

资格评审汇总表

项目编号：E4109005080D03830001002
项目名称：濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	评审项目	评审标准	郑州衡量科技股份有限公司	河南穗昂智能科技有限公司	濮阳市科信电脑有限公司	中国联合网络通信有限公司濮阳市分公司	中电信数智科技有限公司河南分公司
1	具有独立承担民事责任的能力	提供企业法人或者其他组织的营业执照等证明文件或自然人的身份证明	通过	通过	通过	通过	通过
2	具有良好的商业信誉和健全的财务会计制度的证明文件	提供2023年度财务审计报告或银行出具的资信证明，企业成立不足一年的从成立之日起计算	通过	通过	通过	通过	通过
3	有依法缴纳税收和社会保障资金的良好记录	提供2023年度任意一个月的缴纳税收凭据和社会保险凭据，依法免税或不需要缴纳社会保障资金的供应商应提供相应的证明文件	通过	通过	通过	通过	通过
4	履行合同所必须的设备和专业技术能力的材料	具有履行合同所必需的设备和专业技术能力；提供证明或承诺，格式自拟	通过	通过	通过	通过	通过
5	前三年内无重大违法记录声明	参加政府采购活动前三年内，在经营活动中没有重大违法记录（提供承诺，格式自拟）	通过	通过	通过	通过	通过
6	信用记录	根据《关于在政府采购活动中查询及使用信用记录有关问题的通知》（财库[2016]125号）和豫财购【2016】15号的规定，被列入失信被执行人、重大税收违法失信主体、政府采购严重违法失信行为记录名单，拒绝其参与本次政府采购活动。通过“信用中国”网站（http://zxgk.court.gov.cn/shixin/）查询“失信被执行人”、通过“信用中国”网站 www.creditchina.gov.cn 查询“重大税收违法失信主体”、“政府采购严重违法失信行为记录名单”，通过“中国政府采购网”（www.ccgp.gov.cn）对“政府采购严重违法失信行为信息记录”查询（项目开标后，采购人通过互联网对供应商信用信息进行查询并负责保留查询信息，供应商不再提供）	通过	通过	通过	通过	通过
7	其他	法律、行政法规规定的其他条件	通过	通过	通过	通过	未通过
8	本项目（是/否）接受联合体	否	通过	通过	通过	通过	通过
结论			通过	通过	通过	通过	否决投标

资格评审汇总表

项目编号: E4109005080D03830001002

项目名称: 濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

全体评委签字:

吴伟

杨利花

陈少

日期: 2024年12月27日

濮阳市公共资源交易中心

符合性评审汇总表

项目编号：E4109005080D03830001002
项目名称：濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	评审项目	评审标准	郑州衡量科技股份有 限公司	河南穗昂智能科技有 限公司	濮阳市科信电脑有限 公司	中国联合网络通信有 限公司濮阳市分公司
1	响应函、首次报价一 览 表及签字盖章	有法定代表人（单位负责人）或其委托代理人签字 或加盖单位章。由法定代表人（单位负责人） 签 字的，应附法定代表人（单位负责 人）身份证明， 由代理人签字的，应附授权委托书，身份证明或授 权委托书应符合第六章“ 响应文件格式 ”的规定	通过	通过	通过	通过
2	报价	符合第二章“供应商须知 ”规定，供应商的报价不 得超过相应标包最高限价。	通过	通过	通过	通过
3	响应范围	符合第二章“供应商须知 ”规定	通过	通过	通过	通过
4	项目地点	符合第二章“供应商须知 ”规定	通过	通过	通过	通过
5	服务期限	符合第二章“供应商须知 ”规定	通过	通过	通过	通过
6	质量标准	符合第二章“供应商须知 ”规定	通过	通过	通过	通过
7	权利义务	符合第二章“供应商须知 ”规定和第四章“政府采 购合同 条款 ”中的实质性要求和条件	通过	通过	通过	通过
8	服务方案	符合第五章“采购需求 ”中的实质性要求和条件	通过	通过	通过	通过
9	附加条件	响应文件中不得含有采购人不能接受的附加条件	通过	通过	通过	通过
结论			通过	通过	通过	通过

全体评委签字：

吴凤伟 杨利花 陈建

日期：2024年12月27日

磋商汇总表

项目编号: E4109005080D03830001002
项目名称: 濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	评审项目	评审标准	郑州衡量科技股份有限公司	河南穗昂智能科技有限公司	濮阳市科信电脑有限公司	中国联合网络通信有限公司濮阳市分公司
1	磋商	是否对磋商内容进行有效响应	通过	通过	通过	通过
结论			通过	通过	通过	通过

全体评委签字:

吴凤伟 杨利花 陈斌

日期: 2024年12月27日

主观分评审汇总表

项目编号: F4109005080D03830001002

项目名称: 濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	评审项目	标准分	评分标准	郑州衡量科技股份有限公司	河南穗昂智能科技有限公司	濮阳市科信电脑有限公司	中国联合网络通信有限公司濮阳市分公司
1	安全保障措施	5	(1) 根据对本项目具体要求制定安全保障措施, 包括但不限于网络接入实施, 网络、数据、用户登录等不可预见安全因素、突发事件及安全隐患处理方案、保密措施等。 (2) 安全保障措施内容完整无缺项, 可行性强, 科学合理的得5分; (3) 安全保障措施内容不完整、有缺项, 可行性、合理性一般的得3分; (4) 安全保障措施内容不完整、有缺项, 可行性、合理性较差的得1分; 不提供不得分。	3	4.33	2.33	5
2	培训方案	3	培训方案包含但不限于培训计划、培训模式、培训对象、解决问题和取得效果等内容。 (1) 方案详细完整, 科学合理, 针对性和可行性强, 得3分; (2) 方案详细完整, 科学合理, 针对性和可行性较强, 得2分; (3) 方案基本完整, 基本可行, 得1分; (4) 不提供不得分。	2	2	1.67	3
3	售后服务方案	3	根据售后服务方案中售后服务承诺、服务保障措施、售后服务方式、服务响应时间、故障处理措施、售后服务团队、人员培训计划等进行综合评价: (1) 方案非常完善、详细, 针对性及适用性强的, 得3分; (2) 方案较完善、详细, 针对性及适用性较强的, 得2分; (3) 方案欠完善、不详细, 针对性及适用性一般的, 得1分; (4) 不提供不得分。	2	2	1.33	3

主观分评审汇总表

项目编号：F4109005080D03830001002
项目名称：濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	评审项目	标准分	评分标准	郑州衡量科技股份有限公司	河南穗昂智能科技有限公司	濮阳市科信电脑有限公司	中国联合网络通信有限公司濮阳市分公司
4	实施方案	3	评委根据投标人提供的本项目实施方案，包括实施计划、实施流程、项目组织架构、项目过程管理及实施进度等内容综合评价。 (1) 实施方案内容全面且实施计划、流程、进度等设计科学合理、可操作性强、针对性强，得3分； (2) 实施方案内容较为全面且实施计划、流程、进度等设计较为科学合理、基本具备可行性，得2分； (3) 实施方案内容缺失较多且实施计划、流程、进度等设计不科学，得1分 (4) 不提供不得分。	2	2	1.33	3
合计				9	10.33	6.67	14

全体评委签字：

吴凤伟

杨利花

陈建

日期：2024年12月27日

客观分评审汇总表

项目编号：F4109005080D03830001002
项目名称：濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	评审项目	标准分	评分标准	郑州衡量科技股份有限公司	河南穗昂智能科技有限公司	濮阳市科信电脑有限公司	中国联合网络通信有限公司濮阳市分公司
1	采购需求响应	35	供应商所投技术参数完全符合或优于磋商文件要求的，得满分35分。 技术参数中加“★”部分每有一项参数负偏离磋商文件要求的，在满分的基础上扣5分；扣完为止。 技术参数中未加“★”部分每有一项参数负偏离磋商文件要求的，在满分的基础上扣0.5分；扣完为止，不作为废标处理。 注：1.合同签订前及履行过程中发现本项有虚假者，取消其中标资格，并追究供应商相应的法律责任和对采购人进行相应的赔偿。 2.相关证明文件（在技术偏离表中标注证明材料所在响应性文件对应的页码）。	35	35	35	35
2	企业实力	6	投标人具有《质量管理体系认证证书》、《职业健康安全管理体系认证证书》、《环境管理体系认证证书》、《信息安全管理体系认证证书》每章一项得1分，《信息安全服务资质认证证书》得2分，最高得分6分。注：以上电子投标文件附有有效状态证书扫描件并加投标人公章，否则不得分。	3	0	0	6
3	拟派驻项目负责人	4	拟派驻本项目项目负责人具有：具有项目管理（PMP）或计算机相关专业高级及以上证书的，得4分，具有网络工程师（中级）的得2分，不提供不得分。 注：以上证书需提供原件扫描件并加盖供应商公章，且员工社保证明中须有该人员2024年1月以来任意1个月缴纳社保的信息，以证明其人员在本单位，不提供不得分。	0	0	0	4
4	项目团队成员	5	项目组成员具有（除项目负责人）：省级及以上人力资源和社会保障厅认证通过的相关专业高级技术职称得3分，具有注册信息安全工程师证书的得2分。 注：以上证书需提供原件扫描件并加盖供应商公章，且员工社保证明中须有该人员2024年1月以来任意1个月缴纳社保的信息，以证明其人员在本单位，不提供不得分。	0	0	0	5
5	企业业绩	6	投标人2021年1月1日（以合同签订时间为准）以来，投标人具有本项目类似项目业绩，每有1个得2分，本项最多得6分。 注：投标文件中附合同（或协议书）和中标通知书的原件扫描件，不提供不得分。	0	0	0	6

客观分评审汇总表

项目编号：F4109005080D03830001002
项目名称：濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	评审项目	标准分	评分标准	郑州衡量科技股份有限公司	河南穗昂智能科技有限公司	濮阳市科信电脑有限公司	中国联合网络通信有限公司濮阳市分公司
合计				38	35	35	56

全体评委签字： 吴凤伟 杨利花 陈少

日期：2024年12月27日

投标报价评分表

项目编号: E4109005080D03830001002
项目名称: 濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包
日期: 2024年12月27日

序号	投标人名称	投标报价(元)	最后报价(元)	中小微企业扣除价格(元)	评审价格(中小微企业扣除后价格)(元)	投标报价得分
1	中国联合网络通信有限公司濮阳市分公司	595	594.5	0	594.5	30
2	郑州衡量科技股份有限公司					29.75
3	河南穗昂智能科技有限公司					29.77
4	濮阳市科信电脑有限公司					29.97
评标基准价: 594.5		投标报价权重: 0				

全体评委签字: 吴凤伟 杨利花 陈文

日期: 2024年12月27日

评分汇总表

项目编号: E4109005080D03830001002
项目名称: 濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	投标人名称	最终报价 (元)	主观分评审得分	客观分评审得分	投标报价算得分	得分合计	排名
1	中国联合网络通信有限公司濮阳市分公司	594.5	14	56	30	100	1
2	郑州衡量科技股份有限公司					76.75	2
3	河南穗昂智能科技有限公司					75.1	3
4	濮阳市科信电脑有限公司					71.64	4

全体评委签字: 吴伟 杨利花 陈少

日期: 2024年12月27日

推荐中标候选人

项目编号: E4109005080D03830001002
项目名称: 濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

投标人名称	最后报价(元)	评标价格(元)	排名
中国联合网络通信有限公司濮阳市分公司	594.5	594.5	1
郑州衡量科技股份有限公司			2
河南穗昂智能科技有限公司			3
濮阳市科信电脑有限公司			4

全体评委签字： 吴凤伟 杨利花 陈少奎

日期: 2024年12月27日

濮阳市公共资源交易中心

否决投标情况表

项目编号: F4109005080D03830001002
项目名称: 濮阳市社会医疗保险中心濮阳市基层定点医疗机构网络安全接入服务项目第二标包

序号	投标单位	评审流程	否决情况	否决投标原因
1	中电信数智科技有限公司河南分公司	资格评审	否决投标	杨利花:供应商法定代表人为同一人或者存在 控股、管理关系的不同单位; 内容描述不一致; 不符合招标文件要求。 吴凤伟:供应商法定代表人为同一人或者存在 控股、管理关系的不同单位; 内容描述不一致; 不符合招标文件要求。 陈少杰:投标文件未提供招标文件16.6和16.7项承诺(供应商不得存在的情量, 供应商提供承诺, 格式自拟)。由于招标文件资格评审要求与评审系统评审要求不一致, 评审委员会严格按照招标文件的要求评审, 该投标人投标文件没有提供招标文件资格评审第六项规定要求, 资格评审不通过。

全体评委签字: 吴凤伟 杨利花 陈少杰

日期: 2024年12月27日

最后报价

序号	产品名称	品牌型号	数量	单价	备注
1	物联网卡	联通自制	800	300	包含三年流量费
2	CA身份认证	北京世纪龙脉/mTokenGM300	800	120	/
3	零信任客户端	深信服/深信服零信任接入授权软件V2.0	800	174.5	/
备注：/					

注：采用电子招标投标(采购)时，按交易中心系统要求格式填报。

供应商名称(盖单位章)：中国联合网络通信有限公司濮阳分公司

法定代表人或其委托代理人(签字)：王艳艳

日期：2024 年 12 月 9 日



二、商务和技术偏差表

序号	采购文件章节及条款号	响应文件章节及条款号	偏差说明
1	第二章供应商须知 3.1 采购范围 实现基层定点医疗机构安全规范接入省医保信息平台。组织濮阳市基层定点医疗机构通过国家医疗保障局颁发的数字证书及运营商 4G/5G VPDN 网络，完成基层定点医疗机构省医保信息平台准入认证及网络安全接入，满足基层医保业务经办和就医结算需要	二、首次报价一览表响应范围 实现基层定点医疗机构安全规范接入省医保信息平台。组织濮阳市基层定点医疗机构通过国家医疗保障局颁发的数字证书及运营商4G/5G VPDN 网络，完成基层定点医疗机构省医保信息平台准入认证及网络安全接入，满足基层医保业务经办和就医结算需要 见P2	无偏差
2	第二章供应商须知 3.3 项目地点 采购人指定地点	二、首次报价一览表项目地点 采购人指定地点 见P2	无偏差
3	第二章供应商须知 3.4 服务期限 3 年（运维服务及免费流量费用）	二、首次报价一览表服务期限 3 年（运维服务及免费流量费用） 见P2	无偏差
4	第二章供应商须知 3.5 质量标准 合格，符合国家及行业相关标准并满足采购人实际需求，确保信息平台网络安全接入；	二、首次报价一览表质量标准 合格，符合国家及行业相关标准并满足采购人实际需求，确保信息平台网络安全接入； 见P2	无偏差
5	第二章供应商须知 4.2 预算金额 第一标包：600元/基层服务点（2400个基层定点医疗机构）第二标包：600元/基层服务点（800个基层定点医疗机构）4.3 最高限价 第二标包：600 元/基层服务点（800 个基层定点医疗机构），服务商以基层定点单价进行报价，不得超过相应标包最高限价，否则响应文件无效。	二、首次报价一览表报价（元/个），以基层定点单价进行报价，不超过相应标包最高限价。 见P2	无偏差
6	第二章供应商须知11 采购进口产品或服务：本采购项目拒绝进口产品或服务参加磋商	六、资格审查资料6.9不使用进口产品的声明函见 P175	无偏差
7	第二章供应商须知 28 磋商有效期 磋商有效期为 60 天。磋商有效期从提交首次响应文件的截止之日起算。响应文件中承诺的磋商有效期应当不少于磋商文件中载明的磋商有效期	二、首次报价一览表响应有效期 磋商有效期为60天。磋商有效期从提交首次响应文件的截止之日起算。响应文件中承诺的磋商有效期不少于磋商文件中载明的磋商有效期 见P2	无偏差
8	第三章 资格审查、符合性审查和评审方法（综合评分法）*2、符合性审查：权利义务符合第二章“供应商须知”规定和第四章“政	权利义务符合第二章“供应商须知”规定和第四章“政府采购合同条款”中的实质性要求和条件	无偏差

	府采购合同条款”中的实质性要求和条件		
9	物联网卡 1、工业级插拔物联网卡：工作温度-40-105℃、震动5Hz-500Hz、静电保护ESD>4000V、数据保存年限不低于10年，尺寸支持2FF和3FF两种规格 2、传输速率：物联网卡的上行速率不低于5M/S 3、物联网卡特性：能提供物联网通道型业务的物联网卡，开通物联网卡的业务项目后，具备实时传输图片、视频的功能，网络信号稳定，满足正常使用。 4、网络环境：提供4G网络运行环境，提供4G网络测试报告，4G网络覆盖率（RSRP-105dBm & SINR≥-3dB）不能低于96%。 5、流量：提供1年4G网络定向流量，不少于2G/每月 6、物联网业务管理平台：提供物联网业务管理平台，通过软件平台应用程序能够查询卡状态、位置信息、流量使用、套餐类型、客户资料管理（实现机卡绑定）、历史充值记录，服务内容等情况并对异常情况进行报警提示 7、卡品安装及售后：物联网卡的安装及使用如有损坏响应人1小时内对客户故障及时处理 8、加密传输：支持VPDN加密传输，GRE隧道定向APN，绑定固定IP 9、物联网卡套餐：物联网卡支持流量池套餐 10、访问限制：支持定向流量服务 11、平台对接能力：完善的API开放能力接口 12、平台支持运营商类型：所有运营商物联网卡接入 13、卡托（uFi）：提供物联网卡托，要求卡托小巧便捷、即插即用；网络稳定、支持	物联网卡 1、工业级插拔物联网卡：工作温度-40-105℃、震动5Hz-500Hz、静电保护ESD>4000V、数据保存年限10年，尺寸支持2FF和3FF两种规格 2、传输速率：物联网卡的上行速率5M/S 3、物联网卡特性：能提供物联网通道型业务的物联网卡，开通物联网卡的业务项目后，具备实时传输图片、视频的功能，网络信号稳定，满足正常使用。 4、网络环境：提供4G网络运行环境，提供4G网络测试报告，4G网络覆盖率（RSRP-105dBm & SINR-3dB）不能低于96%。 5、流量：提供1年4G网络定向流量，2G/每月 6、物联网业务管理平台：提供物联网业务管理平台，通过软件平台应用程序能够查询卡状态、位置信息、流量使用、套餐类型、客户资料管理（实现机卡绑定）、历史充值记录，服务内容等情况并对异常情况进行报警提示 7、卡品安装及售后：物联网卡的安装及使用如有损坏响应人1小时内对客户故障及时处理 8、加密传输：支持VPDN加密传输，GRE隧道定向APN，绑定固定IP 9、物联网卡套餐：物联网卡支持流量池套餐 10、访问限制：支持定向流量服务 11、平台对接能力：完善的API开放能力接口 12、平台支持运营商类型：所有运营商物联网卡接入 13、卡托（uFi）：提供物联网卡托，要求卡托小巧便捷、即插即用；网络稳定、支持wifi6入网协议。 14、客户列表：具备客户管理（基本资料）、资质审核、企业明细功能模块（提供功能截图见P272 11.1（1）） 15、卡板管理：具有卡板列表、卡板回收、卡板	无偏差

wifi6入网协议。	统计、流量查询、实名列表、我的卡池功能模块（提供功能截图见P272 11.1（2））
14、客户列表：具备客户管理（基本资料）、资质审核、企业明细功能模块（提供功能截图）	16、库存管理：具有库存列表、入库记录、出库记录、标识管理功能模块（提供功能截图见P272 11.1（3））
15、卡板管理：具有卡板列表、卡板统计、流量查询、实名列表、我的卡池功能模块（提供功能截图）	17、运维管理：具有通道管理功能模块（提供功能截图见P273 11.1（4））
16、库存管理：具有库存列表、入库记录、出库记录、标识管理功能模块（提供功能截图）	18、短信管理：具有短信收发、短信记录功能模块（提供功能截图见P273 11.1（5））
17、运维管理：具有通道管理功能模块（提供功能截图）	19、定位管理：★具有定位查询、查询记录功能模块（提供功能截图见P273 11.1（6））
18、短信管理：具有短信收发、短信记录功能模块（提供功能截图）	20、消息中心：具有消息列表、添加通知功能模块
19、定位管理：★具有定位查询、查询记录功能模块（提供功能截图）	21、统计分析：具有利润统计、激活统计、在网统计功能模块（提供功能截图见P273 11.1（7））
20、消息中心：具有消息列表、添加通知功能模块（提供功能截图）	22、续费管理：具有续费服务、套餐变更、前/后向流量池功能模块
21、统计分析：具有利润统计、激活统计、在网统计功能模块（提供功能截图）	23、系统管理：1、具有管理员管理、角色管理、日志列表、更新日志、轮询进度、系统参数、其他操作、停复进度功能模块（提供功能截图见P274 11.1（8））
22、续费管理：具有续费服务、套餐变更、前/后向流量池功能模块（提供功能截图）	24、系统管理：2、★2、省、市、县三级组织架构：系统支持自定义组织架构设置，不同组织架构可分配不同权限（提供功能截图及接入介绍见P274 11.1（9））
23、系统管理：1、具有管理员管理、角色管理、日志列表、更新日志、轮询进度、系统参数、其他操作、停复进度功能模块（提供功能截图）	25、资源管理：★全省ip地址管理：省平台代理网关建立加密隧道访问医保核心业务区网络，并进行IP地址统一管理（提供功能截图及详细介绍见P274 11.1（10））
24、系统管理：2、★2、省、市、县三级组织架构：系统支持自定义组织架构设置，不同组织架构可分配不同权限（提供功能截图及接入介绍）	
25、资源管理：★全省ip地址管理：省平台代理网关建立加密隧道访问医保核心业务区网络，并进行IP地址统一管理（提供功能截图及详细介绍）	

10	CA身份认证 1、产品资质：产品具备国家密码管理局颁发的商用密码产品认证证书 2、接口环境：供电：符合USB规范，由USB总线供电，无需额外电源；主机接口：符合USB2.0规范，兼容USB1.1，兼容3.0规范接口；工作电流<60mA；功率<300 mW；工作温度0° C ~ 70° C；存放温度-20° C ~ 85° C；湿度<90%RH 3、产品要求：符合ISO7816 系列标准；符合CE和FCC标准；采用高性能、大容量内嵌智能芯片（32位高性能智能卡芯片）；用户存储空间128KB；数据存储空间不低于128KB；数据存储空间：不小于10年，可擦写10万次以上；具有唯一硬件序列号，并可查询；支持RSA（1024/2048位）；支持SM1/SM2/SM3/SM4，SSF33（256位）系列算法；支持DES，3DES，AES128/192/256；支持SHA1/SHA256/SHA384/SHA512对称算法支持ECB、CBC、CFB、OFB模式；支持密钥生成、存储、更新等芯片级密钥管理控制；验证及运算过程在硬件内部完成，私钥永不出Key；具有多种对抗攻击的安全检测和保护手段 4、造作系统：支持Windows XP/ Win7/ Win8.1/ Win10；支持Windows Server 2003/2008/2012；支持Linux，Mac OS X操作系统；支持中标麒麟操作系统；支持银河麒麟操作系统；支持统信UOS操作系统 5、接口类型：支持国密SKF；支持Microsoft CryptoAPI（CSP）；支持PKCS#11；支持SSL v3；支持X.509 v3标准证书格式；支持RSA/SM2且同时支持SKF / CSP / P11接口互通调用；支持移动端设备中间件接口；支持跨平台多浏览器（Chrome/ Firefox/Safari / IE /Edge等）	CA身份认证 1、产品资质：产品具备国家密码管理局颁发的商用密码产品认证证书见P275 11.1.2 2、接口环境：供电：符合USB规范，由USB总线供电，无需额外电源；主机接口：符合USB2.0规范，兼容USB1.1，兼容3.0规范接口；工作电流<60mA；功率<300 mW；工作温度0° C ~ 70° C；存放温度-20° C ~ 85° C；湿度<90%RH 3、产品要求：符合ISO7816 系列标准；符合CE和FCC标准；采用高性能、大容量内嵌智能芯片（32位高性能智能卡芯片）；用户存储空间128KB；数据存储空间：10年，可擦写10万次以上；具有唯一硬件序列号，并可查询；支持RSA（1024/2048位）；支持SM1/SM2/SM3/SM4，SSF33（256位）系列算法；支持DES，3DES，AES128/192/256；支持SHA1/SHA256/SHA384/SHA512对称算法支持ECB、CBC、CFB、OFB模式；支持密钥生成、存储、更新等芯片级密钥管理控制；验证及运算过程在硬件内部完成，私钥永不出Key；具有多种对抗攻击的安全检测和保护手段 4、造作系统：支持Windows XP/ Win7/ Win8.1/ Win10；支持Windows Server 2003/2008/2012；支持Linux，Mac OS X操作系统；支持中标麒麟操作系统；支持银河麒麟操作系统；支持统信UOS操作系统 5、接口类型：支持国密SKF；支持Microsoft CryptoAPI（CSP）；支持PKCS#11；支持SSL v3；支持X.509 v3标准证书格式；支持RSA/SM2且同时支持SKF / CSP / P11接口互通调用；支持移动端设备中间件接口；支持跨平台多浏览器（Chrome/ Firefox/Safari / IE /Edge等） 6、外壳封装：支持多种金属外壳、颜色选择 7、权限管理：提供自动锁死功能，支持远程解锁 8、性能参数：生成1024位RSA密钥对所需的时间：1秒；RSA（1024位）签名所需的时间：20次/秒	无偏差
----	---	---	-----

	6、外壳封装：支持多种金属外壳、颜色选择 7、权限管理：提供自动锁死功能，支持远程解锁 8、性能参数：生成1024位RSA密钥对所需的时间：不大于1秒；RSA（1024位）签名所需的时间：不小于20次/秒；RSA验签时间（1024位）：不小于20次/秒；RSA公私钥对生成时间（2048位）：不多于5秒；RSA签名时间（2048位）：不小于12次/秒；RSA验签时间（2048位）：不小于12次/秒；SM2公私钥对生成时间：每次不大于0.1秒；SM2签名时间：不小于30次/秒；SM2验签时间：不小于30次/秒；第一次插入计算机后的硬件识别速度不大于20秒；二次拔插后的识别速度不大于10秒 9、系统兼容：兼容国家医疗保障局身份认证和授权管理系统，能够与证书综合管理系统 FCMS 对接。 10、技术规范：GM/T 0027《智能密码钥匙技术规范》；GM/T0028《密码模块安全技术要求》第二级要求 11、服务：提供三年产品原厂维保服务	；RSA验签时间（1024位）：20次/秒；RSA公私钥对生成时间（2048位）：5秒；RSA签名时间（2048位）：12次/秒；RSA验签时间（2048位）：12次/秒；SM2公私钥对生成时间：每次0.1秒；SM2签名时间：30次/秒；SM2验签时间：30次/秒；第一次插入计算机后的硬件识别速度20秒；二次拔插后的识别速度10秒 9、系统兼容：兼容国家医疗保障局身份认证和授权管理系统，能够与证书综合管理系统 FCMS 对接。 10、技术规范：GM/T 0027《智能密码钥匙技术规范》；GM/T0028《密码模块安全技术要求》第二级要求 11、服务：提供三年产品原厂维保服务见P277 11.1.2.1生产厂商售后服务承诺函	
11	零信任客户端 （1）符合 GM/T0024 标准或GM/T0025 标准要求，以及符合GM/T0028《密码模块安全技术要求》第二级的《商用密码产品认证证书》。（2）零信任客户端支持接入省级控制中心，且控制中心与客户端接口完整适配，保障省级控制中心的访问权限管理等安全策略能够下发至客户端且执行，客户端能够收集控制中心开展信任评估需要的信息，提供接入方式技术可行性文件。（3）零信任客户端需与省级CA身份认证方式进行准入，认证通过与省平台代理网关建立加密隧道，单点登陆访问医保核心业务区网络，提供详细技术文件（需体现技术对接过程及效果截图）。	零信任客户端 （1）我公司所提供零信任客户端符合GM/T0024标准或 GM/T0025 标准要求，以及符合GM/T0028《密码模块安全技术要求》第二级的《商用密码产品认证证书》。 （2）我公司所提供零信任客户端支持接入省级控制中心，且控制中心与客户端接口完整适配，保障省级控制中心的访问权限管理等安全策略能够下发至客户端且执行，客户端能够收集控制中心开展信任评估需要的信息，已提供接入方式技术可行性文件见P278 11.1.3（1）。 （3）我公司所提供零信任客户端可以与省级CA身份认证方式进行准入，认证通过与省平台代理网关建立加密隧道，单点登陆访问医保核心业务	无偏差

(4) 为保障客户端与服务端对接符合此次建设需求,保障顺利接入调试,要求投标人提供由设备生产厂商和网络服务商出具的技术证明文件,文件内容说明已经对接并调试成功,要求证明文件加盖投标人公章。 零信任客户端支持国密加密算法(SM2/SM3/SM4)进行SSL加密,保障SSL隧道接入的安全性。 (6) 零信任客户端可针对接入电脑终端情况进行检测、信息收集和上报能力,并实现可信应用识别,检测项包括但不限于应用种类、应用的进程信息、终端MAC地址、操作系统及版本、操作系统是否存在漏洞、是否运行杀毒软件、是否开启本地系统防火墙、接入地市等,省级控制中心进行信任评估,并下发安全管控策略。提供证明截图及详细介绍。 (7) 零信任客户端可针对发布的应用开启WEB水印,水印内容包括不限于登陆用户名、当前年月日,提供证明截图及详细介绍。 ★(8) 为保障访问医保业务的稳定性,零信任客户端应支持给予TCP的协议优化,针对访问隧道的抗丢包、抗抖动等特性进行增强,提供证明截图及详细介绍。 ★(9) 零信任客户端应兼容主流非国产终端和非国产操作系统、主流国产终端和国产操作系统,提供兼容性列表。 (10) 要求零信任客户端具备医保接入网管理能力,可自定义上传医保虚拟网络域图标,并在客户端切换处显示该图标及图标名称,例如图标名称为河南省医保接入客户端,在客户端成功切换到医保接入网时,桌面显示提升成功提示语,提示语由省医保局统一自定,提供能力效果证明文件。 (11) 在终端访问医保信息业务时,零信任客户端支持检测终端是否接入互联网。如发现终端违规接入互联网情况,零信任客户端自动掉线,断开与医保信息业	区网络,已提供详细技术文件(在技术文件中已体现技术对接过程及效果的截图)见P280 11.1.3 (2) (4) 我公司已提供由设备生产厂商和网络服务商出具的技术证明文件,文件内容说明已经对接并调试成功,证明文件已加盖我公司公章。见P281 11.1.3 (3) (5) 我公司所提供零信任客户端支持国密加密算法(SM2/SM3/SM4)进行SSL加密,保障SSL隧道接入的安全性。 (6) 我公司所提供零信任客户端可针对接入电脑终端情况进行检测、信息收集和上报能力,并实现可信应用识别,检测项包括但不限于应用种类、应用的进程信息、终端MAC地址、操作系统及版本、操作系统是否存在漏洞、是否运行杀毒软件、是否开启本地系统防火墙、接入地市等,省级控制中心进行信任评估,并下发安全管控策略。已提供证明截图及详细介绍。见P286 11.1.3 (4) (7) 我公司所提供零信任客户端可针对发布的应用开启WEB水印,水印内容包括不限于登陆用户名、当前年月日,已提供证明截图及详细介绍。见P289 11.1.3 (5) ★(8) 为保障访问医保业务的稳定性,我公司所提供零信任客户端支持给予TCP的协议优化,针对访问隧道的抗丢包、抗抖动等特性进行增强,已提供证明截图及详细介绍。见P290 11.1.3 (6) ★(9) 我公司所提供零信任客户端兼容主流非国产终端和非国产操作系统、主流国产终端和国产操作系统,已提供兼容性列表。见P292 11.1.3 (7) (10) 我公司所提供零信任客户端具备医保接入网管理能力,可自定义上传医保虚拟网络域图标,并在客户端切换处显示该图标及图标名称,例
---	--

务的连接，提供能力效果证明截图。（12）在终端接入互联网情况下，零信任客户端弹出提醒，提醒已接入互联网无法访问医保信息平台，警示接入人员；同时可在接入互联网情况下访问医保信息平台时进行阻断，提供证明截图及详细技术介绍。（13）为保障零信任软件开发安全，保障产品本身无漏洞，要求所投产品制造商具备中国网络安全审查技术与认证中心的软件安全开发（一级）服务资质认证证书，提供资质复印件。 ★（14）为证明产品方案的成熟性与先进性，所投零信任产品需在2022年或2023年IDC中国零信任网络访问解决方案 厂商评估报告中位列综合排名前三的领导者位置，并出具由IDC盖章确认的证明文件。（15）提供三年原厂维保服务。	如图标名称为河南省医保接入客户端，在客户端成功切换到医保接入网时，桌面显示提升成功提示语，提示语由省医保局统一自定，已提供能力效果证明文件。见P293 11.1.3（8） （11）在终端访问医保信息业务时，我公司所提供零信任客户端支持检测终端是否接入互联网。如发现终端违规接入互联网情况，零信任客户端自动掉线，断开与医保信息业务的连接，已经提供能力效果证明截图。见P295 11.1.3（9） （12）在终端接入互联网情况下，我公司所提供零信任客户端弹出提醒，提醒已接入互联网无法访问医保信息平台，警示接入人员；同时可在接入互联网情况下访问医保信息平台时进行阻断，已提供证明截图及详细技术介绍。见P296 11.1.3（10） ★（13）为保障零信任软件开发安全，保障产品本身无漏洞，我公司所提供产品制造商具备中国网络安全审查技术与认证中心的软件安全开发（一级）服务资质认证证书，已提供资质复印件。见P298 11.1.3（11） ★（14）为证明产品方案的成熟性与先进性，我公司所提供零信任产品在2023年IDC中国零信任网络访问解决方案厂商评估报告中位列综合排名前三的领导者位置，已出具由IDC盖章确认的证明文件。见P299 11.1.3（12） （15）我公司提供三年原厂维保服务。见P300投标资格授权书
---	--

供应商保证：本表未填或未在本表列出的偏差，均视为供应商完全响应采购文件的全部要求。

供应商名称(盖单位章)：中国联合网络通信有限公司濮阳市分公司

法定代表人或其委托代理人(签字)：李艳艳

日期：2024年12月9日

七、服务方案

7.1 项目概况

为搭建安全、高效、全面的网络环境,实现村卫生室(所)、社区卫生服务中心(站)等基层定点医疗机构安全规范接入省医保信息平台,促进“一人一档”全民参保数据库建设,推进五级经办服务下沉及电子处方流转等工作落地应用。

本次采购需要实现全市所有村(社区)级定点医疗机构按照省局要求通过国家医保局颁发的数字证书及运营商4G/5G VPDN 网络,完成省医保信息平台准入认证及网络接入,满足基层医保业务经办和就医结算需要。具体需求如下:

1. 物联网接入服务: 开设网络运营商 4G/5G 专线物联网卡,物联网卡上行速率不低于5M/S, 定向流量不少于2G/月, 支持 VPDN 加密传输, 使用固定的IP地址及专用APN网络, 用于村(社区)级网络连接。建立物联网卡管理平台, 需具备查询卡状态、位置信息、流量使用、接入机构资料管理、机卡绑定等功能并能对异常情况进行报警提示, 具备开放的API 接口, 能够支持所有运营商物联网卡接入, 支持市、县二级组织架构管理, 提供的免费流量3年。

2. 身份认证服务: 村(社区)级须使用国家医保局 CA 身份认证系统颁发的数字证书, 用于网络接入时强身份鉴别。兼容国家医疗保障局身份认证和授权管理系统, 能够与证书综合管理系统对接, 提供三年维保服务。

3. 零信任接入服务: 在村(社区)级访问省医保信息平台时, 通过零信任客户端检测是否接入互联网, 如接入互联网, 客户端将弹出警示并自动断开与省医保信息平台的网络连接。零信任客户端支持接入省级控制中心, 且控制中心与客户端接口完整适配, 保障省级控制中心的访问权限管理等安全策略能够下发至客户端且执行, 零信任客户端需与省级 CA 身份认证方式进行准入, 认证通过与省平台代理网关建立加密隧道, 单点登陆访问医保核心业务区网络。为保障客户端与服务端对接符合此次建设需求, 保障顺利接入调试, 需提供对接成功的相关技术证明文件, 可被验证的案例或提供可被验证的有效实施方法。

4. 安装调试培训服务: 提供全市所有村(社区)级定点医疗机构的首次平台接入上线调试服务和使用的培训工作, 并开展为期三年的售后服务工作。

7.2 安全保障措施

7.2.1 网络接入实施

7.2.1.1 安装与调试

在本项目网络接入实施中，注重调试的系统性，尽可能将设备及附件的单体检测与试验、能独立进行的系统试验安排在施工过程中和系统调试前进行，以保证有足够的时间进行总体调试，缩短工期，并满足调试的质量要求。在调试安排上，先进行分层并行调试，分层调试好后再进行联合调试。

进行测试前组建一个调试小组，调试人员由具有丰富经验的人员组成，并将项目部内各专业组纳入调试小组，以便对调试进行统筹，同时在调试中遇到的问题能在最短时间内解决。调试组负责对整个工程的调试进行组织、安排、调试计划和方案的制定。

系统的调试在系统施工结束后进行。调试前应做好调试准备工作，按设计技术数据、查验设备的规格、型号、数量、备品、备件；按设计的要求检查系统各种控制点，检测点的施工质量，检查系统线路，检查后作好各项记录。确保调试时网络的安全。

系统经我方自检合格后，由我方的技术人员和学校负责老师一道，按编制的调试方案，使用专用的仪器、调试设备进行。施工过程中厂家监理人员对安装的设备、部件、材料及时进行检查、核对，保证安装部位及安装质量符合规范和设计要求。

对于施工进度符合开机条件的各分区控制系统等主要设备进行开机试验，进行功能检查，对系统设备、组件进行模拟试验检查、核对系统编码，保证分区系统运行正常，符合要求。其他各分项的系统安装进度条件符合联动控制试验检查时，与系统进行联动试验检查，检验远程控制功能、显示功能，保证联动控制设施符合规范和设计要求。

7.2.1.2 网络传输单元

网络传输单元主要由交换机、光纤收发器以及光纤等资源组成，实现卡口前端子系统与中心平台之间的互联互通。

7.2.1.3 网络传输设计

网络传输子系统由局域网、接入网和中心专网三部分组成。局域网采用独立网段，专用接入网完成路口数据汇聚至中心机房。中心专网完成平台服务器等中心设备互联。

7.2.2 突发事件及安全隐患处理方案

项目是在复杂的自然和社会环境中进行的，受众多因素的影响，非常可能发生损失、损害及危险，项目的过程和结果常常是出乎人们的意料，所以项目过程中存在一定的风险。为了保障项目的顺利进行，要充分认识到项目风险管理的重要性。对项目风险进行管理，成为项目管理的重要方面。

针对信息工程开发项目，风险的重要来源往往是系统变更引起的，但并不是所有风险都是由变更引起。对于一定要发生的变更，控制不必要的、随心所欲的变更，可减少因变更带来的风险。

完全避开或消除风险，或者只享受权益而不承担风险，是不可能的。需要对项目风险进行认真的分析，进行科学的管理，是能够避开不利条件，少受损失，取得预期的结果，实现项目目标的前提。

7.2.2.1 项目风险与风险管理

项目风险是一种不确定的事件或条件，一旦发生，会对项目目标产生某种正面或负面的影响。风险有其成因，同时，如果风险发生，会导致某种后果。项目风险既包括对项目目标的威胁，也包括促进项目目标的机会。风险源于存在于项目的不确定因素中。已知风险是那些已经经过识别和分析的风险，对于已知风险，进行相应的计划是可能的。对未知风险，虽然依据以往类似项目的经验，采取一定的应对措施，但往往是不易管理或者无法管理。

项目的不同阶段会有不同的风险，风险大多数随着项目的进展而变化，不确定性也随着变化。最大的不确定性存在于项目的早期，因此早期阶段做出的决策对以后阶段和项目目标的实现影响最大。

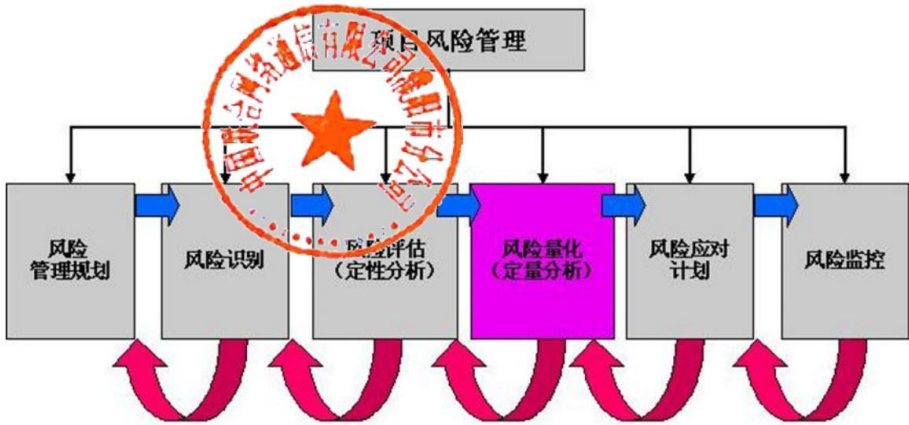
风险具有风险事件的随机性、风险的相对性、风险的可变性、等属性。

为了深入、全面的认识项目风险，并有针对性的进行管理，可以从不同的角度、根据不同的标准进行对风险分类。如：按风险后果划分、按风险来源划分、按风险影响范围划分等。

项目风险管理是对项目风险进行识别、分析和应对的系统的过程，并以此为基础合理的使用多种管理方法、技术和手段对项目活动涉及的风险实行有效的控制。包括把对于项

目目标而言正面事件的概率和影响结果扩大到最大和把负面事件的概率和影响结果减小到最小。

项目风险管理主要包括一下过程：



7.2.2.2 风险管理规划

风险管理规划是规划和设计如何进行项目风险管理的过程，对能否进行项目风险管理、完成项目目标至关重要。

风险管理规划通过规划会议的形式制定。

项目管理规划的依据是：

- 项目计划
- 经验与实践
- 项目利益相关者的风险敏感度与承受能力
- 历史数据
- 授权情况

风险影响大小=损失程度×可能性

7.2.2.3 风险识别

根据WBS工作分解结构，结合以往项目的经验，召开项目组会议，采取“头脑风暴法”进行风险识别。

1) 风险分析

2) 风险事件

3) 风险来源和类型

首先要识别风险的来源，由此可预测风险事件的发生和识别风险症状。在项目启动、人员、计划、质量、成本、进度、合同、安全、技术、沟通等各管理要素中对对应着可能的风险条件，要对这些因素进行逐一的分析。

我司采用流程图（鱼刺图）和访谈等工具、方法帮助我们识别风险。

IT项目常见风险参考：

1、人力资源风险

人员的时间和精力不能满足

人员拒绝参加到项目组

项目组人员不稳定

没有合适的培训讲师

2、硬件资源和环境风险

缺少必要的软件

硬件设备不具备或到货不及时

办公环境落后

测试所需的软硬件资源不满足

测试环境的准备不充分

3、客户需求风险

客户需求不明确

客户需求发生变更

客户需求发生重大变化

4、技术风险

项目经理或项目人员的能力不足

项目组未正确理解客户需求

项目组设计的方案不能完全满足客户需求

没有合适的需求分析方法和建模工具

测试范围不合理，无法明确定义测试项

测试用例的选择缺乏代表性、不覆盖

5、质量风险

需求发生质量问题

设计发生质量问题

各单元模块集成后，整个系统出现重大问题

系统性能指标不能达到客户需求明确定义的验收指标

产品出现性能问题

对已安装的软、硬件产品的测试产生新的问题

试运行阶段发现软、硬件产品存在问题

6、客户关系风险

沟通不畅

无法与用户对交付形式、交付时间和交付内容达成一致

用户对软件产品不认可，不在交付清单和试运行报告上签字

客户承诺

合同风险

收款风险

对方组织结构调整

7.2.2.4 风险分析

风险分析是一种评价风险的过程，帮助项目管理人员决定在具体的风险面前采取必要的态度和应对方式。

我司尽量采用量化方法进行风险分析，同时也考虑定性的风险分析。通过量化风险分析，项目管理人员能够按优先顺序排列风险，并建立阈值，以决定哪种风险应收到重视。

1、定性风险分析：

定性风险分析时评估已识别风险的影响和可能性的过程。

风险概率（Risk probability）：某事件发生的可能性有多大，发生的频率是多少。

定量风险分析：

定量风险分析过程的目标是量化分析每一风险的概率及其对项目目标造成的后果，也分析项目总体风险的程度。

项目风险值=概率（P）×影响（I）

7.2.2.5 风险应对

针对风险量化结果，为降低风险的负面效应制定风险应对策略和技术手段，从而尽量做到：

改变风险后果的性质

改变风险发生的概率

改变风险后果大小

掌握应对风险的四项基本策略：规避、转移、接受、减轻。

项目组制定风险应对计划并执行，包括：风险管理计划、应急计划和应急储备等措施。

7.2.2.6 风险控制

风险控制包括：随时追踪风险已经、正在和将要发生的变化；预测和判断风险的应对是否会引起更新的风险发生；对用于风险管理的资源配置进行调整；调整风险应对计划，采取临时紧急应变措施等。

良好的风险监督和控制过程，能提供有效信息，帮助项目在风险发生前做出有效决策。



7.2.3 保密措施

为了进一步加强本项目信息安全保障工作，结合本项目实际情况，特制定本保密制度。

。

运维工作人员必须具有保密意识，对维护内容众的数据保证完全保密。

运维工作人员不传播、私录监控资料尤其是涉及个人隐私、声誉；

未经用户批准，不对外查阅、检索监控资料。社会外来人员及本中心查看资料必须经领导同意方可进入监控指挥中心查看。

未经用户批准，运维工作人员不得擅自改变监控系统设施、设备的位置和用途。

有关监控数据运维人员不得删除、更改、甚至故意破坏、损毁原始视频资料及相关档案记录。

因不遵守保密制度而造成严重不良后果的，由泄密人员及公司承担法律责任。

7.2.3.1 保密原则

严格遵守各项安全保密制度，加强维护工程师的保密意识，制定有效的管理措施和技术措施，防止重要数据、文件、资料的丢失及泄漏。

有关计费清单、采购人资料、业务数据、重要文件等均属机密，不得任意抄录、复制及带出法院，也不得转告与工作无关的人员。

重要文件、数据的销毁，应全部送入碎纸机，不得任意丢弃。安全保密工作应有专人负责，定期向信息组提交《安全工作报告》。

离职人员签署保密协议书，防止重要数据、文件、资料的丢失及泄漏。

7.2.3.2 安全保密要求

- 1) 若我方中标，我方提供其所配人员真实的个人资料，提交采购人进行使用资格审查。
- 2) 确保遵守本项目的保密规定，并签订保密协议。
- 3) 未经业主管理人员的许可不得将各种带有信息的介质带出单位。
- 4) 未经业主管理人员的许可不得进入系统操作。
- 5) 未经业主管理人员的许可不得进入本项目信息系统平台查看、复制、增加、删改信息和数据。

7.3 培训方案

7.3.1 培训计划及安排

用户培训作为工程实施的一个重要环节，对整个项目的实施至关重要。我司承诺拟通过系统的培训，使得用户人员得到日常工作需要的专业技术知识和经验，从而保障整个系统的顺利运行。

本项目培训包含技术培训和产品使用培训。

7.3.1.1 培训方式

为了使培训达到最佳效果，使用户获得尽可能多的知识和经验，我们将采用包括现场培训在内的多种途径对用户进行培训：

- 现场培训：即在设备的集成安装、调试以及故障处理过程中，对用户技术人员进行实际的操作和故障处理培训。
- 集中培训：组织讨论会或讲座，由我司资深顾问通过讨论会等互动方式，与管理层、技术人员讨论有关内部管理、流程、技术等方面的内容。讲座研讨由项目顾问负责进行。

7.3.1.2 培训范围与培训时间安排、人数、次数

针对本项目，我们将按照招标文件要求为用户进行现场培训、网络基础知识培训以及服务期内的网络知识更新培训。分别是：

- 现场培训

根据用户要求，我们对用户方相关技术人员集中进行设备安装集成培训，人数不限。

现场培训是我方根据用户的具体应用情况，对用户相关的技术人员集中进行设备安装和集成的培训，培训内容主要为向用户讲解路由器和交换机相关的原理、相关设备及软件的配置、安装和维护注意事项，并给予适当实际操作机会，对学习产生的问题随即解答，让用户相关技术人员在系统安装、调试和以后的维护过程中均能得心应手。

➤ 集中培训

根据用户要求，由设备原厂对用户的技术人员进行培训。

我方将根据培训对象确定培训内容，并培训教员，主要培训教员具有相应的专业资格和实际工作经历并至少有三年的教学经验，我方会挑选技术水平高、项目经验丰富并且直接参与本项目实施的工程师担任培训教员，保证培训的质量和效果，培训均采用中文授课方式进行，我司承诺将免费提供中文培训教材、专业的培训讲师、培训场地以及必须的实验环境等。

以上培训的师资费、教材费、培训场地费以及必须的实验环境等费用由我公司承担。

培训场地选择将经用户方认可。

7.3.1.3 培训考核及反馈

为保证培训效果达到预期目的，培训期间学员均需填写《培训反馈表》，以及时了解培训中出现的偏差，以实现技术的转移和掌握，提高培训质量。在培训结束前，我们将对学员进行培训效果测试，有关测试内容，我们将与项目单位共同制定。

培训反馈表：

项目名称：	项目编号：		
	项目单位：		
培训内容	培训评价		
	讲课效果	理解程度	实用性
建议和意见：			

签字	项目单位	公司
	年 月 日	年 月 日

7.3.1.4 总体培训内容

我公司按招标要求，提供招标模块培训内容：

- 平台的运行维护、容灾备份、迁移、安装等
- 平台升级改造运行维护、日常操作使用等

具体各模块培训及安排如后附。

7.3.1.5 总体培训计划

我公司按招标要求，提供招标模块培训：

总培训课时不低于50课时，具体培训时间地点与采购人协商后确定。

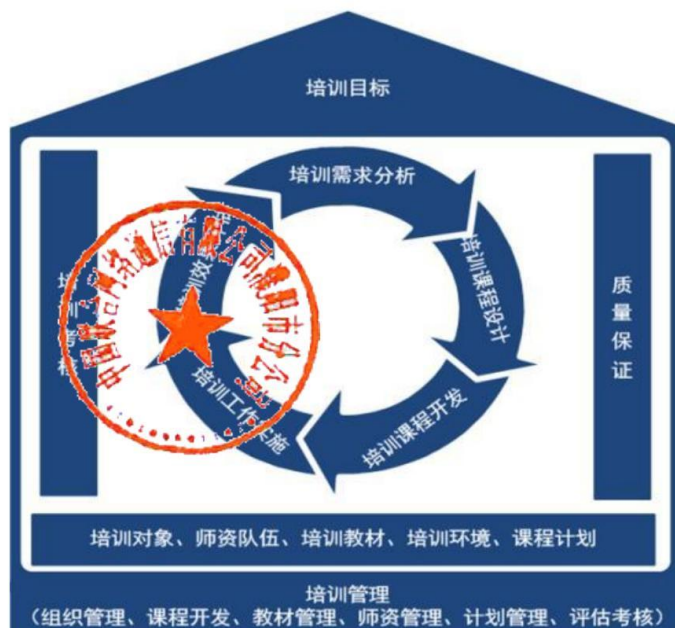
7.3.1.6 整体培训方案

人员培训作为工程实施的一个重要环节，对整个项目的实施至关重要。我司拟通过系统的培训，使得用户方工作人员得到日常工作需要的专业技术知识和经验，从而保障整个系统的顺利运行。

我们对用户培训的目的是让用户方工作人员能够掌握有关系统软件、设备的使用、维护和管理的工作，达到能独立进行管理、故障、日常测试维护等工作的目的，保证我们提供的软、硬件产品能够正常、安全地运行。培训内容将以专业化为宗旨，使每个接受培训的人都成为该领域的专家，为用户建立起一支训练有素的技术队伍，为今后更好的发展奠定良好的基础。

7.3.2 培训模式

我司根据多年来实施类似项目培训工作中总结的经验，在认真研读、分析本项目培训内容和培训要求的基础上制定了本项目培训方案，并遵循以下培训过程体系：



本项目技术培训过程体系各环节主要内容，如下：

序号	培训过程阶段	主要内容
1	培训需求分析	分析培训的要求、内容、对象及方式以及达成的目标等
2	培训课程设计	制定符合各级用户要求的数据管理、系统管理和系统操作等课程设计
3	培训课程开发	整理项目培训思路、编写培训教材资料等
4	培训工作实施	培训实施准备、授课呈现、学员管理等
5	培训效果评估	培训考核及培训质量保证等

7.3.3 培训目的

为了使本项目所涉及的高级管理人员、技术管理人员和日常使用维护人员能全面地了解整个系统，增强维护和使用系统的技能，具备系统管理和一定的技术功底，我们将负责组织对项目各级领导、管理和技术及业务人员进行全面高质量的培训。我们将针对项目建设单位最终用户分层次提供培训，以便对工程实施进行有效的管理，同时保证工程验收移交后，项目建设单位能够胜任系统的全部运行、操作、维护以及故障分析处理。

培训的目的是使管理和使用系统的人员不仅对整个系统有足够的认识，而且能完全胜任所承担的工作，确保整个系统安全可靠地运行，并达到最大效益。为此，我们将针对人员各自的工作性质，对不同职责的工作人员分类进行专门培训，使他们掌握相应的专

业技能。针对系统管理人员等进行全面的系统管理、日常运行与维护、故障处理等技术培训工作，使有关人员能够正确、熟练、有效地进行系统业务的操作、处理、管理和维护。

我们将提供详细的培训课程和产品、技术知识讲座。培训教员由本公司最富有经验的教师以及原厂商培训教师担任。通过培训，使项目单位相关人员在培训后能够独立地对系统进行管理、维护。

7.3.4 培训对象

对用户的培训包括对项目日常使用维护人员、相关技术人员、项目高级管理人员及用户方认为有必要参加培训的其它相关人员。

7.3.5 培训内容

培训内容注重实用性和前瞻性，理论教学与实践操作相结合，并根据发展趋势适时调整培训内容和方案。

7.3.6 解决问题和取得效果

我们将组织成立专门的培训管理小组，由项目核心业务小组的成员构成。培训管理小组主要负责拟订详细的培训计划、组织方式、培训制度与考核办法，并经项目管理组织机构审核后发布。

为充分保证本工程项目竣工投入使用后，能够正常、安全、可靠、高效地运行，能最大发挥产品功能和效用，我们在对用户的要求充分了解的基础上，在实施前将做好充分的准备工作，在项目开展后，按需求分析、评审、安装、调试、培训、技术支持步骤展开工作。

在培训环节，按照理论和现场实际应用相结合的方式，主要培训内容为设备、日常使用操作、运维、保养与管理、常见故障的排除、紧急情况的处理等，同时为操作和维护人员免费提供完善的设备用户手册、运维手册、实训指导书等，并按照贵单位使用设备的相关功能，设计相对应的实验，供维护人员实操。

在培训前项目组将提供各种培训的详细方案及培训教材 ppt。为确保设备能够安全、稳定地运行，同时还需要让设备管理人员能够对设备进行独立配置，运维管理和简单排错的能力，我方提供针对本相关人员的一次集中专业技术培训，以及设备安装调试的各项目现场相关技术培训。

7.4 实施方案

我司解决方案使用成熟的实施方法论。此方法致力于降低大型项目实施过程中面临的风险来保障业务目标的达成。风险的管理和减缓对这个实施模型是极为重要的。

在项目实施之前，我们对项目进行一次探索性咨询规划。规划包括战略规划咨询和业务规划咨询。指的是在深刻理解行业和业务特征的基础上制定客户IT发展规划。

● 在**定义阶段**，为客户IT规划制定后需要一个健全的管控体系帮助其落实执行。这个管控体系，业界也称为“IT治理”。通过IT治理，可以实现客户组织架构、项目管理、招标办法、信息安全、人力资源等管理控制。从而提高客户信息化的执行力和领导力；其次就是标准化，云服务实施的过程就是客户标准化和规范化的过程，准确的说，先有标准化后有信息化。

● 在**构建阶段**，我们利用我司现有的项目管理方法解决了主要的项目管理问题，使得项目能够按时按预算完成，并为设计高质量的产品提供了保证。它侧重于对整个项目的启动、进行和结束的管理，解决了以下几方面的问题：

- 范围和变更管理
- 项目计划
- 风险降低
- 交付管理
- 配置管理
- 问题和解决方案
- 质量
- 沟通
- 故障管理

● 在**测试阶段**，包括用户体验和性能测试。端对端的测试必须在这个阶段完成，并且在这个阶段结束时，整个解决方案必须已经能够在生产环境中部署。操作文档和培训需求也需要在本阶段中完成。

在**上线阶段**，一旦在测试环境中最后构建完成并且用户体验的测试也已经结束，整个解决方案就会被部署到生产环境。并提供后期的运维、知识转移和监控等各种措施，保证整个项目的运行稳定。

7.4.1.1 实施计划

项目计划阶段是定义项目或阶段目标以及所需的资源。

计划是项目管理的基础，并且是重要的组成部分，因此计划编制对项目来说非常重要，没有一个有效的计划，项目的成功几率将大打折扣。项目计划是一个综合的概念，凡是为实现项目目标而进行的活动都应该纳入到计划中。

项目计划确定具体需要做什么，明确由谁来做和需要什么支持、确定用多长时间和项目成本的具体规划。项目计划制定是贯穿整个项目生命周期的持续不断的工作，计划过程是一个反复的过程。计划工作的多少应与项目的规模和计划所提供的资料和信息用途大小相关。详细的项目计划过程包括：

- 确定项目工作范围。
- 确定为执行项目所需要工作范围内的活动，明确每项活动的职责。
- 确定这些活动的逻辑关系和完成顺序。
- 估算每项活动的历时时间和资源。
- 成本管理计划。
- 风险管理计划。
- 沟通管理计划。
- 人员管理计划。
- 质量管理计划。
- 采购管理计划。
- 集成管理计划。

7.4.1.1.1 项目工作范围确定

项目工作范围的确定是为了有效地完成项目目标，界定项目主要工作内容的过程。确定项目工作范围的过程，也就是制定项目工作范围计划的过程。一般项目工作分解结构的方法来实现，确保找出完成项目工作范围的所以工作要素。

项目工作范围的控制，是项目整体控制过程的一部分，应与其控制过程紧密结合，因为工作范围的每一个变更都会直接或间接影响到项目的进度、成本、质量控制等。建立范围变更的控制系统，就是为项目执行时的实际变更进行有效的沟通、确认和管理。

7.4.1.1.2 项目计划的制定

项目活动就是为了达到项目目标（或各阶段目标）确定的交付成果（或交付物）而进行的一系列工作单元。项目管理在完成工作范围定义和分解以后，其范围定义就为活动的界定提供了依据。

当项目工作的活动已经详细、清晰的确定后，首先，要确定的是工作包的逻辑关系。其次，完成各活动间的关系确认，特别是活动间的先后依赖关系，最好同时完成活动历时和资源使用的确认，因为一项活动的历时与其先后活动和其他相关联活动有着紧密的联系。

因此，活动依赖关系确认的正确与否，将会直接影响到项目的进度安排、资源调配和费用的开支。

工作范围的确定是范围计划的确立和认可，也是项目各项计划制定的基础。项目最基本和必要的计划有范围计划、进度计划、费用计划、资源调配计划等。为了保证项目的有效性、完整性和合理性，项目还应该额外制定质量计划、沟通计划、风险计划、采购计划、人力资源计划等辅助性计划，其中辅助性计划也常常是基本计划的一部分。

项目计划的各项子计划过程彼此之间相互依赖，前一过程没有完成，后一过程将无法开始，反过来后一过程又可以检验前一计划的准确性、正确性。

7.4.2 实施流程

7.4.2.1 项目启动阶段

项目启动过程是批准项目和阶段的开始。项目启动是双方确定合作关系，进行项目立项，确定项目章程。

项目立项的目的，是在决策层对项目投资、实施的认可。一般情况下，被确定立项投资和实施的项目，与企业短期或长期的战略目标相一致，保证企业的影响力和可持续发展。

项目立项后，项目章程的制定和项目启动会议及项目章程的发布是项目启动过程的一个标志。

7.4.2.1.1 定义项目范围

- 1、 定义项目目标；
- 2、 定义项目指标；
- 3、 定义系统实施方案；
- 4、 项目整体方案；
- 5、 批准项目。

7.4.2.1.2 组织保障

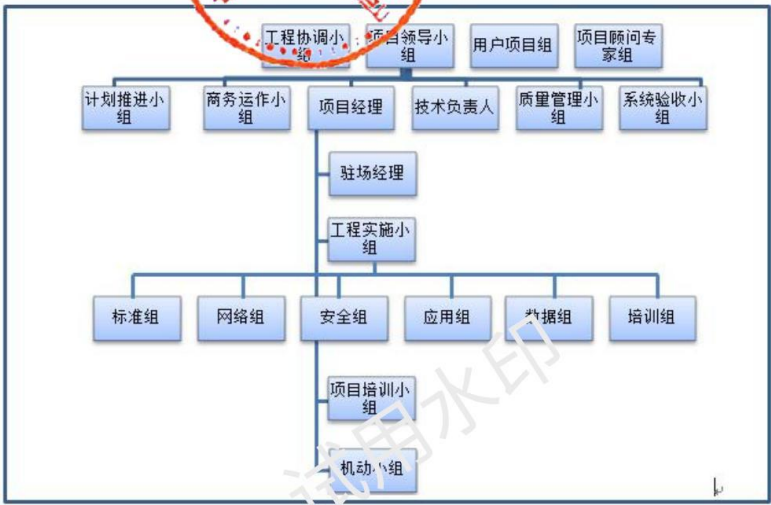
为保证本项目的顺利实施，需要成立完善的项目组织，为项目提供全面的服务，项目组织架构是用来确定在项目中各个人员的权限、职责、责任、报告和沟通方式。

7.4.2.1.3 成立项目组

由用户和我司公司共同成立项目组。采用项目领导小组下的项目经理负责制，并明确规定所属下级各小组的职责及组间协调关系。

根据项目组织架构，共分为几个小组：工程领导小组、工程总协调小组、计划推进小组、商务运作小组、质量管理小组和工程实施小组等。各小组分别承担实施中的不同任务，同时又精诚合作，共同努力，保证圆满完成设备安装调试及系统集成任务。

下面是我公司为本项目成立项目组的组织与机构：



7.4.2.1.4 项目成员岗位职责

1. 项目领导小组

- 负责整个工程建设过程中的重大事项的协调；
- 对整个工程的实施进度进行监控；
- 负责与项目单位的协调。

2. 项目协调小组

- 负责向有关领导和工程领导小组汇报工程实施进度；
- 负责管理协调工程建设中的日常事务；
- 负责工程实施过程中的公司内部运作关系的协调工作；
- 协调工程实施中设备提供商的工作。

负责联系与厂商方面进行技术上的交流、指导与厂商商务合同的签订，督促设备订购、到货、报关、转运分发的进行；并对整个项目中的关键技术进行把关；组织人力、物力对技术难点进行攻关；管理、监督技术培训工作的组织和实施；督促培训教材的编写；督

促技术文档的编写和移交；负责组织工程验收的进行；负责管理、监督技术支持和售后服务体系的运转。

管理、监督工程的实施，督促到货验收、安装调试、系统联调、系统运行的顺利进行；协调解决在工程实施过程中所出现的重大问题；并定期听取项目经理对工程实施进度的汇报，并提出指导性的建议；负责组织工程验收的进行。

3. 项目经理

项目经理在工程实施小组中为主，并领导实施小组开展工作。

协助工程总协调小组开展工作；

按照工程实施进度表，组织安排各实施人员的工作任务；

负责指导工程的实施并掌握工程的实施进度；

负责与项目单位的技术交流；

督促各实施人员按期完成文档整理工作；

帮助各实施人员解决工程实施中的难题；

汇集工程实施中产生的用户报告，向上级领导汇报有关的问题；

组织定期的工程例会；

有责任向工程总协调小组提出对工程中需要的重大技术更改；

为工程实施人员提供便利的帮助条件

4. 驻场经理

负责本项目与客户沟通与项目相关的所有事宜；

驻场人员的管理；

项目紧急事件的现场支持；

公司二线、原厂支持人员的申请等。

5. 商务运作小组

向厂商下单、订购设备；

督促厂商按期供货；

若是从国外供应货物，还应按标书的规定，及时向用户汇报货物装运、到货情况；负责报关，并向当地商检局或有关部门申请对货物的质量、规格、数量和质量进行检验，并出具验证证书；同时提供办理免税手续涉及的文档、进口环节涉及的文档；

转运货物到用户指定地点；

记录整个运转过程，形成文档；

6. 工程实施小组

由我司公司的工程师、厂家工程师和用户负责集成工作的协调配合人员组成。条件为：
：熟悉本项目涉及的系统软硬件平台及集成，具有多年系统集成项目实施经验及相应认证的专业工程师。

设备到货后，负责接收货物并协助项目单位进行验货，出具“设备到货验收报告”，若有故障，还要出具“设备到货验收故障报告”；

按照参考手册，进行设备的安装配置等，并负责系统联调和系统运行的初期维护；

承担用户的现场培训工作；

进行系统自检；

记录和整理施工过程中的技术文档和相关资料；

各实施人员定期向项目经理汇报工程进展情况；

各实施人员要相互交流、共同推进工程的进展。

项目实施完毕后，挑选出最熟悉整个系统的四名工程师进行驻场服务。

7. 计划推进小组

按照整个工程的进展计划，考核项目经理和各施工人员工作完成情况，督促工程按计划实施；

督促各项目组按计划提交技术文档；

设立档案管理员，统一管理各项目小组实施过程中的各种记录档案、其它测试文档、验收文档等；集中管理工程实施中的会议纪要和各种报告。

负责将技术文档提交给用户。

8. 质量管理小组

不定期组织专家对工程质量进行评定，督促各项目组将工程保质保量的完成。

9. 项目验收小组

在初步验收或最终验收前夕由项目领导小组负责临时组建；

验收小组的成员由用户和我司公司双方提供；

组长由用户人员担任，副组长由我司公司人员担任。

10. 项目培训小组

由我司公司方的专业工程师组成。条件为：具有丰富培训经验的专业工程师。

按照要求制定培训计划；

编写培训教程；

按照培训计划负责培训授课、考核工作。

11. 后台技术支持小组

在项目施工工作完成后，负责项目的售后服务工作。

由系统集成小组及用户1-2名组成。

由指派的客户服务小组负责人任维护组长。

12. 机动小组

后勤保障小组，当工程施工小组的某成员因某种原因不能正常工作时，则由机动小组中派遣人员补充。

当工程施工小组确实因工作量大，不能按时完成工作计划时，机动小组将负责支援。

7.4.2.1.5 确定项目组织

- 1、 确定项目组织和角色；
- 2、 通知人员所担当的角色；
- 3、 通知核心小组的角色；
- 4、 建立项目变更控制委员会（或小组）。

7.4.2.1.6 建立项目组工作环境

- 1、 系统规划；
- 2、 建设环境；
- 3、 测试环境；
- 4、 运行环境；
- 5、 项目工作环境。

7.4.2.2 项目启动会议

召开项目启动会议：

- 1、介绍项目情况、明确任务；
- 2、时间进度安排、资源组织结构。

7.4.2.2.1 项目实施阶段

项目生命周期的中间阶段是执行和控制阶段。项目的大部分工作是在这一阶段完成的。这一阶段的开始，是以需求确认的完成为标志。项目实施阶段，是根据项目计划来执行任务；同时通过控制过程，定期来监督和测量项目的进展来判断项目实际的执行情况与计

划的差异，并采取纠正措施。因此项目实施过程虽然是执行项目计划的过程，但同时也是检验项目计划的过程。

项目实施是为了实现项目目标，完成项目规定的最终交付成果，依据项目基准计划，通过一系列具体、实际的活动，准确、及时地完成项目中的各项工作，并得到客户满意和认可的过程。

7.4.2.2.1.1 项目执行

项目的执行，强调的不仅仅是实施准备完毕，项目按照实施前正式确定的项目计划和技术方案开始执行具体的每一项活动，直到项目目标的实现。同时，强调项目组成员应该注意项目计划和方案在实施过程中的指导意义，执行任何一项任务，不偏离项目管理的轨迹，也是对项目计划和方案的一个有效检验过程。

7.4.2.2.1.2 项目控制

项目的控制，即有效的控制项目，其关键是及时定期的检测项目的实际过程，并与项目计划进行比较，如果偏离，应采取纠正措施，处理隐患，降低项目风险。对项目的任何变化都应加以重视。

项目控制的目的是在预算成本内、有限资源内、按照进度要求、在相关技术和质量指标下实现项目目标，达到客户满意。

项目的控制过程，就是按照项目基准计划启动实施，在实施过程中与实际情况进行比较分析，必要时修改项目计划，并安装新的项目计划执行的过程。可以看出，项目控制是一个动态的过程，在不断的对项目中的各种偏差加以调整。

项目控制的主要内容如下：进度控制、变更控制、质量控制及费用控制。

项目控制的方法及原则如下：

- 严格遵守项目计划，必要时调整；
- 专门角色负责相应的变更沟通；
- 项目沟通要及时、准确；
- 不断的监督项目中的各项工作；
- 确认和批准的程序严格遵守；
- 清楚变更流程和要求；
- 变更文件及相关备忘录应由变更主体方签字确认；
- 保证项目团队的协作精神。

在项目实施阶段，按照项目建设规范，对于项目主要里程碑做到明确描述：

- (1) 完成系统需求调研；
- (2) 需求调研报告经项目组签字确认后进行系统设计：；
- (3) 系统设计经项目组签字确认后进行系统的详细设计，提供详细项目文档资料；
- (4) 系统集成项目实施过程中，提供系统需要的《项目进度报告》、《问题和风险报告》等项目过程资料；
- (5) 系统测试，提供详细测试计划方案，并完成系统测试工作，并向项目组提供相关文档，如：《测试计划》、《测试记录》、《测试报告》等；
- (6) 完成功能部署与联调工作，并向项目组提供相关文档，如：《培训计划》、《培训记录》、《用户操作手册》、《售后服务规范》、《系统安装维护手册》等；
- (7) 完成该系统与相关业务系统间的接口工作；
- (8) 完成上线工作后，提供《系统运行报告》；
- (9) 系统总验收（出具《验收报告》）；
- (10) 项目进入维护期。

7.4.2.2.1.3 需求调研

需求调研工作，对项目起着关键作用，有时决定项目的成败。

首先进行系统需求调研，选取有代表性的部门进行实地调研，然后将需求文档下发到其它各部门听取意见反馈；需求调研结束并通过后，进行系统设计和实施。

确定业务过程需求；

确定系统功能需求；

确定需求界面；

确定转换需求；

确定需求增加；

明确不足的地方；

精炼业务过程描述和模型；

确定报告或需求说明书；

形成的文档：需求调研报告或系统需求说明书。

本着友好合作的原则，建设队伍由我司和客户相关人员共同组成，实施过程中，将把通用的管理规范和方法提供给客户，争取为客户带出一支熟悉实施的队伍。

系统的建设分为三个阶段：设计、实施和联调。

系统的设计的工作包括需求分析、系统设计；

在设计的同时，建立环境，并对所选的系统软、硬件进行安装、调试，对详细设计时的某些关键技术进行验证，使将来的实施更加顺畅。

项目实施开始，严格按招标文件要求建设。

项目组按照项目制度，规定制定详细的工作作息制度、文档配置规范、人员IP地址分配规范、施工纪律等，做好相关人员的技术培训，对关键岗位进行人员备份，以防不测，然后进入实施环节。

7.4.2.2.1.4 系统联调与测试

需要进行系统的组装、系统的压力测试、功能测试和集成系统测试；

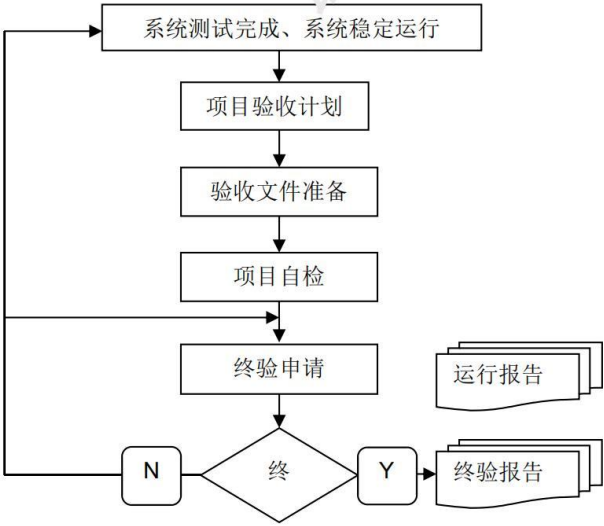
系统联调阶段形成的文档有《测试说明书》、《测试报告》、《系统安装维护手册》等。

7.4.2.2.2 项目验收阶段

项目收尾工作一般包括项目工作范围的再确认、项目相关文件的准备、项目的验收和项目的后评价等工作。项目收尾过程结束，标志项目验收和项目结束。

项目验收是完成项目交付成果的检验和交接，同时其目的是从项目中获得相应经验，以便指导和改善未来项目。

7.4.2.2.2.1 项目验收程序



7.4.2.2.2.2 项目工作范围的再确认

项目收尾阶段对工作范围的确认，是依据合同中规定的项目工作内容和实际的工作成果及相关成果文件，主要有两个方面：一是项目目标是否按照要求完成，形成客户可接收的交付成果；二是项目的工作范围是否有大的变动和变更，是项目最终审计的依据之一，也是合同履行情况的证明。

7.4.2.2.2.3 项目相关文件的准备

项目文件的准备，是为项目验收打基础，是项目收尾阶段的非常重要的一个环节。因为项目文件是整个项目生命周期的详细记录，是项目成果的重要表现形式。项目文件既是项目评价和项目验收的标准，也是项目交接、维护和后评价的重要原始证明。对项目文件的要求必须是真实的。

7.4.2.2.2.4 项目的验收

按计划进行对项目的验收，对项目本身的意义和作用是非常重要的。

项目验收除了范围确认外，主要包括项目文件和项目质量的验收。

验收流程，见文档《项目验收程序》部分内容。

7.4.2.2.2.5 项目的评价

很多项目在收尾阶段，往往认为项目验收完了，项目就结束了。项目的整个过程可能存在某些缺失，也有可能有很好的经验。因此项目收尾阶段还有一个重要的工作就是项目后的评价。评价的目的是评估项目绩效，总结项目得失。

7.4.3 项目组织架构

职务/职称		职责
项目组	总经理	对项目进度、工程质量做宏观指导； 重要阶段的工作评审；
	大项目经理	对项目出现的重大问题进行协调和指导； 有效解决项目所需的人力资源。
	大项目经理	及时与客户沟通，配合项目经理协调客户关系； 协助项目经理解决、解答有关工程合同的问题； 主要由本项目的销售经理和系统设计师组成。
	总工程师	从技术角度对整个项目负责； 制定并审核本项目中的技术实施方案；

	工程师	处理工程中出现的技术难点； 关键技术难题的攻关与解决； 参与规划与制订工程测试方案与工程质量标准；
项目执行组	大项目经理	从整个项目的执行角度负责项目的整体运作及统筹规划，并就工程的实施结果向项目总协调人负责； 负责制订项目计划与预算，落实项目各阶段的子项任务； 有效安排资源，组织、协调项目组成员的工作； 依托技术专家，确定的技术规范审核设备配置，确保配置无误； 定期提交项目进展状态报告，存在的问题，下一步的具体实施计划； 协调客户方的配套准备工作以及现场实施时客户配合工作。
	工程师	接受项目经理分配的任务，按项目计划要求具体实施工程项目；
	根据项目需要XX人	按时保质完成软件产品开发、维护、工程现场实施工作； 在工程现场向客户提供必要的现场操作说明； 将工程中出现的问题及时反映项目经理；
	工程师	及时记录现场操作内容，形成必要的工程实施文档。
项目监控	工程师	监督与检查工程质量； 定义工程所需的产品； 整理产品的规范配置文档
	工程师	在质量控制小组和技术专家组的指导下完成工程测试文档；测试手段的准备。对工程内容进行系统测试；及时将所发现的问题向质量控制小组和有关的部门通报。
培训	工程师	由组长负责，制订培训计划，落实培训时间和场地，对项目所涉及的技术与产品给予用户培训，一般分为集中培训和现场培训，并根据需要编写相应的培训教材和配置手册。
	工程师	
文档	档案组	负责工程技术文档的制作，协助工程师完成产品配置文档； 汇集并整理工程实施文档，记录所有开、完工、验收及方案修改情况； 完成工程验收所需的技术/操作手册，包括交付给用户使用的各种产品说明，技术说明和手册； 将常规文档在工程验收后移交技术支持中心备案。
维护	工程师	由我公司的售后技术服务人员组成，负责项目的技术支持和售后服务，包括电话服务、现场服务及故障解除、更换备件等，提供项目验收后的技术支持和服务，确保系统的可靠运行。
项目验收组		由项目领导组、项目监控组和项目执行组组长、公司领导、用户方领导组成，人员名单经双方认可后，按设计方案及合同对系统设计实施、设备清单、性能和功能测试、实施文档等进行综合验收评审，并形成验收结论。

7.5 项目过程管理管理

7.5.1 项目管理方案

7.5.1.1 项目管理概况

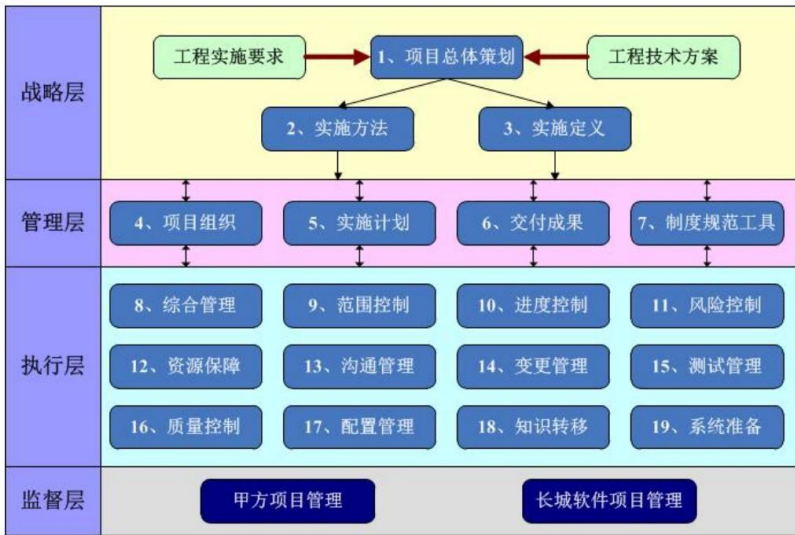
为了确保项目的顺利实施，必须有一套科学、完整和有效的项目管理方法。

项目管理是一套完整的科学方法或过程，它通常被运用于项目的整个生命周期。这些管理方法确保了项目实施过程的严密性和可预言性。项目管理要解决团队的合作、项目人员的承诺与事物的落实、项目管理还要保证项目质量的不断改进，要作好项目时间和项目开销的合理平衡。通过这个过程，项目组成人员能用一种系统的方法来计划和管理他们各自的工作。

项目管理直接关系到整个项目的成败，一个工程从立项到实施，到最后提交给用户及提交后系统的维护和产品维修，都必须有严格的制度和流程。这样做，不但能确保我们的工作可以按步骤有计划地进行，最重要的是能确实保证用户的利益，保证了产品及服务能满足用户的需要，并提高我们自身的服务能力。

7.5.1.1.1 项目管理思路

我司公司对本项目实施和管理的思路是从四个层次考虑的，分别是战略层、管理层、执行层、监督层，如下图所示：



在战略层我们从本项目实施要求和工程技术方案出发，分析项目难点和关键任务，制定项目实施管理总体策略，并对项目实施范围进行明确定义，提出项目实施管理方法，从宏观层面制定项目实施和管理的策略、方法。

在管理层我们关注项目的组织、计划、制度规范、使用的工具和交付成果，通过与业主方管理层的充分沟通、交流，在经验、知识、项目特点的基础上建立项目实施组织并制定实施计划，对项目实施过程的关键阶段任务和里程碑进行定义，同时制定项目实施管理的制度、规范，选择合适的项目实施管理、测试等工具，保证项目的可管理性。

执行层主要考虑项目管理方面的内容，如进度控制、范围控制、风险控制、沟通管理等，从项目具体实施的各方面因素考虑，做好项目前期准备、工程管理工作，此外还要考虑知识转移的管理，使项目建设成果被用户最大程度的使用，以期对用户的工作有更大的帮助。

监督层为项目实施管理引入过程监督机制，由业主方项目管理人员和我司公司项目管理专家参与项目实施的全过程，行使监督管理职能，为项目成功提供更多保障。

7.5.1.1.2 项目管理方式

我司公司历来重视工程实施中项目的管理，并以 ISO9001 质量体系作为我们提供优质服务的保证。一个工程从立项到实施，到最后提交给用户，再到提交后系统的维护和产品维修，都有非常严格的制度和流程。这样不但能确保我们的工作可以按步骤有计划地进行，更重要的是确实保证了用户的利益，保证了我们提供的产品及服务满足用户的需要，并提高了我们自身的服务能力。

根据我公司 ISO9001 质量体系文件的要求以及我司公司的一贯做法，我司公司对本项目的管理采用项目经理负责制。我司公司的项目经理是受我司公司的法定代表人委托对所承担工程项目的全过程全面负责的项目管理者，是我司公司法人代表在本项目中的代表人。项目经理负责整个项目的管理，对项目的成败负全部责任，他的工作就是掌管我司公司参与本项目的各部门和人员，确保实现项目所有的目标。

我司公司的项目经理是我司公司在工程实施全过程所有工作的总负责人，是项目管理的总责任者，是项目动态管理的体现者，是项目生产要素合理投入和调优组合的组织者。项目经理是项目目标的全面体现者，既要对项目的成果性目标负责，又要对我司公司的效率性目标负责。

我司公司项目经理还负责协调我司公司与业主方以及其他各方面关系，使之互相紧密协作与配合的桥梁和纽带。他对项目管理目标的实现承担着全部责任，即承担合同责任、履行合同义务、执行合同条款、处理合同纠纷、受法律的约束和保护。

7.5.1.1.3 项目管理流程

项目管理的流程安排是保障项目顺利实施的关键，整个项目过程应该包括：

1、工程准备阶段

- ✓ 项目组成立
- ✓ 合同签订
- ✓ 制定项目进度计划
- ✓ 勘察施工现场
- ✓ 编制施工方案（施工作业指导书）
- ✓ 施工作业指导书评审

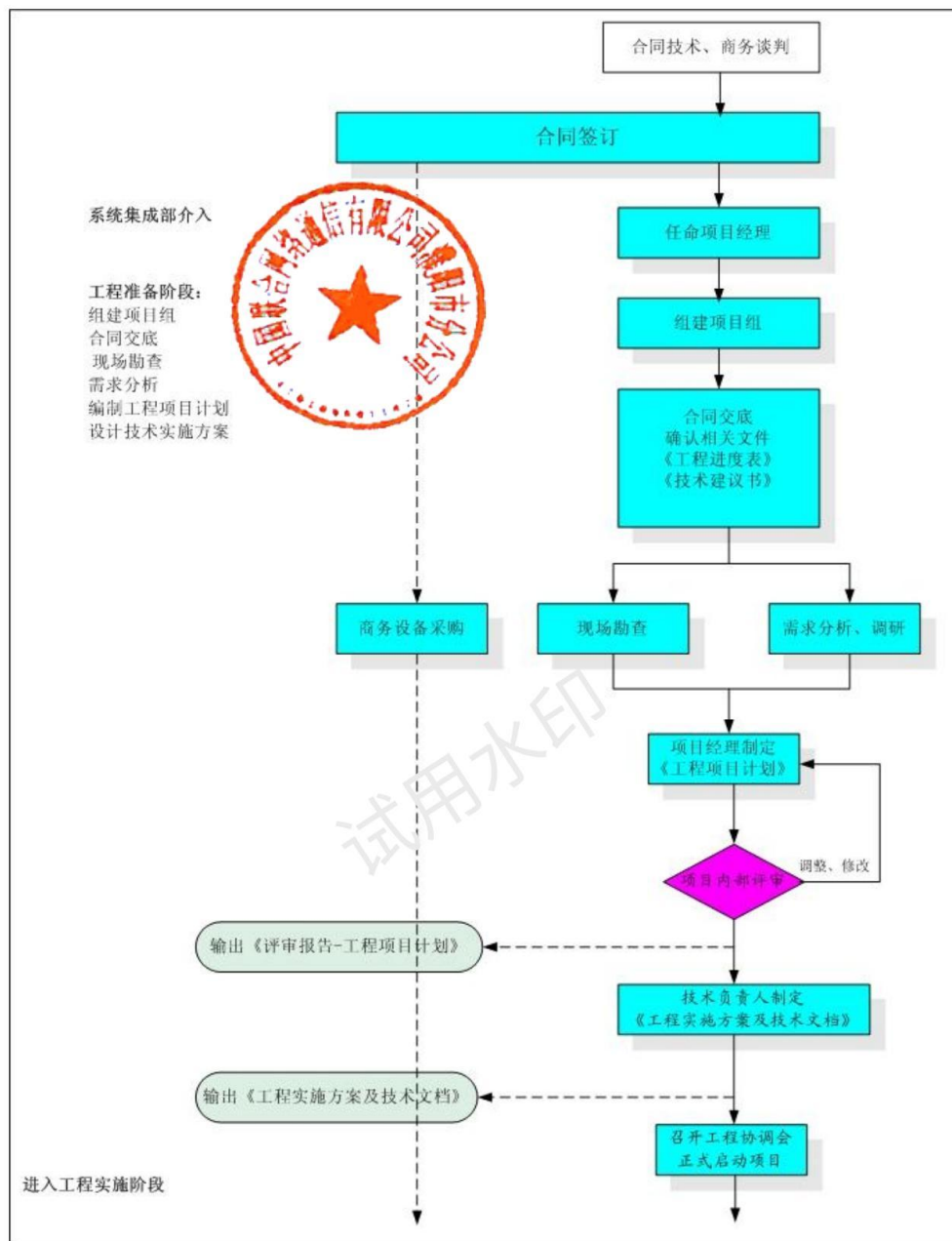
2、工程实施阶段

- ✓ 制定施工计划
- ✓ 召开施工会议
- ✓ 组织到货并完成验收
- ✓ 设备加电测试
- ✓ 安装和调试
- ✓ 清理施工现场
- ✓ 标签及现场整理
- ✓ 项目割接

3、工程验收测试阶段

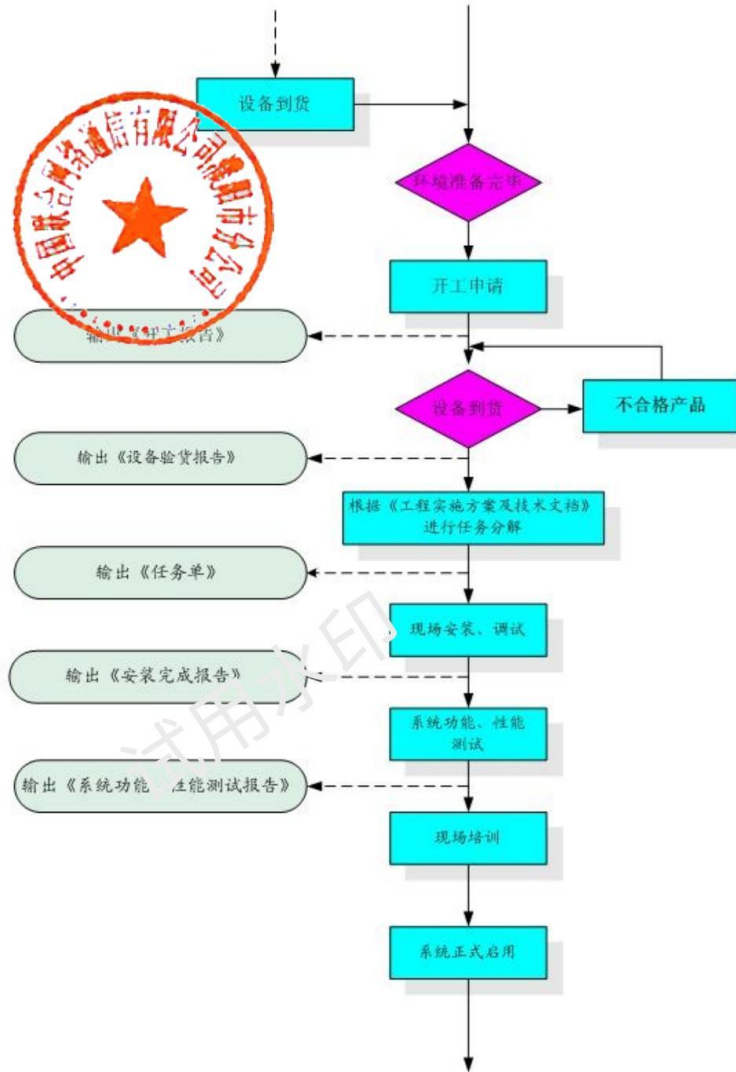
- ✓ 系统初验申请
- ✓ 系统初验
- ✓ 提交施工文档及技术文档
- ✓ 系统试运行、遗留问题处理
- ✓ 系统申请终验
- ✓ 系统终验

管理的项目流程图如下：

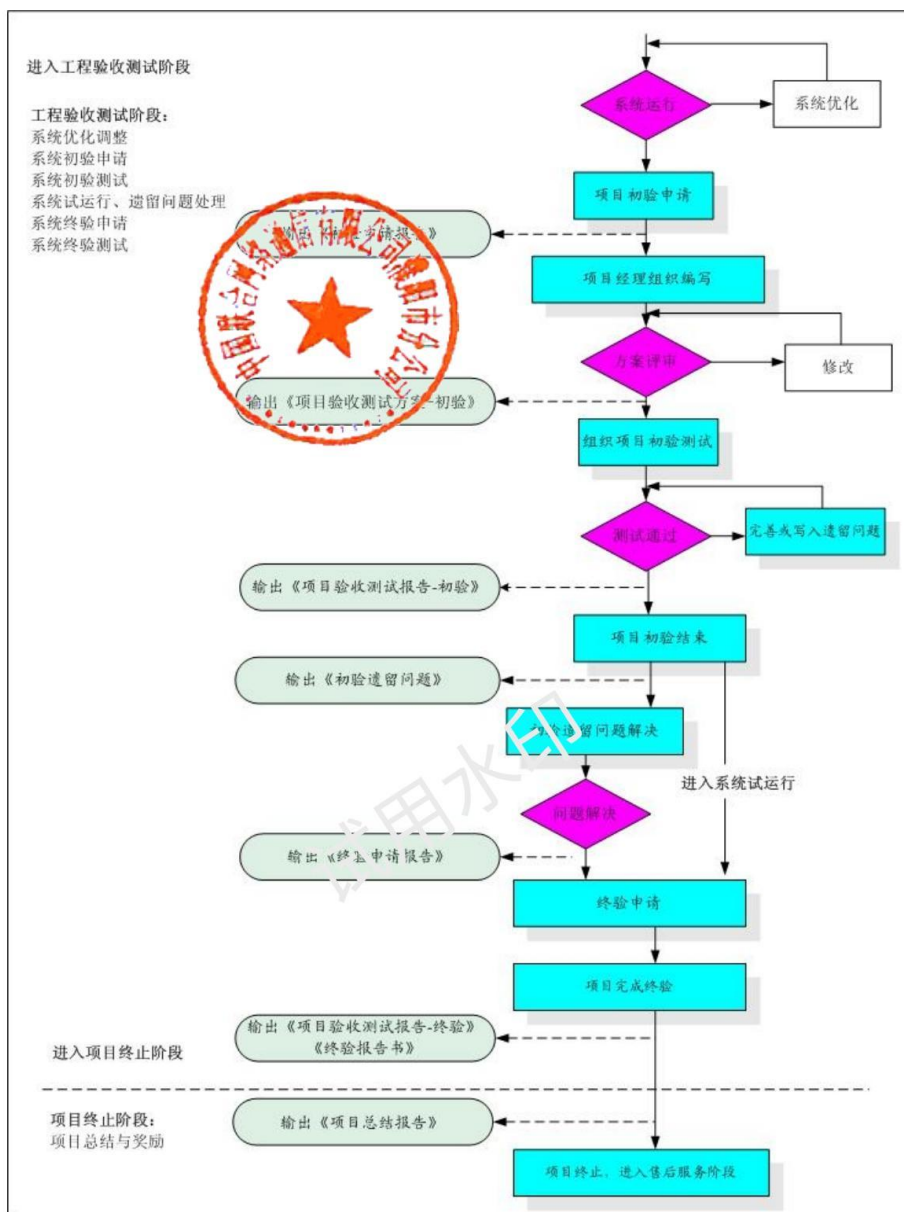


进入工程实施阶段

工程实施阶段：
设备验收
工程任务分解
安装、调试
系统启用测试
现场培训



进入工程验收测试阶段



7.5.1.1.4 项目管理规范

为了对系统工作进行有效管理，并能及时控制、调整、解决实施中的问题，我们将在实施过程中遵守以下管理规范：

(1) 定期召开项目审查会议

定期召开的项目审查会议贯穿整个项目的实施过程，由项目调度管理员负责召集相关人员定期召开，内容包括：

审查项目进程

解决存在问题

检查落实后续的工作

(2) 项目分阶段

通过分解目标，细化任务，实现对项目的进度与质量控制。项目执行过程将分为三个阶段，实施前期、实施中期和实施后期。

(3) 全过程文档记录

由质量管理组和设计规划组，定在各个阶段要提交的所有文档，以及相应编写人员、文档模板、提交及认可方式，通过文档提交清单方式，进行交接。

(4) 定期汇报制度和及时汇报制度

项目执行全过程采取项目周报制度；

对货物运输情况、技术方案制定情况采取隔日汇报制度；

对安装预配和发货情况采取隔日汇报制度；

对现场安装调试情况、系统联调情况采取每日汇报制度；

对系统试运行情况采取每日汇报制度；

对各种应急情况采取实时直报项目经理制度。

所有汇报内容均使用相应的表格填写。下面以项目执行工作日志为例详细说明：

项目执行工作日志			
项目名称		用户单位	
报告日期	年月日	联系人/联系方式	
公司名称		报告人/联系方式	
参加人员		工时	
实施内容			
问题及风险			
解决方法			
用户意见			

项目执行工作日志	
备注	

(5) 遵循现场实施规范

各项目执行小组在进驻项目执行现场后，将严格遵守我司公司现场实施规范。现场实施规范主要内容如下：

1. 在客户现场，项目组成员严格遵守用户方的管理规范和管理制度；
2. 严禁做吸烟、玩游戏、上网聊天等与工作无关的事情；
3. 因工作是由需要使用用户电话时，须应得到客户的允许；
4. 未经客户许可，不得擅自登录用户计算机系统，不得擅自开、关客户的设备；
5. 调整用户原有（尤其是正在使用的）设备参数前，必须获得用户许可；
6. 施工结束后，必须将实施现场清理干净，并经客户检查后方可离开；
7. 无论任何理由，不许和客户发生争吵；
8. 严禁接受用户的馈赠。

(6) 建立全方位的沟通渠道

为保证系统的顺利实施，同时在实施过程中向项目单位的技术人员提供及时的技术支持。我司公司客户服务中心专门为本项目指派了专职服务经理，同时，我司公司将向项目单位的技术人员公布所有实施人员的移动电话号码，以提供 24 小时的服务。

7.5.1.2 项目管理方法

项目的工程实施管理工作中，主要采用以下基本方法：

7.5.1.2.1 目标规划法

围绕质量目标、进度目标进行研究确定、分解、综合、计划安排、制定措施等。由粗而细，分阶段地根据可能获得的工程信息逐步细化、补充和修正。

7.5.1.2.2 动态控制法

在本项目实施过程中，通过对过程、目标和活动的动态跟踪，全面、及时、准确地掌握工程信息，定期地将实际目标和计划目标进行对比，发现问题和偏离时，加以纠正，以保证项目总目标的实现。本项目的质量管理将基于 PDCA 循环法（戴明环法）对质量进行动态控制。

7.5.1.2.3 信息管理法

本项目在开展工作时，将对所需要的工程信息进行收集、整理、分析、处理和传递，以不断地预测或发现问题，不断地进行规划、决策、执行和检查。

7.5.1.2.4 合同管理法

本项目在工作中，将根据用户和供货方的合同进行监督、检查，对合同双方争议进行调解和处理，以保证合同的全面履行。

7.5.1.2.5 测试法

对本项目的单元成果进行测试是保证工程质量的重要技术手段。本项目将依靠我司公司的技术优势，对工程各个部分进行各种类型的测试，以判断其功能和性能是否满足设计要求。

7.5.1.3 项目管理制度

7.5.1.3.1 会议制度

每周召开一次会议，提前一天与用户方协商具体时间和议题，并发出会议通知。通知内容包括：时间、地点、议题。会后一日内发出会议纪要。会议纪要由项目经理签署。

不定期召开内部工作会议，由项目经理根据工作需要确定时间、地点和议题。会后整理成会议纪要，由项目经理和用户共同签署。

7.5.1.3.2 管理日志制度

日志内容包括一日大事、要事，工作的活动、决定以及资源（人力、物力、时间等）投入情况。日志编写要一日一记，不间断，既要简明扼要，又要数据翔实。

7.5.1.3.3 工作报告制度

项目经理定期或不定期以书面形式提出工作计划和要求，各小组根据工作计划确定实施方案，组织小组成员执行，并将完成情况报告项目经理。

7.5.1.3.4 技术交底制度

在项目施工完成后，项目组向客户方进行全面技术交底（设计意图、实施要求、质量标准、技术措施），并根据讨论决定的事项做出书面纪要。

7.5.1.3.5 开工报告审批制度

当工程施工准备工作完成时，我司公司提出《工程开工报告书》，经客户审批后，开始施工。

7.5.1.3.6 变更设计制度

如因设计方案错漏，或发现实地情况与设计不符时，须提出变更设计申请，经与客户方同意后变更设计，设计完成后，填写变更设计通知单，并签发《设计变更指令》。

7.5.1.3.7 隐蔽工程检查制度

隐蔽前，首先进行自检，并将相关资料报监理单位。我公司将需检查的隐蔽工程在隐蔽前三日提出计划报监理单位，由监理单位参加隐蔽工程施工检查，并签字认可。

7.5.1.3.8 工程进度监督及报告制度

按照合同规定的计划进度组织实施，我司公司在项目的各环节以及每周以书面报告的形式向客户方报告各项工程实际进度及计划的对比和形象进度情况。

7.5.1.3.9 硬件设备检验及复验制度

工程实施前，我司公司工程师和客户方将检查进场硬件设备，加电测试相关配套设备，对于相关设备进行检验。

7.5.1.3.10 快速沟通

项目实施过程中建立的快速沟通管理机制是为了确保整个项目有序、高效实施的重要保证。项目快速沟通的过程包括信息的产生、收集、分析、决策和保存五个步骤。项目沟通管理在成功所必须的因素一人、想法和信息之间提供了一个关键连接。

7.5.1.4 进度管理

为了确保项目按期完成，必须对项目的进度进行持续的监控管理。通过制定项目计划和对计划的定期回顾检查，按照一定的汇报机制，管理项目的执行情况，并根据实际情况，对项目计划进行必要的调整。我们所建议的进度管理主要手段包括：

7.5.1.4.1 项目例会

由项目经理每周召集举行项目例会，对项目的实施工作完成情况进行总结并确定下周计划，同时在会上对提出的争议和问题进行讨论。项目周例会通常为每周五的下午 3 点举行，参加人员是双方项目组成员（双方项目经理必须参加）。例会结束后整理《周项目总结报告》，发送给双方项目执行负责人。

由项目经理根据项目情况召集举行项目月度例会，主要讨论总体的项目进展、问题和变更的状态、后续的工作进程和任务分配等并形成会议纪要。参加人员是项目经理及项目组核心成员。双方的项目经理应在月末提交《项目状态报告》至双方项目执行负责人。

在实施过程中发生的临时性会议，视情况随时召集，参加人员是项目经理及项目组核心成员，结果报告双方项目总监，由双方高层协商确定。

所有会议均应在会议结束后产生《会议纪要》，通知双方的项目经理。

7.5.1.4.2 项目状态报告

在项目执行过程中，项目经理根据项目的情况，应定期（周或月）向软件项目部经理提交项目状态报告并抄送质量保证部经理。汇报项目的进度、质量、成本方面进展以及完成、未完成工作、存在问题、下一步的工作计划等内容，并在此基础上形成对客户方的项目状态报告，具体的格式参见相应的模版。

7.5.1.4.3 项目里程碑/阶段评估验收

在项目里程碑点或者阶段点，项目经理组织双方相关人员进行评估和验收，就本阶段/里程碑完成情况进行确认，如果需要进行变更则进行沟通和协商，结束后形成《会议纪要》、《阶段验收报告》，并提交给双方项目执行负责人，由双方高层协商确定。

7.5.1.5 风险管理

7.5.1.5.1 风险分析

尽早进行风险分析，能够减少项目实施过程中的不确定性。它不仅使各层次的项目管理者建立风险意识，重视风险问题，防范于未然，而且在各个阶段、各个方面实施有效的风险控制，形成一个前后连贯的管理过程。作为面对项目风险的有效手段，全面风险管理强调风险的事先分析与评价，风险因素分析是确定一个项目的风险范围，并将这些风险因素逐一列出以作为全面风险管理的对象。罗列风险因素通常要从多角度、多方位进行，形成对项目系统的全方位的透视，风险因素的分析可以采用以下方面进行分析：

1、按项目系统要素进行分析。这主要有以下方面的系统要素风险：

项目环境要素风险，最常见的有政治风险、法律风险、经济风险、自然条件、社会风险等；

项目的行为主体产生的风险，如承包商（分包商、供应商）技术及管理能力不足，不能保证安全质量，无法按时交工等产生的风险；项目管理者的能力、职业道德、公正性差等产生的风险；

其他方面的风险，如外围主体（政府部门、相关单位）等产生的风险。

2、按风险对目标的影响分析。这是按照项目的目标系统结构进行分析的，它体现的是风险作用的结果，它包括以下几个方面的风险：

工期风险，如造成局部的（工程活动、分项工程）或整个工程的工期延长，不能及时完成项目；

费用风险，这包括财务风险、成本超支、投资追加等；

质量风险，这包括工程等不能通过验收，工程试生产不合格、经过评价工程质量未达到标准或要求；

法律责任风险，可能因此被起诉或承担相关法律法规的或合同的责任。

3、按管理的过程和要素分析，这个分析包括极其复杂的内容，但也常常是分析风险责任的主要依据，它主要包括：

高层战略风险，如指导方针或战略思想可能有错误而造成项目总体目标设计的错误等；

环境调查和预测的风险；

决策风险，如错误的选择，错误的投标决策、报价等；

项目策划风险；

技术设计风险；

计划风险，如目标的错误理解，方案错误等；

实施控制中的风险，如合同、供货、新技术新工艺、分包层、工程管理失误等方面的风险。

7.5.1.5.2 风险识别

从总体上可以将该项目的风险分为宏观和微观两部分，宏观方面的风险指针对该项目的特点而使项目的实施具有的风险，微观风险则指在项目施工过程中会出现的风险。

7.5.1.5.2.1 宏观风险分析

从项目的整体规划上看，本项目作为一项大型的信息化工程建设项目，其具有以下特点：

系统庞大，建设内容多；

项目投资金额大，工程进度时间要求短；

由于项目的这些特点，使项目的建设存在以下风险性：

1、项目建设的统筹规划、协调实施方面的风险性

这一风险属于项目管理的风险，主要体现为合理的项目计划、预算项目成本、资源配置、质量管理及项目管理技术选择等方面，由于项目的规模巨大，建设内容多，建设内容存在交叉与关联，因此使项目的建设不确定性、复杂性并存，带来项目统筹规划、协调实施的风险性。

2、项目投资大而周期相对短造成的组织、实施方面的风险性

组织风险中的一个重要的风险就是项目决策时所确定的项目范围、时间与费用之间的矛盾。此系统的应用软件开发任务多、工作量大，而项目工期相对短，这造成了项目范围和时间的矛盾，因此给如何合理地组织人力与资源，制定可行的项目进度计划带来了困难，形成了项目实施的一定风险。

3、项目建设经验欠缺造成的实施风险性

造成这一风险的主要因素为项目规模大，涉及学科领域广，包括网络、硬件及应用软件领域，且部分建设内容欠缺先前案例及成功经验，使系统的建设无先例可循，需在建设中摸索，从而使项目的顺利实施在进度控制、技术实现等方面存在一定风险性。

4、项目受不可控因素影响产生的风险性

该项目受不可控因素的影响主要表现在以下几个方面：

本项目的建设是一个“一把手工程”，要求最高领导层在深刻理解信息化的本质基础上给予高度关注和重视，提供充分的资源支持。

相关单位目前均有其独立的运作机制，可能存在着对本项目的理解、配合和支持不够风险。

本系统建设是一项投资大、知识密集、高风险的系统工程，项目管理不到位，缺少足够的经验，不严格按信息化建设规定办事是等都有可能加大本项目失败的风险。

系统建设过程中如若缺乏一种有效的监督管理机制，将致使许多工程项目在质量、进度、投资等方面都无法得到很好的保证和控制，出了问题就互相推诿，项目中途下马或完工后难以达到预期建设目标。

5、项目由于外部因素影响可能存在的风险性

项目外部风险主要是指项目的政治、经济环境的变化，包括与项目相关的规章或标准的变化，组织中机构的变化，如机构合并、自然灾害等。这类风险对项目的影响和项目性质的关系较大。

7.5.1.5.2.2 微观风险分析

项目过程的每个阶段都存在着不同的风险，这些风险与该阶段的工作内容紧密相关。

1、合同签约立项阶段可能存在的风险：

项目宏观目标不清；

项目范围不明确（范围太大太小都不可以）；

用户参与少或和用户沟通少；

对需求了解不够；

没有进行可行性研究。

2、项目启动阶段可能存在的风险：

项目具体目标不清；

项目范围不够精确；

用户参与不够；

本项目的规划不够准确；

3、项目计划阶段可能存在的风险：

一、 项目队伍缺乏经验，如缺乏有经验的项目经理；

二、 没有变更控制计划，以至于变更没有依据，该变更的不变，不该变的也变，这

样得来的设计势必会失败或者偏离用户需求；

三、 仓促计划，可能带来进度方面的风险；

四、 漏项，由于设计人员的疏忽某个功能没有考虑进去；

4、项目执行与控制阶段可能存在的风险

五、 设备环境没有具备好；

六、 计划错误带来的实施困难；

七、 项目团队实施能力差；

八、 项目范围改变（突然要增加或修改一些功能，需要重新考虑设计）；

九、 项目进度改变（要求提前完成任务等）；

十、 人员离开，在一个项目实施的过程中，需要有一定的连续性，需要移交和交接，

有时人员离开对项目的影响会很大；

十一、 项目团队内部沟通不够，导致对项目设计和实施的理解上有偏差；

十二、 没有有效的备份方案；

十三、 没有切实可行的验收计划；

十四、 项目人员经验不足；

5、收尾阶段可能存在的风险：

一、 质量差；

二、 客户不满意；

6、维护阶段可能存在风险：

系统运行不稳定；

客户人事变化；

7.5.1.5.3 风险控制

1、风险分配

项目风险必须在项目参加者（包括投资者、业主、项目管理者、承包商、供应商等）之间进行合理的分配，只有每个参加者都有一定的风险责任，才有可能对项目管理和控制的积极性和创造性，只有合理的分配风险才能调动各方面的积极性，才能有项目的高效益。合理分配风险要依照以下几个原则进行

从工程整体效益的角度出发，最大限度地发挥各方面的积极性。

项目参与各方如果都不承担任何风险，则他也就没有任何责任，当然也就没有控制的积极性，就不可能搞好工作。因此只有让各方承担相应的风险责任，通过风险的分配以加强责任心和积极性，达到能更好地计划与控制。其有效的做法应为合同管理的机制到位，并面向各个承包商和参与方的工程合同，应站在工程总体的高度上进行控制和实施，公平合理，责、权、利平衡。

一是风险的责任和权力应是平衡的。有承担风险的责任，也要给承担者以控制和处理的权力，但如果已有某些权力，则同样也要承担相应的风险责任；二是风险与机会尽可能对等，对于风险的承担者应该同时享受风险控制获得的收益和机会收益，也只有这样才能使参与者勇于去承担风险；三是承担的可能性和合理性，承担者应该拥有预测、计划、控制的条件和可能性，有迅速采取控制风险措施的时间、信息等条件，只有这样，参与者才能理性地承担风险。

2、风险对策

任何项目都存在不同的风险，风险的承担者应对不同的风险有着不同的准备和对策，这应把它列入计划中的一部分，只有在项目的运营过程中，对产生的不同风险采取相应的风险对策，才能进行良好的风险控制，尽可能地减小风险可能产生的危害，以确保效益。

通常的风险对策为：采取先进的技术措施和完善的组织措施，以减小风险产生的可能性和可能产生的影响。如选择有弹性的、抗风险能力强的技术方案，进行预先的技术模拟试验，采用可靠的保护和安全措施。对管理的项目选派得力的技术和管理人员，采取有效的管理组织形式，并在实施的过程中实行严密的控制，加强计划工作，抓紧阶段控制和中间决策等。

3、实施中的全面风险控制

工程实施中的风险控制贯穿于项目控制（进度、成本、质量、合同控制等）的全过程中，是项目控制中不可或缺的重要环节，也影响项目实施的最终结果。

加强风险的预控和预警工作。在工程的实施过程中，要不断地收集和分析各种信息和动态，捕捉风险的前奏信号，以便更好地准备和采取有效的风险对策，以对抗可能发生的风险。

在风险发生时，及时采取措施以控制风险的影响，这是降低损失，防范风险的有效办法。

在风险状态下，依然必须保证工程按计划保证完成并达到预定的目标，防止工程中断和成本超支，唯有如此才能有机会对已发生和还可能发生的风险进行良好的控制，并争取获得风险的赔偿，如向保险单位、风险责任者提出索赔，以尽可能地减少风险的损失。

7.5.1.5.4 本项目存在的风险

项目的可能存在的风险具体来讲有如下方面：

1、项目如何保证各级人员统一认识，避免因为认识的不同，造成系统实施的不一致，或无法按照预定的目标实施，是需要特别防范的风险。

2、避免项目变更而给项目实施带来风险。

3、本项目的实施主要依赖各种硬件设备实现，如何解决实施过程中设备缺陷、故障导致的项目风险，需要重点防范。

4、项目实施过程中，相关责任人下认真、不积极按合同执行而给项目实施造成危害。如货物不能按期到货又不积极组织到货，项目设备有出现故障、问题而不及时解决等情况，影响项目的施工。

7.5.1.5.5 本项目风险的控制和应急方案

针对项目涉及范围广而造成的互联问题，在分系统施工中，首先采取对单一项目在施工过程中，严格加强质量管理的办法，使每个分系统都能够实现自己的调试正常，同时，要加强在各系统之间互相配合的检验测试，保证系统建成后是互联互通的。

针对工期短的情况，要求项目各方按照合同规定，明确项目机构组成，派遣固定的合格人员进行施工，并保证人员到位。

为保证项目工作一直，在施工前就设计方案、实施方案，要求各项目单位人员、施工方要熟练了解，并严格遵守和执行。

在项目实施过程中，各种设计方案、实施方案一经审批制定，除非遇到特殊情况，一般不允许更改。对于需要变更的情况，要严格审查变更原因的合理性、可实现性以及成本、工期等内容，并征得相关各方取得一致再予以变更。

对于设备缺陷、故障对带来的项目风险，要提前对主要的关键设备准备一些备件，便于发现问题是予以及时更换。对于设备缺陷造成的问题，要积极避免，在遇到相关问题时要立即采取妥善办法积极解决，避免将问题拖延而对整个项目造成影响。

对合同货物无法按期到货的情况，要立即给相关责任人下达整改通知书，要求其及时到货。对相关责任人不认真、不及时按合同执行的情况，要及时、严格的按照合同相关条款，要求其承担违约责任。

7.5.1.5.6 变更管理

项目发生变更时，如果管理不好，就会直接导致项目延期或失败，所以变更管理在整个项目的管理中处于重要位置。

大型复杂项目的变更往往会导致项目建设目标的偏离，造成投资的浪费和成本的不可控。因此对于项目的变更要严格控制，尤其对于重大变更必须由项目各方都参加的联席会议评审通过，对于重大的技术变更，必须由专家委员会评审通过。

项目变更管理主要是控制影响项目变更的因素，并有效控制变更的影响。

7.5.1.5.7 变更的类型

纳入本项目变更管理的变更类型主要包括：范围变更、业务需求变更、技术架构变更、进度变更、交付物变更。

从变更提出人的角度，又可以分为中标人提出的项目变更和招标人提出的变更。

如果是我方提出的项目变更，我们将提前对变更的影响和范围进行评估，并评估其变更对其他相关项目的影响，经招标人确认后方可实施变更。我方确保自身申请变更的合理性，在成本上可以接受，对受影响的交付物按照新基准进行相应调整。

项目终验前，对招标人要求发生的变更，我方应无条件接受，不对此额外申请费用。

7.5.1.5.8 变更产生的原因

造成项目变更的原因很多，具体包括如下：

项目的变更需求一旦执行，有可能会影响到项目计划的调整，这点在项目管理中要注意及时调整并发布给相关项目组成员。

7.5.1.5.9 变更控制流程

1、首先由需求人提出变更需求，提交给项目经理。项目经理接收到变更需要后，查看是否合理、信息是否全面；

2、项目经理委托有经验的实施组长或专家对变更需求进行分析，主要从变更对项目的质量、进度、费用、流程等各方面进行影响分析；

3、项目经理根据分析报告决定变更需求是否能实施，如果不能实施，提出解决建议并召开由项目联合办公室、项目领导小组参加的变更会议；

4、通过变更会议，对变更进行裁决是否可行；

5、项目经理应及时跟踪变更的执行，并分析对项目的实际影响。

7.5.1.5.10 变更控制文档

项目的变更需求一旦执行，有可能影响到项目计划的调整，这点在项目管理中要注意及时调整并发布给相关项目组成员。

项目的变更管理要结合项目管理信息系统的变更管理工具，变更的提交、评审、跟踪、实施以及变更相关配置文档的修订更改等都需要记录。

相关文档包括：《项目变更申请表》、《项目变更通知单》、《项目变更跟踪表》。

7.5.1.6 需求管理

需求是整个项目的设计开发和实现入口，对于需求的管理是非常有必要的。需求管理指识别、分析、建立客户需求，监控需求的状态，控制需求的变更过程，进行客户需求的追溯等活动。

7.5.1.6.1 需求管理的主要活动

需求管理为项目在需求方面建立和维护与客户的共识，并将所建立的客户需求作为估算、策划、实施和管理项目的基础；控制管理需求及其变更，使项目开发计划、工作产品和活动与客户需求保持一致；进行客户需求的追溯，可改善产品质量、降低维护成本、实现重用。需求管理的活动贯穿项目的整个生命周期。

需求管理强调：

(1) 控制对需求基线的变动。

(2) 保持项目计划与需求一致。

(3) 控制单个需求和需求文档的版本情况。

(4) 管理需求和联系链之间的联系或管理单个需求和其它项目可交付物之间的依赖关系。

(5) 跟踪基线中需求的状态。

需求管理的主要活动包括变更控制、版本控制、需求跟踪等几个方面，如图所示：

7.5.1.6.2 需求变更控制

当客户方提出新需求或有新的政策法规、管理制度下达时，要对已有需求进行需求变更。

（一）目的

修改“原需求文档”中不正确的内容，产生新的需求文档。

控制需求文档的变更，防止发生混淆。

（二）启动准则

项目组一方（来自开发方或客户方）提出变更“原需求文档”的申请（一般是新需求或新政策下达后）。

（三）主要步骤

- 1、提交需求变更申请
- 2、需求变更评审与审批
- 3、软件需求变更执行
- 4、需求变更追踪

（四）变更管理的控制流程

7.5.1.6.3 需求版本控制

版本控制是需求管理中必不可少的功能，特别是在多人协作的团队中，版本控制工具可以提高效率，消除很多由于版本带来的问题。

通过需求管理工具，可以记录需求变化的每一个版本，可以根据实际的业务流程需要定制版本自动变化的规则，定制为当需求文档发生变化、需求负责人、状态发生变化、或需求的某些重要字段发生变化，就自动记录需求的一个版本，需求管理工具不仅可以记录需求的版本，还可以恢复到需求的任何一个版本，这极大的方便了需求管理者的工作。

7.5.1.7 质量管理

本公司在软件行业的多年积累，沉淀和组织了非常先进的行业标准、项目执行和质量管理体系，在质量保证方面有非常成熟的管理理念和工具，形成了遵循 CMMI3 的规范和可执行的内部体系标准文档，并不断在完善和丰富。

7.5.1.7.1 质量保障措施

- 1、资深的质量经理与质保组

针对本项目，将派遣资深的质量经理参与质量保证组（简称 SQA 组）。SQA 组负责确保项目遵守质量保证体系的标准要求，确保遵循项目计划书中描述的要求，确保交付的软件及其文档以及非交付的软件在需求、设计及管理等诸多方面的质量。

2、全程参与的质量经理

质量经理，即质量保证组组长，监控项目成员的软件活动，并对软件产品与可适用的标准、过程和软件开发计划的符合性进行评价，为双方项目领导小组监控项目的软件生产提供适当的可视性。

3、合理的质量控制流程

质量经理负责对项目进行监控与分析，将结果报告给由双方高层人员组成的项目领导小组。项目经理批准发布给用户的所有文档和软件，必须得到质量经理的复核和批准。

7.5.1.7.2 额外的质量保障机构

项目执行部（PMO）：

除项目组设立质量保证及文档管理组外，为保证项目执行质量，公司设有专门的项目执行机构——项目执行部（PMO），是公司对项目质量控制和进度控制的监察部门，定期审查项目进度质及量，发现问题，协调解决。

7.5.1.8 资源管理

项目人力资源管理是为了保证所有项目参与人的能力和积极性得到最有效的利用而采取的一系列步骤。包括组织规划、人员选择和人力资源调配等。项目人力资源管理是项目启动初期最重要的活动。我公司将安排责任心强、技术高的人员参加项目设计和实施。另外，除项目组中安排的人员外，还提供一支后援队伍，随时根据项目情况的需要进行人员补充。

7.5.1.8.1 人力资源规划

通过人力资源规划，以确定项目的角色、职责、汇报关系并制定人员配置管理计划。人员配置管理计划包括何时需要什么资源、需要锁定的周期、人员释放的时间安排等。

人力资源计划主要使用到的工具包括组织机构图和岗位描述。通过组织机构图展示项目团队成员及其通报关系；岗位描述详细列出项目完成所需的角色、职责、职权和能力。

人员配备管理计划使用到的工具包括资源使用直方图、甘特图等。

7.5.1.8.2 项目团队组建

项目团队组建指获取完成项目工作所需的人力资源。

通过团队组建，获取适当的人员，并可靠地分配到指定的岗位上。完成项目计划的更新，将相应的人选指定到项目任务中。

形成项目人员资源的可利用情况表，资源可利用情况表记录了项目团队每名成员在项目上可投入的时间。制定可靠的最终进度计划取决于较好地了解每个成员在时间安排，避免冲突。

7.5.1.8.3 项目团队建设

项目团队的建设是指提高项目团队成员的能力和交互作用，从而提高项目绩效。包括：

- 1、提供项目团队成员的技能、以便提供其完成项目活动的能力；
- 2、提高团队成员之间的信任感和凝聚力，以通过更多的团队协作提高生产力。

团队建设的方式包括：

- 1、培训；
- 2、团队建设活动；
- 3、项目规章制度和规则的制定和明确；
- 4、集中办公；
- 5、奖励和表彰。

7.5.1.8.4 项目团队管理

项目团队管理指跟踪团队成员绩效，提供反馈、解决问题并协调各种变更，以提高项目绩效。主要内容包括人员管理和问题管理。

（一）人员管理办法

- 1、项目经理确定项目组内部人员，明确人员角色、所需技能、主要工作任务、参与项目时间等内容。
- 2、对于外部人员，需要明确单位或部门、角色和需要做的主要工作。
- 3、项目组的成员安排保证项目能按进度计划实施。项目组中项目负责人、项目经理、项目工程师、文档管理人员等各个角色有同等规模同类项目的实施经历。
- 4、项目组人员要每周提交工作周报，向项目经理汇报本周工作的进展情况和下周的工作计划，以及工作中存在的问题。
- 5、项目经理要对项目组内部人员的工作进行考核，并制定相应的奖惩措施。
- 6、项目经理指定专人负责整个项目周期中的文档管理和配置管理。
- 7、项目执行期间，保证项目人员保持稳定不变。如有特殊原因造成项目人员发生变动时，我们将事先通知客户方，并在征得客户方同意的前提下进行人员的调整。人员变更数量和要求遵守客户方规定。

（二）问题与冲突管理办法

项目团队管理常用的方法和工具包括冲突解决和问题登记跟踪。

1、冲突解决

项目团队之间不可避免的发生这样那样的冲突，如何成功的解决冲突，对项目的成败非常关键。成功的冲突管理可以提高生产力并促进积极的工作关系。

冲突的来源包括资源缺乏、进度安排的先后顺序和个人工作风格等。团队规则、团队制度规范可有效的减少项目冲突。

2、问题登记

对于项目过程发现的问题，可通过书面登记簿的形式来记录负责问题的责任人、问题要求解决的时间。

问题登记簿有助于团队成员监控问题的绩效，并消除团队的意见分歧、安排未预见到的职责安排。

通过团队管理，用于发现人员配备的变化，并为人力资源管理寻找纠正措施。包括人员配备的调整、额外的培训等、奖励措施等，并制定有关预防的措施，降低人力资源问题发生的概率和影响。

7.5.1.9 沟通管理

项目执行是一个团队任务，信息不畅容易导致工作偏离目标，或者是成员之间产生误解。项目执行过程中，我方将通过建立制度化的沟通渠道等方式，加强与客户方和监理方的沟通。

首先，我公司遵守客户方项目管理相关规定，接受客户方项目管理机构和项目负责人的领导，接受项目监理方的监理，指定负责人与客户方和监理方保持沟通和协调。

其次，我公司将建立项目例会制度，就项目进展情况、存在的问题、需要协调的主要事项、下一阶段工作计划等与客户方和监理方进行适时的沟通协调。

7.5.1.9.1 沟通汇报体系

沟通汇报体系是指通过建立适当的机制和流程，保证在项目涉及的范围内，将准确一致的信息在适当的时间、通过适当的渠道和工具传递给适当的对象，从而确保整个项目团队相关人员都能够及时了解项目目标、领导的指示、项目进展，并体验项目带来的工作环境改善和变化等。

主要工作包括：

- 1、制定清晰、一致、适时的沟通方法和计划；

- 2、按计划适时沟通，传递一致、清晰的信息；
- 3、获取沟通目标方的充分参与及反馈，取得项目全体人员的广泛支持；
- 4、根据本项目要求，设计不同形式的沟通方式，并定义恰当的沟通计划，有效实施沟通活动，包括：项目周（月）报、项目周例会、项目进度状态报告、项目高层决策会议、专题讨论会、项目信息发布等。

7.5.1.9.2 沟通管理的主要过程

1、沟通计划

沟通计划包括决定项目涉及人的信息和沟通需求：谁需要什么信息；什么时候需要；怎么获得。虽然所有的项目都需要沟通项目信息，但信息需求和传播方式差别很大。确认涉及人的信息需求和决定满足需求的适当方式是项目获得成功的重要因素。

项目执行过程中，沟通计划通常体现在项目计划和公司的管理规程中。

2、信息传播

信息发送是指将需要的信息及时地传送给项目涉及人，它包括实施沟通管理计划以及对突发的信息请求作出反应。发送者有责任使信息清晰、没有歧意和完整以便接收者能正确地接收。发送者也有责任确保信息被正确地理解。接收者有责任确保完整接收和正确地理解信息。沟通有很多类型：

书面的和口头的，耳听的和口讲的。

内部的（项目内）和外部的（与客户、媒体、公众的沟通）。

正式的（报告，指示等）和非正式的（备忘录，特别安排的谈话等）。

垂直的（组织内上下级之间）和水平的（与同级别之间）。

3、执行报告

执行报告包括收集和发布执行信息，从而向项目涉及人提供为达到项目目标如何使用资源的信息。执行报告一般应提供范围、进度、成本、质量等信息。许多执行报告也要提供风险和采购的信息。执行报告应写得具有综合性或针对某一特例。这样的过程有：

状况报告：描述项目当前的状况。

进展报告：描述项目小组已完成的工作。

预测报告：对未来项目的状况和进展作出预计。

项目执行过程中，执行报告的任务通常体现为小组周会、项目周报、项目月报等。

4、行政总结

项目或阶段在达到目标或因其他原因而终止后需要一个总结。行政总结包括对项目结果的鉴定和记录，以便由发起人、委托人或顾客正式接受项目的产品。行政总结包括项目

记录的收集、确保项目记录反映最终的设计书、项目成功和效益的分析以及对此类信息的立卷以备将来之用。

行政总结在项目进行中不应被拖延，项目的每一阶段应以适当的方式结束，以确保重要和有用的信息不会被丢失。

项目执行过程中，行政总结的任务通常体现为里程碑总结、阶段总结或项目总结等。

7.5.1.9.3 沟通机制

将建立管理各层之间的有效沟通机制，通过多种渠道来规范各类信息在组织内部快速流转，对于保证项目建设进度，避免信息不通所造成的延误、浪费等问题至关重要。

在沟通机制方面有多种方式，如日报、周报、会议纪要、工作联系单、会议等多种方式，其中定期的会议制度至关重要。

会议制度方面，我们建议在项目组内部开展两类重要会议，主要表现为项目周例会和项目定期汇报会。

1、项目周例会

(1) 目的

完成情况，讨论下周任务安排，协调项目问题。

(2) 主要内容

项目状态检查及进度跟踪；

当周重要事项的汇报；

下周详细工作计划；

变更请求状态检查；

近期需提交的提交件状态检查；

项目成员工作情况检查。

(3) 会议时间

属定期会议。

(4) 与会人员

项目经理，有关领导，各组长。

(5) 会议结果

会议纪要。

2、项目定期汇报会

(1) 目的

向有关领导汇报项目达到的主要里程碑情况，或重要情况单项汇报。

(2) 主要内容

项目的进展时间；

项目的完成进度；

项目的成本控制情况；

项目的完成质量；

下一阶段详细的工作计划。

(3) 会议时间

重要阶段或重要事件需要汇报时，属不定期会议。

(4) 与会人员

项目经理，有关领导，各组长。

(5) 会议结果

会议纪要。



7.5.1.10 监理配合

在项目实施各个阶段，我司公司将严格按照监理要求提交相关文档，并配合其工作。

1、项目启动阶段

在合同签订后，及时提交开工报审文件及相关材料，主要包括：总体实施方案 / 计划、进度计划、人员组织计划、档案提交计划、质量保证计划等，配合监理完成审核确认工作。

2、项目实施阶段

实施前期，按照项目里程碑计划，提交产品清单、到货验收文档、详细设计、部署实施、测试、验收、服务保障等相关方案和计划文档，提交服务保障相关的方案、计划、服务体系保障等文档，配合监理完成审核、修改、确认等工作。

实施过程中，及时提交项目工作报告、各类计划跟踪表、各项实施和服务保障记录以及各类统计分析报告等，配合监理的跟踪与检查工作。

实施完毕，尽快汇总各阶段、各类测试记录 / 测试结果，形成测试报告；汇总各项服务记录和成果，形成服务报告，提交监理审核并完成签署。

3、项目验收阶段

提交各阶段验收申请以及全部交付物，配合监理完成审核、修改、确认工作。

7.5.1.11 综合管理

项目整体管理包括在项目生命周期中协调所有其他项目管理知识领域所涉及的过程。它确保项目所有的组成要素在正确的时间结合在一起，以成功地完成项目。项目整体管理主要包括项目计划的制定、项目计划执行、整体变更控制。

7.5.1.11.1 项目计划的制定

项目计划是一个用来协调所有其他计划，以指导项目执行和控制项目的文件。

在制定项目开发计划的同时，也要依据项目计划确定配置管理计划和质量保证计划。项目计划必须经过领导层的评审，认定其合理性，批准后项目组按照计划实施。

7.5.1.11.2 项目计划的执行

项目计划的执行是指管理和运行项目计划中所规定的工作，在整体管理里项目计划和项目执行是不可分割的活动。

我司公司的项目经理在项目计划的执行中采用了诸如 MSProject 的管理工具，能提高管理的效率，项目组成员通过每周的例会，汇报已完成的工作和发现的问题，便于项目经理全面掌握项目的情况以作出合理有效的决定。

配置管理员负责按照配置管理计划对项目的各种配置项进行配置以及版本管理，确保产品在软件生命周期中的完整性和可追溯性。配置管理活动包括标识配置项、建立各种基线、控制版本和变更、保证变更被适当的实施，使开发人员、测试人员、项目管理者、质量保证人员以及客户能方便的通过软件配置管理获得有用的信息。

质量保证负责人依据质量保证计划定期或不定期对项目的执行情况进行过程评审，对发现的问题进行跟踪，直到问题关闭为止。

7.5.1.11.3 整体变更控制

变更的整体控制是指在项目生命周期的整个过程中对变更的识别、评价和管理等工作。

变更的流程为：变更提出人提出变更事项，项目经理和变更提出人统一意见后填写变更申请单（项目变更单），报项目领导层和客户进行审批，审批通过后由项目经理负责执行变更。

7.5.1.11.4 高层管理者的支持

项目经理能否成功的领导项目，其中一个非常重要的因素，就是看他们从高层经理那里获得支持的程度。对于本项目，我司公司给予了高度的重视，除了项目组的固定成员外，还有一定的资源作为后备力量，可以供项目进行调度。

7.5.2 项目实施进度

7.5.2.1 项目实施组织计划

7.5.2.1.1 分工界面

编号	阶段	任务	主要负责方	辅助方
1	准备阶段	合同签订	濮阳市社会医疗保险中心、我司	—
2		成立项目组织	我司、濮阳市社会医疗保险中心	—
3		实施计划	我司	客户确认
4		设备订购、供货	我司	—
5		实施前人员培训	我司	—
6		入场证办理	我司	客户协助
7		实施环境准备	濮阳市社会医疗保险中心	—
8		详细实施方案	我司	客户确认
9		IP规划、策略规划	濮阳市社会医疗保险中心	我司协助
10		详细迁移方案	我司制定	客户确认
11		网络实施及测试工具准备	我司	—
12	项目到货	到货接收	濮阳市社会医疗保险中心	我司协助
13		到货验收	濮阳市社会医疗保险中心	我司协助
14	项目实施	开工申请	我司申请	客户审核
15		设备及材料保管	濮阳市社会医疗保险中心	—
16		设备安装	我司	—
17		单项测试	我司	—
18		网络迁移	我司	客户协助
19		阶段评审	我司、濮阳市社会医疗保险中心	—
20	系统测试	调测	我司	—

编号	阶段	任 务	主负责方	辅助方
21		确认测试	濮阳市社会医疗保险中心	我司协助
22		阶段评审	濮阳市社会医疗保险中心、 我司	—
23	试运行与培训	设备试运行	濮阳市社会医疗保险中心、 我司	—
24		故障排除	我司	客户协助
25		现场技术培训方案	我司	客户审核
26		现场技术培训	我司、濮阳市社会医疗保险 中心	—
27	项目验收与移交	竣工资料	我司	客户审核
28		项目验收总结会	我司、濮阳市社会医疗保险 中心	—
29		验收报告签署	濮阳市社会医疗保险中心	—

7.5.2.1.2 时间计划

我公司承诺：在合同签订后，按照濮阳市社会医疗保险中心指定周期完成供货、安装、调试和验收。

项目建设期：10 日历天。

7.5.2.2 项目实施过程及质量保证

7.5.2.2.1 项目启动

工作计划

编号	任务描述	项目资源	备注
1	启动项目	我司、濮阳市社会医疗保险中心	
2	根据合同整理工作范围	我司、濮阳市社会医疗保险中心	
3	组织与用户的设计联络会	我司、濮阳市社会医疗保险中心	

工作流程

项目开始后，技术服务部任命项目经理和支持工程师，由项目经理负责发起后续的项目活动。

项目经理从委托方取得全部的与该项目相关的文件，其他任何渠道取得的文件只有参考作用，不能作为依据。

项目经理须仔细阅读合同中与工程相关的相关条款，主要包括：

项目中工作范围；

项目中其他各方的关系、分工、责任；

项目主要阶段、各阶段的标志；

项目中的主要技术承诺；

召开内部项目协调会，包括该项目售前、售前工程师或其他与本项目相关的人参加，了解项目的背景；

提交《项目计划》报上级经理；

督促并等待销售部门发起第一次设计联络会预备会的电话会议，明确在设联会之前双方须准备的相关资料，以传真或电子邮件的方式将联络会内容和用户须准备的资料发给用户并确认对方收到；

项目经理着手准备设计联络会的文档。

7.5.2.2.2 设计联络会

工作计划

编号	任务描述	项目资源	备注
1	组织会议	我司、濮阳市社会医疗保险中心	
2	与用户沟通项目管理方式	我司、濮阳市社会医疗保险中心	
3	确定双方的项目组织结构	我司、濮阳市社会医疗保险中心	
4	与用户建立汇报制度	我司、濮阳市社会医疗保险中心	
5	发货计划与到货计划 验货计划 方案讨论、设计规划初稿讨论及确定 工程界面确认 现场勘察计划 设备安装的机房要求和电源要求及准备计划 设备安装环境准备计划 用户培训计划 项目总体进度计划 验收计划 工程联系名单	我司、濮阳市社会医疗保险中心	

工作流程

设计联络会由我司发起，在会上向用户明确我方的项目经理，随后的会议由项目经理组织。

项目经理首先向用户讲解我方的项目管理流程，人员组成和职责。

项目经理应与用户明确双方的组织结构及接口流程，项目的沟通制度（包括汇报渠道、汇报周期），在会议纪要中反应。

在前 3 项内容明确后，讨论如下内容（每一项有后续任务的都要明确到责任人、时间）：

发货计划与到货计划；

验货计划；

方案讨论、设计规划初稿讨论及确定；

工程界面确认；

现场勘察计划；

设备安装的机房要求和电源要求及准备计划；

设备安装环境准备计划；

用户培训计划；

项目总体进度计划；

验收计划；

工程联系名单；

书写《会议纪要》，与会人员签字

项目经理根据设联会内容更新《项目计划》，提交双方上级批准；必要时对《项目计划》中的内容细化或简化，摘取必要的内容发给相关人员。

7.5.2.2.3 提出机房及配套设施要求

工作计划

编号	任务描述	项目资源	备注
1	督促各方，保证项目进度	我司、濮阳市社会医疗保险中心	

工作流程

项目经理要依照设计联络会的《会议纪要》中明确的内容和时间计划督促各方面的工作，如果出现影响进度的变动，需要有书面文件得到相关人员的确认。一般来说需要督促的工作包括但不限于以下：

现场勘察

用户机房准备

用户线路准备

用户业务接入的相关细节落实

某些技术问题的预先测试与确定

设计规划的最终细节的定稿

发货、验货

工程材料的确定与发货

项目经理定期提交《项目进展报告》给甲方，在《项目进展报告》中解释出现变更的原因。

7.5.2.2.4 安装环境检查

工作计划

编号	任务描述	项目资源	备注
1	与用户组织现场勘察	我司、濮阳市社会医疗保险中心	
2	进行现场勘察	我司、濮阳市社会医疗保险中心	

工作流程

现场勘察的目的是为了：

明确用户的现场准备工作内容

检查现场环境能否满足设备安装的要求

最终明确工程材料的型号

当需要制作和提供相关图纸资料的时候，项目经理要在现场勘察之前与用户讨论《现场勘察报告》的内容和提供的相关资料内容格式，明确并定稿。

项目经理应向用户明确《现场勘察报告》将作为工程实施的依据，减少用户现场环境变更的几率。

勘察前做好勘察前的准备工作（例如先明确各地勘察接待人员应是当地负责该项目的人员，事先将《现场勘察报告》的内容传真到各地先行准备，应提供各地机房的平面图纸复印件等）

工程师在进行现场勘察时应向用户明确《现场勘察报告》将作为工程实施的依据。

工程师在进行现场勘察时要在《现场勘察报告》中认真填写相关表格，如实反映现场情况，并让最终用户签字，必要时可留存最终用户一份拷贝。

工程师提交用户签字的《现场勘察报告》交项目经理处，项目经理检查汇总后与用户双方各留一份。

7.5.2.2.5 设备到货验收

工作计划

注：设备抵达现场后，由用户方、我方共同参与验收。

编号	任务描述	项目资源	备注
1	与用户组织验货	我司、濮阳市社会医疗保险中心	
2	进行验货	我司、濮阳市社会医疗保险中心	

工作流程

项目经理从商务部门/委托方取得《验货单》和《装箱单》，了解到货情况。

项目经理应协调用户、销售、委托方，确定发货、到货和验货时间和方式。

项目经理将《验货单》和《装箱单》分发到现场验货的工程师手中

现场验货的工程师验货步骤如下：

清点箱数，核实是否与发货单一致，记录签字。

检查箱子的外包装是否完好，记录签字。

清点箱中的货物，记录签字。

当上面任何步骤有意外时，验货人员应立即与相关人员（包括商务、项目经理、销售等），查找问题原因，必须现场解决。

如实纪录《验货单》中的各项，与用户签收《验货单》。

验货人员将签收的《验货单》汇总到项目经理处，项目经理做出《货物差异单》，和《验货单》一起反馈给委托方。

7.5.2.2.6 安装调试及初验

工作计划

编号	任务描述	项目资源	备注
1	设备安装调试及初验	我司、濮阳市社会医疗保险中心	

工作流程

在调试前，我方将向招标人提供详细调试计划、调试方法和调试要求，在招标人研究同意后启动系统调试阶段；

项目经理要与现场工程师明确每个节点的时间计划；

现场工程师要按照既定的时间计划进行现场工作，当变化超出自己的控制范围，导致不能按计划执行时，需及时与项目经理联系寻求解决办法；

项目经理将系统调试工作进度及相关情况定期向招标人报告；

现场工程师应严格按照相应设备专用安装规范进行设备安装；

现场工程师必须与用户在现场签署安装报告；

现场工程师在单点安装过程中确定卡板、端口及其他任何设备故障时，必须立即通告项目经理请求处理办法，如果处于厂家保修期的，应在 2 天之内将该设备寄给委托方指定的人员/地点；

现场工程师在进行设备配置、调试时要依照规划设计，如果发现规划设计中有错误，需征得支持工程师同意后方可现场修改，由支持工程师统一分发；

现场工程师离开现场时，需要清理现场，获得用户同意后方可离开。

7.5.2.2.7 系统测试

工作计划

编号	任务描述	项目资源	备注
1	制定测试方案	我司、濮阳市社会医疗保险中心	
2	对网络进行测试，验证	我司、濮阳市社会医疗保险中心	

工作流程

在工程安装结束前，现场工程师应与用户针对网络和系统的实际情况和合同要求，进行网络、系统的功能和性能的测试方案论证，形成最终的测试方案。

当设备依照设计规划安装、调试完毕，项目经理组织工程师根据《测试方案》对网络进行测试，并填写《测试纪录》。

当《测试记录》表明网络性能或功能未能达到预期目标时，项目组必须查明原因，执行整改措施，整改后再次进行测试，直到测试结果达到预期目标。

系统测试达到预期目标后，经招标方同意可进入 3 个月试运行。

7.5.2.2.8 系统试运行

工作计划

编号	任务描述	项目资源	备注
1	通过试运行测试网络是否可以达到预期建设目标	我司、濮阳市社会医疗保险中心	

工作流程

初验测试通过后，项目进入 3 个月的试运行。

试运行主要测试本次网络建设是否可以满足预期目标。

试运行期间逐渐将业务在所建网络上投入使用。

试运行期间根据业务运行情况对网络运行优化。

试运行结束后，签署《试运行报告》，作为项目终验的依据

7.5.2.2.9 项目终验

工程计划

编号	任务描述	项目资源	备注
1	与用户签署《项目终验报告》	项目经理组织	

工作流程

项目经理应仔细阅读合同，明确合同中的验收标准

项目经理应与用户明确验收的标准，形成《项目终验报告》

项目经理组织相关人员进行项目验收，签署《项目终验报告》

最终验收过程中提供以下文档：

《项目终验报告》

《项目竣工报告》（拓扑结构图、配置文档、安装报告资料等）

《维护手册》

7.5.2.3 供货安排

7.5.2.3.1 设备发货及货物包装、标注标准

本项目中所有设备及模块我方保证产品质量，随机附件，产品合格证，装箱单、随机资料及包装等设备和附（配）件符合其规定的性能，无瑕疵和缺陷，我方对质量问题负责包退、包换包修。产品符合招标书的要求，技术参数可靠。

货物提供原厂包装，以防货物在运输中损坏，并提供原厂包装证明。包装中以醒目的中文印刷字体在各包装箱上标明通用规范的运输标记或标志，如项目名称、货物名称与合同号、以及濮阳市社会医疗保险中心股份有限公司、我司双方名称等相关信息。每个箱子侧面清楚标明交货地点的全称；装箱单清楚注明每个交货地点的总箱数；包装箱内每件辅件都进行标签，标明“备件”或“工具”及具体名称，并注明合同号、箱号及安装站。濮阳市社会医疗保险中心股份有限公司有权不接收未按上述规定包装的合同设备、技术文件。

提供清晰、正确、完整的有关的技术资料，如样本、图纸、操作手册、维修指南及服务手册、产品产地证明书、质量保证书和系统操作说明书等，并随同货物一起发运。

7.5.2.3.2 设备运输及交货标准

我方负责设备安全、及时运输到用户指定的地点，运输所发生的费用由我方负责承担。运输过程中造成的设备故障或缺陷由我方承担。

我方在合同签订后即开始订货，并保证在合同规定日期内将货物运送至用户指定的地点，货物交货时间为我方派专人将所供合同所有货物运至用户方要求的最终目的地之时。

货物交货的同时向用户提交标明货物内容的明细单一式五份以及合同要求的相关文件，包括但不限于合同货物、全部配件、装箱单、生产厂家的检验证书、质量合格证书（由生产厂商签发）、原产地出厂证明文件原件、产品使用说明书及其它应当随箱的技术资料等。

7.5.2.3.3 到货验收

设备到达用户指定交货地点后，用户方应有专人接收和负责货物的看管，并在规定的时间内配合我方完成货物的验收，验收内容主要包括以下内容：

按照装箱单清点货外包装是否完整；

货物及配件是否完整；

设备加电自检和软件自主测试 主机硬件是否运行正常；

7.5.2.4 验收标准

7.5.2.4.1 验收原则

为了保证本项目实施工作完全符合项目设计的要求与合同中相关条款的约定，确保系统开通后，可以顺利运行，需要在项目实施完毕，并进行了一段稳定的试运行后，进行验收工作。

本项目的验收工作，本着坚持实事求是、客观公正、科学简便、讲求实效的原则，进行全面、认真、系统地检查验收。

7.5.2.4.2 项目验收参加方

项目建设单位：濮阳市社会医疗保险中心

项目实施单位：中国联合网络通信有限公司濮阳市分公司

7.5.2.4.3 到货验收

设备到货后，我司将会同用户共同对所有到货设备统一进行开箱检查和验收，并进行加电测试。

设备到货验收包括设备整体方案涉及产品的拆包验收。验收的内容和过程如下：

向用户提供设备、安装材料、工具、软件包和文件的发货清单，根据标书要求对全部设备的型号、规格、数量、外型、包装、资料、文件（如装箱单、保修单、随箱介质等）进行验收。

同时，对所有设备进行加电测试，确保设备能够正常运转。

如果到货设备与合同不符，或发生加电后设备无法正常工作现象，商务人员将依据合同进行货物的更换，直至满足合同的要求。

验收结果合格后，则产生一份由双方共同参与的验收清单，并注明日期。

7.5.2.4.4 系统验收

通过3个月试运行后，用户和我司将对系统进行最终验收。最终验收通过后，则该系统交付给用户正式运行，此后由用户技术人员负责系统的运行和日常维护、管理，我司提供相应的技术支持和服务。最终验收的内容是通过分析系统运行记录、业务系统的运行，评判系统的性能、稳定性、可靠性以及容错的能力。最终验收的结果要求提供由参加终验的各方签字的最终验收报告，并且给出最终验收的明确结果。当系统通过最终验收后，即进入系统运行维护阶段。

7.5.2.4.5 测试的方法

7.5.2.4.6 测试计划

项目系统安装调试工作完毕后，对于系统中存在的问题、错误和故障隐患，需要通过试运行测试及时发现并改正。

本节详细说明本项目的系统测试工作。

7.5.2.4.7 测试目的

系统测试时，首先对系统的各个子系统进行充分测试，然后将经过测试的各个子系统整合成一个完整的系统来测试。这是检验系统是否达到设计方案中描述的功能要求的有效方法。

系统测试的目的是选取易于发生错误的测试数据、方法和措施，以挑剔的态度，找出系统中的错误，记录下来，并改正错误，达到：

完成项目招标文件的功能要求

建设完成的系统达到设计要求

系统的高可用性、高可靠性、高性能；

保证系统的安全性、兼容性、操作性、效果、灾难和故障恢复能力

7.5.2.4.8 测试原则

系统测试是一个繁杂的工作，需要有计划、按步骤地进行，要选择好测试用例，测试数据不仅包括正确数据，还应包括错误数据和异常数据。

本项目的测试步骤按次序进行，先单元测试，再子系统测试，然后系统测试，最后是验收测试。不同测试内容使用的测试方法、测试人员不同。系统测试通过后，才可以正式投入运行。

本项目的系统测试原则是：统一安排，充分准备，全面、标准、规范地进行系统测试，测试结果客户最终确认。

7.5.2.4.9 测试时间安排

根据进度计划，系统测试时间安排在系统实施完成后。

由于各子系统实施先后不同，以及各子系统的测试所需时间的具体差别。总体上，遵循建成一项、测试一项，最后进行整体功能联合调试的原则。

7.5.2.4.10 测试内容

系统测试内容如下：

编号	测试内容		
1	硬件运行状态检查项目		
	单板状态检查	电源模块状态检查	风扇状态检查
	整机指示灯状态检查	机框防尘网检查	机房温度、湿度检查
	设备地线检查		
2	设备运行情况检查项目		
	设备运行情况检查	网络报文分析	设备对接运行状况检查
3	网络整体运行情况调查		
	网络运行问题调查	网络变更情况调查	网络历史故障调查

7.6 服务能力

7.6.1 服务内容

7.6.1.1 服务范围

本项目服务的服务范围为招标文件采购内容中涉及的所有产品及服务相关的技术要求。至少包括本次项目产品硬件维修更换，功能范围内的修改、完善、补丁更新以及版本升级，运维支持、软件升级、性能调优、应用对接、技术咨询、定期巡检和各种突发事件的应急处理等。

我司将在招标方定义的重要服务期内，提供重点技术保障服务。包括重大活动期间的技术保障服务、客户网络攻防演练服务、根据产品的运行情况，定期向用户提出产品安全性、稳定性、可靠性等方面的合理化建议及解决方案服务等。

7.6.1.2 服务期限

我司承诺为本次投标产品提供为期3年的质保服务，并提供质保期外服务。

7.6.1.3 服务内容

为了更好地为我们的客户服务，我司将遵循以下条款提供售后服务和技术支持。

序号	售后服务项目	质保期内 服务	质保期外服务 (免费)	质保期外服 务(收费)	增值服 务
1	安装及技术支持服务	√	/	√	/
2	原厂培训服务	√	/	√	/
3	软硬件升级服务	√	/	√	/
4	特征库、病毒库、漏洞库 等升级	√	/	√	/
5	设备维保服务	√	/	√	/

6	存储部件替换服务	√	/	√	/
7	服务档案管理	√	√	/	/
8	定期巡检服务	√	/	√	/
9	故障共享服务	√	√	/	/
10	定期回访服务	√	√	/	/
11	远程电话、邮件支持	√	√	/	/
12	远程登录支持服务	√	√	/	/
13	Internet 服务	√	√	/	/
14	定期提供技术动态	√	√	/	/
15	一般故障处理	√	√	/	/
16	重大活动期间保障服务	√	/	√	/
17	重大节假日前原厂巡检服务	√	/	√	√
18	安全通告服务	√	√	/	/

7.6.2 质量保证期内服务

质量保证期从全网现场验收通过之日开始计算，时间为3年。我方（我司）为用户提供3年的质量保证期。质量保证期内所有因更换或修理货物或部件而导致货物停止运行的时间从其质保期内扣除。

我司在质量保证期间，对因中标产品本身或我方原因造成的各种软硬件故障，均将迅速修复。

7.6.2.1 安装及技术支持服务

我司为用户所采购产品提供现场安装服务。安装服务的工作主要包括：安装前的安装环境调研、工具准备、环境准备，用户方需要配合的内容清单、产品安装时的注意事项清单、正式上线安装部署以及产品的连通性测试、可用性测试、策略配置等工作。

产品安装完成后，向用户交接并指导用户如何使用设备安装手册、用户使用手册、设备维护手册、技术白皮书、技术授权书等在内工程技术资料。在设备开通后，如发生系统应用软硬件或设备固件扩展升级等情况，我司负责现场升级，并向用户提供必要的技术资料。

在设备投入运行后，我司如对其系统软硬件有所改进，将及时通知用户，并为用户提供最新版本使用。如果由于维修服务失误或产品故障造成最终用户损失，除承担赔偿责任外，还需提供处理方案。

系统运行过程中如果出现技术故障（如硬件故障、软硬件故障、配置丢失等）或与其他软硬件发生冲突，我司及时提供紧急预案方案，保证24小时内解决此类问题，以恢复故障使得系统得以正常运行。

7.6.2.2 原厂培训服务

在实施阶段，我司将根据用户和项目需要，至少为用户提供现场和集中两种形式的培训。确保管理员和相关使用者能够独立地发现问题、定位问题，并能够处理简单问题，必要时联系供应商解决相关复杂问题。

7.6.2.3 设备升级服务

软硬件更新包括新版本软硬件的安装或者软硬件版本的维护。同一版本（Version），不同系列（Release）之间提供升级。

我司为本项目中的安全产品提供软硬件版本升级服务，升级频率为不定期。升级服务内容包括：功能优化、性能调优、兼容性升级、补丁升级、客户定制化需求升级等。如遇到重大高危漏洞，我司将会第一时间通知用户进行升级。

软硬件系统升级服务由我司技术服务中心承担，也可在我司的指导下，由客户自行升级更新。用户可通过我司指定的路径下载升级包，对于特殊需求的客户，我司提供定期光盘方式邮寄服务。升级过程均支持WEBUI浏览器管理界面升级方式。

7.6.2.4 特征库、病毒库、漏洞库等升级

我司对于具有特征库、病毒库、漏洞库等的安全产品，需要定期进行更新，一般升级频率为一周一次。如遇到重大高危漏洞、流行病毒或恶意程序，我司将会第一时间通知用户进行升级，并指导用户对防护策略或配置进行更新，使用户网络具备高危漏洞、流行病毒和恶意

程序的检测和防御能力。升级包的获取可通过我司指定的路径下载，对于特殊需求的客户，我司提供定期光盘方式邮寄服务。

7.6.2.5 设备维保服务

对于送修的未超过保修范围的产品，我司技术服务中心提供维修服务。维修范围包括但不限于与整机维修、配件维修、系统维修等。维修期间可根据用户和合同需要提供备机服务。

7.6.2.6 存储部件替换服务

当用户处的我司硬件产品需要返厂进行维修时，根据国家法律法规或行业、用户自身要求需要在返厂维修前将产品中的非易失性存储部件（即当没有电流通过时，所存储的资料不会消失的存储部件，例如：机械硬盘、固态硬盘、CF存储卡、SD存储卡、TF存储卡等）剥离，自行保管的情况。当发生上述情况时，我司为用户提供非易失性存储部件替换服务，用户可在我司工程师的指导下自行将产品中的非易失性存储部件拆除，或选择由我司工程师上门服务的方式将产品中的非易失性存储部件拆除。设备返厂维修时，我司公司会补充缺失的存储部件保证产品的正常运行。

存储部件替换服务只包含非易失性存储部件的硬件服务。如用户在存储部件替换服务过程中需要工程师上门，须同时购买产品现场服务。

7.6.2.7 服务档案管理

我司将在与用户建立起联系之日起，为用户建立技术服务档案，服务档案包括客户方的联系人及其联系方式、我司销售联系人及联系方式、售后联系人及其联系方式、项目不同阶段的问题及其处理情况、需求及其需求满足情况、待解决的问题等。

在售后阶段，服务档案对用户提出的问题和需求进行记录跟踪，并委派相应的工程师处理，及时给予响应。对于无法立即解答的问题，我司将对用户提出的问题进行备案，在寻求到解决方案后立即通知用户。为了保障服务档案管理有效运行，我司售后服务中心制定了定期考评机制，对用户服务档案进行审查，确保客户的问题和需求都得以解决和反馈。

7.6.2.8 定期巡检服务

在质保期内根据用户需要，为用户提供不少于2次的上门巡检服务。定期巡检的主要目的是规避信息系统可能出现的故障，消除风险隐患，对客户信息系统进行定期巡检，提早发现系统可能存在的风险进行规避。巡检内容包括但不限于：

与用户交流沟通产品在使用和操作方面存在的问题，并进行现场解决，不能现场解决的，与客户确定好时间点，在规定的时间内给出合理的解决方案。

对产品运行状态和产品运行日志进行查看，以发现产品运行过程中是否存在问题和异常，如存在问题和异常，将协助用户进行排查，直到问题解决。

协助用户对系统中记录的安全日志进行分析，以发现网络中存在的安全隐患和风险，并帮助客户提供解决方案。

协助用户对产品安全策略及产品性能进行优化，确保产品在使用过程中发挥其最大的效能。

巡检报告：每次巡检结束后，向客户提供巡检报告，报告内容包括：运行状况、存在的问题、策略调整和优化记录等，并对系统的优化和今后运行维护给出建议。

7.6.2.9 备品备件服务

我司在全国各分公司、分支机构均建有备品备件库，以满足各地客户需要。

7.6.2.10 性能调优服务

在质量保证期为用户提供性能调优服务，频率根据客户使用情况和需要来确定。此服务主要对系统和各功能模块的运行效率、性能进行分析，并根据分析结果从以下几个方面进行优化：操作系统优化、服务程序优化（含底层开发系统的优化）、安全策略的优化（参数调整）、网络环境的优化、重新部署等。

7.6.2.11 故障共享服务

我司提供用户所有货物在全世界范围内的实例分析和故障解决文档共享，并形成定期通报制度，帮助用户高效、准确的处理产品中遇到的故障和问题。故障解决文档的信息来源主要包括：热线服务的故障报修、定期巡检发现的故障问题、产品测试发现的故障问题等。所有

收集的故障问题及其解决方案，将会按照产品类别、问题类型等多个维度进行汇总，并按需共享给客户使用。

7.6.2.12 设备迁移服务

我司承诺针对本项目提供设备迁移服务。对于客户在产品服务期内所需要的安全设备迁移等需求提供必要的现场服务。设备迁移服务的具体工作内容包括：设备或系统配置备份、设备安全下线、新的部署环境的调研、上线环境需求整理、上线后配置及日志信息核查，必要时协助客户进行配置调整和优化。

7.6.2.13 设备更换服务

当主机系统在保修期内，一旦硬件系统出现故障，客户可通知我司，经我司工程师确认设备故障后，若是故障部件需要返修或更换，我司会在返修期间内提供能够正常使用的替代部件，更换的任何零配件均为其原厂家生产的或是经其认可的，所有的替代零配件均为未使用和未经修复的产品，除非最终用户提供书面许可，否则不可使用其他替代配件。

7.6.2.14 定期回访服务

为保证产品在客户方的使用效果，我司技术服务中心提供定期上门回访服务，并对产品进行检查、调试和维护，以便了解产品在客户网络环境中的运行情况，确保产品运行良好。回访过程中记录的所有问题都将报告给技术支持中心，并记入客户服务档案，以便跟踪问题后续的处理情况及客户的满意度情况。

7.6.2.15 远程电话、邮件支持

我司为客户提供售后“7×24”的远程电话技术支持服务和电子邮件支持服务，由我司经验丰富的客服专员接听来电，提供专业的技术支持服务。一般问题的解决方案回复不超过4小时，紧急故障响应时间小于30分钟。电话和邮件支持服务内容将记入客户服务档案，以便跟踪问题后续的处理情况及客户的满意度情况。

7.6.2.16 远程登录支持服务

我司建立有与用户连网的技术支持与响应中心，设置专人进行7*24小时值班，必要时，经客户允许，可以远程登录系统，进行设备维护、系统检查、故障诊断、软件调整等。主动检查、发现、修复各种原因引起的软件故障。

7.6.2.17 Internet服务

为保证客户能够通过多条路径及时获得我司的服务，我司在公司官网和微信公众号里提供线上销售咨询、培训业务咨询、技术支持咨询、安全服务咨询等，并提供行业最新技术解决方案、产品安全通告、公司及安全技术动态等内容、最新前沿技术动态、安全技术研究、网络安全实时动态、公司市场活动等内容，以帮助客户了解行业最新技术动态。

7.6.2.18 定期提供技术动态

为更好服务与客户，协助客户提升网络安全能力。我司可根据客户需要定期发送或推送安全事件动态、技术动态、行业动态等信息，内容可根据客户需求进行定制，提供形式可以是邮件方，光盘邮寄方等方式。

7.6.2.19 一般故障处理

客户方采购产品系统发生故障时，我司会立刻协调厂商技术人员进行响应。技术工程师在故障报修后，首先对故障级别和问题类型进行分析判断，安排对应部门人员进行故障处理。一般问题能够远程解决的，售后服务人员可通过远程电话指导客户方操作处理，如远程无法解决的，我司将就近安排技术支持人员现场解决。具体解决实效根据问题复杂程度决定。

7.6.2.20 重大活动期间保障服务

为帮助客户网络和业务在重大活动期间安全、稳定，我司专门成立特殊时期运现场维护障小组，提升服务级别，提高备件范围，提前深入健康检查，做好应急保障计划并在活动期间全程值守，保证客户网络和业务在遭到攻击时能够第一时间采取应急措施，将损失降到最低。

7.6.2.21 重大节假日前原厂巡检服务

重大节假日前原厂巡检服务主要是为保障客户网络、业务和数据在重大节假日期间能够安全、稳定、正常提供服务所提供的定向巡检服务。我司根据历年网络安全经验，制定了具备行业特性的安全巡检方案，在重大节假日对客户网络 and 核心资产的安全性进行安全检查，并根据巡检结果提供安全加固方案，确保网络和业务的安全可靠。

7.6.2.22 安全通告服务

安全通告服务通过我司安全运营服务中心每周汇总最新的安全漏洞信息、病毒传播信息、重大安全事故、安全法律法规、业界最新动态等，统一通过邮件发送给用户，使用户实时掌握最新的安全动态与安全资讯。

7.6.3 质量保证期外服务

7.6.3.1 安装及技术支持服务

我司为用户所采购产品提供现场安装服务。安装服务的工作主要包括：安装前的安装环境调研、工具准备、环境准备，用户方需要配合的内容清单、产品安装时的注意事项清单、正式上线安装部署以及产品的连通性测试、可用性测试、策略配置等工作。

产品安装完成后，向用户交接并指导用户如何使用设备安装手册、用户使用手册、设备维护手册、技术白皮书、技术授权书等在内工程技术资料。在设备开通后，如发生系统应用软硬件或设备固件扩展升级等情况，我司负责现场升级，并向用户提供必要的技术资料。

在设备投入运行后，我司如对其系统软硬件有所改进，将及时通知用户，并为用户提供最新版本使用。如果由于维修服务失误或产品故障造成最终用户损失，除承担赔偿责任外，还需提供处理方案。

系统运行过程中如果出现技术故障（如硬件故障、软硬件故障、配置丢失等）或与其他软硬件发生冲突，我司及时提供紧急预案方案，保证24小时内解决此类问题，以恢复故障使得系统得以正常运行。

7.6.3.2 原厂培训服务

在实施阶段，我司将根据用户和项目需要，至少为用户提供现场和集中两种形式的培训。确保管理员和相关使用者能够独立地发现问题、定位问题，并能够处理简单问题，必要时联系供应商解决相关复杂问题。

7.6.3.3 升级服务

软硬件更新包括新版本的软硬件的安装或者软硬件版本的维护。同一版本（Version），不同系列（Release）之间提供升级。

我司为本项目中的安全产品提供软硬件版本升级服务，升级频率为不定期。升级服务内容包括：功能优化、性能调优、兼容性升级、补丁升级、客户定制化需求升级等。如遇到重大高危漏洞，我司将会第一时间通知用户进行升级。

软硬件系统升级服务由我司技术服务中心承担，也可在我司的指导下，由客户自行升级更新。用户可通过我司指定的路径下载升级包，对于特殊需求的客户，我司提供定期光盘方式邮寄服务。升级过程均支持WEBUI浏览器管理界面升级方式。

7.6.3.4 特征库、病毒库、漏洞库等升级

我司对于具有特征库、病毒库、漏洞库等的安全产品，需要定期进行更新，一般升级频率为一周一次。如遇到重大高危漏洞、流行病毒或恶意程序，我司将会第一时间通知用户进行升级，并指导用户对防护策略或配置进行更新，使用户网络具备高危漏洞、流行病毒和恶意程序的检测和防御能力。升级包的获取可通过我司指定的路径下载，对于特殊需求的客户，我司提供定期光盘方式邮寄服务。

7.6.3.5 设备维保服务

对于送修的未超过保修范围的产品，我司技术服务中心提供维修服务。维修范围包括但不限于与整机维修、配件维修、系统维修等。维修期间可根据用户和合同需要提供备机服务。

7.6.3.6 存储部件替换服务

当用户处的我司硬件产品需要返厂进行维修时，根据国家法律法规或行业、用户自身要求需要在返厂维修前将产品中的非易失性存储部件（即当没有电流通过时，所存储的资料不会

消失的存储部件，例如：机械硬盘、固态硬盘、CF存储卡、SD存储卡、TF存储卡等）剥离，自行保管的情况。当发生上述情况时，我司为用户提供非易失性存储部件替换服务，用户可在我司工程师的指导下自行将产品中的非易失性存储部件拆除，或选择由我司工程师上门服务的方式将产品中的非易失性存储部件拆除。设备返厂维修时，我司会补充缺失的存储部件保证产品的正常运行。

存储部件替换服务只包含非易失性存储部件的硬件服务。如用户在存储部件替换服务过程中需要工程师上门，须同时购买产品现场服务。

7.6.3.7 服务档案管理

质保期外，我司依然为用户提供服务档案管理服务，对用户提出的问题和需求进行记录跟踪，并委派相应的工程师处理，及时给予响应。对于无法立即解答的问题，我司将对用户提出的问题进行备案，在寻求到解决方案后立即通知用户。为了保障服务档案管理有效运行，我司售后服务中心制定了定期考评机制，对用户服务档案进行审查，确保客户的问题和需求都得以解决和反馈。

7.6.3.8 安全巡检服务

在质保期外根据用户需要，为用户提供上门巡检服务。安全巡检的主要目的是规避信息系统可能出现的故障，消除风险隐患，对客户信息系统进行安全巡检，提早发现系统可能存在的风险进行规避。巡检内容包括但不限于：

与用户交流沟通产品在使用和操作方面存在的问题，并进行现场解决，不能现场解决的，与客户确定好时间点，在规定的时间内给出合理的解决方案。

对产品运行状态和产品运行日志进行查看，以发现产品运行过程中是否存在问题和异常，如存在问题和异常，将协助用户进行排查，直到问题解决。

协助用户对系统中记录的安全日志进行分析，以发现网络中存在的安全隐患和风险，并帮助客户提供解决方案。

协助用户对产品安全策略及产品性能进行优化，确保产品在使用过程中发挥其最大的效能。

巡检报告：每次巡检结束后，向客户提供巡检报告，报告内容包括：运行状况、存在的问题、策略调整和优化记录等，并对系统的优化和今后运行维护给出建议。

7.6.3.9 备品备件服务

我司在全国各分公司、分支机构均建有备品备件库，以满足各地客户需要。

7.6.3.10 性能调优服务

在质量保证期外为用户提供性能调优服务，频率根据客户使用情况和需要来确定。此服务主要对系统和各功能模块的运行效率、性能进行分析，并根据分析结果从以下几个方面进行优化：操作系统优化、服务程序优化（含底层开发系统的优化）、安全策略的优化（参数调整）、网络环境的优化、重新部署等。

7.6.3.11 故障共享服务

我司提供用户所有货物在全世界范围内的实例分析和故障解决文档共享，并形成定期通报制度，帮助用户高效、准确的处理产品中遇到的故障和问题。故障解决文档的信息来源主要包括：热线服务的故障报修、定期巡检发现的故障问题、产品测试发现的故障问题等。所有收集的故障问题及其解决方案，将会按照产品类别、问题类型等多个维度进行汇总，并按需共享给客户使用。

7.6.3.12 设备迁移服务

我司承诺针对本项目提供设备迁移服务，针对于客户在产品服务期内所需要的安全设备迁移等需求提供必要的现场服务。设备迁移服务的具体工作内容包括：设备或系统配置备份、设备安全下线、新的部署环境的调研、上线环境需求整理、上线后配置及日志信息核查，必要时协助客户进行配置调整和优化。

7.6.3.13 更换服务

当主机系统在保修期内，一旦硬件系统出现故障，客户可通知我司，经我司工程师确认设备故障后，若是故障部件需要返修或更换，我司会在返修期间内提供能够正常使用的替代部件，更换的任何零配件均为其原厂家生产的或是经其认可的，所有的替代零配件均为未使用和未经修复的产品，除非最终用户提供书面许可，否则不可使用其他替代配件。

7.6.3.14 驻场运维服务

根据项目和客户需要，我司将为客户提供现场维护服务，驻场运维服务内容包括本项目所采购所有产品的日常运维工作，即安全设备的策略建立、完善、变更；设备的配置、安全日志分析，安全事件监控与处理、安全设备硬件及软件的故障响应处理等。

7.6.3.15 上门回访服务

为保证产品在客户方的使用效果，我司技术服务中心提供上门回访服务，并对产品进行检查、调试和维护，以便了解产品在客户网络环境中的运行情况，确保产品运行良好。回访过程中记录的所有问题都将报告给技术支持中心，并记入客户服务档案，以便跟踪问题后续的处理情况及客户的满意度情况。

7.6.3.16 远程电话、邮件支持

我司为客户提供售后“7×24”的远程电话技术支持服务和电子邮件支持服务，由我司经验丰富的客服专员接听来电，提供专业的技术支持服务。一般问题的解决方案回复不超过2小时，紧急故障响应时间小于30分钟。电话和邮件支持服务内容将记入客户服务档案，以便跟踪问题后续的处理情况及客户的满意度情况。

7.6.3.17 远程登录支持服务

我司建立有与用户连网的技术支持与响应中心，设置专人进行7*24小时值班，必要时，经客户允许，可以远程登录系统，进行设备维护、系统检查、故障诊断、软件调整等。主动检查、发现、修复各种原因引起的软件故障。

7.6.3.18 Internet服务

为保证客户能够通过多条路径及时获得我司的服务，我司在公司官网和微信公众号里提供线上销售咨询、培训业务咨询、技术支持咨询、安全服务咨询等，并提供行业最新技术解决方案、产品安全通告、公司及安全技术动态等内容、最新前沿技术动态、安全技术研究、网络安全实时动态、公司市场活动等内容，以帮助客户了解行业最新技术动态。

7.6.3.19 定期提供技术动态

为更好服务与客户，协助客户提升网络安全能力。我司可根据客户需要定期发送或推送安全事件动态、技术动态、行业动态等信息，内容可根据客户需求进行定制，提供形式可以是邮件方，光盘邮寄方等方式。

7.6.3.20 一般故障处理

客户方采购产品系统发生故障时，我司会立刻协调厂商技术人员进行响应。技术工程师在故障报修后，首先对故障级别和问题类型进行分析判断，安排对应部门人员进行故障处理。一般问题能够远程解决的，售后服务人员可通过远程电话指导客户方操作处理，如远程无法解决的，我司将就近安排技术支持人员现场解决。具体解决实效根据问题复杂程度决定。

7.6.4 重大活动期间保障服务

为帮助客户网络和业务在重大活动期间安全、稳定，我司专门成立特殊时期运维现场维护保障小组，提升服务级别，提高备件范围，提前深入健康检查，做好应急保障计划并在活动期间全程值守，保证客户网络和业务在遭到攻击时能够第一时间采取应急措施，将损失降到最低。

7.6.5 软件版本定制服务

为满足客户个性化需求，我司对所有合同客户开放定制开发业务，包括Logo定制，软件版本定制，软件功能定制等。

7.6.6 专属安全专家服务

我司的专属安全专家服务为客户分配专属的支持专家，除公开的联系方式之外，客户可以直接联系专属的专家，享受更加专业和个性化的服务，跟踪并解决故障问题。

7.6.7 重大节假日前原厂巡检服务

重大节假日前原厂巡检服务主要是为保障客户网络、业务和数据在重大节假日期间能够安全、稳定、正常提供服务所提供的定向巡检服务。我司根据历年网络安全经验，制定了具备

行业特性的安全巡检方案，在重大节假日对客户网络 and 核心资产的安全性进行安全检查，并根据巡检结果提供安全加固方案，确保网络和业务的安全可靠。

7.6.8 定期技术交流

按照客户要求，我司每年提供定期的技术交流与技术培训，便于用户掌握系统的使用和维护。客户技术人员提出的技术交流需求，我司技术人员将会详细分析，并编制有针对性的交流方案，以解答客户疑问。

7.6.9 安全通告服务

安全通告服务通过我司安全云服务中心每周汇总最新的安全漏洞信息、病毒传播信息、重大安全事故、安全法律法规、业界最新动态等，统一通过邮件发送给用户，使用户实时掌握最新的安全动态与安全资讯。

7.7 售后服务方案

7.7.1 售后服务承诺

我司在本项目中，承诺做到：

- 1、能够及时响应采购人的委托事项；
- 2、针对本项目委派的固定售后服务人员配置全面，职责清晰，分工明确，积极组织落实，有详细的售后服务方案及措施；
- 3、严格做到文件中的售后服务响应时间；

7.7.2 服务保障措施

我司本着对用户负责的基本原则，为了严谨、认真地为用户服务，保障用户的切身利益，详细地细化售后服务分工响应程序。根据用户服务请求分辨是要求网络支持、硬件维修、还是软件维护，然后做出不同的分工响应，提供全面的系统整体支持服务，使用户系统运行更为可靠、稳定。售后服务分工响应流程如下图所示：



7.7.2.1 售后服务响应时间

我方承诺在收到通知后在甲方规定的响应时间内以合理的速度免费维护或修复有缺陷的系统组件。

7.7.2.2 应急保障措施

7.7.2.2.1 应急响应总体概述

为科学应对信息安全突发事件，建立健全信息安全应急响应机制，有效预防、及时控制和最大限度地消除信息安全各类突发事件的危害和影响，制订本应急预案，旨在解决以下几种故障：

应对系统自身出现的各类故障；

应对应断电、硬件设备故障等原因引起的各类故障；

应对因遭到攻击等恶意入侵引起的各类故障；

针对本系统，我们建议采取以下应急工作原则：

（1）预防为主。立足安全防护，加强预警，定期检查维护，保证系统稳定运行。

（2）快速反应。及时获取充分而准确的信息，果断决策，迅速处置，最大程度地减少损失和影响。

(3) 分级负责。按照“谁主管谁负责”的原则，建立和完善安全责任制及联动工作机制。加强各部门间的协调与配合，形成合力，共同履行应急处置工作的管理职责。

(4) 常备不懈。规范应急处置措施与操作流程，定期进行预案演练，确保应急预案切实有效，实现网络与信息安全突发事件应急处置的科学化、程序化与规范化。

7.7.2.2.2 应急组织机构和职责

采购项目在建设过程中，应成立一个专门的应急组织机构，成员包括客户及各信息化部门、集成商、系统硬件提供商、安全防护和数据库等应用软件提供商、系统运行网络承建商，各单位必须制定专人负责，安全小组组长由信息系统安全管理人员担任。

此次采购项目，我司针对可能出现的不同故障，提供不同的解决思路。

7.7.2.2.3 预测与预警

我司针对系统运行中各种可能发生的事件，建立了完善预测预警机制，整合监测信息资源，借助于我司的IT运维体系的相关管理流程，建立健全系统运行各类事件预测预警系统，开展风险分析，做到早发现、早报告、早处置。以下应急方案内容可以在项目实施之前和客户一同修改和完善确认。

7.7.2.2.4 应急处置

本项目的应急处置分为四个阶段，具体如下：

1、信息报告

系统运行中一旦发生突发事件，所在部门或当事人要保持镇静，在第一时间向本单位应急办公室和有关部门报告。报告内容包括时间、地点、事件的性质、影响范围、事件发展趋势和已经采取的措施、单位全称和联系电话等。重大事件必须在0.5小时内向客户突发事件应急领导小组报告，不得迟报、谎报、瞒报和漏报。

2、先期处置

事件发生后，事发地突发事件应急办公室要立即采取措施控制事态进一步发展，组织开展应急工作，并及时向上一级领导报告。

各职能处室、实际单位在报告重大突发事件信息的同时，要根据职责和规定的权限启动相关应急预案，及时、有效地进行处置，控制事态。

3、应急响应

对已处置但未能有效控制事态、或需客户协调处置的重大或特别重大的事件，由突发事件应急专业办公室向客户领导报告，经批准后启动相应应急预案。

4、指挥与协调

需要处置的事件，由突发事件应急领导小组统一指挥或指导各有关地区和部门开展处置工作。主要包括：

- (1) 组织协调有关地区和部门负责人及专家参与应急处置；
- (2) 制定并组织实施应急处置方案，防止引发次生、衍生事件；
- (3) 及时向领导报告应急处置工作进展情况。

事发地所在的单位负责成立现场应急指挥机构，在突发事件应急领导小组的指挥或指导下，负责现场的应急处置工作。

但针对不同的故障，我们除按照上述方式处置外，提出一些针对性的措施，具体如下：

7.7.2.2.4.1 系统出现故障处置

系统自身出现故障后，集成组将积极协调各子项目现场服务人员第一时间根据系统运行日志、错误日志等定位故障原因，并提出解决方案，及时消除故障；如果现场人员第一时间不能解决问题，则及时向项目经理汇报情况，项目经理及时组织人员，直接去现场或远程协助解决故障。

7.7.2.2.4.2 数据库故障处置

在系统运行过程中，必须确保系统数据安全。为此，各数据库系统必须实现异地备份，防止出现数据故障。在出现数据库故障后，必须采取正确有效的应对措施，尽快恢复数据，将损失降至最小：

- 1、一旦数据库崩溃，应立即向安全责任人报告，同时通知各单位暂缓上传上报数据。
- 2、安全责任人协调技术人员，尽快恢复数据，保证系统正常运行，并查明故障原因，及时维修，如遇无法解决的问题，立即向上级单位或软硬件提供商请求支援。
- 3、如果数据无法恢复，应立即向有关厂商请求紧急支援。

7.7.2.2.4.3 系统遭受攻击处置

在系统运行过程中，要采取安全防范措施，重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日备份，并将它们保存于安全处，确保系统正常运行，如果系统遭到恶意攻击，则应启动相应的应急措施，保证系统安全运行：

- 1、一旦软件遭到破坏性攻击，应立即向系统安全负责人员报告，并将系统停止运行。

- 2、如果数据遭到破坏，系统安全负责人员负责软件系统和数据的恢复。
- 3、系统安全负责人检查日志等资料，确认攻击来源。
- 4、安全领导小组认为情况极为严重的，应立即向公安部门或上级机关报告。

7.7.2.2.4.4 病毒安全紧急处置

在系统运行过程中，要安装病毒防护系统，如果发现病毒，则应启动相应的应急措施，保证系统安全运行：

- 1、当发现计算机感染有病毒后，应立即将该机从网络上隔离出来。
- 2、对该设备的硬盘进行数据备份。
- 3、启用反病毒软件对该机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作。
- 4、如发现反病毒软件无法清楚该病毒，应立即向安全小组负责人报告。
- 5、信息安全小组相关负责人员在接到通报后，应在十分钟内赶到现场。
- 6、经技术人员确认确实无法查杀该病毒后，应作好相关记录，同时立即向信息安全领导小组副组长报告，并迅速联系有关产品商研究解决。
- 7、安全领导小组经会商后，认为情况极为严重，应立即向公安部门或上级机关报告。
- 8、如果感染病毒的设备是服务器或者主机系统，经领导小组组长同意，应立即告知各下属单位做好相应的清查工作。

7.7.2.2.4.5 其他安全处置

当系统网络出现故障、电源中断、发生资源灾害后，也应启动相应的应急措施，保证系统安全运行，此类故障的软件处理措施基本同以上几种处理方式。

7.7.2.2.5 善后评估

1、善后处置

事发地所在的单位要积极稳妥、深入细致地做好善后处置工作。

因突发事件对用户的正常经营造成影响的，要及时、充分地做好解释工作，必要时适当给予一定的补偿。

2、调查与评估

突发事件应急领导小组要会同事发地各单位的应急办公室，对重大网络运行突发事件的起因、性质、影响、责任、经验教训等问题进行调查评估，并上报。

突发事件应急领导小组要组织各突发事件应急办公室，在每年第一季度对上年度发生的网络运行突发事件进行全面评估，并上报。

3、应急记录

应急办公室应督促有关职能部门做好应急记录。记录的内容包括：

事件的发生情况；

启动的预案等级；

应急预案的执行情况；

应急预案的执行结果；

存在问题及改进意见。



7.7.3 售后服务方式

7.7.3.1 我们对本项目服务的理解

对于项目，实现整个项目的可用性和实现系统的投资效益是本项目的重要目标。

传统被动的、孤立的、分散的“救火队”式服务管理模式，已经让IT部门疲惫不堪。如何简化IT管理，更好地满足用户在集成及相关业务方面对服务的需求，已经成为IT部门的一个重大挑战。我司在本次集成服务方案中的服务体系是在实践中不断摸索和总结中形成的，通过以上对本项目的理解，我司主要从以下几方面开展工作：

1、坚持统一规划、统一建设、统一管理思路

以往的服务管理实践表明，在集成工程建设初期，缺乏完整的系统框架设计、技术标准，将为整个工程的服务工作带来很大的技术困难。如果不形成统一的集成服务组织结构，也会带来许多沟通障碍、降低服务工作的效率。

2、引入先进的服务理论和服务管理工具

对现在比较流行的ITIL理论进行学习消化，将它应用到集成的服务体系管理实践中；选用适当的系统监控软件，将以前的事后应急处理变为对系统事件的提前监控。

3、优化服务管理流程

加大对重大系统故障的应急预案编制力度，强化对服务工作的技术总结，提高整个服务体系工作的处理能力和效率。

4、加强培训力度

提高普通业务人员的计算机应用水平和对专业系统的业务使用技能；加强信息中心技术人员的专业技能培训，多学习新的IT技术；提高技术人员的实际处理问题能力，从各个方面对各行政单位各类用户提供培训服务，使相关人员的信息化水平迅速提高。

5、各服务体系的可实施性和针对性

7.7.3.2 技术支持服务体系

1、可实施性

(1) 技术支持服务体系的可实施性体现在针对不同的服务对象，有专门的支持小组来负责，在技术支持的人员方面充分保障了技术支持服务的开展；

(2) 针对不同的工程实施阶段，我司安排对应的技术支持服务来服务，在服务对象方面具有很强的可实施性；

(3) 我司针对用户对于服务的不同需要提供多种服务方式，利用本地、远程、和专项三维立体的服务模式来为各行政单位用户以及其他系统承建商服务，更好的保证了用户平等的享受服务的权利。

2、针对性

(1) 技术支持服务体系能够针对不同的用户提供有区别的服务内容，并且利用各小组的合理分工保证提供给用户的服务具有组织上的针对性；

(2) 技术支持服务针对不同的工程实施时间段提出合理的服务规划和方法，使各用户在接受技术支持服务时具有工程阶段的针对性。

7.7.3.3 售后服务体系

1、可实施性

(1) 区分技术支持服务体系，与技术支持服务体系分别承担不同的服务工作和内容，通过两套独立的体系以及两组不同的人马来共同保证售后服务的顺利、平稳、高效的实施；

(2) 利用我司的售后服务档案机制加强售后服务问题库的建立，逐步积累问题经验，为以后的售后服务打下坚实的基础，为售后的顺利实施提供经验的积累；

(3) 在售后服务体系建立过程中，提供完备的具体措施和应急措施，加大售后服务的可实施性，把具体的控制措施落实到实处。

2、针对性

- (1) 针对不同的用户提供不同的售后服务内容；
- (2) 针对不同的内容提供相对应的售后服务方式来保证。
- (3) 质保期后我司将以最低的运行费用继续提供售后服务支持。

7.7.4 服务响应时间

- 提供每周 7*24 小时的热线电话咨询，为用户解答技术疑难；响应时间：立即；
- 我们承诺以下维护响应时间

设备或系统发生故障响应时间：重大故障≤30 分钟；较大故障≤60 分钟；一般故障≤60 分钟；其他故障≤60 分钟。修复时间：重大故障≤4 小时；较大故障≤8 小时；一般故障≤24 小时；其他故障≤48 小时，保证用户正常使用。

7.7.5 故障处理措施

根据应用系统出现维护问题的严重程度，我公司设定不同的故障级别，采取不同的故障响应方法。

我公司将售后技术支持工作主要分为四类，一般性技术支持、重大事件的技术支持、相关信息的反馈和常见问题培训等。

1、一般性技术支持问题

一般性技术支持指客户来电咨询有关问题，包括软件使用中的问题、与软件有关的业务问题以及不需要进行审批的一般性技术问题的处理；

对于一般性的咨询问题，要做好记录工作，填写《服务请求登记表》，并归档；

对于不需要领导审批的一般性技术问题，处理完成后填写《服务请求跟踪表》，并归档

2、重大事件的技术支持

重大事件的技术支持指客户由于误操作，会对业务处理结果产生影响的重大事件，或由于硬件故障引起的软件重安装、数据需恢复等涉及应用软件技术支持问题，以及应用系统软件出现影响系统整体业务处理的重大故障性问题；

此类问题，首先由售后服务经理向客户方有关领导反映，并发出正式报告，同时附上《重大请求审批表》，由技术部门和相关业务部门审批同意后，交由我公司的技术支持人员进行处理，处理完成后由相关支持人员填写《重大请求处理记录表》，并归档；

对于客户方领导不同意进行处理的请求，不得擅自进行处理。

3、相关信息的反馈

参与技术支持与售后服务的人员，要及时回答用户通过各种方式提出的有关问题，并尽快给出解决建议或初步解决建议，每星期将此信息反馈公司，便于公司有针对性对问题进行分类，对重复率高的问题编写常见问题手册；

为了使公司及时了解技术支持的工作状况，技术支持人员每星期应将本周处理的记录表及时整理反馈；

归档每月受理的重大请求及其处理意见和处理结果，统计每月重大请求涉及的技术问题、业务问题和问题原因；

每位支持人员每周需要进行支持总结，总结本周以来的收获及体会，放入公司相关目录下归档；

所有相关归档文件由专人保管，存放在指定位置，统一管理。

技术支持与售后服务项目经理根据技术支持人员统计的支持记录，需要进行归类分析，同时便于采取一些有针对性的对策。

4、技术支持与售后服务问题培训

根据整理和不断丰富技术支持常见问题手册，采取对系统维护人员不定期培训的方式，不断提高客户方系统维护人员的系统维护水平。

7.7.6 售后服务团队

应急指挥部职责：负责整体应急工作的指挥、协调和决策。成员：由机房运维主管担任总指挥，下设副指挥一名，负责具体协调工作。

现场救援组职责：负责现场救援、设备抢修及人员疏散。成员：由机房运维工程师、保安队长、消防专员组成。

通讯联络组职责：负责应急过程中的内外部通讯联络。成员：由行政专员担任组长，负责联络相关部门和人员。

后勤保障组职责：负责应急物资供应、生活保障及医疗救护。成员：由后勤主管负责，配备必要的后勤人员。

技术支持组职责：负责提供技术支持，协助处理应急事件。成员：由系统管理员、网络工程师、数据库管理员组成。

7.7.7 人员培训计划。

对于人员培训，对目前事后工作存在的问题，提出各自的观点，并向公司提出建议。通过参加培训交流，学习先进工作经验，交流工作体会，希望对今后工作有更加深刻全面的认识，并将参加培训的学习资料和工作体会与同事分享，共同促进今后事的各项工作。



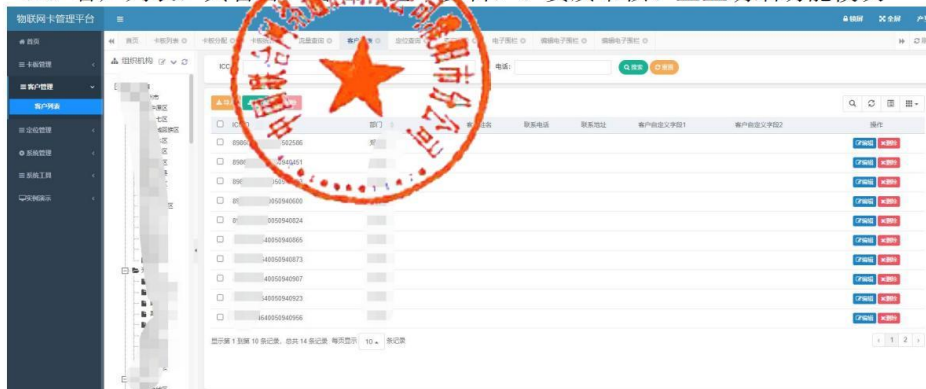
试用水印

十一、其他资料

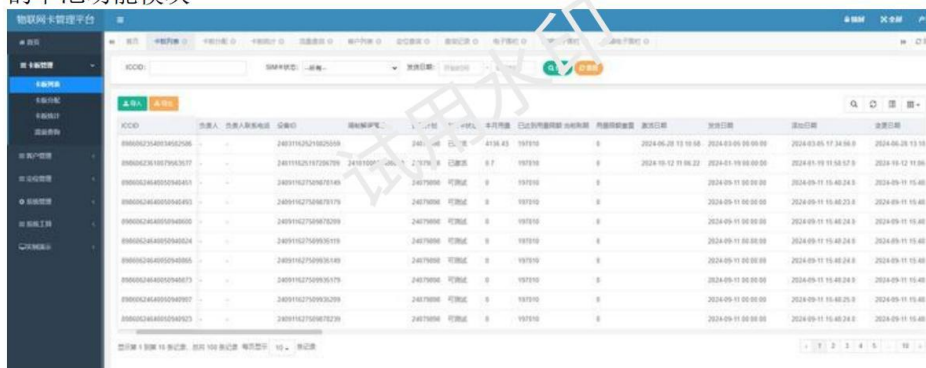
11.1 采购需求响应

11.1.1 物联网卡

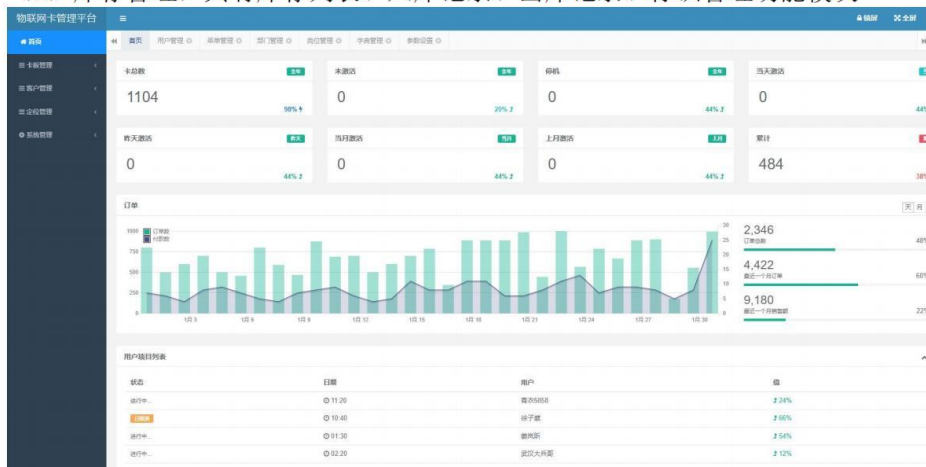
(1) 客户列表：具备客户管理（基本资料）、资质审核、企业明细功能模块



(2) 卡板管理：具有卡板列表、卡板回收、卡板统计、流量查询、实名列表、我的卡池功能模块



(3) 库存管理: 具有库存列表、入库记录、出库记录、标识管理功能模块



(4) 运维管理：具有通道管理功能模块

物联网卡管理平台

系统管理

设备管理

应用管理

数据管理

参数设置

卡状态

卡流量统计

客户订单

首页

系统设置

用户管理

设备管理

应用管理

数据管理

参数设置

卡状态

卡流量统计

客户订单

参数名称: 参数值: 系统内容: 所有 创建时间: 升序降序 刷新 重置

新增 修改 删除 添加 删除

搜索 重置

序号	参数主键	参数名称	参数值	系统内容	备注	创建时间	操作
1	主框架菜单默认品牌名称	main-blue	蓝色 main-14	2024-09-29 10:05:54	[编辑] [删除]		
2	用户管理-每页初始条数	123456	初始化管理器 1234	2024-09-29 10:05:54	[编辑] [删除]		
3	主框架菜单-侧边栏	system-dark	深黑主题theme--	2024-09-29 10:05:54	[编辑] [删除]		
4	账号登录-用户名正则表达式	^[a-z0-9]{4,16}\$	验证并限制使用功能。	2024-09-29 10:05:54	[编辑] [删除]		
5	用户管理-是否开启实名认证	0	默认不开启实名认证。0:	2024-09-29 10:05:54	[编辑] [删除]		
6	用户管理-是否开启人脸识别	1	0: 初始值为强制开启。	2024-09-29 10:05:54	[编辑] [删除]		
7	用户管理-是否开启密码强度	0	初始值为强制开启(弱密码)	2024-09-29 10:05:54	[编辑] [删除]		
8	主框架菜单-侧边栏-设备管理	system-index2	侧边栏侧边栏风格 (4-	2024-09-29 10:05:54	[编辑] [删除]		
9	主框架菜单-侧边栏-应用管理	system-index-view	侧边栏侧边栏风格。	2024-09-29 10:05:54	[编辑] [删除]		
10	主框架菜单-侧边栏-数据管理	system-index-tagView	侧边栏侧边栏侧边栏。	2024-09-29 10:05:54	[编辑] [删除]		

显示第 1 到第 10 条记录, 总共 11 条记录 每页显示 10 条记录

1 2

(5) 具有短信收发、短信记录功能模块

[illegible]

(6) 定位管理: ★具有定位查询、查询记录功能模块

(7) 统计分析：具有利润统计、激活统计、在网统计功能模块



11.1.2 CA身份认证 (Ukey)

(1) 符合 GM/T0024 标准或 GM/T0025 标准要求, 以及符合 GM/T0028 《密码模块安全技术要求》第二级的《商用密码产品认证证书》。



商用密码产品认证证书

证书编号: GM.4004410620230075

委托人名称及所在地

深信服科技股份有限公司
深圳市南山区学苑大道 1001 号南山智园 A1 栋一层

生产者(制造商)名称及所在地

深信服科技股份有限公司
深圳市南山区学苑大道 1001 号南山智园 A1 栋一层

生产企业名称及所在地

深信服科技股份有限公司
深圳市宝安区石岩街道石新社区宏发佳特利高新园厂一栋 4-5 楼

产品名称和型号、版本

深信服 SDP 安全网关
aTrust-1000-S2010C V2.0

产品标准和技术要求

GM/T 0025《SSL VPN 网关产品规范》
GM/T 0028《密码模块安全技术要求》第二部分要求

上述产品符合商用密码产品认证规则的要求, 特此发证。

颁发日期: 2023 年 2 月 8 日

有效期至: 2028 年 2 月 7 日

证书有效期内本证书的有效性由发证机构的定期监督获得维持。



牛路宏



国家密码管理局商用密码检测中心

中国·北京·万丰路300号 www.scctc.org.cn 证书通过此网站查询



11.1.2.1 生产厂商售后服务承诺函

生产厂商售后服务承诺函

致：濮阳市社会医疗保险中心

我们北京世纪龙脉科技有限公司是按中华人民共和国法律成立的
一家制造商，主要营业地点设在北京市海淀区五道口东王庄甲1号3
幢303号。

北京世纪龙脉科技有限公司作为项目名称：濮阳市社会医疗保险
中心濮阳市基层定点医疗机构网络安全接入服务项目/项目编号：—
濮阳市直磋商采购-2024-36 中 CA 身份认证（Ukey）的生产厂商，我
公司承诺提供包含但不限于以下服务内容：

1. 所购设备北京世纪龙脉科技有限公司将提供：年原厂免费质
保、免费现场服务和 7*24 小时快速服务，包括保修、电话支持、现
场支持、备品备件服务、软件升级等，技术服务热线支持中文。
2. 在技术服务期内，用户所提出的维修要求即刻做出实质性响
应，提供应急策略。

制造厂商名称：北京世纪龙脉科技有限公司（公章）

日期：2024年12月8日

11.1.3 零信任客户端

(1) 零信任客户端支持接入省级控制中心，且控制中心与客户端接口完整适配，保障省级控制中心的访问权限管理等安全策略能够下发至客户端且执行，客户端能够收集控制中心开展信任评估需要的信息，提供接入方式技术可行性文件。



深信服零信任具备用户权限管理功能，模型采用RBAC（Role-Based Access Control）授权模型，即通过角色进行访问控制。aTrust在RBAC的基础上，基于灵活性和实际业务场景考虑，额外增加了两种权限来源：基于个人的权限授予及基于组织架构的权限授予。允许管理员绕过角色，直接给个人用户或组织架构授权，满足多样化的权限管理需求。在aTrust权限管理模型下，用户、组织架构、角色、应用的关系如下：

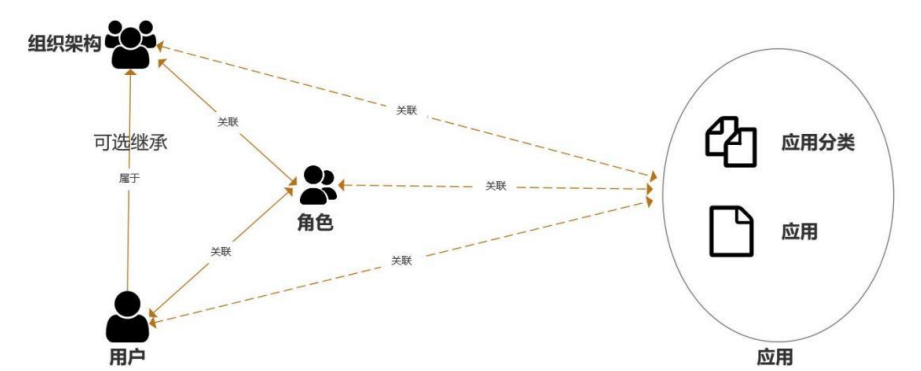


图 用户权限模型

如上图所示，用户的权限可以来自3个关联关系：

- 1) 用户直接关联的应用/应用分类

2) 用户关联的角色所关联的应用/应用分类

3) 用户继承上级组织架构所关联的应用/应用分类（包括组织架构关联的角色所关联的应用/应用分类），其中支持取消继承上级组织架构的权限

用户登录上线后，最终获得的权限范围，取上述3个关联关系的应用并集。

移动应用中心支持应用下载权限的管理，使得不同组织或者不同角色的员工具备不同应用的下载权限。通过细致的应用下载权限管理，防止非工作需要的员工越权访问移动应用和数据造成的数据安全泄密风险。



终端列表信息

控制台将收集已安装客户端的终端信息，包括：

1) 终端基本信息，例如终端名称、品牌、操作系统、MAC地址（注：MAC地址采集需要用户授权，移动端因操作系统限制不支持MAC地址采集）；

2) 终端标识信息，例如aTrust基于终端信息计算的终端唯一标识、硬件特征码、外部ID、资产类型、标签；

3) 终端授信信息，例如授信状态、绑定用户等；

4) 终端使用情况信息，例如首次录入时间、首次接入时间、接入状态、终端闲置时长、历史登录用户等；

5) 安装的aTrust客户端信息，例如aTrust版本号；

6) 用户上线信息，例如最后上线用户、组织架构、接入方式、网络区域、接入IP、最后上线时间、在线状态等等。

管理员可基于以上信息对终端资产进行管理。

终端匹配规则

管理员可以基于实际管理需要灵活调整终端匹配规则，客户端上报终端信息匹配时优先匹配硬件特征码，硬件特征码匹配不上时再根据勾选条件进行全量匹配，目前支持终端MAC地址、终端名称等条件。

(2) 零信任客户端需与省级CA身份认证方式进行准入，认证通过与省平台代理网关建立加密隧道，单点登陆访问医保核心业务区网络，提供详细技术文件（需体现技术对接过程及效果截图）。

深信服零信任可在WEB应用启用HTTP/HTTPS隧道应用开启单点登录功能，HTTP/HTTPS隧道应用目前支持票据共享方式单点登录，而WEB应用既支持账号代填实现单点登录，也支持票据共享方式单点登录。

通过共享aTrust票据凭证，获取用户信息并实现应用的单点登录。主要适用于由aTrust代理的OAuth2.0协议统一身份认证平台，以实现aTrust和统一身份认证平台的单点登录，目前有OAuth对接和票据注入两种工作模式。

OAuth对接单点登录过程如下：

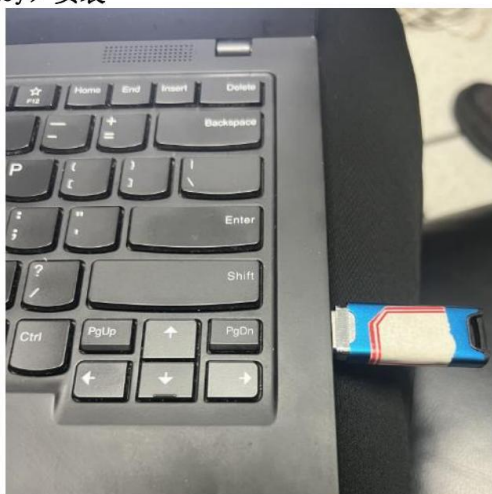
- 1) 当应用未登录时，页面302重定向至aTrust登录页面；然后aTrust将用户的票据信息回传给应用（回调地址）；
- 2) 应用再到aTrust验证用户票据的有效性，从而获取用户信息并完成应用登录。

票据注入单点登录过程如下：

当应用未登录时，零信任网关将识别其为改写地址，并截获请求流量；将aTrust用户的票据信息注入在应用请求头部；

应用再到aTrust验证用户票据的有效性，从而获取用户信息并完成应用的登录。

身份认证（Ukey）安装



插入UKEY后正常情况下，客户端会自动识别用户信息，并自动输入用户名，如下图，此时只需要输入默认密码即可，默认密码一般为123456或者12345678。



如下图，当输入密码完成后，点击我已阅读并同意《用户协议》，点击登录，即说明已完成零信任客户端的登录。此时已经可以访问业务系统。



(3) 为保障客户端与服务端对接符合此次建设需求，保障顺利接入调试，要求投标人提供由设备生产厂商和网络服务商出具的技术证明文件，文件内容说明已经对接并调试成功，要求证明文件同时加盖投标人公章。

零信任客户端安装

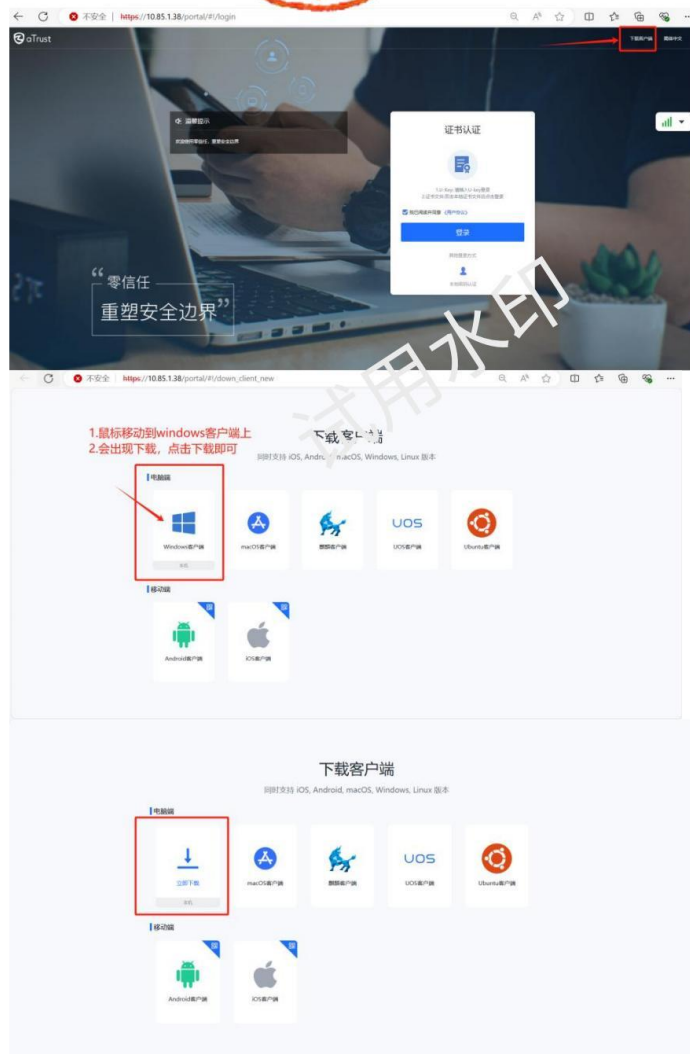
客户端下载

1) 卡托插入终端电脑

在下载客户端前，先将带有物联网卡的卡托插入终端USB口，确保与零信任的设备网络是联通。

2) 首先在电脑上打开浏览器

(推荐使用Chrome谷歌浏览器)，在浏览器地址栏输入零信任访问地址 <https://10.85.1.38/>，如下图所示，在右上角下载客户端，按照系统类型，如为windows系统，选择windows点击下载即可。



3) 客户端安装

如下图所示，下载完成后，双击安装包，会弹出安装界面，点击立即安装。



用户登录

安装完成后会自动打开客户端，同时提示安装完成。这时候将认证UKEY插入或安装前插入到终端。如下图



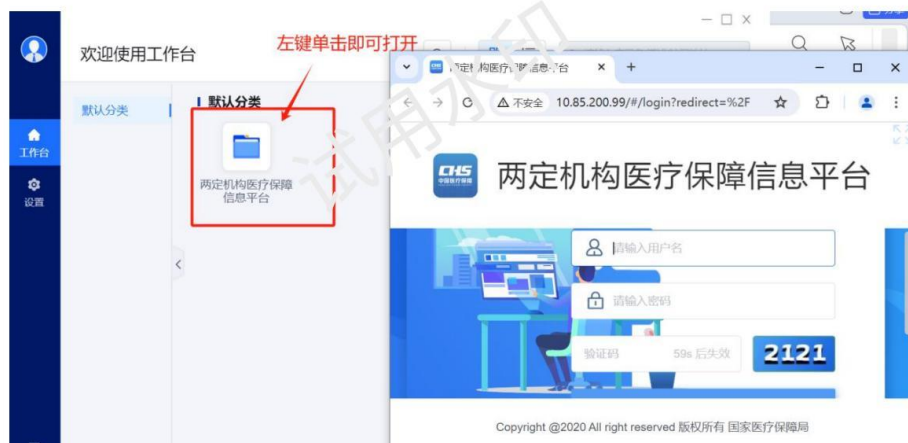
如下图，当输入密码完成后，点击我已阅读并同意《用户协议》，点击登录，即说明已完成零信任客户端的登录，此时已经可以访问业务系统。



访问医保业务系统

访问医保业务系统方式支持两种方式:

方式1: 直接点击客户端界面的对应业务系统资源,



方式2, 浏览器上输入<http://10.85.200.99/>或其他已经在零信任上发布的资源的地址, 也可以进行打开, 然后正常访问业务系统即可。

注意: 登录客户端后, 医保业务访问同原先正常访问一致, 原先如何访问现在也是如何访问。



零信任使用注意事项

零信任客户端登录时需要有带物联网卡的卡托（能访问到零信任的地址和端口10.85.1.38和42，443和441端口），如打开客户到接入页面，而不是输入密码的登录界面，先检查网络是否可达。



如下图，如果telnet 10.85.1.38 的443端口正在连接xxx的情况，同时等待一会后出现连接失败的提示，说明网络不可达，需要确认卡托是否正常插入，以及4G卡是否正常。



1) 安装时一定要关闭杀毒软件, 如果出现非输入账号密码错误的问题, 或者登录后无法使用的问题。首先检查是否开了杀毒软件, 关闭杀毒软件后, 重新安装打开, 或尝试重启后, 关闭杀毒软件重复此步骤。如果该方式仍无法解决, 联系零信任管理员。

2) 登录客户端后, 目前已做了网络限制, 当接入零信任客户端后, 原来如连接了互联网, 则无法上网, 需要退出客户端才可恢复。以此确保医保网和互联网存在网络隔离。所以当登录零信任客户端后如发现无法上网的问题属于正常情况

(4) 零信任客户端可针对接入电脑终端情况进行检测、信息收集和上报能力, 并实现可信应用识别, 检测项包括但不限于应用种类、应用的进程信息、终端MAC地址、操作系统及版本、操作系统是否存在漏洞、是否运行杀毒软件、是否开启本地系统防火墙、接入地市等, 省级控制中心进行信任评估, 并下发安全管控策略。

用户安装了深信服零信任客户端后, 客户端可上报终端信息至服务端, 提供终端安全检测的能力, 对接入的终端当前的环境(如操作系统、防火墙、杀毒软件、应用进程)进行收集和上报, 上报给aTrust控制中心进行信任评估的策略管理。开启SPA服务隐身后, 只有授权过的aTrust客户端才能连接控制中心和代理网关, 才能进行认证、授权和代理访问。

终端列表信息

控制台将收集已安装客户端的终端信息, 包括:

1) 终端基本信息, 例如终端名称、品牌、操作系统、MAC地址(注: MAC地址采集需要用户授权, 移动端因操作系统限制不支持MAC地址采集);

2) 终端标识信息, 例如aTrust基于终端信息计算的终端唯一标识、硬件特征码、外部ID、资产类型、标签;

3) 终端授信信息，例如授信状态、绑定用户等；

4) 终端使用情况信息，例如首次录入时间、首次接入时间、接入状态、终端闲置时长、历史登录用户等；

5) 安装的aTrust客户端信息，例如aTrust版本号；

6) 用户上线信息，例如最后上线用户、组织架构、接入方式、网络区域、接入IP、最后上线时间、在线状态等等。

管理员可基于以上信息对终端资产进行管理。

终端匹配规则

管理员可以基于实际管理需要灵活调整终端匹配规则，客户端上报终端信息匹配时优先匹配硬件特征码，硬件特征码匹配不上时再根据勾选条件进行全量匹配，目前支持终端MAC地址、终端名称等条件。

终端导入导出

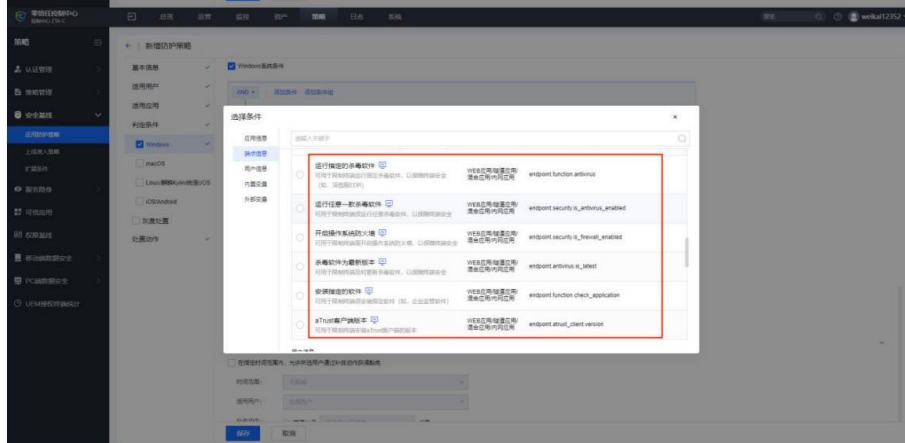
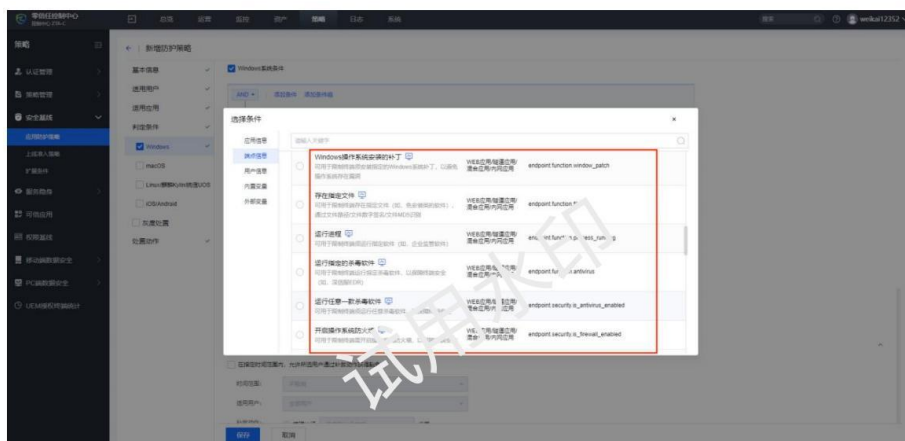
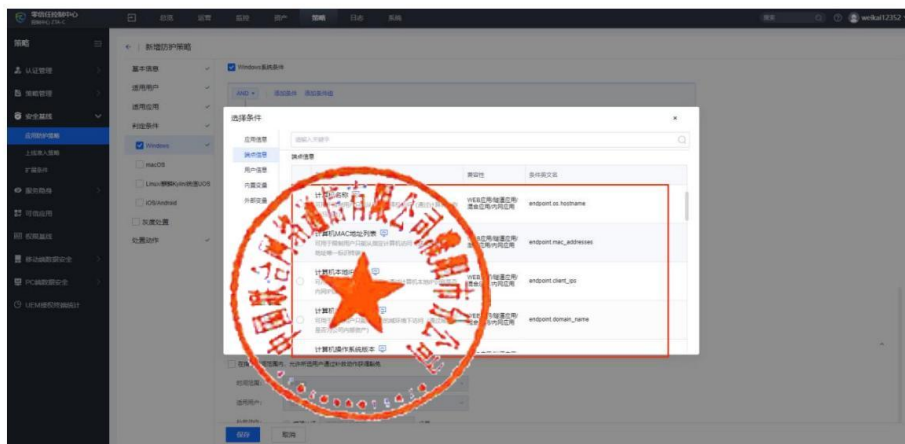
管理员可以通过下载导入模板，按照格式要求填写终端数据后导入的方式批量新增/更新终端信息；同时支持批量导出终端信息，可通过勾选或筛选指定导出范围。

终端搜索

支持按终端名称、MAC地址、最后登录用户、用户显示名、用户描述进行单个搜索、批量搜索，同时支持按操作系统、UEM授权类型、终端闲置时长、资产类型、标签、在线状态、授信状态、windows域控、接入状态、首次在线时间、最后活跃时间等条件进行筛选。

终端编辑/删除

支持在页面编辑终端的资产类型、标签，同时支持删除终端信息。

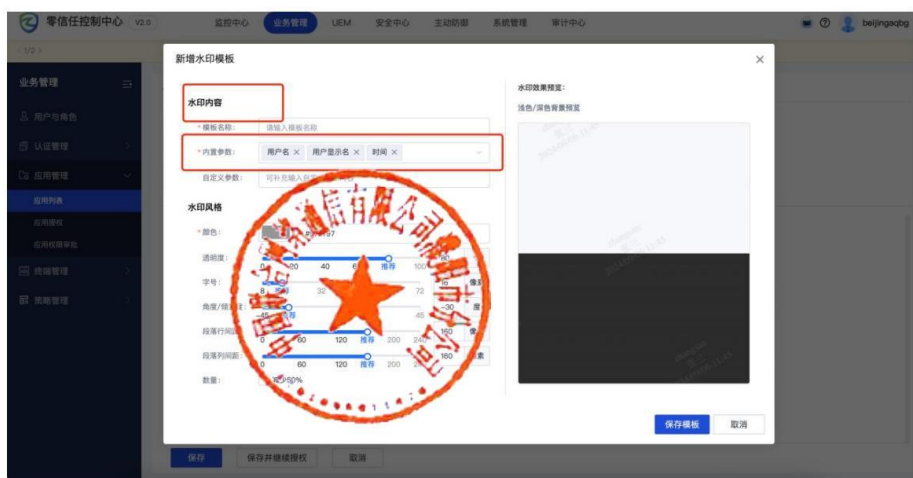


(5) 零信任客户端可针对发布的应用开启WEB水印，水印内容包括不限于登陆用户名、当前年月日，提供证明截图及详细技术介绍。

深信服零信任支持WEB水印：aTrust支持明文水印，水印内容包括用户名和日期，该功能不依赖客户端。通过WEB水印，可以防止通过截屏、拍照等方式泄露WEB页面内容。

为了弥补传统隧道技术的缺陷，同时避免WEB资源的兼容性问题，aTrust在隧道技术上创新性提出了隧道转WEB技术。aTrust通过客户端将访问流量经过隧道技术代理，再转发到本地WEB代理服务，由WEB代理服务器将流量代理至上游资源服务器。经过隧道代理的访问流量，能保留隧道应用兼容性好、传输速度快的优势；而将隧道代理转为WEB代理，能实现应用层的功能（URL审计、WEB水印等）。





★（6）为保障访问医保业务的稳定性，零信任客户端应支持给予TCP的协议优化，针对访问隧道的抗丢包、抗抖动等特性进行增强，提供证明截图及详细介绍。

深信服零信任客户端支持给予TCP的协议优化，针对访问隧道的抗丢包、抗抖动等特性进行增强。

弱网宽带优化

通过对TCP协议的专项优化，隧道具备抗丢包、抗抖动、平稳发送的优点，实现弱网环境的访问加速，并具备以下优势：

抗丢包：通过TCP拥塞控制算法优化，解决因为丢包导致发送窗口大幅减少，从而具备较强的抗丢包能力；

抗抖动：通过基于反馈的自主控制算法，解决网络事件导致带宽抖动，从而具备较强的抗抖动能力。

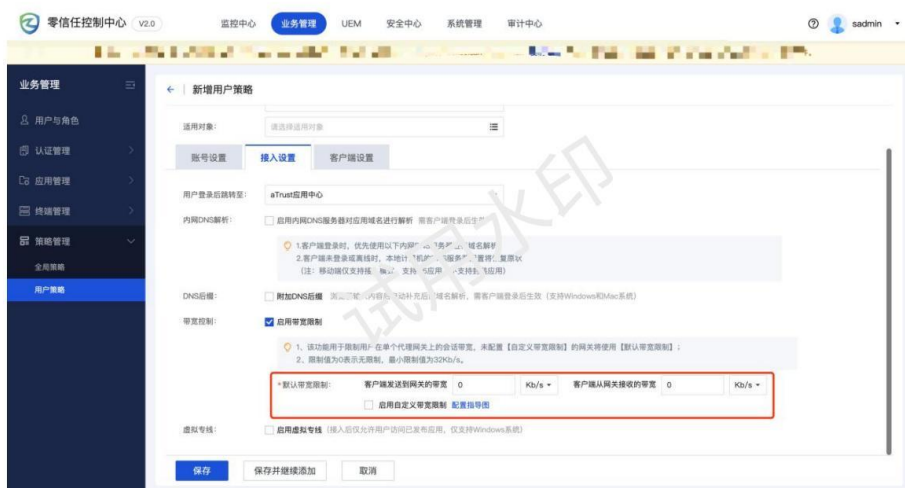
时延优化

通过自研的 Local Handshake 和 Early Data 技术，将新建连接耗时优化至0RTT，大幅降低业务访问的网络时延，实现同等网络环境下访问速度达到甚至超越直连访问。

注意：时延优化仅对PC端短隧道资源访问生效。

禁止浏览器接入

为了通过aTrust客户端访问隧道应用、加强ACL安全策略等，管理员可通过勾选此项禁止用户通过浏览器认证和访问Web应用，并支持自定义禁止接入的提示和是否显示客户端下载链接。



★(7) 零信任客户端应兼容主流非国产终端和非国产操作系统、主流国产终端和国产操作系统，提供兼容性列表。

操作系统	操作系统版本	芯片架构	芯片	固态硬盘接入150GB以上固态硬盘	USB	应用DMM、PC配置配置(CPU、内存、硬盘)	备注说明
Windows	Win7 SP1	386	奔腾 4	支持	支持	支持	仅支持Win7 SP1
	Win10		奔腾 4	支持	支持	支持	虚拟机网络模式仅支持网桥模式
	Win11		奔腾 4	支持	支持	支持	仅支持Win10 1809及以后版本
	Windows server 2008		奔腾 4	支持	支持	支持	
	Windows server 2016		奔腾 4	支持	支持	支持	
	Windows server 2019		奔腾 4	支持	支持	支持	
	Win10	ARM	奔腾 4	支持	支持	支持	
	Win11		奔腾 4	支持	支持	支持	
	Windows server 2016		奔腾 4	支持	支持	支持	
	Windows server 2019		奔腾 4	支持	支持	支持	虚拟机网络模式、USB不支持Windows ARM平台
macOS	MacOS 10.15	386/ARM	奔腾 4	支持	支持	支持	
	MacOS 11.1		奔腾 4	支持	支持	支持	
	MacOS 12.1		奔腾 4	支持	支持	支持	
	MacOS 13.1		奔腾 4	支持	支持	支持	
	MacOS 14.1		奔腾 4	支持	支持	支持	
	MacOS 15.1	386	奔腾 4	支持	支持	支持	
	MacOS 16.1		奔腾 4	支持	支持	支持	
	MacOS 17.1		奔腾 4	支持	支持	支持	
	MacOS 18.1		奔腾 4	支持	支持	支持	
	MacOS 19.1		奔腾 4	支持	支持	支持	
iOS	iOS 12.0	ARM	海思麒麟960	支持	支持	支持	
	iOS 13.0		海思麒麟960	支持	支持	支持	
	iOS 14.0		海思麒麟960	支持	支持	支持	
	iOS 15.0		海思麒麟960	支持	支持	支持	
	iOS 16.0		海思麒麟960	支持	支持	支持	
	iOS 17.0	MIPS	海思麒麟960	支持	支持	支持	
	iOS 18.0		海思麒麟960	支持	支持	支持	
	iOS 19.0		海思麒麟960	支持	支持	支持	
	iOS 20.0		海思麒麟960	支持	支持	支持	
	iOS 21.0		海思麒麟960	支持	支持	支持	
Android	Android 10.0	Loongarch	龙芯3000	支持	支持	支持	
	Android 11.0		龙芯3000	支持	支持	支持	
	Android 12.0		龙芯3000	支持	支持	支持	
	Android 13.0		龙芯3000	支持	支持	支持	
	Android 14.0		龙芯3000	支持	支持	支持	
	Android 15.0	V10	海思麒麟960	支持	支持	支持	
	Android 16.0		海思麒麟960	支持	支持	支持	
	Android 17.0		海思麒麟960	支持	支持	支持	
	Android 18.0		海思麒麟960	支持	支持	支持	
	Android 19.0		海思麒麟960	支持	支持	支持	
Harmony	Harmony 1.0	Loongarch	龙芯3000	支持	支持	支持	
	Harmony 2.0		龙芯3000	支持	支持	支持	
	Harmony 3.0		龙芯3000	支持	支持	支持	
	Harmony 4.0		龙芯3000	支持	支持	支持	
	Harmony 5.0		龙芯3000	支持	支持	支持	
	Harmony 6.0	V10 (SP1)	海思麒麟960	支持	支持	支持	
	Harmony 7.0		海思麒麟960	支持	支持	支持	
	Harmony 8.0		海思麒麟960	支持	支持	支持	
	Harmony 9.0		海思麒麟960	支持	支持	支持	
	Harmony 10.0		海思麒麟960	支持	支持	支持	

注：不支持Windows XP系统，因为Trust客户端设备使用Electron框架，该版本不支持该系统，无法定制。（QQ、飞信等众多主流APP采用“electron X”），不支持。因此，桌面端只能选择支持Windows 8及以上的系统。

2. Windows Server不支持太多语言，同时使用Trust客户端时，必须从Trust客户端中选择不支持中文。

3. 不存在 [Windows 7+ARM]、[Windows Server 2008 + ARM] 组合。

4. 不存在 [Erlin V10 - Longhorn2]、[Erlin V10-Server9000]、[Erlin V10-Home9000] 组合。

5. 不支持在信任域内安装不支持中文的操作系统和杀毒软件。

6. 必须将网络域和网络名称设置为Windows 8兼容模式。

7. SFTP在、桌面网络和功能都不支持Hadoop，Centos系统，原则上不推荐使用。

8. SFTP在、桌面网络和功能都不支持Hadoop，Centos系统，原则上不推荐使用。

9. 不支持WinSCP 6.10.12及以上版本，因为WinSCP的信任域信任策略有问题，造成与Aerospike 3.7.1以上版本无法互操作。

(8) 要求零信任客户端具备医保接入网管理能力，可自定义上传医保虚拟网络域图标，并在客户端切换处显示该图标及图标名称，例如图标名称为河南省医保接入客户端，在客户端成功切换到医保接入网时，桌面显示提升成功提示语，提示语由省医保局统一制定，提供能力效果证明文件。

深信服零信任支持管理员可在网络域管理节点定义虚拟网络域实体对象，每个虚拟网络域实体对象由以下元素组成：

1) 虚拟网络域图标：在客户端虚拟网络域切换处将显示该图标，图标可从内置的图标库中选择，也可由管理员自定义上传；

2) 虚拟网络域名称：在客户端虚拟网络域切换处将显示该名称，名称由管理员自定义；

3) 虚拟网络域描述：供管理员对虚拟网络域进行描述，方便管理；

4) 虚拟网络域连接成功提示语：客户端成功切换到该虚拟网络域时，将会在桌面显示切换成功提示语，该提示语支持管理员自定义；

5) 终端出站规则：出站规则用来限制本地终端对远端设备发起的网络请求，虚拟网络域默认会阻断所有的网络出站请求，您可以在列表中定义该网络域下的出站规则，配置维度包括系统平台、进程信息、网络协议（TCP/UDP/ICMP）、目的地址（ip和域名）、端口、禁止/允许访问等。（注：WEB模式应用、客户端接入地址、代理网关地址默认放通，不受规则影响）

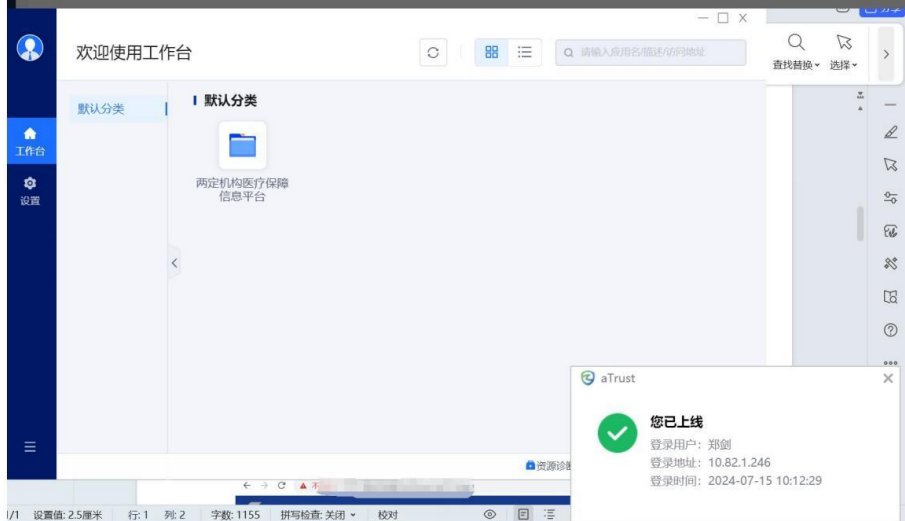
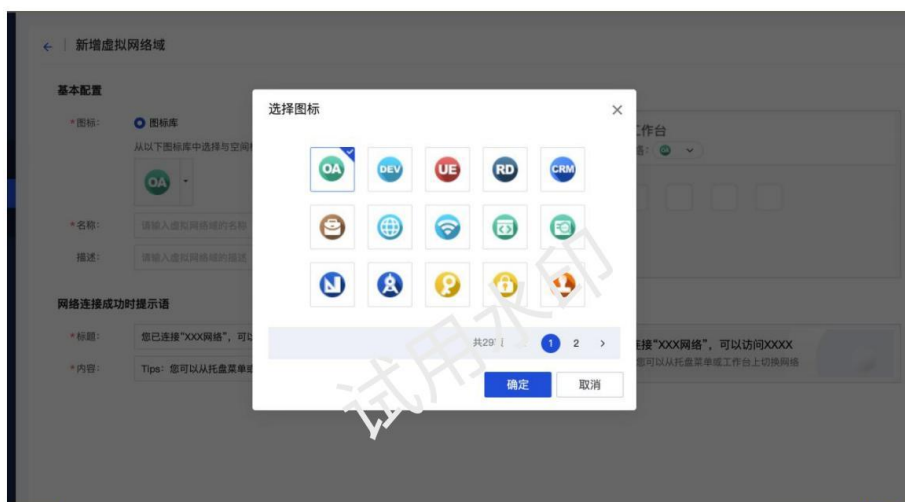
6) 终端进站规则：进站规则用来限制远端设备对本地终端发起的网络请求，虚拟网络域默认会放通所有的网络进站请求，您可以在列表中定义该网络域下的进站规则，配置维度包括系统平台、源地址、禁止/允许访问、本地终端进程信息等。

定义的网络域实体对象可在网络切换策略中被引用，为了简化一机两网场景下的配置，系统默认内置了两个网络域对象：

1) 零信任网络：该内置网络域默认放通隧道应用地址访问，禁止其它网络地址访问；

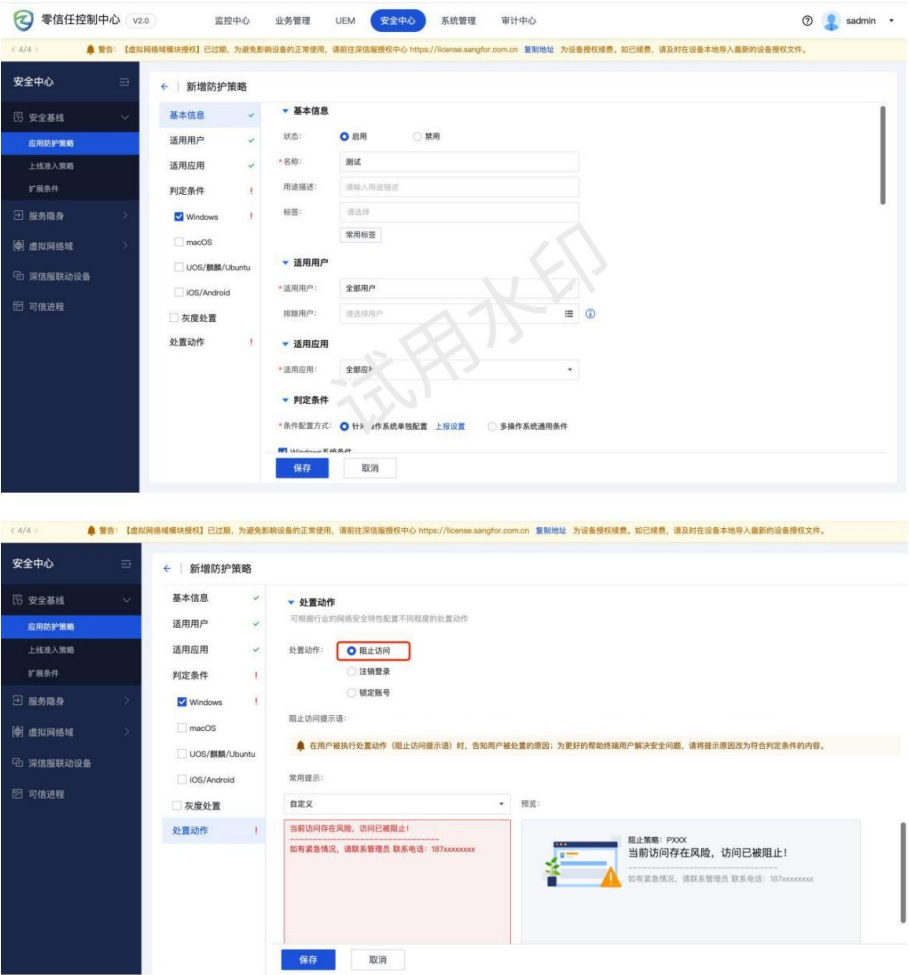
2) 终端本地网络：该内置网络域默认禁止隧道应用地址访问，放通其它网络地址访问。

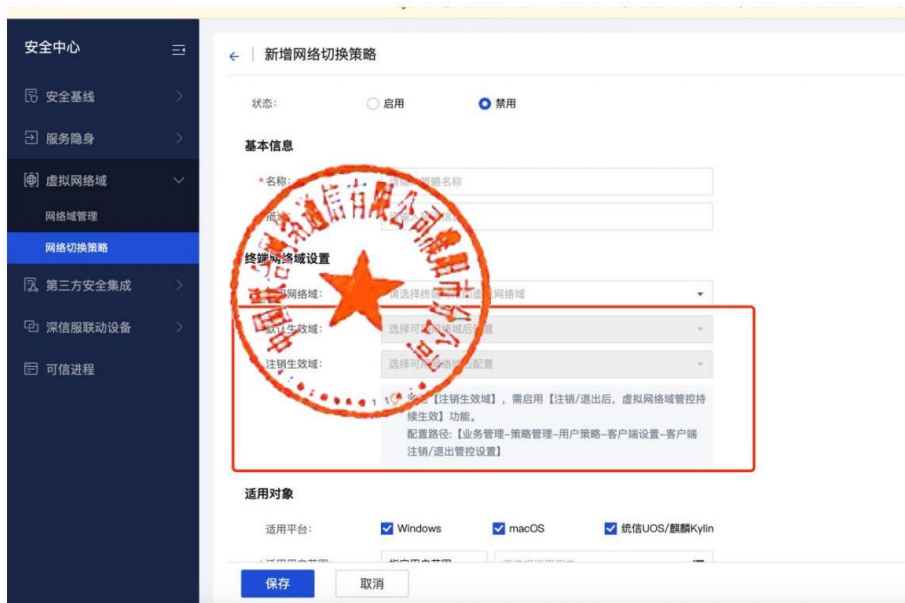
3) 管理员可对内置网络域对象进行编辑、删除操作。



(9) 在终端访问医保信息业务时，零信任客户端支持检测终端是否接入互联网。如发现终端违规接入互联网情况，零信任客户端自动掉线，断开与医保信息业务的连接，提供能力效果证明截图。

基于零信任理念，深信服零信任重构终端安全体系，针对接入医保网的Windows终端、国产化终端、移动终端采取终端基线检查、接入认证管控等手段，面向同一终端、同一时间进行同一网络域的访问控制，并且对不同网络间产生的数据进行安全隔离。从而解决终端环境安全不可视、入网身份安全不可知、访问行为安全不可控、终端安全管理不统一的政务终端难题。





(10) 在终端接入互联网情况下, 零信任客户端弹出提醒, 提醒已接入互联网无法访问医保信息平台, 警示接入人员; 同时可在接入互联网情况下访问医保信息平台时进行阻断, 提供证明截图及详细技术介绍。

深信服零信任支持在终端接入互联网情况下, 零信任客户端弹出提醒, 提醒已接入互联网无法访问医保信息平台。警示接入人员; 同时可在接入互联网情况下访问医保信息平台时进行阻断

非法外联检测: 通过零信任客户端进行非法外联检测, 当检测到终端互联网地址不是医保网统一的互联网出口地址范围时, 认定为违规外联, 可直接阻断或告警, 降低因各市基层卫生机构私建互联网出口、私接路由wifi行为引入医保网的安全风险。

同时具备NAT精准溯源能力, 通过零信任设备将用户流量打上身份标签, 实现流量身份化, 通过身份标签快速精准定位和溯源, 不受NAT网络影响。