 NL-SAS 盘的配比为 1:4:5，配置双活、智能分层、多路径、重删软件许可。	2	套		
33	光纤交换机	48 口光纤交换机，激活 36 口带模块	2	台		
34	虚拟化软件	80 颗 CPU 许可	1	套		
35	云平台管理软件	80 个 CPU 许可	1	套		
36	备份一体机	一体化备份设备，支持 Windows、Linux、Unix 系统的实时备份与恢复；支持 VMware、H3Cloud、FusionSphere、Cnware 等主流虚拟化环境下的实时备份与恢复；支持多种数据库的实时备份与恢复：Oracle、MySQL、MongoDB、人大金仓、南大通用、武汉达梦、TRS（拓尔思）等；配置数据重删、快照等功能；提供 300TB（其中 50TB 为实时备份）裸容量及相应授权。	1	台		

37	平台管理服务器	≤2U 机架式服务器,配置 2 个英特尔 10 核及以上，主频≥2.2Hz CPU；配置≥128GB 内存;配置≥5*600GB 10K SAS 热插拔硬盘；配置磁盘阵列卡≥1GB 缓存，支持 RAID0,1,5,6,10，带掉电保护；配置≥4*GE 以太电口卡；冗余电源	8	台		
38	平台计算服务器	≤2U 机架式服务器,配置 2 个英特尔 12 核及以上，主频≥2.3Hz CPU；配置≥256GB 内存;配置≥2*300GB 10K SAS 热插拔硬盘，≥24TB NL-SAS 热插拔硬盘，≥1.6TB 固态硬盘；配置磁盘阵列卡≥1GB 缓存，支持 RAID0,1,5,6,10，带掉电保护；配置≥4*GE 以太电口卡；冗余电源	2	台		
39	平台存储服务器	≤2U 机架式服务器,配置 2 个英特尔 10 核及以上，主频≥2.4Hz CPU；配置≥128GB 内存;配置≥2*300GB 10K SAS 热插拔硬盘，≥24TB NL-SAS 热插拔硬盘；配置磁盘阵列卡≥1GB 缓存，支持 RAID0,1,5,6,10，带掉电保护；配置≥4*GE 以太电口卡；冗余电源	2	台		
机房系统						
40	空调系统	精密空调，可为设备机房、传输机房、UPS 室、通讯室提供恒温恒湿环境	2	套		
41	UPS	四组 600KVA UPS，冗余备份，含电池、线缆和监控系统	2	套		
42	基础建设	机房防雷接地、水电接入、电力引入	1	项		
43	机房装修	门、墙面、地面、吊顶、照明建设，电磁防护等安全防护措施建设	1	项		
44	综合管线	桥架、管路、线缆及相关防护措施	1	项		
45	机房监控	视频监控、门禁、环境监控、消防系统等	1	项		
服务与链路						
46	万兆互联网出口链路	数据中心万兆互联网出口链路（五年）	2	条		
47	等保咨询服务	三级等保合规建设	1	项		
48	等保测评服务	三级等保测评服务	1	项		

二、 云平台建设清单

应用分类	应用角色	功能及参数	单位	数量	单价	总价
SLB 服务	SLB 节点	提供SLB流量分发服务,每台服务器配置2*10G网卡	项	1		
	SLB Tengine 节点	提供七层负载均衡能力(Session 保持能功能）				
	SLB Master	SLB Master 用于控制 LVS 节点的配置，规则下发。				
	SLB AG	用于 SLB 集群管理，一个 IDC 2 台。				
ECS 服务	AOS Master+AG	集群 Master 每 Pod 一组 Master，2 台 AG。	项	1		
	Region Master	部署 RMS/RHS/Region Master/RabbitMQ 等服务				
	Region Tair	用于读取 Region Master 数据库的缓存服务，减少应用对数据的直接读取				
	沉香 DB	用于集群部署				
	Dayu DB	集群部署及包管理服务				
	ECS VNC	提供 ECS VM 客户的 VNC 管理功能，公网 IP 通过 LVS 提供。				
	3rd ODBS	弹性计算 ODBS，一主一备。异地机房单独部署，杭州可共享。				
	IGW	Internet 网关服务器,每台新增 2 块双端口万兆卡。				
	NGW	NAT 网关服务器，每台新增 2 块双端口万兆卡。				
	VGW	VPC 网关服务器，每台新增 2 块双端口万兆卡。				
	MGW	专线接入网关服务器,每台新增 2 块双端口万兆卡。				
	NC	ECS 服务 Node Controller				
RDS 服务	SLB 节点（RDS VIP)	提供SLB流量分发服务,每台服务器配置一块2端口万兆网卡	项	1		
	SLB Master	用于 SLB 集群管理，共享 ECS 集群 SLB Master.				
	SLB AG	用于 SLB 集群管理，一个 IDC 2 台,可以与 ECS SLB 共享。				
	Proxy API	用于管理 Proxy 服务器				
	Proxy	数量计算公式：节点数*10%				
	Aurora	负责 RDS 服务中所有实例的高可用				
	Redis	超过 200 台，每增加 100 台扩容 2 台				
	FTP 上传服务器	FTP 上传服务器，为用户提供 MSSQL 离线数据同步(镜像上传)功能。(官网业务)				
	DRC	MySQL 在线数据同步服务(适用于官网业务）				
	xFTP 备份服务器（可替换为本地 OSS)	备份数据库节点中用户数据，数据量视 DB 容量，网络带宽而定； 2 台为互备避免单机故障，经验值可支持 100 组数据节点的备份；				

	DB Node	数据库服务器，支持 MSSQL、MYSQL.				
OSS 服务	LVS 服务器(OSS VIP)	提供 SLB 流量分发服务,配置 2*10 网卡	项	1		
	OSS Webserver	OSS 前端 webserver 部署数量视所需提供并发 QPS 量级确定				
	AOS Master+AG	集群 Master 加上 2 台 AG				
	NC/KVServer	提供 OSS 存储服务				
云盾服务	DDoS 攻击检测服务器	DDoS 攻击检测服务器，万兆连接流量镜像设备	项	1		
	流量计费+攻击阻断服务器	用于 VM 流量计费和攻击阻断,万兆连接流量镜像设备,每台 15G 处理能力。				
	流量分析及大数据提取服务器	流量分析及大数据提取服务器，用于提取 http、DNS 等大数据以及恶意主机攻击证据提取,万兆连接流量镜像设备，每台 15G 处理能力。				
	DDoS 设备管理服务器	操作系统为 windows 2008 64 位				
	DDoS 清洗 API 服务器	DDoS 自动防御程序，提供 API 调用				
	DDoS 分析统计器及 DB	用于流量分析数据包存储				
	Syslog 服务器	用于压缩回传至科创城数据，1Gbps 压缩为 3Mbps 左右。				
OPS 服务	LVS 服务器	提供负载均衡服务,每台服务器配置一块 2 端口万兆网卡	项	1		
	基础配管					
	Yum 源					
	DNS/NTP(NC)	域名解析、时间同步(for NC)				
	DNS(VM)	域名解析(for VM)				
	Syslog 服务器	日志管理				
	Console 服务器					
	网络工具机					
	OOB 服务器	服务器带外管理、装机				
	网络管理系统 agent					
	Clone 服务器	提供 OS clone 安装服务				
	登录服务器(跳板机)	一个大 Region(安全域)一套				
	Alimonitor-superagent	监控系统，如果带外网络与阿里云大 Region 打通，不需要单独配置千兆网卡				
	Alimonitor-monitor					
	Dragoon-monitor					
	Dragoon-superagent					
	Staragent-server					
	消磁机	硬盘消磁设备				

三、 1 号地块建设清单

序号	系统名称	系统需求	单位	数量	单价	合价
一、	综合管线系统	详见“详细应用系统要求”	项	1		
二、	智能化网络系统	详见“详细应用系统要求”	项	1		
三、	楼宇自控系统	详见“详细应用系统要求”	项	1		
四、	能源监测系统	详见“详细应用系统要求”	项	1		
五、	信息发布系统	详见“详细应用系统要求”	项	1		
六、	视频监控系统	详见“详细应用系统要求”	项	1		
七、	门禁管理系统	详见“详细应用系统要求”	项	1		
八、	梯控管理系统	详见“详细应用系统要求”	项	1		
九、	车辆管理系统	详见“详细应用系统要求”	项	1		
十、	入侵报警系统	详见“详细应用系统要求”	项	1		
十一、	电子巡更系统	详见“详细应用系统要求”	项	1		
十二、	无线对讲系统	详见“详细应用系统要求”	项	1		
十三、	智慧灯杆系统	详见“详细应用系统要求”	项	1		
十四、	智能照明系统	详见“详细应用系统要求”	项	1		
十五、	智慧灌溉系统	详见“详细应用系统要求”	项	1		
十六、	智慧井盖系统	详见“详细应用系统要求”	项	1		
十七、	房屋安全动态监测系统	详见“详细应用系统要求”	项	1		
十八、	公共广播系统	详见“详细应用系统要求”	项	1		
十九、	弱电机房	详见“详细应用系统要求”	项	1		
二十、	展示中心室内配套（1 号楼）	详见“详细应用系统要求”	项	1		
二十一、	管理服务运营中心	详见“详细应用系统要求”	项	1		

二十二、	智慧餐厅	详见“详细应用系统要求”	项	1		
二十三、	智慧服务平台	详见“详细应用系统要求”	项	1		

四、 2 号地块建设清单

序号	系统名称	系统需求	单位	数量	单价	合价
一、	综合管线系统	详见“详细应用系统要求”	项	1		
二、	智能化网络系统	详见“详细应用系统要求”	项	1		
三、	楼宇自控系统	详见“详细应用系统要求”	项	1		
四、	能源监测系统	详见“详细应用系统要求”	项	1		
五、	信息发布系统	详见“详细应用系统要求”	项	1		
六、	视频监控系统	详见“详细应用系统要求”	项	1		
七、	门禁管理系统	详见“详细应用系统要求”	项	1		
八、	梯控管理系统	详见“详细应用系统要求”	项	1		
九、	车辆管理系统	详见“详细应用系统要求”	项	1		
十、	入侵报警系统	详见“详细应用系统要求”	项	1		
十一、	电子巡更系统	详见“详细应用系统要求”	项	1		
十二、	无线对讲系统	详见“详细应用系统要求”	项	1		
十三、	智慧灯杆系统	详见“详细应用系统要求”	项	1		
十四、	智能照明系统	详见“详细应用系统要求”	项	1		
十五、	智慧灌溉系统	详见“详细应用系统要求”	项	1		
十六、	智慧井盖系统	详见“详细应用系统要求”	项	1		
十七、	房屋安全动态监测系统	详见“详细应用系统要求”	项	1		
十八、	公共广播系统	详见“详细应用系统要求”	项	1		
十九、	弱电机房	详见“详细应用系统要求”	项	1		

五、 3 号地块建设清单

序号	系统名称	系统需求	单位	数量	单价	合价
一、	综合管线系统	详见“详细应用系统要求”	项	1		
二、	智能化网络系统	详见“详细应用系统要求”	项	1		
三、	楼宇自控系统	详见“详细应用系统要求”	项	1		
四、	能源监测系统	详见“详细应用系统要求”	项	1		
五、	信息发布系统	详见“详细应用系统要求”	项	1		
六、	视频监控系统	详见“详细应用系统要求”	项	1		
七、	门禁管理系统	详见“详细应用系统要求”	项	1		
八、	梯控管理系统	详见“详细应用系统要求”	项	1		
九、	车辆管理系统	详见“详细应用系统要求”	项	1		
十、	入侵报警系统	详见“详细应用系统要求”	项	1		
十一、	电子巡更系统	详见“详细应用系统要求”	项	1		
十二、	无线对讲系统	详见“详细应用系统要求”	项	1		
十三、	智慧灯杆系统	详见“详细应用系统要求”	项	1		
十四、	智能照明系统	详见“详细应用系统要求”	项	1		
十五、	智慧灌溉系统	详见“详细应用系统要求”	项	1		
十六、	智慧井盖系统	详见“详细应用系统要求”	项	1		
十七、	房屋安全动态监测系统	详见“详细应用系统要求”	项	1		
十八、	公共广播系统	详见“详细应用系统要求”	项	1		
十九、	弱电机房	详见“详细应用系统要求”	项	1		

六、 4 号地块建设清单

序号	系统名称	系统需求	单位	数量	单价	合价
一、	综合管线系统	详见“详细应用系统要求”	项	1		
二、	智能化网络系统	详见“详细应用系统要求”	项	1		
三、	楼宇自控系统	详见“详细应用系统要求”	项	1		
四、	能源监测系统	详见“详细应用系统要求”	项	1		
五、	信息发布系统	详见“详细应用系统要求”	项	1		
六、	视频监控系统	详见“详细应用系统要求”	项	1		
七、	门禁管理系统	详见“详细应用系统要求”	项	1		
八、	梯控管理系统	详见“详细应用系统要求”	项	1		
九、	车辆管理系统	详见“详细应用系统要求”	项	1		
十、	入侵报警系统	详见“详细应用系统要求”	项	1		
十一、	电子巡更系统	详见“详细应用系统要求”	项	1		
十二、	无线对讲系统	详见“详细应用系统要求”	项	1		
十三、	智慧灯杆系统	详见“详细应用系统要求”	项	1		
十四、	智能照明系统	详见“详细应用系统要求”	项	1		
十五、	智慧灌溉系统	详见“详细应用系统要求”	项	1		
十六、	智慧井盖系统	详见“详细应用系统要求”	项	1		
十七、	房屋安全动态监测系统	详见“详细应用系统要求”	项	1		
十八、	公共广播系统	详见“详细应用系统要求”	项	1		
十九、	多媒体会议系统	详见“详细应用系统要求”	项	1		
二十、	弱电机房	详见“详细应用系统要求”	项	1		

注：1、第四章建设内容工程量清单总价不得高于招标文件要求的最高限价

2、建设内容工程量清单内容详见“附件：工程量清单”附件

3、建设内容工程量清单内容如果和附件有差异以“附件：工程量清单”附件为准

第五章　商务文件格式

商务文件

（填写正本或副本）

项目名称：_____

项目编号 ：_____

投标人名称：_____（盖公章）

投标人地址：_____

法定代表人或其授权代表：_____（签名或盖章）

日期：_2022__年_____月_____日

一、 投 标 函

致：德阳市数字科技城开发有限公司：

1、根据招标人_____招标文件及答疑、补充文件有关规定，我方经考察现场和研究上述工程招标文件及其它有关文件后，我方同意招标人建设内容工程量清单中的全部施工内容。

总价为人民币_____元整（￥_____元）；

2、一旦我方中标，我方保证按照质量标准及按招标人工期要求完成本工程施工。

3、我方将按照招标文件的规定履行合同所有条款责任和义务。

4、我方已详细审查全部招标文件，包括修改文件（如果有）以及全部参考资料和有关附件。完全理解并同意放弃对这方面不明及误解的权利。

56、如果在规定开标时间和日期后，我方在投标有效期内撤回投标或我单位中标后未按招标方要求及时进场及签定工程施工合同、办理总包备案、签订补充协议，我方同意承担违约责任。

6、我方同意提供按照招标人可能要求的与其投标有关的一切数据和资料。

7、 我方完全理解招标人不一定接受最低价的投标，并同意招标人对此可以不作任何解释。

8、 我方将按招标文件要求，提供保证金或保函。

9、我方保证在此次投标期间，不以任何方式行贿及串标，如有发现，愿被取消投标资格并同意招标人没收投标保证金。

10、 我方知道并同意，如果接到中标通知后未按招标人要求的时间签署合同及补充协议或坚持提出附加条件,投标人有权另选其他中标单位并承担违约责任。

投标人：_____（公章）
法定代表人或其授权代表：_____（签字或盖章）
日　　期：_____年_____月_____日

二、 法定代表人资格证明书

单位名称：_____

地址： _____

成立时间：_____

经营期限：_____

姓名：_____性别：_____

年龄：_____职务：_____系_____（投标单位名称）的法定代表人。为施工、竣工和保修工程，签署上述工程的投标文件、进行合同谈判、签署合同和处理与之有关的一切事务。

特此证明

附：法定代表人身份证复印件

投标人：_____（公章）
法定代表人或其授权代表：_____（签字或盖章）
日 期：____年____月____日

三、 授权委托书

本授权委托书申明：我_____（姓名）系_____（投标单位名称）的法定代表人，现授权委托_____（单位名称）的_____（姓名，身份证号码_____）为我公司代理人，以本公司的名义参加_____（招标单位）的_____（项目名称）的投标活动。代理人在开标、评标、合同谈判过程中所签署的一切文件和处理与之有关的一切事务，我均予以承认。

代理人无转委托权。特此委托。

各方在此分别签字，以兹证明。

附：委托代表人身份证复印件

代理人：_____ 性别：_____ 年龄：_____

身份证号码：_____ 职务：_____

投标单位：_____（盖章）

法定代表人：_____（签字、盖章）

授权委托日期：_____年_____月_____日

四、 报价汇总表

项目编号：SZKJ-ZB-2022-002　　货币单位： 元

<table>
<tr><td>项目名称</td><td colspan="6"></td></tr>
<tr><td>投标单位</td><td colspan="6"></td></tr>
<tr><td rowspan="8">投标报价
（元）</td><td colspan="2">一、数据中心建设</td><td colspan="4"></td></tr>
<tr><td colspan="2">二、云平台建设</td><td colspan="4"></td></tr>
<tr><td colspan="2">三、1 号地块建设</td><td colspan="4"></td></tr>
<tr><td colspan="2">四、2 号地块建设</td><td colspan="4"></td></tr>
<tr><td colspan="2">五、3 号地块建设</td><td colspan="4"></td></tr>
<tr><td colspan="2">六、4 号地块建设</td><td colspan="4"></td></tr>
<tr><td colspan="6">总报价：大写：_____
小写：_____</td></tr>
<tr><td>工期要求</td><td colspan="6">工期：250 天。</td></tr>
<tr><td>项目负责人</td><td>姓名</td><td></td><td>身份证号</td><td></td><td>资质证书</td><td></td></tr>
<tr><td>备　注</td><td colspan="6"></td></tr>
</table>

注：1、报价一经涂改，应在涂改处加盖单位公章或投标人代表签字或盖章，否则其投标作无效标处理。

2、投标费用包括项目实施所需的人工费、服务费、税费、服务费及其他一切费用。

3、投标人按格式填列，不得自行更改。否则引起的不利后果由投标人承担。

4、总价不得高于招标文件要求的最高限价，否则其投标作无效标处理。

投标人：_____（公章）

法定代表人或其授权代表：_____（签字或盖章）

日　　期：　　年　　月　　日

五、 工程量报价清单

根据招标文件第四章内容提供（格式自拟）

六、 联合体投标声明文件

致：德阳市数字科技城开发有限公司（招标人）：

兹有_____自愿组成联合体，共同参加“_____（项目名称）项目（项目编号：_____）的投标。现就联合体参加本项目投标的有关事宜达成下列协议：

一、联合体各方应承担的工作和义务具体如下：

牵头方_____（公司全称）

成员方_____（成员公司全称）

由_____代表联合体办理参加本项目投标的有关事宜（包括但不限于：派出投标人代表、提交投标文件及参加开标、谈判、澄清等），在此过程中，联合体各方授权同一人为本项目的被授权代表，投标人代表签字及牵头方盖章的一切文件和处理结果，联合体均予以认可并对此承担责任。

2、联合体各方约定由_____（公司全称）代表联合体办理投标保证金事宜。

3、根据招标文件的要求，本项目采用最低价中标，联合体只能确定由其中一方的条件参与商务部分的评标。因此，联合体各方约定以_____（公司全称）的条件参与商务部分的提交。

4、牵头方_____（公司全称）：_____（工作及义务的具体内容）

成员方_____（成员公司全称）：_____（工作及义务的具体内容）

三、若中标，牵头方将代表联合体与招标人就合同签订事宜进行协商；若协商一致，则联合体各方将共同与招标人签订合同，并就合同约定的事项对招标人承担连带责任。

四、本协议自签署之日起生效，合同履行完毕后自动失效。

附；营业执照复印件

牵头方：_____（盖单位公章）

法定代表人或其委托代理人：_____（签字或盖章）

成员一：_____（盖单位公章）

法定代表人或其委托代理人：_____（签字或盖章）

签署日期：____年____月____日

七、 投标人应提交的资格证明材料

1、 营业执照复印件

2、 企业资质证书复印件

3、 项目负责人资质资料及资质证书复印件（格式自拟）

4、 其他项目人员资料及资质证书复印件

八、 投标报价需要的其他资料（若有）

第六章　技术文件格式

技术文件

（填写正本或副本）

项目名称：_____

项目编号 ：_____

投标人名称：_____（盖公章）

投标人地址：_____

法定代表人或其授权代表：_____（签名或盖章）

日期：_2022__年_____月_____日

一、 技术文件内容承诺

技术文件主要对技术需求进行承诺（格式自拟）

二、 技术偏差表

序 号	招标文件技术要求	投标技术偏差	偏离情况说明
1			
2			
3			

投标人：_____（公章）
法定代表人或其授权代表：_____（签字或盖章）
日　　期：_____年_____月_____日

各投标单位投标时，若对招标人的技术条款出现偏差，请例入偏差表内，作为招标人评标依据之一。