

招 标 文 件

(货物类)

采购项目名称：公安交管信息系统软硬件更新升级项目

采购项目编号：DQB-2025077-ZB

陕西省公安厅交通警察总队

陕西德勤招标有限公司共同编制

2025年10月10日

第一章 投标邀请

陕西德勤招标有限公司（以下简称“代理机构”）受陕西省公安厅交通警察总队委托，拟对公安交管信息系统软硬件更新升级项目进行国内公开招标，兹邀请符合本次招标要求的供应商参加投标。

一、采购项目编号：**DQB-2025077-ZB**

二、采购项目名称：公安交管信息系统软硬件更新升级项目

三、招标项目简介

公安交管信息系统软硬件更新升级项目

四、供应商参加本次政府采购活动应具备的条件

（一）满足《中华人民共和国政府采购法》第二十二条规定；

（二）落实政府采购政策需满足的资格要求：

1.执行政府采购促进中小企业发展的相关政策

无

（三）本项目的特定资格要求：

采购包1：

1、营业执照等主体资格证明文件：提供营业执照/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。

2、财务状况报告：提供**2024**年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。

3、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关文件证明。

4、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据，凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。

5、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。

6、控股管理关系：提供直接控股和管理关系清单。若与其他投标供应商存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。

7、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务。

8、信用记录：供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）。

9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件（附在资格证明文件中）；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供法人给分支机构出具的授权书。

10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。

采购包2：

1、营业执照等主体资格证明文件：提供营业执照/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。

2、财务状况报告：提供**2024**年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料

提供任何一种即可）。

3、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关文件证明。

4、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据，凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。

5、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。

6、控股管理关系：提供直接控股和管理关系清单。若与其他投标供应商存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。

7、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务。

8、信用记录：供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）。

9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件（附在资格证明文件中）；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供法人给分支机构出具的授权书。

10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。

采购包3：

1、营业执照等主体资格证明文件：提供营业执照/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。

2、财务状况报告：提供2024年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。

3、社保缴纳证明：提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关文件证明。

4、税收缴纳证明：提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据，凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。

5、近三年无重大违法、违纪书面声明：提供《近三年无重大违法、违纪书面声明》。

6、控股管理关系：提供直接控股和管理关系清单。若与其他投标供应商存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。

7、书面声明：提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、检测等服务。

8、信用记录：供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）。

9、法定代表人授权委托书：法定代表人参加投标的，须提供本人身份证复印件（附在资格证明文件中）；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供法人给分支机构出具的授权书。

10、本项目不接受联合体投标，不允许分包：投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。

五、电子化采购相关事项

本项目实行电子化采购，使用的电子化交易系统为：陕西省政府采购综合管理平台的项目电子化交易系统（以下简称“项目电子化交易系统”），登录方式及地址：通过陕西省政府采购网（<http://www.ccgp-shaanxi.gov.cn/>）首页供应商用户登录陕

西省政府采购综合管理平台（以下简称“政府采购平台”），进入项目电子化交易系统。供应商应当按照以下要求，参与本次电子化采购活动。

（一）供应商应当自行在陕西省政府采购网-办事指南查看相应的系统操作指南，并严格按照操作指南要求进行系统操作。在登录、使用政府采购平台前，应当按照要求完成供应商注册和信息完善，加入政府采购平台供应商库。

（二）供应商应当使用纳入陕西省政府采购综合管理平台数字证书互认范围的数字证书及签章（以下简称“互认的证书及签章”）进行系统操作。供应商使用互认的证书及签章登录政府采购平台进行的一切操作和资料传递，以及加盖电子签章确认采购过程中制作、交换的电子数据，均属于供应商真实意思表示，由供应商对其系统操作行为和电子签章确认的事项承担法律责任。

已办理互认的证书及签章的供应商，校验互认的证书及签章有效性后，即可按照系统操作要求进行身份信息绑定、权限设置和系统操作；未办理互认的证书及签章的供应商，按要求办理互认的证书及签章并校验有效性后，按照系统操作要求进行身份信息绑定、权限设置和系统操作。互认的证书及签章的办理与校验，可查看陕西省政府采购网-办事指南-CA及签章服务。

供应商应当加强互认的证书及签章日常校验和妥善保管，确保在参加采购活动期间互认的证书及签章能够正常使用；供应商应当严格互认的证书及签章的内部授权管理，防止非授权操作。

（三）供应商应当自行准备电子化采购所需的计算机终端、软硬件及网络环境，承担因准备不足产生的不利后果。

（四）政府采购平台技术支持：

在线客服：通过陕西省政府采购网-在线客服进行咨询

技术服务电话：029-96702

CA及签章服务：通过陕西省政府采购网-办事指南-CA及签章服务进行查询

六、招标文件获取时间、方式及地址

（一）招标文件获取时间：详见采购公告

（二）在招标文件获取开始时间前，采购人或代理机构将本项目招标文件上传至项目电子化交易系统，向供应商提供。供应商通过项目电子化交易系统获取招标文件。成功获取招标文件的，供应商将收到已获取招标文件的回执函。未成功获取招标文件的供应商，不得参与本次采购活动，不得对招标文件提起质疑。

成功获取招标文件后，采购人或代理机构进行澄清或者修改的，澄清或者修改的内容可能影响投标文件编制的，采购人或代理机构将通过项目电子化交易系统发布澄清或者修改后的招标文件，供应商应当重新获取招标文件；澄清或者修改后的招标文件发布日期距提交投标文件截止日期不足15日的，采购人或代理机构顺延提交投标文件的截止时间。供应商未重新获取招标文件或者未按照澄清或者修改后的招标文件编制投标文件进行投标的，自行承担不利后果。

注：获取的招标文件主体格式包括pdf、word两种格式版本，其中以pdf格式为准。

七、投标文件提交截止时间及开标时间、地点、方式

（一）投标文件提交截止时间及开标时间：详见采购公告

（二）投标文件提交方式、地点：供应商应当在投标文件提交截止时间前，通过项目电子化交易系统提交投标文件。成功提交的，供应商将收到已提交投标文件的回执函。

（三）本项目采取网上开标，即采购人或代理机构通过项目电子化交易系统“开标/开启大厅”组织在线开标。

八、本投标邀请在陕西省政府采购网以公告形式发布

九、供应商信用融资

根据《陕西省财政厅关于加快推进我省中小企业政府采购信用融资工作的通知》（陕财办采〔2020〕15号）和《陕西省中小企业政府采购信用融资办法》（陕财办采〔2018〕23号）文件要求，为助力解决政府采购成交供应商资金不足、融资难、融资贵的困难，促进供应商依法诚信参加政府采购活动，有融资需求的供应商可登录陕西省政府采购网—陕西省政府采购金融服务平台（<http://www.ccgp-shaanxi.gov.cn/zcdservice/zcd/shanxi/>），选择符合自身情况的“政采贷”银行及其产品，凭项目中标（成交）结果、中标（成交）通知书等信息在线向银行提出贷款意向申请、查看贷款审批情况等。

十、联系方式

采购人：陕西省公安厅交通警察总队

地址： 西安市雁塔区长安南路123号

邮编： /

联系人： 陕西省公安厅交通管理总队

联系电话： 029-87680153

代理机构：陕西德勤招标有限公司

地址： 陕西省西安市高新区丈八一路1号汇鑫中心D座2206室

邮编： /

联系人： 李浩、姜仕路、李维婧、李寅辰

联系电话： 02981169855

采购监督机构：财政厅政府采购管理处

联系人： 柴老师、杨老师

联系电话： 029-68936409、029-68936410

第二章 投标人须知

2.1 投标人须知前附表

序号	应知事项	说明和要求
1	采购预算（实质性要求）	<p>本项目各包采购预算金额如下：</p> <p>采购包1：5,312,980.00元</p> <p>采购包2：1,171,300.00元</p> <p>采购包3：148,000.00元</p> <p>投标人的采购包投标报价高于采购包采购预算的，其投标文件将按无效处理。</p>
2	最高限价（实质性要求）	<p>详见第三章。</p> <p>投标人的采购包投标报价高于最高限价的，其投标文件将按无效处理。</p>
3	评标方法	<p>采购包1：综合评分法</p> <p>采购包2：综合评分法</p> <p>采购包3：综合评分法</p> <p>（详见第五章）</p>
4	是否接受联合体	<p>采购包1：不接受</p> <p>采购包2：不接受</p> <p>采购包3：不接受</p> <p>如以联合体投标的，联合体各方均应当具备本招标文件要求的资格条件和能力。</p> <p>（1）联合体各方均应具有承担本项目必备的条件，如相应的人力、物力、资金等。</p> <p>（2）招标文件对投标人资格条件有特殊要求的，联合体各个成员都应当具备规定的相应资格条件。</p> <p>（3）同一专业的单位组成的联合体，应当按照资质等级较低的单位确定联合体的资质等级。如：某联合体由三个单位组成，其中两个单位资质等级为甲级，另一单位资质等级为较甲级更低的乙级，则该联合体资质等级为乙级。</p>
5	落实节能、环保产品政策	<p>1.根据《财政部发展改革委生态环境部市场监管总局关于调整优化节能产品、环境标志产品政府采购执行机制的通知》（财库〔2019〕9号）相关要求，政府采购节能产品、环境标志产品实施品目清单管理。财政部、发展改革委、生态环境部等部门确定实施政府优先采购和强制采购的产品类别，以品目清单的形式发布并适时调整。</p> <p>2.本项目采购的无产品属于节能产品政府采购品目清单中应强制采购的产品范围，供应商应当提供国家确定的认证机构出具的、处于有效期之内的节能产品认证证书，否则作无效投标处理。</p> <p>3.本项目采购的无产品属于节能产品政府采购品目清单中应优先采购的产品范围，本项目采购的无产品属于环境标志产品政府采购品目清单中应优先采购的产品范围，评审得分/响应报价相同的，按供应商提供的优先采购产品认证证书数量由多到少顺序排列。</p>

6	小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除（仅非预留份额采购项目或预留份额采购项目中的非预留部分采购包适用）	关于本项目采购包中执行小微企业（监狱企业、残疾人福利性单位视同小微企业）价格扣除情况、具体扣除比例和规则详见第五章。
7	充分、公平竞争保障措施（实质性要求）	<p>核心产品允许有多个，不同供应商提供了任意一个相同品牌的核心产品，即视为提供相同品牌的供应商。</p> <p>使用综合评分法的采购项目，提供相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的同品牌投标人获得中标人推荐资格；评审得分相同的，由采购人或者采购人委托评标委员会采取随机抽取方式确定一个投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。</p> <p>采用最低评标价法的采购项目，提供相同品牌产品的不同投标人参加同一合同项下投标的，以其中通过资格审查、符合性审查且报价最低的参加评标；报价相同的，由采购人或者采购人委托评标委员会按照随机抽取方式确定一个参加评标的投标人，其他投标无效。</p> <p>核心产品清单详见第三章。</p> <p>在符合性审查环节提供核心产品品牌不足3个的，视为有效投标人不足3家。</p>
8	不正当竞争预防措施（实质性要求）	在评标过程中，评标委员会认为投标人投标报价明显低于其他通过符合性审查投标人的投标报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内通过项目电子化交易系统进行书面说明，必要时提交相关证明材料。投标人提交的书面说明，应当加盖投标人公章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则视为不能证明其投标报价合理性。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效投标处理。
9	投标保证金	<p>采购包1保证金金额：106,000.00元</p> <p>采购包2保证金金额：23,000.00元</p> <p>采购包3保证金金额：2,800.00元</p> <p>缴交渠道：电子保函,转账、支票、汇票等（需通过实体账户、户名及开户行信息）</p> <p>开户名称：陕西德勤招标有限公司</p> <p>开户银行：光大银行西安丈八东路支行</p> <p>银行账号：52880188000130714</p>
10	标书费信息	免费获取
11	履约保证金（实质性要求）	<p>采购包1：不缴纳</p> <p>采购包2：不缴纳</p> <p>采购包3：不缴纳</p>
12	投标有效期（实质性要求）	提交投标文件的截止之日起不少于90天。

13	招标代理服务费 (实质性要求)	本项目收取代理服务费 代理服务费用收取对象：中标/成交供应商 代理服务费收费标准：按照以下标准收取（不足5000按5000收取）：成交金额100万元以下，费率1.5%，成交金额100～500万元，费率1.1%，成交金额500～1000万元，费率0.8%，采购代理服务费收费按差额定率累进法计算。
14	采购结果公告	采购结果将在陕西省政府采购网予以公告。
15	中标通知书	采购结果公告发布的同时，采购人或代理机构通过项目电子化交易系统向中标供应商发出中标通知书；中标供应商通过项目电子化交易系统获取中标通知书。
16	政府采购合同公告、备案	政府采购合同签订之日起2个工作日内，采购人将政府采购合同在“陕西省政府采购网”予以公告；政府采购合同签订之日起7个工作日内，采购人将本项目采购合同通过政府采购平台进行备案。
17	进口产品	不允许
18	是否组织潜在供应商现场考察	采购包1：组织现场踏勘：否 采购包2：组织现场踏勘：否 采购包3：组织现场踏勘：否
19	特殊情况	出现下列情形之一的，采购人或者采购代理机构应当中止电子化采购活动，并保留相关证明材料备查： （一）交易系统发生故障（包括感染病毒、应用或数据库出错）而无法正常使用的； （二）因组织场所停电、断网等原因，导致采购活动无法继续通过交易系统实施的； （三）其他无法保证电子化交易的公平、公正和安全的情况。 出现上述的情形，不影响采购公平、公正的，采购人或者代理机构可以待上述情形消除后继续组织采购活动；影响或者可能影响采购公平、公正的，采购人或者代理机构应当依法废标。

2.2总则

2.2.1适用范围

一、本招标文件仅适用于本次公开招标采购项目。

二、本招标文件的最终解释权由陕西省公安厅交通警察总队和陕西德勤招标有限公司享有。对招标文件中供应商参加本次政府采购活动应当具备的条件，招标项目技术、服务、商务及其他要求，评标细则及标准由陕西省公安厅交通警察总队负责解释。除上述招标文件内容，其他内容由陕西德勤招标有限公司负责解释。

2.2.2有关定义

一、“采购人”是指依法进行政府采购的各级国家机关、事业单位、团体组织。本次招标的采购人是陕西省公安厅交通警察总队。

二、“投标人”是指按照采购公告规定获取了招标文件，拟参加投标和向采购人提供货物、工程或服务的法人、其他组织或者自然人。

三、“代理机构”是指政府采购集中采购机构和从事政府采购代理业务的社会中介机构。本项目的代理机构是陕西德勤招标有限公司。

四、“网上开标”是指代理机构通过项目电子化交易系统在线完成签到、开标、唱标和记录等活动，供应商通过项目电子化交易系统在线完成投标文件解密、参与开标活动。

五、“电子评标”是指通过项目电子化交易系统在线完成资格审查小组和评审小组组建，开展资格和符合性审查、比较与评价、出具评标报告、推荐中标候选人等活动。

2.3招标文件

2.3.1招标文件的构成

一、招标文件是投标人准备投标文件和参加投标的依据，同时也是资格审查、评标的重要依据。招标文件用以阐明招标项目所需的资质、技术、服务及报价等要求、招标投标程序、有关规定和注意事项以及合同主要条款等。本招标文件包括以下内容：

- （一）投标邀请；
- （二）投标人须知；
- （三）招标项目技术、服务、商务及其他要求；
- （四）资格审查；
- （五）评标办法；
- （六）投标文件格式；
- （七）拟签订采购合同文本。

二、投标人应认真阅读和充分理解招标文件中所有的事项、格式条款和规范要求。投标人没有对招标文件全面做出实质性响应所产生的风险由投标人承担。

2.3.2 招标文件的澄清和修改

一、在投标文件提交截止时间前，采购人或者代理机构可以对已发出的招标文件进行必要的澄清或者修改。

二、澄清或者修改的内容为招标文件的组成部分，采购人或者代理机构将在陕西省政府采购网发布更正公告，投标人应及时关注本项目更正公告信息，按更正后公告要求进行响应。更正内容可能影响投标文件编制的，采购人或者代理机构将通过项目电子化交易系统发布更正后的招标文件，投标人应依据更正后的招标文件编制投标文件。若投标人未按前述要求进行投标响应的，自行承担不利后果。

2.4 投标文件

2.4.1 投标文件的语言

一、投标人提交的投标文件以及投标人与采购人或代理机构就有关投标的所有来往书面文件均须使用中文。投标文件中如附有外文资料，主要部分要对应翻译成中文并附在相关外文资料后面。未翻译的外文资料，评标委员会将其视为无效材料。

二、翻译的中文资料与外文资料如果出现差异和矛盾时，以中文为准。涉嫌提供虚假材料的按照相关法律法规处理。

三、如因未翻译而造成对投标人的不利后果，由投标人承担。

2.4.2 计量单位

除招标文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3 投标货币

本次项目均以人民币报价。

2.4.4 知识产权

一、投标人应保证在本项目中使用的任何技术、产品和服务（包括部分使用），不会产生因第三方提出侵犯其专利权、商标权或其它知识产权而引起的法律和经济纠纷，如因专利权、商标权或其它知识产权而引起法律和经济纠纷，由投标人承担所有相关责任。采购人享有本项目实施过程中产生的知识成果及知识产权。

二、投标人将在采购项目实施过程中采用自有或者第三方知识成果的，使用该知识成果后，投标人需提供开发接口和开发手册等技术资料，并承诺提供无限期支持，采购人享有使用权（含采购人委托第三方在该项目后续开发的使用权）。

三、如采用投标人所不拥有的知识产权，则在投标报价中必须包括合法使用该知识产权的相关费用。

2.4.5 投标文件的组成

投标人应当按照招标文件的要求编制投标文件。投标文件应当对招标文件提出的要求和条件作出明确响应。

投标文件具体内容详见第六章。

2.4.6 投标文件格式

一、投标人应按照招标文件第六章中提供的“投标文件格式”填写相关内容。

二、对于没有格式要求的投标文件由投标人自行编写。

2.4.7 投标报价（实质性要求）

一、投标人的报价是投标人响应招标项目要求的全部工作内容的价格体现，包括投标人完成本项目所需的一切费用。

二、投标人每种货物及服务内容只允许有一个报价，并且在合同履行过程中是固定不变的，任何有选择或可调整的报价将不予接受，并按无效投标处理。

三、投标文件报价出现前后不一致的，按照招标文件第五章评标办法规定予以修正，修正后的报价经投标人通过项目电子化交易系统进行确认，并加盖投标人（法定名称）电子签章，投标人未在规定时间内确认的，其投标无效。

2.4.8 投标有效期（实质性要求）

投标有效期详见第二章“投标人须知前附表”，投标文件未明确投标有效期或者投标有效期小于“投标人须知前附表”中投标有效期要求的，其投标文件按无效处理。

2.4.9 投标文件的制作、签章和加密（实质性要求）

一、投标文件应当根据招标文件进行编制，投标人应通过陕西省政府采购网-办事指南-CA及签章服务下载投标（响应）客户端，使用客户端编制投标文件。

二、投标人应按照客户端操作要求，对应招标文件的每项实质性要求，逐一如实响应；未如实响应或者响应内容不符合招标文件对应项的要求的，其投标文件作无效处理。

三、投标人完成投标文件编制后，应按照招标文件第一章明确的签章要求，使用互认的证书及签章对投标文件进行电子签章和加密。

四、招标文件澄清或者修改的内容可能影响投标文件编制的，代理机构将重新发布澄清或者修改后的招标文件，投标人应重新获取澄清或者修改后的招标文件，按照澄清或者修改后的招标文件进行投标文件编制、签章和加密。

2.4.10 投标文件的提交

一、（实质性要求）投标人应当在投标文件提交截止时间前，通过项目电子化交易系统完成投标文件提交。

二、在投标文件提交截止时间后，采购人或者代理机构不再接受投标人提交投标文件。投标人应充分考虑影响投标文件提交的各种因素，确保在投标文件提交截止时间前完成提交。

2.4.11 投标文件的补充、修改、撤回（实质性要求）

投标文件提交截止时间前，投标人可以补充、修改或者撤回已成功提交的投标文件；对投标文件进行补充、修改的，应当先行撤回已提交的投标文件，补充、修改后重新提交。

供应商投标文件撤回后，视为未提交过投标文件。

2.5 开标、资格审查、评标和中标

2.5.1 开标及开标程序

一、本项目为网上开标项目。网上开标的开始时间为投标文件提交截止时间。成功提交或解密电子投标文件的投标人不足3家的，不予开标，采购人或代理机构将作废标处理。

二、开标准备工作

开标/开启前30分钟内，供应商需登录项目电子化交易系统-“供应商开标大厅”-进入开标选择对应项目包组操作签到，签到完成后等待代理机构开标/开启。

三、解密投标文件（实质性要求）

投标文件提交截止时间后，成功提交投标文件的投标人符合招标文件规定数量的，代理机构将启动投标文件解密程序，解密时间为30分钟；投标人应在规定的解密时间内，使用互认的证书及签章通过项目电子化采购系统进行投标文件解密。

四、开标

解密时间截止或者所有投标人投标文件均完成解密后（以发生在先的时间为准），由代理机构通过项目电子化交易系统对投标人名称、投标文件解密情况、投标报价进行展示。

开标过程中，各方主体均应遵守互联网有关规定，不得发表与采购活动无关的言论。投标人对开标过程和开标记录有疑义，以及认为采购人或代理机构相关工作人员有需要回避的情形的，及时向工作人员提出询问或者回避申请。采购人或代理机构对投标人提出的询问或者回避申请应当及时处理。

投标人完成投标文件解密后，自主决定是否参加网上在线开标，未参加的，视同认可开标结果。

2.5.2 查询及使用信用记录

开标结束后，采购人或代理机构根据《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）的要求，通过“信用中国”网站（www.creditchina.gov.cn）、“中国政府采购网”网站（www.ccgp.gov.cn）等渠道，查询投标人在投标文件提交截止时间前的信用记录并保存信用记录结果网页截图，拒绝列入失信被执行人名单、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中的供应商参加本项目的采购活动。

两个以上的自然人、法人或者其他组织组成一个联合体，以一个投标人的身份共同参加政府采购活动的，将对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

2.5.3 资格审查

详见招标文件第四章。

2.5.4 评标

详见招标文件第五章。

2.5.5 中标通知书

一、采购人或者评标委员会确认中标供应商后，代理机构在陕西省政府采购网发布中标结果公告、通过项目电子化交易系统发出中标通知书，中标供应商通过项目电子化交易系统获取中标通知书。

二、中标通知书是采购人和中标供应商签订政府采购合同的依据，是合同的有效组成部分。如果出现政府采购法律法规、规章制度规定的中标无效情形的，将以公告形式宣布发出的中标通知书无效，中标通知书将自动失效，并依法重新确定中标供应商或者重新开展采购活动。

三、中标通知书对采购人和中标供应商均具有法律效力。

2.6 签订及履行合同和验收

2.6.1 签订合同

一、采购人应在中标通知书发出之日起三十日内与中标人签订采购合同。

二、采购人和中标人签订的采购合同不得对招标文件确定的事项以及中标人的投标文件作实质性修改。

2.6.2 合同分包和转包（实质性要求）

2.6.2.1 合同分包

一、投标人根据招标文件的规定和采购项目的实际情况，拟在中标后将中标项目的非主体、非关键性工作分包的，应当在投标文件中载明分包承担主体，分包承担主体应当具备相应资质条件且不得再次分包。分包供应商履行的分包项目的品牌、规格型号及技术要求等，必须与中标的品牌、规格型号及技术要求一致。

二、分包履行合同的部分应当为采购项目的非主体、非关键性工作，不属于中标人的主要合同义务。

三、采购合同实行分包履行的，中标人就采购项目和分包项目向采购人负责，分包供应商就分包项目承担责任。

四、中小企业依据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的政策获取政府采购合同后，小型、微型企业不得将合同分包或转包给大型、中型企业，中型企业不得将合同分包或转包给大型企业。

采购包1：不允许合同分包。

采购包2：不允许合同分包。

采购包3：不允许合同分包。

2.6.2.2 合同转包

一、严禁中标人将本项目转包。本项目所称转包，是指将本项目转给他人或者将本项目全部肢解以后以分包的名义分别转给他人的行为。

二、中标人转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3 采购人增加合同标的的权利

采购合同履行过程中，采购人需要追加与合同标的相同的货物或者服务的，在不改变合同其他条款的前提下，可以与中标人

协商签订补充合同，但所有补充合同的采购金额不得超过原合同采购金额的百分之十。

2.6.4 履行合同

一、合同一经签订，双方应严格履行合同规定的义务。

二、在合同履行过程中，如发生合同纠纷，合同双方应按照《中华人民共和国民法典》规定及合同条款约定进行处理。

2.6.5 履约验收方案

采购包1：

政府采购合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典》。采购人按照政府采购合同规定的技术、服务、安全标准组织对供应商履约情况进行验收，并出具验收书。

采购包2：

政府采购合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典》。采购人按照政府采购合同规定的技术、服务、安全标准组织对供应商履约情况进行验收，并出具验收书。

采购包3：

政府采购合同的履行、违约责任和解决争议的方法等适用《中华人民共和国民法典》。采购人按照政府采购合同规定的技术、服务、安全标准组织对供应商履约情况进行验收，并出具验收书。

2.6.6 资金支付

采购人按财政部门的相关规定及采购合同的约定进行支付。

2.7 纪律要求

2.7.1 评标活动纪律要求

采购人、代理机构应保证评标活动在严格保密的情况下进行，采购人、代理机构、投标人和评标委员会成员应当严格遵守政府采购法律法规规章制度和本项目招标文件以及代理机构现场管理规定，接受采购人委派的监督人员的监督，任何单位和个人不得非法干预和影响评标过程和结果。对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

对各投标人的商业秘密，评标委员会成员应予以保密，不得泄露给其他投标人。

2.7.2 投标人不得具有的情形（实质性要求）

一、有下列情形之一的，视为投标人串通投标：

- （一）不同投标人的投标文件由同一单位或者个人编制；
- （二）不同投标人委托同一单位或者个人办理投标事宜；
- （三）不同投标人的投标文件载明的项目管理成员或者联系人员为同一人；
- （四）不同投标人的投标文件异常一致或者投标报价呈规律性差异；
- （五）不同投标人的投标文件相互混装。

二、提供虚假材料谋取中标；

三、采取不正当手段诋毁、排挤其他投标人；

四、与采购人或代理机构、其他投标人恶意串通；

五、向采购人或代理机构、评标委员会成员行贿或者提供其他不正当利益；

六、在招标过程中与采购人或代理机构进行协商谈判；

七、中标后无正当理由拒不与采购人签订政府采购合同；

八、未按照采购文件确定的事项签订政府采购合同；

九、将政府采购合同转包或者违规分包；

十、提供假冒伪劣产品；

十一、擅自变更、中止或者终止政府采购合同；

十二、拒绝有关部门的监督检查或者向监督检查部门提供虚假情况；

十三、法律法规规定的其他禁止情形。

投标人有上述情形的，按照规定追究法律责任，具备一至十一条情形之一的，其投标文件无效，或取消被确认为中标供应商的资格或认定中标无效。

2.8 询问、质疑和投诉

一、询问、质疑、投诉的接收和处理严格按照《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购质疑和投诉办法》等规定办理。

二、供应商询问、质疑的答复主体：

根据委托代理协议约定，供应商对招标文件中采购需求的询问、质疑由 陕西德勤招标有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由陕西德勤招标有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 陕西德勤招标有限公司 负责答复。

三、供应商提出的询问，应当明确询问事项，如以书面形式提出的，应由供应商签字并加盖公章。

为提高采购效率，降低社会成本，鼓励询问主体对于不损害国家及社会利益或自身合法权益的问题或情形采用询问方式处理解决（包含但不限于文字错误、标点符号、不影响投标文件的编制的情形）。

四、供应商认为采购文件、采购过程、中标或者成交结果使自己的权益受到损害的，可以在知道或者应知其权益受到损害之日起7个工作日内，以书面形式向采购人、代理机构提出质疑。供应商应在法定质疑期内一次性提出针对同一采购程序环节的质疑。供应商应知其权益受到损害之日，是指：

- （一）对可以质疑的采购文件提出质疑的，为收到采购文件之日或者采购文件公告期限届满之日
- （二）对采购过程提出质疑的，为各采购程序环节结束之日；
- （三）对中标或者成交结果提出质疑的，为中标或者成交结果公告期限届满之日。

五、本项目不接受在线提交质疑，供应商通过书面形式线下向采购人或代理机构提交质疑资料。

六、供应商提出质疑时应当准备的资料

- （一）质疑书正本1份；（政府采购供应商质疑函范本详见附件一）
- （二）法定代表人或主要负责人授权委托书1份（委托代理人办理质疑事宜的需提供）；
- （三）法定代表人或主要负责人身份证复印件1份；
- （四）委托代理人身份证复印件1份（委托代理人办理质疑事宜的需提供）；
- （五）针对质疑事项必要的证明材料（针对招标文件提出的质疑，需提交从项目电子化交易系统获取的招标文件回执单）。

答复主体：代理机构

联系人：李浩、姜仕路、李维婧、李寅辰

联系电话：02981169855

地址：陕西省西安市高新区丈八一路1号汇鑫中心D座2206室

邮编：/

注：根据《中华人民共和国政府采购法》的规定，供应商质疑不得超出采购文件、采购过程、采购结果的范围。

七、供应商对采购人或代理机构的质疑答复不满意，或者采购人或代理机构未在规定期限内作出答复的，供应商可以在答复期满后15个工作日内向同级财政部门提起投诉。

投诉受理单位：本采购项目同级财政部门。（政府采购供应商投诉书范本详见附件二）

第三章 招标项目技术、服务、商务及其他要求

（注：当采购包的评标方法为综合评分法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。带“▲”号条款为允许负偏离的参数需求，若未响应或者不满足，将在综合评审中予以扣分处理。）

（注：当采购包的评标方法为最低评标价法时带“★”的参数需求为实质性要求，供应商必须响应并满足的参数需求，采购人、采购代理机构应当根据项目实际需求合理设定，并明确具体要求。）

3.1采购项目概况

公安交管信息系统软硬件更新升级项目。

3.2采购内容

采购包1：

采购包预算金额（元）：5,312,980.00

采购包最高限价（元）：5,312,980.00

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额 (元)	计量 单位	所属行业	是否核 心产品	是否允许 进口产品	是否属于 节能产品	是否属于环境 标志产品
1	公安交管信息系统软硬件更新升级	1.00	5,312,980.00	项	软件和信息技术服务业	否	否	否	否

采购包2：

采购包预算金额（元）：1,171,300.00

采购包最高限价（元）：1,171,300.00

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额 (元)	计量 单位	所属行业	是否核 心产品	是否允许 进口产品	是否属于 节能产品	是否属于环境 标志产品
1	公安交管信息系统软硬件更新升级项目密码改造部分	1.00	1,171,300.00	项	软件和信息技术服务业	否	否	否	否

采购包3：

采购包预算金额（元）：148,000.00

采购包最高限价（元）：148,000.00

供应商报价不允许超过标的金额

（招单价的）供应商报价不允许超过标的单价

序号	标的名称	数量	标的金额（元）	计量单位	所属行业	是否核心产品	是否允许进口产品	是否属于节能产品	是否属于环境标志产品
1	公安交管信息系统软硬件更新升级及密码改造部分监理	1.00	148,000.00	项	软件和信息 技术服务业	否	否	否	否

3.3技术要求

采购包1：
标的名称：公安交管信息系统软硬件更新升级

序号	参数性质	技术参数与性能指标
		<p>（一）建设目标</p> <p>我省公安交通管理综合应用平台（以下简称“综合应用平台”）于2012年底正式建成上线，将交通管理主要业务系统（包括机动车、驾驶证、违法、事故、剧毒品、信息平台）整合统一平台实现省级集中管理，承载全省交通安全管理核心数据，涉及全省车驾管、交通违法、交通事故等重要基础信息。2018年对综合应用平台工作数据库存储设备进行了双活冗余配置（采用非国产化技术架构），并于2021年硬盘紧急扩容，2021年分布式改造一期建设交通管理大数据分布式管理应用平台(TDMS)基础环境（采用非国产化技术架构），实现了综合平台分布式数据库的运行监控和管理以及综合平台应用升级，2023年分布式改造二期建设在第一期基础上对交通管理大数据分布式管理应用平台(TDMS)进行扩容，提升综合平台的业务和服务能力，扩容升级了大数据集群软硬件（采用国产化技术）。</p> <p>随着近些年平台功能的持续完善、应用的不断推广、相关系统的扩展延伸，平台工作数据库系统其运行压力日趋增大，综合应用平台工作数据库存储容量已无法满足当前工作需要，且早期建设的大数据集群部分硬件已运行超12年，软件维保授权服务已经到期，为保障平台工作数据库系统的稳定性和可靠性，避免工作数据库资源不足对综合应用平台、互联网交通安全综合服务管理平台、集成指挥平台等系统的业务影响。亟待改造扩容综合应用平台工作数据库存储容量和解决已到期大数据软件的授权服务。为确保公安交管信息系统软硬件更新升级项目有效保障以上业务需求，制定本项目建设目标具体如下：</p> <p>机房运行环境改善</p> <p>本次项目针对陕西交警总队3楼数据中心机房两列主要机柜进行冷通道、列间空调、UPS供电系统、动环系统等功能进行改造完善，提升数据中心机房业务承载能力。针对3楼视频会议区域UPS供电接入实现以下具体业务目标：</p> <p>1、通道改造、制冷循环</p> <p>集中化冷通道封闭改造，通过隔离冷热气流、优化气流组织，提升空调制冷效率、避免局部热岛效应，延长设备寿命降低能耗并保障机房设备稳定运行。</p> <p>2、增设空调、制冷完善</p> <p>增加3台列间空调，强化机房制冷量，提升局部散热效率、降低能耗，有效应对机房内综合应用平台工作数据库存储、大数据计算服务器等高密度设备的散热需求有效改善。</p> <p>3、动环改造、预防突发</p> <p>动环系统改造，实现对设备运行状态、温湿度、能耗等参数的实时监测与智能管理，保障机房安全稳定运行和突发事件预防，提升运维效率。</p> <p>4、UPS更新、稳定供电</p>

针对2台超期服役的UPS主机以及1套240节电池组进行集中更换，提升供电系统可靠性，消除主机故障导致的机房设备大面积停电，杜绝因UPS电池故障引发的火灾、漏液等安全风险，优化能效与运营成本。

5、UPS接入、会议续航

三楼视频会议室UPS供电改造，由地下室配电间125KVA UPS输入输出配电柜输出1路电缆至3楼电井内新增UPS配电箱，并最终对大会议室、电视电话会议室和业务培训室区域进行UPS供电。

基础软硬件环境改造

根据公安部交通管理科学研究所《信息系统软硬件运行环境适配情况公示》已完成适配改造的微服务化集成指挥平台、公安交通管理综合应用平台部分模块硬件替代改造以及数据中台服务器硬件需求补充完善，并配套满足本次项目业务使用的虚拟化软件和国产化操作系统，进一步提升陕西交警总队核心业务运行环境基础设施支撑服务能力。

公安交通管理综合应用平台分布式大数据SNS续保

公安交通管理综合应用平台作为陕西交警总队的核心业务系统之一，当前分布式大数据MRS集群和DWS集群软件SNS服务即将到期，亟待软件服务续保，确保核心业务系统的服务连续性和业务运行可靠性、突发性服务保障，实现以下具体业务目标：

1、MRS集群SNS软件续保

根据当前现网MRS集群软件SNS服务年限，延长集群软件服务年限不少于3年，确保公安交通管理综合应用平台业务系统服务的连续性、稳定性服务保障应对突发系统故障和日常服务支撑，确保系统持续服务安全。

2、DWS集群SNS软件续保

根据当前现网DWS集群软件SNS服务年限，延长集群软件服务年限不少于3年，确保公安交通管理综合应用平台业务系统服务的连续性、稳定性服务保障应对突发系统故障和日常服务支撑，确保系统持续服务安全。

（二）建设内容

依据公安部交管局印发的《公安交通管理综合应用平台建设指导意见》（公交管[2010]196号）、《关于印发<2020年道路交通安全管理工作要点>的通知》（公交管〔2020〕1号）、《公安交通管理科技发展规划（2021-2023年）》等文件要求，本次项目建设内容主要包含陕西交警总队3楼数据中心机房运行环境改善、3楼视频会议区域UPS供电接入、基础软硬件环境改造以及公安交通管理综合应用平台分布式大数据集群软件SNS服务续保，实现陕西交警总队核心业务系统的阶段性提档升级和国产化改造，满足业务的紧急必要性需求，提升业务系统的稳定性、可靠性和安全性，有效支撑核心业务系统的运行保障，更好地为全省公安交管工作提供服务支撑。

1.机房运行环境改善

对陕西交警总队三楼信息机房第二排中心区域共计45个机柜进行集中式冷通道封闭改造，包含封闭套件1套、整体机房环境监控套件1套、同时为满足封闭冷通道内的制冷系统效率，新增3台列间空调。封闭冷通道通过优化机房内的气流组织，减少冷热空气混合，提高制冷效率，从而降低能耗。结合当前机房UPS主机及电池组运维现状，主机部分已经累计使用13年，电池组部分累计已使用6年，本次一并将该部分模块进行替换，更换2台主机以及一套电池组以保证核心设备的正常运转。对三楼大会议室、电视电话会议室和业务培训室区域做UPS供电改造。

2.基础软硬件环境改造

根据公安部、陕西省国产化相关政策要求以及公安部交通管理科学研究所《信息系统软硬件运行环境适配情况公示》情况，项目对已满足适配改造条件的集成指挥平台进行服务器硬件改造并配套基础软件；对公安交通管理综合应用平台工作数据库存储设备配套相关网络交换设备；对陕西交警总队2024年牵头建设的全省数据中台系统功能完善所需的软硬件设施补充完善，实现对总队关键核心业务的支撑服务能力的进一步提升。具体建设内容如下：

一、基础硬件环境建设

应用服务器：由于数据中台业务随着数据量以及研判分析的需求逐步增加，为充分保障相关业务的数据服务提升实战应用，因此需规划完善3台GPU服务器用于比对服务以及3台通用服务器用于数据分析服务。

HBase节点服务器改造扩容：现网大数据集群中HBase节点共计14台X86服务器，且使用年限较久，当前性能较低不足以支撑当前业务数据规模，根据国产化相关政策进行替代以及扩容8节点大数据节点用以满足3-5年的数据增长需求。

大数据存储节点硬盘改造：现网大数据存储节点根据业务量的不断加速增长，需要进行4T盘改造到8T盘，并进行数据的均衡处理。

二、基础软件支撑建设

根据HBase节点服务器改造扩容服务器硬件配套软件授权，提供≥256个vCPU的license授权，满足当前综合应用平台业务需要和大数据集群的统一管理需求。

根据服务器硬件的需求，按照1:1配套响应服务器国产化操作系统，提共计28套，其中22套用于公安交通管理综合应用平台大数据集群改造扩容服务器，6套用于数据中台服务器；

3.分布式大数据软件续保

本次项目需对综合应用平台分布式集群大数据软件SNS服务延续，现网MRS集群和DWS集群软件SNS服务全部截止到2025年9月21软件服务到期，到期后原厂定位支持将会停止服务，由于大数据业务的版本、安全特性、组件补丁等需原厂能力定期支持，因此本次项目对现网大数据软件SNS服务延续到2028年12月31日，来确保综合应用平台分布式大数据系统在服务期限内可继续保障原厂提供400电话支持、产品故障问题的分析和定位、定期巡检服务以及组件补丁升级等服务支撑。

（三）建设规模

本次项目建设主要根据《公安交通管理综合应用平台建设指导意见》（公交管[2010]196号）、《关于印发<2020年道路交通安全管理工作要点>的通知》（公交管〔2020〕1号）、《公安交通管理科技发展规划（2021-2023年）》等文件要求，在机房改造建设中，需要考虑到系统的稳定性、可靠性和安全性，以保障业务连续性与数据安全。机房的总体建设在立足“满足现在、适应未来”的建设策略的基础上，综合考虑各系统的先进性、高可靠性、高安全性、可持续发展性、节能性、易管理维护性、开放性、实用性、均衡性,满足《数据中心设计规范》（GB50174-2017）等机房建设相关国家规范，将中心机房建设成分区明确，功能完备，符合B级标准的现代化机房。

1.硬件设备

本次项目硬件设备建设内容包括信息化基础设施硬件设备和机房改造硬件设备两部分组成，具体规模如下：

硬件设备

项目信息化建设硬件部分主要包含公安交通集指指挥平台、公安交通管理综合应用平台、数据中台所需的通用服务器、GPU服务器组成，整体业务系统全部部署在公安信息网内，具体情况详见下表：

建设内容表

序号	设备名称	部署位置	设备类型	数量	单位
1	通用服务器	公安网	硬件设备	3	台
2	GPU服务器	公安网	硬件设备	3	台

3	改造HBase节点服务器（核心产品）	公安网	硬件设备	14	台
4	扩容HBase节点服务器	公安网	硬件设备	4	台
5	改造HBase节点硬盘	公安网	硬件设备	228	块
6	堡垒机	公安网	硬件设备	2	台
7	工作站	公安网、互联网	硬件设备	5	台

机房设备

项目机房改造建设主要对总队3楼机房将原有机房右侧二排中心区域机柜组进行集中化冷通道封闭改造，同时追加3台列间空调满足冷通道内日常设备散热制冷管控，建设冷通道内监控与管理系统，包含（环境监控、设备监控、能耗管理以及远程监控），为满足机房日常核心设备的正常运转防止突发性供电故障导致的核心业务系统停摆，更换负一楼原有UPS套件设备，包括2台机组以及1套电池组，对3楼视频会议室原有配电箱进行改造接入地下室125KVAUPS电池组内对大会议、电视电话会议室和业务培训室区域进行UPS供电。以下为建设内容：

建设内容表

序号	设备名称	部署位置	设备类型	数量
1	45台机柜冷通道封闭组件1套	总队3F机房	硬件设备	1
2	列间空调	总队3F机房	硬件设备	3
3	空调配电箱	总队3F机房	硬件设备	1
4	机房动环系统	总队3F机房	硬件设备	1
5	UPS主机	总队3F机房	硬件设备	2
6	电池组	总队3F机房	硬件设备	1
7	监控中心主机	总队3F机房	硬件设备	1
8	机房改造装修	总队3F机房	机房装修	1
9	3楼视频会议室UPS供电改造	总队3F会议室	机房装修	1

2.成品软件

本次项目成品软件主要由综合应用平台MRS集群软件SNS、综合应用平台DWS集群软件SNS、虚拟化软件、操作系统4部分组成，其中综合应用平台分布式大数据MRS集群和DWS集群软件当前SNS服务截止日期于2025年9月21日，本次项目延续到2028年12月31日，确保综合应用平台分布式大数据系统在服务期限内可继续保障原厂提供400电话支持、产品故障问题的分析和定位、定期巡检服务以及组件补丁升级等服务支撑，以下为具体建设内容：

建设内容表

序号	设备名称	部署位置	设备类型	数量	单位
1	综合应用平台MRS集群软件SNS	公安网	成品软件	1	套
2	综合应用平台DWS集群软件SNS	公安网	成品软件	1	套
3	操作系统	公安网	成品软件	24	套

3.数据和应用迁移

本次项目数据和应用迁移集成指挥平台微服务化版本适配改造迁移服务（应用迁移）、现网存储数据迁移服务（数据迁移）2个部分，以下为建设内容：

建设内容表

序号	设备名称	设备类型	工作量（人月）
1	核心应用系统接口对接服务	应用迁移	7
2	HBase数据节点迁移	数据迁移	8
3	现网存储数据迁移服务	数据迁移	6
4	暴露面梳理服务	安全服务	2
5	漏洞扫描服务	安全服务	2
6	渗透测试服务	安全服务	1

三、现状分析

业务现状分析

机房现状分析

机房基础设施是交警总队信息化建设和智慧公安发展的重要组成部分，现各处机房基础设施情况如下：

交管总队机房：位于大楼3楼，面积约340m²，于2024年新建改造一套20柜模块化机房（红色区域），2024年已对机房整体承重完成红框部分的局部安全承重评估。

其余区域部署68台机柜，使用年限已达13年之久，机柜内IT、网络设备基本已满配使用。同时现场3台空调及2台UPS设备均已超出设备使用年限，UPS主机已累计使用13年，电池组模块已累计使用6年，主机报警频繁且多次自检仍无法消除故障。电池组内阻异常升高，市电异常断电后难以有效支撑抢修恢复时间，严重威胁供电安全。机房内现有世图兹品牌机房精密空调已超期服役，且空调本身故障不断，3台中已有1台空调因故障已无法运行且无维修价值，部分空调室外机已停止运行，现有地送风模式风量不均匀，传导效率低下且制冷不均衡，存在多个分散的局部热点，夏季部分高温日期需要用到大功率风扇进行统一散热。机房当前在用电、制冷、气流管理等方面存在不足，导致能源效率低下。大量电力消耗在包括电源设备、冷却设备和照明设施在内的网络关键物理基础设施上，增加了总队的能源消耗和碳排放。三楼区域为大会议室、电视电话会议室和业务培训室，目前所有设备均采用市电供电异常断电后无法正常维持业务开展。

空调部分现状

随着信息技术的迅猛发展，数据机房作为客户IT系统的核心支撑设施，其重要性日益凸显。然而，当前许多普通数据机房在建设和运维过程中面临着诸多问题，亟需进行改造和优化。

首先，普通数据机房的扩展性较差。由于前期规划不足，机房容量往往难以满足业务快速增长的需求，导致频繁扩容和升级，增加了客户的运营成本和时间成本。同时，机房内的设备布局和线缆管理也缺乏规范性，影响了设备的维护和管理效率。

其次，能耗高是普通数据机房面临的另一大挑战。传统机房建设在用电、制冷、气流管理等方面存在不足，导致能源效率低下。大量电力消耗在包括电源设备、冷却设备和照明设施在内的网络关键物理基础设施上，增加了客户的能源消耗和碳排放。

此外，机房运维难度大也是当前普遍存在的问题。由于设备种类繁多、品牌不一，加上运维人员交替频繁，导致运维人员对设备了解不足，管理混乱。故障响应和故障处理跟踪也容易出现混乱，影响了IT系统的稳定性和可用性。

机房内现有世图兹品牌机房精密空调已超期服役，且空调本身故障不断，3台中已有1台空调因故障已无法运行且无维修价值，导致机房内冷热不匀，严重影响机房内设备的稳定运行，且夏季即将来临，空调更换改造迫在眉睫。

为了解决上述问题，提高机房的能效、可靠性和运维效率，我们提出了加装封闭冷通道的改造方案。封闭冷

通道通过优化机房内的气流组织，减少冷热空气混合，提高制冷效率，从而降低能耗。同时，它还可以改善机房内的设备布局和线缆管理，提高设备的可维护性和管理效率。

UPS部分现状

对机房核心设备UPS（不间断电源）系统进行例行巡检时，发现UPS（型号：伊顿 PW9390）主机报警提示"电池测试失败"，多次自检仍无法消除故障。经深度检测发现电池组内阻异常升高，已严重威胁供电安全。为保障机房核心设备稳定运行，建议更换UPS主机及电池组，具体报告如下：

1、设备基本信息

UPS型号：伊顿 PW9390

投入使用时间：2012年（已使用13年）

电池组配置：240节200Ah铅酸蓄电池（2019年，已使用6年）

2、检测异常表现

（1）主机面板持续显示"电池测试失败"告警，伴随蜂鸣提示；

（2）检测数据：

1#机组电池组内阻均值达17.95 mΩ（远超标准值≤6 mΩ），最高单节内阻84 mΩ（出厂值应≤3 mΩ）

2#机组电池组内阻均值达8.29 mΩ（远超标准值≤6 mΩ），最高单节内阻53 mΩ（出厂值应≤3 mΩ）

（3）电池外观检查发现个别电池壳体有漏液现象。

3、风险分析

当前电池组已无法满足突发停电时设备的持续供电需求，若遇市电中断，可能导致服务器等设备异常关机，引发数据丢失或系统损坏。

根据《YDT 799-2010通信用阀控式密封铅酸蓄电池》规定电池容量小于80%时，需要更换，通常工程经验电池使用3-5年，UPS电池内阻超过出厂值的5倍时需立即更换，当前电池已超期服役且70%以上的电池内阻超过出厂值的5倍。

设备厂商检测报告明确：本型号电池出厂内阻阈值为1.53 mΩ。

《YD/T 1970.1-2009 通信局(站)电源系统维护技术要求 第1部分：总则》规定交流不间断电源（UPS）使用年限为8年，现主机已使用13年。

上述设备指标已严重超标，有着极大的运行风险。

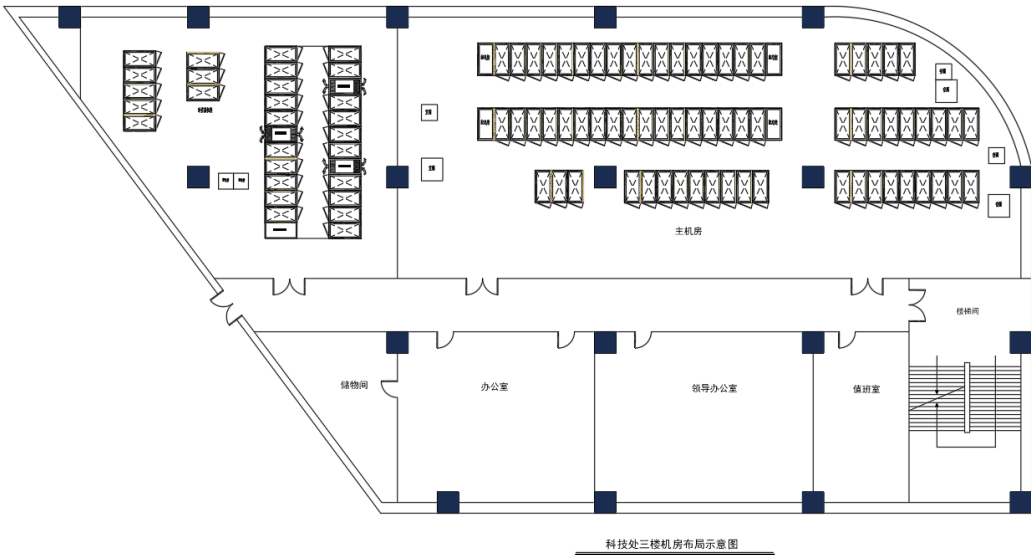
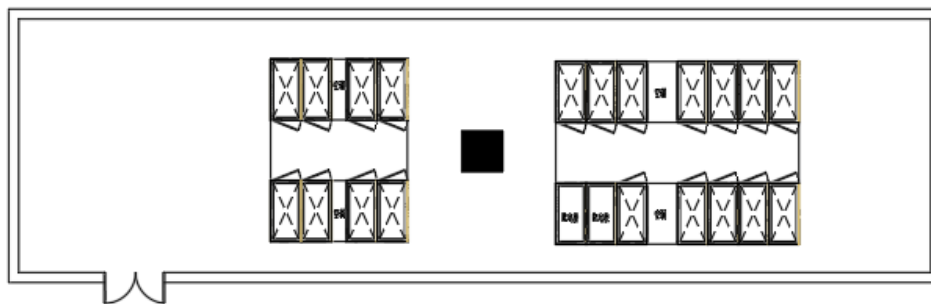


图 31 交管总队机房部署现状

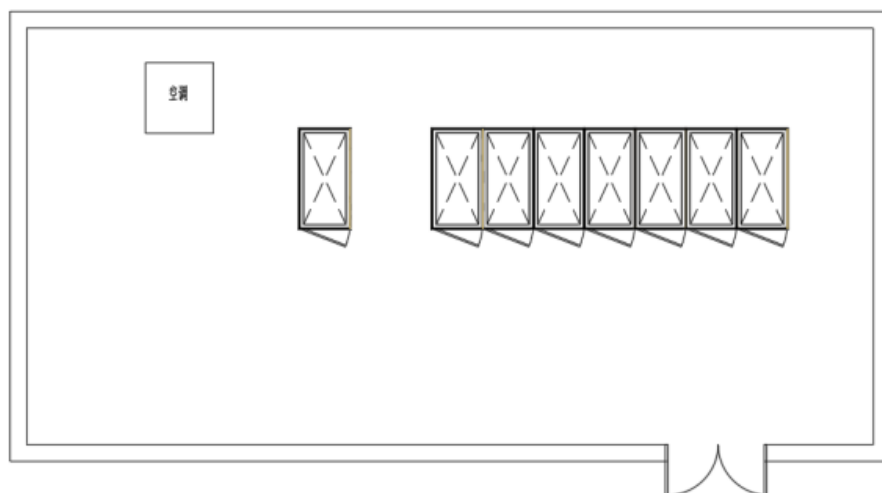
指挥中心机房：位于大楼4楼，面积约90m²，于2019年建成，部署2套模块化机房，共20台机柜，机柜内IT、网络设备基本已满配使用。辅机房部署7台机柜，主要用作视频会议系统使用，空调已超过使用年限，24年底实战平台和数据中台项目计划填充到机柜空间中来，机会空间使用预计到70%。



指挥中心四楼主机房布局示意图

图 32指挥中心机房部署现状

车管处机房：位于大楼1楼，面积约50m²，部署8台机柜，机柜内IT、网络设备基本已使用50%。



车管所一楼机房布局示意图

图 33车管处机房部署现状

基础软硬件现状分析

本次项目主要涉及交警总队公安交通管理综合应用平台、公安交通集成指挥平台、数据中台的系统建设和基础软硬件支撑，针对该三大业务系统平台主要由Hadoop大数据集群节点、MPPDB数仓集群节点、交通管理大数据分布式管理应用平台、Oracle数据库节点、应用服务器5个部分组成，截止目前交警总队公安交通管理综合应用平台、公安交通集成指挥平台已进行阶段性分布式国产化改造，数据中台于2024年建设全部采用ARM国产化服务器建设

公安交通管理综合应用平台，共计66台服务器（其中29台为ARM国产化服务器），包含45台Hadoop大数据集群节点、5台MPPDB数仓集群节点、6台交通管理大数据分布式管理应用平台、6台Oracle数据库节点、4台应用服务器。

公安交通集成指挥平台，共计53台服务器（其中37台大数据集群全部采用ARM国产化服务器），包含37台Hadoop大数据集群节点、7台交通管理大数据分布式管理应用平台、2台Oracle数据库节点、7台应用服务器。

数据中台主要为应用服务器，共计**34台ARM**国产化服务器，**34套**国产化操作系统。

序号	应用系统名称	Hadoop大数据集群节点（MRS）	MPPDB数仓集群节点（DWS）	交通管理大数据分布式管理应用平台（TDMS）	Oracle数据库节点	应用服务器	服务器数量	国产化操作系统
1	公安交通管理综合应用平台	45	5	6	6	4	66	否
2	公安交通集成指挥平台	37		7	2	7	53	否
3	数据中台					34	34	100%
服务器数量合计							153	

大数据集群现状分析

当前综合应用平台大数据集群共**45**台服务器，部署了**Hbase**分布式存储系统、**Kafka**分布式消息队列系统、**Elasticsearch**分布式搜索引擎组件。

其中**Hbase**存储总量**1.25PB**，截止**2025.05.07**使用量**759TB**，剩余**521TB**。全省社会化服务改造后，数据增长量从二期的**6TB/月**提高到**28TB/月**，按照总容量**80%**冗余，仅够未来**10**个月的使用。

Elasticsearch节点为**X86**架构，内存**256GB**，使用率**50%**；存储总量**86.09TB**，使用量**2.17TB**，近一年增长量**0.1TB**，性能无明显影响变化，满足业务使用需要，仅需要考虑国产化改造即可。

Kafka节点为**X86**架构，内存**256GB**，性能满足业务使用需用，仅需要考虑国产化改造即可。

根据当前业务情况，由于全省社会化服务改造业务于**2024**年逐步的建设完善，导致数据量近一年时间激增，因此本期需要仅考虑**Hbase**节点的现网改造以及扩容，满足**3-5**年的业务增长需求，**Elasticsearch**、**Kafka**节点改造放到后期建设，优先保障综合应用平台业务发展的数据增长需求。

软件SNS现状分析

当前交警总队现网主要部署**MRS**和**DWS**软件，其中**MRS**共计**3104vcpu**，**DWS**为**192vcpu**；**MRS**和**DWS**软件即将在**2025年9月21日**维保到期。**MRS**和**DWS**软件维保到期后，将无法进行现网变更和扩容操作，仅能维持现状正常使用；也无法继续享用厂商提供的软件技术支持和软件补丁版本支持服务。对现网**MRS**和**DWS**带来一定的使用限制，需要对**MRS**和**DWS**软件进行续保。

项目建设的必要性

为贯彻落实《全国主干公路交通安全防控体系三年规划》，根据《公安交通管理综合应用平台建设指导意见》、《公安交通集成指挥平台建设指导意见》要求，随着国产化技术的不断发展，公安交通管理工作总队的核心业务具备升级改造条件，亟待满足业务需求的情况下，完善机房环境提供一个高效、安全的信息化运行环境，同时扩容改造服务器、存储以及基础软件等支撑陕西交警总队交通管理核心业务系统的运行，提升整体管理水平，确保核心交通管理信息系统满足业务稳定运行和日常执法和管理需求。并通过集中管理和优化配置，可以提高资源利用效率，减少重复投资，降低运营成本。

目前随着信息技术的快速发展，原有的机房设备无法满足当前的技术需求，需要更新换代以提高数据处理能力和系统的稳定性，为未来的技术发展和业务扩展提供坚实存储、计算、网络基础硬件底座和基础软件支撑，自陕西省公安厅交通管理总队公安交通管理综合应用平台、集成指挥平台、数据中台建设以来，系统在道路交通安全防控体系建设中发挥了应有的作用，提供了交管业务日常所需的各类数据支撑，通过相关数据的分析应用，基本实现道路交通态势智能感知、缉查布控、违章处理等分析研判和业务处理，构建快速高效交通管理体系、常态实战的新型勤务机制。但是，近几年来，我们与先进发达地区的差距正在不断扩大，要达到部、省级的相关业务考核要求也越来越力不从心，迫切需要加强核心业务系统的相关的运行环境升级、新增过国产化服务器、存储以及操作系统等设备，进一步提升陕西省交通综合管控能力。

四、需求分析

机房改造需求

随着信息技术的迅猛发展，交管总队机房作为总队信息化系统的核心支撑设施，其重要性日益凸显。然而，当前交管总队机房在建设和运维过程中面临着诸多问题，亟需进行改造和优化。

首先，交管总队机房的扩展性较差。由于前期规划不足，机房容量往往难以满足业务快速增长的需求，导致频繁扩容和升级，增加了企业的运营成本和时间成本。同时，机房内的设备布局和线缆管理也缺乏规范性，影响了设备的维护和管理效率。

其次，能耗高是当期交管总队机房面临的另一大挑战。交管总队机房建设在用电、制冷、气流管理等方面存在不足，导致能源效率低下。老旧的精密空调故障频繁、UPS主机以及电池系统超期服役已累计超过十年，大量电力消耗在包括电源设备、冷却设备和照明设施在内的网络关键物理基础设施上，增加了企业的能源消耗和碳排放。

三楼区域为大会议室、电视电话会议室和业务培训室，目前所有设备均采用市电供电异常断电后无法正常维持业务开展。

此外，机房运维难度大也是当前普遍存在的问题。由于设备种类繁多、品牌不一，原有的动环系统版本老旧信息，感知数据接口缺乏且数据更新不及时，加上运维人员交替频繁，导致运维人员对设备了解不足，管理混乱。故障响应和故障处理跟踪也容易出现混乱，影响了IT系统的稳定性和可用性。

为了解决上述问题，提高机房的能效、可靠性和运维效率，本次提出整体性交管总队机房微改造解决方案。

针对45台核心区机柜进行冷通道封闭，配套内部环境检测系统。同时为满足内部制冷量需求，增加3台列间空调。封闭冷通道通过物理隔离冷热气流，有效提高了制冷系统的效率。在封闭冷通道内，冷空气能够精准地送达服务器进风口，避免了与热空气的混合，从而确保了服务器运行在最佳温度范围内。延长了服务器的使用寿命，减少了因过热导致的故障率，提升了整体系统的稳定性。封闭冷通道改造有助于实现节能减排。通过优化气流组织，减少了不必要的冷量损失，降低了空调系统的能耗。随着交管总队机房规模的扩大和设备密度的增加，传统散热方式已难以满足高效散热的需求。封闭冷通道作为一种先进的散热解决方案，能够适应未来数据中心的发展趋势，通过优化机房内的气流组织，减少冷热空气混合，提高制冷效率，从而降低能耗。同时，通过本次改造改善机房内的设备布局和线缆管理，提高设备的可维护性和管理效率。

更新2台UPS主机（型号：伊顿PW9390），以及配套240节200Ah铅酸蓄电池，原有系统主机报警且电池测试失败部分电池内阻升高，为保障机房核心设备稳定运行，本次将通过全新的UPS系统进行改造替换。

新增一套机房动力环境系统，围绕实时性、精准性、智能化、可扩展性及运维效率提升展开，以实现对机房动力设备（如UPS、配电柜、机柜）与环境参数（温湿度、漏水、烟雾等）的全方位监控与主动管理。

三楼大会议室、电视电话会议室和业务培训室区域UPS供电改造，对原有配电箱进行改造，考虑到3楼区域为会议区，音视频设备接U电整体负载不超过30KW,由地下室配电间125KVA UPS输入输出配电柜输出1路电缆至3楼电井内新增UPS配电箱，并最终对大会议室、电视电话会议室和业务培训室区域进行UPS供电。

基础软硬件需求

随着公安交通管理综合应用平台、公安交通集成指挥平台、数据中台等业务开展的不断完善和提升。

一、基础硬件环境建设

扩容数据中台 3台GPU服务器用于比对服务，3台通用服务器用于数据分析服务功能系统部署
改造现网14台X86架构的HBase节点服务器，并扩容4台HBase节点服务器，全部采用12*8TB容量改造扩容
改造现网19台大数据存储节点服务器硬盘，由12*4TB硬盘，全部改造为12*8TB硬盘，实现存储的规模扩容同时，减少大数据节点建设，减少预算投资。

二、基础软件支撑建设

新增服务器国产化操作系统，提共计24套，其中18套用于公安交通管理综合应用平台大数据集群改造扩容服务器，6套用于数据中台服务器。

软件SNS续保需求

本次项目建设需要对MRS和DWS软件进行续保，续保时间延续到2028年12月31日，确保在截止到期期间对MRS和DWS进行现网变更和升级扩容操作。同时享受厂家提供的原厂技术支持和软件补丁版本支持服务。

在MRS和DWS软件维保时间延续到2028年12月31日，将享受厂家提供的如下服务：

- （1）提供400电话支持，接到服务请求后，在服务等级规定的响应时间内电话支持现网问题分析、诊断及定位，提供问题解决方式；
- （2）提供产品知识服务，如原厂网站知识库、产品资料和自助服务工具等资源；
- （3）提供定期巡检服务：在定期巡检中基于MRS巡检工具和日常巡检辅助问题定位，诊断组件存在问题并分析和修复，并提供组件补丁升级服务。

大数据集群扩容需求

2024年因全省社会化服务改造地市数据逐步接入到总队六合一座，导致数据量整体激增且为持续性数据增长变化，整体数据量从前期项目规划的6TB/月增长到目前24.5TB/月，从2024年1月1号截止2025年6月19日累计数据统计情况具体如下表

序号	时间段	使用情况（TB）	增量（TB）
1	2024-01-01	375	累计增长434TB 0.82TB/天 24.5TB/月
2	2024-04-14	422	
3	2024-05-05	575	
4	2024-12-31	693	
5	2025-01-01	693	
6	2025-05-18	769	
7	2025-06-19	809	

当前现网Hbase节点存储可用容量共计1280TB，截止2025.05.07资源使用量已达759TB，剩余521TB。
当前容量不足已支撑，按照总容量80%冗余，仅够满足未来9个月的使用，即截止到25年底数据节点容量已无法

承载当前增长的业务数据存储。

按照大数据分布式存储三副本策略，考虑未来5年数据增长，数据增长量24.5TB/月，冗余系数0.7设计规划本次项目分布式大数据存储所需容量，具体计算如下：

现网数据节点裸容量情况为：

$$33 \text{ (节点数)} \times 12 \text{ (盘位)} \times 4TB \text{ (硬盘裸容量)} = 1584TB$$

现网数据可用总容量情况为：

$$759TB \text{ (已使用)} + 521TB \text{ (剩余量)} = 1280TB$$

数据节点可用容量转换率为：

$$\frac{1280TB \text{ (现网数据可用总容量)}}{1584TB \text{ (现网数据节点裸容量)}} \approx 80.8\%$$

五年数据增量总可用容量为：

$$24.5TB \text{ (月增量)} \times 12 \text{ (月)} \times 5 \text{ (年)} = 1470TB$$

五年数据总规划裸容量为：

$$\frac{(1470TB \text{ (5年增量)} + 759TB \text{ (已使用量)})}{0.8 \text{ (冗余系数)} \times 0.808 \text{ (可用容量转换率系数)}} \approx 3449TB \text{ (向上取整)}$$

本次项目需新增数据裸总量为：

$$3449TB \text{ (五年总裸容量)} - 1584TB \text{ (现网裸容量)} = 1865TB$$

五、建设方案

架构设计

总体架构

从本次项目总体业务架构逻辑上将项目内容按照系统建设分为四层，从底往上依次为：

（1）基础设施运行环境：实现对上层公安交通综合应用平台、公安交通集成指挥平台微服务化平台、数据中台等业务系统和数据服务的软硬件基础环境支撑，基础硬件支撑包含机房硬件设备、通用服务器、GPU服务器；基础软件支持包含SNS软件、虚拟化软件、国产化操作系统。

（2）分布式系统基础平台：实现了数据资源的管理、数据存储组件、调度管理、消息服务、非结构化数据存储、索引数据存储、运算数据存储、以及数据计算等，属于分布式系统的数据基础支撑平台。

（3）分布式系统服务平台：实现分布式基础平台的数据存储、数据组织、高可用的访问机制、异常处理机制、对于交通管理综合应用平台各种数据服务能力、访问权限控制、访问日志等服务管理功能。

（4）核心业务系统应用端：实现公安交通综合应用平台、公安交通集成指挥平台微服务化平台、数据中台等系统的面向陕西省交通管理服务的统一窗口服务。本次项目部分应用模块需进行微服务化国产化适配改造以及功能模块提升。

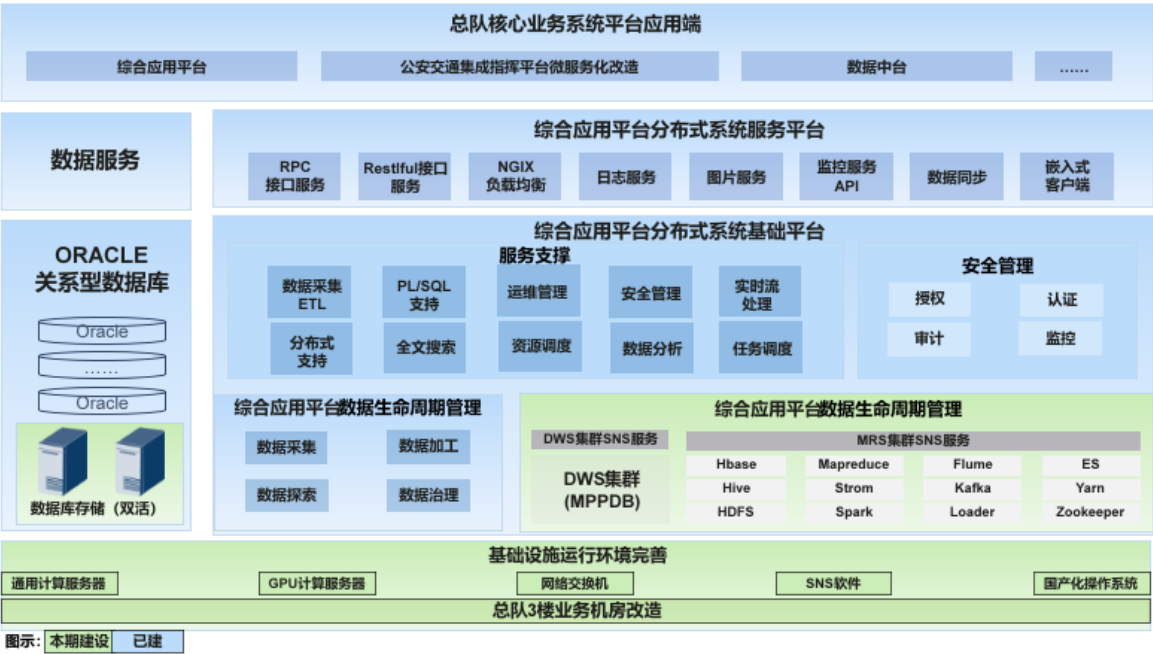


图 5-1总体架构图

数据架构

从数据应用角度分成OLTP和OLAP两种类型，分别围绕图片数据、日志数据和业务数据进行数据交换和数据服务，数据流程架构具体如下图所示：

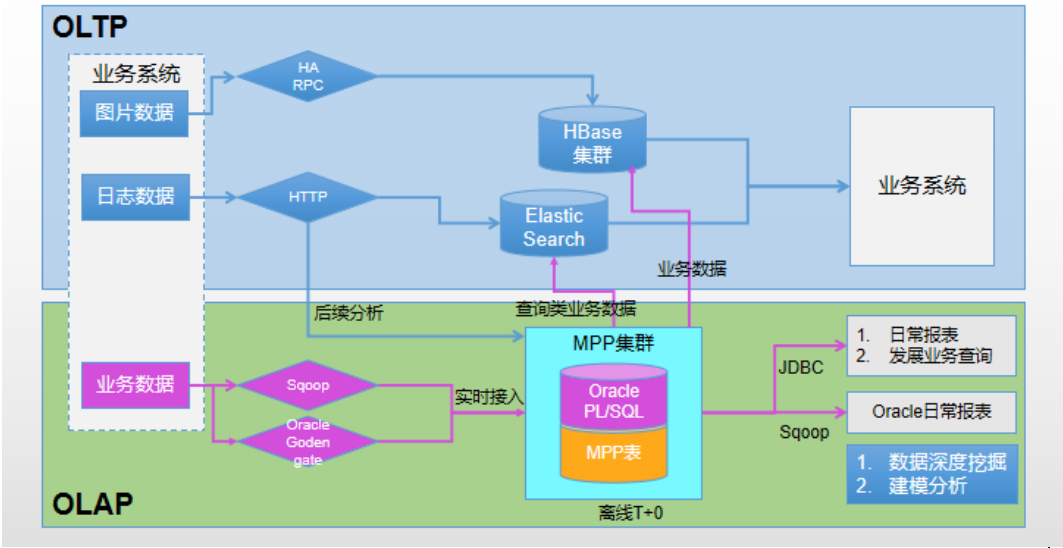


图 5-2数据架构图

网络架构

本次项目建设系统网络位置全部部署于公安信息网内，为保障整体业务系统的稳定性和可靠性，系统组网由业务系统应用端、综合应用平台Oracle核心业务库、分布式综合应用平台三个模块组成，其中业务系统应用端主要新增新购3台通用服务器和3台GPU服务器用于部署数据中台比对业务功能模块进行业务组网；分布式综合应用平台主要针对现网DWS集群（作为系统MPPDB节点针对结构化数据提供并行关系型数据计算服务）、MRS集群（由管控节点、Hbase节点提供存储服务、ES节点提供索引服务、Kafka节点提供消息服务共用组成）进行SNS软件续保，新网组网环境不变。整体网络架构具体如下图：

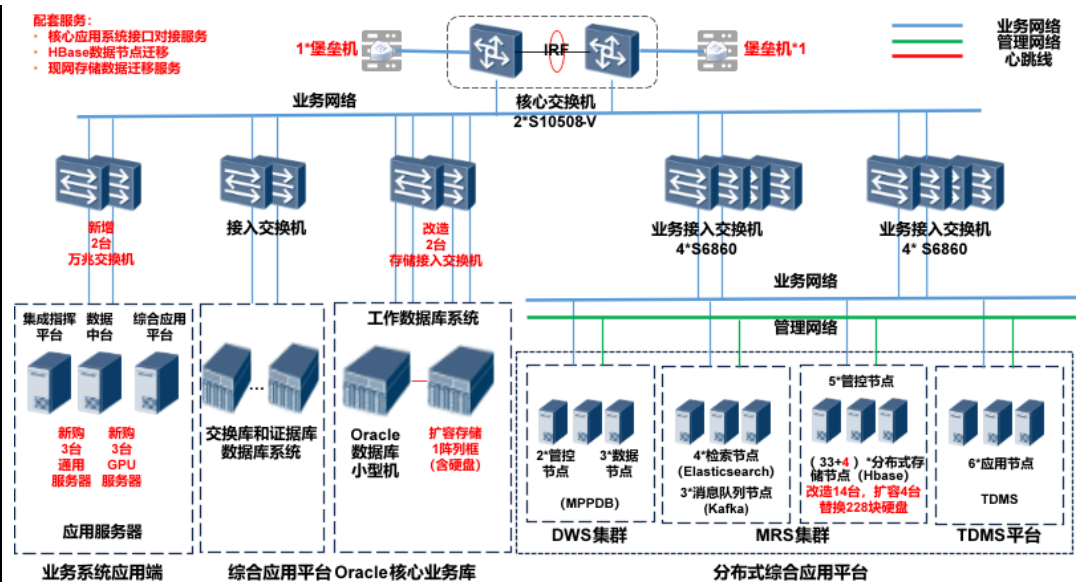


图 5-3网络架构图

机房改造方案

封闭冷通道改造方案设计

冷通道布局设计

在普通交管总队机房加装封闭冷通道的改造方案中，冷通道的布局设计是至关重要的环节。冷通道布局设计的核心目标是优化气流组织，提高能效，从而实现节能减排。

首先，冷通道的布局应考虑机柜的排列方式。机柜应采用长排列的方式，以便于低成本处理冷热通道的隔离。在机柜的上部，应安装钢化玻璃等隔离材料，形成封闭的冷通道，以最大限度地减少冷热气流的混合，提高能效。

其次，冷通道的宽度和高度设计需合理。冷通道的宽度应略大于机柜的宽度，以确保机柜前后的冷气流能够顺畅流动。冷通道的高度设计则需考虑机柜顶部与天花板之间的距离，既要保证冷气流能够充分进入机柜，又要避免过高的空间导致气流短路。在本改造方案中，冷通道上部顶盖设计比机柜顶部高350mm，以确保足够的空间供冷气流通过。

此外，冷通道的入口和出口应设置合理的密封装置，如移门等，以防止热空气回流进入冷通道。这些密封装置应具备良好的耐磨性、耐蚀性，并经过精细加工，以确保气流输出的密封性。

最后，冷通道的布局设计还需考虑日常维护和检修的便利性。在冷通道的上部或侧面，应设置活动天窗或检修口，以便于维护人员进入冷通道进行检修工作。同时，冷通道的布局应避免与机房内的其他设施发生冲突，如电线、通风系统等。

综上所述，冷通道的布局设计是封闭冷通道改造方案中的关键环节，合理的布局设计能够优化气流组织，提高能效，降低能耗，为交管总队机房的稳定运行提供有力保障。

制冷设备选型与配置

在封闭冷通道改造方案中，制冷设备的选型与配置是至关重要的一环。针对普通交管总队机房的特定环境和需求，我们需要精心挑选高效、可靠的制冷设备，以确保机房内的温度、湿度等参数始终处于最佳状态。

首先，考虑到交管总队机房对制冷量的高需求，我们计划选用高效节能的空调机组作为主要的制冷设备。在选型时，我们将综合评估不同品牌、型号的机组，重点考虑其制冷效率、能耗比、稳定性以及维护成本等因素。为了确保在单台设备故障时仍能维持机房环境稳定，

其次，针对封闭冷通道的特殊结构，我们需要配置与之相匹配的制冷功率机组。从而实现有效的散热。在选型时，我们将根据机房的实际布局和管道长度等因素，精确计算所需的功率和制冷量，以确保冷却效果的最大化

综上所述，在封闭冷通道改造方案的制冷设备选型与配置中，我们将以高效、可靠、节能为原则，精心挑选并合理配置各类制冷设备，以确保机房内的温度、湿度等参数始终处于最佳状态。

气流组织优化设计

在普通交管总队机房加装封闭冷通道的改造方案中，气流组织的优化设计是至关重要的一环。优化的气流组织不仅能提高机房的冷却效率，还能有效降低能耗，确保设备稳定运行。

首先，针对封闭冷通道内的气流组织，应确保冷风通过地板下的静压箱均匀送入冷通道，形成稳定的气流流场。冷通道封闭后，冷风在通道内二次均压，能更加精准地送达服务器机柜的前端，避免冷风在输送过程中的浪费和冷热气流的混合。同时，机柜的排列方式应采用面对面、背靠背的布置，以最大化利用冷风资源，提高冷却效率。

其次，热气流的管理同样重要。服务器产生的热气流应通过机柜后部或上部排出，直接进入热通道，并通过天花板上方的回风口返回空调系统。这一过程应确保热气流不与冷气流再次混合，以提高空调系统的回风温度和蒸发器的换热效率。

此外，考虑到机房内可能存在局部热点问题，可以在热点区域安装额外的送风装置，如带动力的风扇或局部送风地板，以增加这些区域的送风量，确保整体温度的均匀性。

最后，引入智能控制系统对气流组织进行实时监测和调节也是必要的。通过传感器监测机房内的温度和湿度，智能系统可以自动调节送风量和送风温度，以适应不同负载条件下的冷却需求。这不仅能提高机房的能效，还能为设备提供一个更加稳定、可靠的运行环境。

综上所述，通过合理的气流组织优化设计，普通交管总队机房加装封闭冷通道的改造方案将能够显著提升冷却效率，降低能耗，确保设备稳定运行。

监控与管理系统设计

在封闭冷通道改造方案中，监控与管理系统的的设计是确保改造效果得以持续、高效运行的关键环节。本节将详细阐述监控与管理系统的构成及功能设计。

监控与管理系统主要包括环境监控、设备监控、能耗管理及远程操控四大模块。环境监控模块负责实时监测机房内的温度、湿度、空气质量等关键环境参数，确保封闭冷通道内的环境条件始终处于最优状态。设备监控模块则对封闭冷通道内的空调、风机、门禁等设备进行全面监控，及时发现并预警潜在故障，保障机房设备的稳定运行。

能耗管理模块通过集成智能电表、能耗传感器等设备，实现对机房能耗的精准计量与分析，为节能降耗提供数据支持。同时，该模块还能根据实际需求自动调节设备运行参数，实现能耗的最优化分配。

远程操控模块则依托先进的物联网技术，实现监控与管理系统的远程访问与控制。运维人员无需亲临现场，即可通过电脑或移动设备实时查看机房状态、调整监控参数、下发控制指令，极大提高了运维效率与响应速度。

综上所述，监控与管理系统的的设计旨在构建一个全面、智能、高效的机房管理体系，为封闭冷通道的稳定运行提供坚实保障。通过该系统的实施，将有效提升机房的整体管理水平，降低运维成本，为企业的数字化转型与业务发展提供有力支撑。

UPS改造设计

在旧机房拆除原有UPS并更换新UPS的方案设计中，需综合考虑安全性、兼容性、可扩展性及业务连续性，确保改造过程风险可控且满足未来需求。以下是详细的方案设计框架：

一、前期评估与规划

现状调研

	<p>原UPS系统参数：记录旧UPS的容量、输入/输出电压、电池配置（品牌、容量、数量）、安装位置及承重要求。</p> <p>负载分析：统计当前负载功率、关键设备（服务器、网络设备）的电力需求及冗余要求。</p> <p>机房环境：评估空间布局、散热条件、配电柜容量及接地系统状态。</p> <p>需求定义</p> <p>新UPS选型：根据负载增长（预留20%-30%余量）、效率（选择高频机或模块化UPS）、输入电压范围及并机能力确定型号。</p> <p>兼容性验证：确认新UPS与现有配电系统（ATS、PDU）、电池组及系统的接口匹配性。</p> <p>风险评估与预案</p> <p>断电风险：规划临时供电方案（如租用移动式UPS或柴油发电机）。</p> <p>施工安全：制定旧电池拆除的防漏液、防短路操作流程。</p>
	<p>二、拆除旧UPS方案</p> <p>断电与隔离</p> <p>通知业务部门停机窗口，关闭UPS输出并断开输入电源。</p> <p>对UPS系统进行完全放电，确保电容残压归零。</p> <p>在配电柜侧加装隔离锁（Lockout/Tagout），防止误操作。</p> <p>设备拆除步骤</p> <p>电池组拆除：</p> <p>穿戴防酸护具，按电池串并联顺序断开连接线，避免短路。</p> <p>使用专用托盘搬运电池，按环保要求回收处理（需资质企业处理）。</p> <p>主机与配件拆除：</p> <p>拆卸UPS主机、外部旁路柜及监控模块，标记线缆端口。</p> <p>检查承重支架锈蚀情况，评估是否需保留或更换。</p> <p>场地清理</p> <p>清理电池漏液残留（使用碳酸氢钠中和酸性物质）。</p> <p>修复地面承重结构（如因电池组长期压迫导致的破损）。</p>
	<p>三、新UPS安装方案</p> <p>基础设施准备</p> <p>散热优化：预留UPS前后散热空间（$\geq 1\text{m}$），调整空调出风口方向或增设通风孔。</p> <p>配电改造：升级输入/输出电缆规格（如原为70mm²升级至95mm²），配置独立断路器。</p> <p>设备安装步骤</p> <p>主机就位：使用液压叉车或吊装设备平稳放置UPS主机，调整水平度（误差$\leq 2\text{mm/m}$）。</p> <p>电池组安装：</p> <p>采用抗震架固定锂电池或铅酸电池组，确保间距$\geq 20\text{mm}$（散热与维护通道）。</p> <p>连接电池时使用扭矩扳手（按厂家要求力矩值），避免接触不良。</p> <p>线缆连接：</p> <p>输入/输出线缆屏蔽层接地，避免环路干扰。</p> <p>配置并机线（若多台UPS并联）、干接点信号线与系统集成。</p> <p>接地与防雷</p> <p>独立接地线（截面积$\geq 35\text{mm}^2$），接地电阻$\leq 1\Omega$。</p> <p>在UPS输入端加装二级防雷器（$I_n \geq 40\text{kA}$）。</p>

四、测试与验收

功能性测试

空载测试：开机检查UPS自检状态、风扇运行及面板告警功能。

带载测试：逐步加载至100%额定容量，监测输出电压波动（ $\leq \pm 2\%$ ）、谐波畸变率（ $\leq 3\%$ ）。

切换测试：模拟市电中断，验证电池切换时间（ $\leq 10\text{ms}$ ）及满载续航时间。

并机与冗余测试

若为N+X冗余配置，断开一台UPS验证负载无缝切换。

测试并机系统的均流偏差（ $\leq 5\%$ ）。

环境与安全验收

红外热成像检测接线端子温升（ $\Delta T \leq 40^\circ\text{C}$ ）。

检查电池间氢气浓度（锂电池无需通风，铅酸电池需安装氢气探测器）。

五、文档与运维移交

技术文档

提供新UPS的电气图、电池配置表、操作手册及保修协议。

更新机房承重图纸与配电系统拓扑图。

培训与监控

对运维团队进行新UPS操作、故障代码解读及应急处理培训。

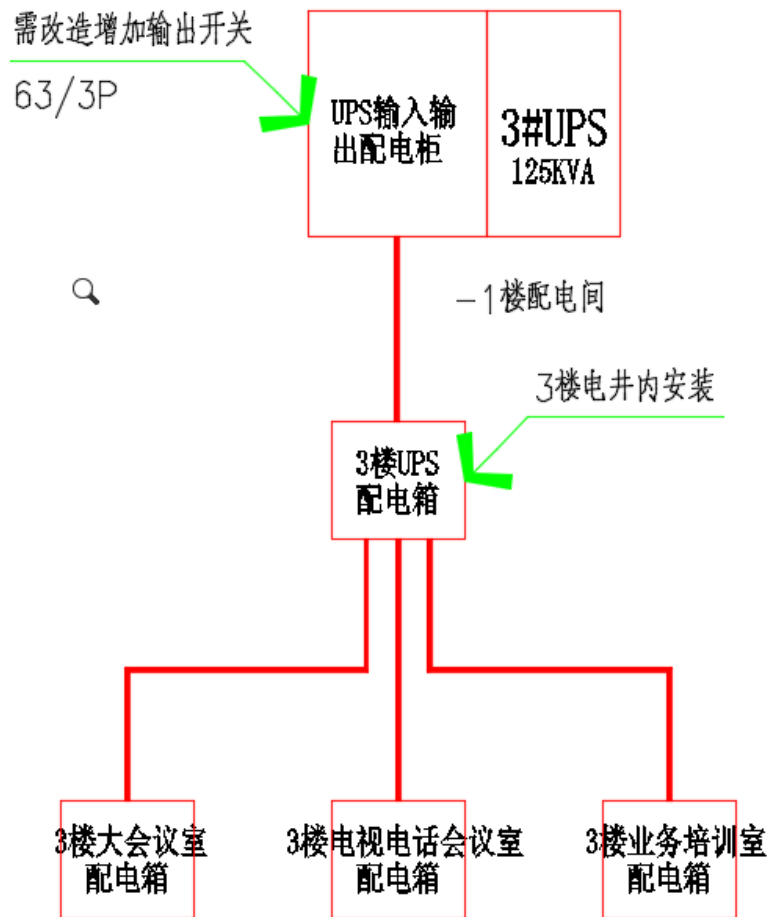
集成UPS状态至动环系统，设置短信/邮件告警（如电池低电压、过温）。

六、周期评估

施工周期：大型系统（ $\geq 100\text{kVA}$ ）需1-2周（含定制钢架与配电改造）。

七、三楼视频会议室UPS供电改造

三楼大会议室、电视电话会议室和业务培训室区域UPS供电改造，对原有配电箱进行改造，考虑到3楼区域为会议区，音视频设备接U电整体负载不超过30KW,由地下室配电间125KVA UPS输入输出配电柜输出1路电缆至3楼电井内新增UPS配电箱，并最终对大会议室、电视电话会议室和业务培训室区域进行UPS供电。



3楼视频会议室UPS供电拓扑图

施工步骤

利用节假日对三楼会议室端三处配电柜/箱供电改造，在3楼电井安装UPS输入输出配电箱，敷设从负一层配电间至3楼电井安装UPS输入输出配电箱之间的电线电缆；敷设从3楼电井新增UPS输入输出配电箱到三楼会议室端三处配电柜/箱供电之间的电线电缆；

对原3#125KVA UPS输出配电柜进行改造，增加一楼3楼视频会议室UPS供电总空开80A/3P，将第3阶段提前敷设好从负一层配电间至3楼电井安装UPS输入输出配电箱之间的电线电缆接至新增空开输出端：（待切换停机当天，进行线缆上柜工作）；

施工与实施计划

施工流程与步骤

前期准备

1. 现场勘查：由专业团队对机房进行全面勘查，记录现有设备布局、空间尺寸、电源及网络布线情况，确保改造方案的可行性。



2. 图纸设计：根据勘查结果，设计封闭冷通道的具体布局图纸，包括冷通道尺寸、材料选择、门窗位置、通风口设计等，并与机房管理人员确认。



机房机柜改造后布局图



机房机柜现有布局图

3. 材料采购：依据设计图纸，采购所需材料，如冷通道框架材料、保温板材、密封条、门禁系统等，确保所有材料符合质量要求。

二、施工准备

1. 安全防护：设置施工安全区域，配备必要的防护设备，如安全帽、防护眼镜、工作手套等，确保施工人员安全。
2. 设备搬迁计划：制定详细的设备搬迁计划，确保在封闭冷通道搭建过程中，机房内重要设备能够安全、有序地迁移至临时位置。

三、施工实施

1. 搭建框架：按照设计图纸，开始搭建冷通道的框架，确保结构稳固。
2. 安装板材：在框架完成后，安装保温板材，确保冷通道内部与外界有效隔离。
3. 安装配套设施：包括门禁系统、通风口、温湿度监测传感器等，确保冷通道的功能完善。
4. 调试与验收：完成所有安装后，进行冷通道系统的调试，确保其正常运行，并邀请相关部门进行验收。
- 通过以上步骤，确保封闭冷通道改造项目高效、安全地完成。

施工进度安排

为确保普通交管总队机房加装封闭冷通道改造项目的顺利进行，特制定以下施工进度安排，以明确各阶段的任务与时间节点，保证工程高效、有序地完成。

一、前期准备阶段（第1-2周）

- 第1周：完成项目启动会议，明确各方职责与分工；完成现场勘查，收集机房布局、设备配置等基础数据；制定详细的施工图纸与技术方案，并获得相关审批。
- 第2周：根据施工图纸，采购所需封闭冷通道组件、辅助材料及安全设备；组织施工队伍进行技术培训与安全教育，确保施工人员熟悉操作流程与安全规范。

二、施工阶段（第3-8周）

- 第3-4周：进行机房内设备的临时迁移与保护措施实施，确保施工期间设备安全；开始搭建封闭冷通道框架，安装顶部与侧面封闭结构，同步进行冷却系统调试与对接。
- 第5周：完成封闭冷通道所有组件的安装与调试，确保密封性能良好，冷量分配均匀；恢复机房内设备原位，并进行初步功能测试。
- 第6周：UPS电池组更换,全新动环系统部署，各接口模块对接安装，测试系统效果，评估供电稳定情况。
- 第7-8周：进行全面的系统联调，包括冷通道与机房空调系统的协同工作，确保改造效果达到预期；组织项目验收前的自检，整改发现的问题。

通过上述详细的施工进度安排，我们将确保改造工程按时、按质、按量完成，为交管总队机房的高效运行提供坚实保障。

质量控制与验收标准

在普通交管总队机房加装封闭冷通道改造项目中，质量控制与验收标准是确保工程质量和后续运行效果的关键环节。本节将详细阐述质量控制措施及验收标准，以确保改造工程达到预期目标。

质量控制方面，首先需建立严格的质量管理体系，明确各阶段的质量责任人，确保从设计、采购到施工、调试的每一个环节都符合质量要求。施工过程中，将采用先进的施工工艺和技术，加强对施工人员的培训和管理，提高施工质量和效率。同时，将实施严格的质量检查和监督，定期对施工质量和进度进行检查评估，及时发现并纠正问题。

验收标准方面，将依据国家相关标准和行业规范，结合项目实际情况，制定详细的验收标准和流程。验收内容包括但不限于封闭冷通道的结构完整性、密封性、冷热空气隔离效果、设备运行状态等。验收过程中，将采用

专业的检测设备和仪器，对各项指标进行准确测量和评估，确保改造工程符合设计要求和质量标准。

此外，还将建立质量追溯机制，对施工过程中出现的任何问题记录和跟踪，确保问题得到及时解决。同时，将定期对改造后的交管总队机房进行维护和检查，确保封闭冷通道长期稳定运行，为交管总队机房提供可靠的保障。

综上所述，通过严格的质量控制措施和明确的验收标准，将确保普通交管总队机房加装封闭冷通道改造项目的高质量完成，为交管总队机房的能效提升和稳定运行提供有力支持。

项目预算与效益分析

改造项目预算明细

本次总队交管总队机房加装封闭冷通道以及UPS系统更新改造项目的预算明细如下：

- 1.购置费用与辅助设施与材料费用：包含（冷通道及动环线路改造、UPS），主要用于采购封闭冷通道所需的隔断材料、门体系统、气流组织优化装置、线缆配电箱、UPS机头、电池、动环设备等核心设备。这些设备需具备良好的密封性和耐用性，以确保改造后的机房能够有效隔绝外界热空气，提高冷却效率。
- 2.设备承重加固、机房局部装修及其他
- 综上所述，本次改造项目总预算各项费用均经过细致核算，旨在确保改造工程的高质量和高效益。

节能效益分析

在普通交管总队机房加装封闭冷通道的改造方案中，节能效益是评估该方案经济性和可行性的指标。以下是对节能效益的详细分析：

首先，封闭冷通道的设计能够显著提高机房的能源利用效率。通过封闭冷通道，冷热空气得到了有效的隔离，避免了冷热空气的混合，从而提高了空调的制冷效率。据统计，采用封闭冷通道后，空调室内风机的送风量可减少至传统开放式的30%，电功耗相应降低，节能效果可达20%以上。

其次，封闭冷通道的建立有助于减少数据中心制冷能耗。数据中心制冷能耗通常占到数据中心总能耗的三分之一左右，因此合理的冷却方案对数据中心的经济效益至关重要。通过加装封闭冷通道，机房的制冷能耗将显著降低，从而节约了大量的能源消耗。

此外，节能效益还体现在机房整体能耗的降低上。封闭冷通道不仅提高了制冷效率，还改善了机房内部的气流组织，避免了局部热岛效应的产生。这使得机房的整体能耗保持在较低水平，有助于提升数据中心的能效水平。

从经济效益角度来看，加装封闭冷通道的初期投资将在较短时间内得到回报。由于节能效果显著，机房的运营成本将大幅降低，回报周期通常较短。同时，该方案还符合国家关于数据中心能效的相关标准和政策要求，有助于提升数据中心的绿色形象和市场竞争力。

综上所述，普通交管总队机房加装封闭冷通道的改造方案在节能效益方面具有显著优势，是实现机房节能减排、提升能效水平的有效途径。

投资回报率评估

在普通交管总队机房加装封闭冷通道的改造方案中，投资回报率（ROI）评估是项目预算与效益分析的核心环节。ROI通过衡量改造项目带来的经济效益与初始投资成本之间的关系，为投资者提供直观的决策依据。

具体而言，投资回报率计算公式为： $ROI = (投资收益 - 投资成本) / 投资成本 \times 100\%$ 。在本改造项目中，投资收益可包括节能降耗带来的电费节省、设备寿命延长带来的维护成本降低以及因机房环境改善而提升的运行稳定性等间接收益。投资成本则涵盖封闭冷通道设备购置、安装施工、调试运行等全部费用。

为准确评估投资回报率，需对改造前后的能耗数据进行详细对比分析，预测节能效果及节省的电费金额。同

时，考虑设备使用寿命及长期维护成本的变化，综合评估项目的经济效益。此外，还应将投资回收期纳入考量，即改造项目产生的经济效益能够抵消初始投资所需的时间。

改造目标与预期效果

本次交管总队机房加装封闭冷通道改造方案的核心目标在于显著提升机房的能效管理水平与设备运行稳定性。具体而言，改造目标可细化为以下几个方面：

- 1. 能效提升：通过构建封闭冷通道，有效隔离冷热空气，减少冷量损失，预计能耗将降低**15%-20%**。这一目标的实现，不仅能大幅减少机房的运营成本，还能积极响应国家节能减排的号召，提升总队的绿色形象。
- 2. 温度均匀性优化：封闭冷通道能够确保服务器机柜周围温度分布更加均匀，避免局部过热现象，从而提升服务器的运行效率与稳定性。预期改造后，机房内温度波动范围将控制在**±2℃**以内，有效延长IT设备的使用寿命。
- 3. 提升供电系统可靠性：消除因设备老化导致的断电风险，确保关键业务连续运行。更换老化**UPS**主机及电池组，采用高冗余设计。杜绝因**UPS**故障引发的火灾、漏液等安全风险。
- 4. 运维效率提升：改造后，封闭的冷通道设计将简化机房的日常维护工作，运维人员无需频繁调整空调设置或处理因温度不均引发的报警，预计运维工作量可减少约**30%**，运维效率显著提升。
- 5. 适应性与可扩展性增强：改造方案将充分考虑机房未来的扩展需求，封闭冷通道的设计便于快速增减机柜，确保机房随着业务发展灵活调整，满足长期运营的需要。

综上所述，本次改造旨在通过技术革新，实现机房能效、稳定性、运维效率及适应性的全面提升，为企业的数字化转型提供坚实的基础设施保障。

风险与应对措施

可能面临的风险

在普通交管总队机房加装封闭冷通道改造过程中，可能会面临多方面的风险，这些风险若处理不当，可能会影响改造进度、增加成本，甚至威胁到机房的正常运行和数据安全。以下是可能面临的主要风险：

- 1. 技术实施风险：封闭冷通道的设计、安装需精确匹配机房现有布局和设备，技术实施不当可能导致冷热气流混乱，影响散热效果。此外，新设备的兼容性问题也可能引发故障。
- 2. 运营中断风险：改造期间，机房可能需要部分或全部停机，这可能导致业务中断，影响客户服务和企业运营。数据迁移和备份过程中的任何失误都可能造成数据丢失或损坏。
- 3. 成本超支风险：改造方案可能因设计变更、材料涨价、施工延期等因素导致成本超出预算，增加企业财务负担。
- 4. 安全风险：改造过程中，物理安全（如门禁系统调整）和网络安全（如线路重新布局可能引入的安全漏洞）都可能受到威胁，需严格防范。
- 5. 环境适应性风险：封闭冷通道可能改变机房内微环境，如湿度、温度分布不均，若未能有效监测和调整，可能对设备稳定运行构成威胁。

综上所述，普通交管总队机房加装封闭冷通道改造是一个复杂且需谨慎对待的项目，需全面评估并有效应对上述风险，确保改造顺利实施并达到预期效果。

风险应对策略

在普通交管总队机房加装封闭冷通道改造过程中，可能面临多种风险，为确保项目顺利实施并达到预期效果，需制定针对性的风险应对策略。

- 1. 技术风险：针对改造过程中可能出现的技术难题，如设备安装调试失败、冷通道密封性能不佳等，我们应采取预先技术评估和测试的策略。在项目启动前，组织专家团队对技术方案进行详细评审，确保技术的可行性

和可靠性。同时，准备备用技术方案和应急处理预案，以便在出现问题时能够迅速切换并解决问题。

2. 施工风险：改造施工可能影响机房的正常运行，存在数据丢失或设备损坏的风险。为此，我们将采取分阶段施工的方式，尽量减少对机房运行的影响。在每个施工阶段前，制定详细的施工计划和安全措施，并安排专业人员监督执行。同时，做好数据备份和设备保护工作，确保施工过程中的数据安全和设备安全。

3. 管理风险：项目管理和协调不善可能导致进度延误或成本超支。为应对这一风险，我们将建立项目管理团队，明确各成员的职责和任务，制定详细的项目计划和时间表。同时，加强项目沟通和协调，定期召开项目会议，及时解决项目中出现的问题，确保项目按计划顺利推进。

4. 人员风险：操作人员技术水平和安全意识不足可能影响改造效果。我们将加强对操作人员的培训和教育，提高他们的技术水平和安全意识。同时，制定严格的操作规程和安全制度，确保操作过程的规范性和安全性。

通过以上风险应对策略的实施，我们将有效降低改造过程中的风险，确保项目的顺利实施和成功完成。

应急预案制定

在普通交管总队机房加装封闭冷通道改造过程中，制定周密的应急预案是确保项目顺利进行及后续运维安全的关键环节。应急预案的制定需涵盖以下几个方面：

1. 紧急停机流程：明确在出现严重设备故障、火灾、电力中断等紧急情况下，如何快速、有序地关闭所有非关键设备，以保护数据安全和硬件完整性。包括备用电源启动程序、数据备份及恢复步骤等。

2. 人员疏散与救援：制定详细的人员疏散路线和集合点，确保所有工作人员了解在紧急情况下的安全撤离流程。同时，与当地消防、医疗部门建立联动机制，确保快速响应和救援。

3. 设备故障应对：针对改造过程中可能出现的特定设备故障（如冷却系统故障、门禁失灵等），预设快速修复方案或替代方案，包括备用设备的即时启用和专业技术团队的紧急调度。

4. 环境监控与报警：加强改造后的环境系统，确保对温度、湿度、烟雾、漏水等关键指标进行24小时不间断监控，并设置多级报警机制，以便及时发现并处理潜在风险。

5. 培训与演练：定期组织应急预案的培训与实战演练，提升团队应对突发事件的能力，确保每位成员熟悉自身职责，能够在紧急情况下迅速、准确地采取行动。

通过上述应急预案的制定与实施，可以有效降低改造过程中的风险，保障改造工作的平稳过渡及机房的长期稳定运行。

机房维护

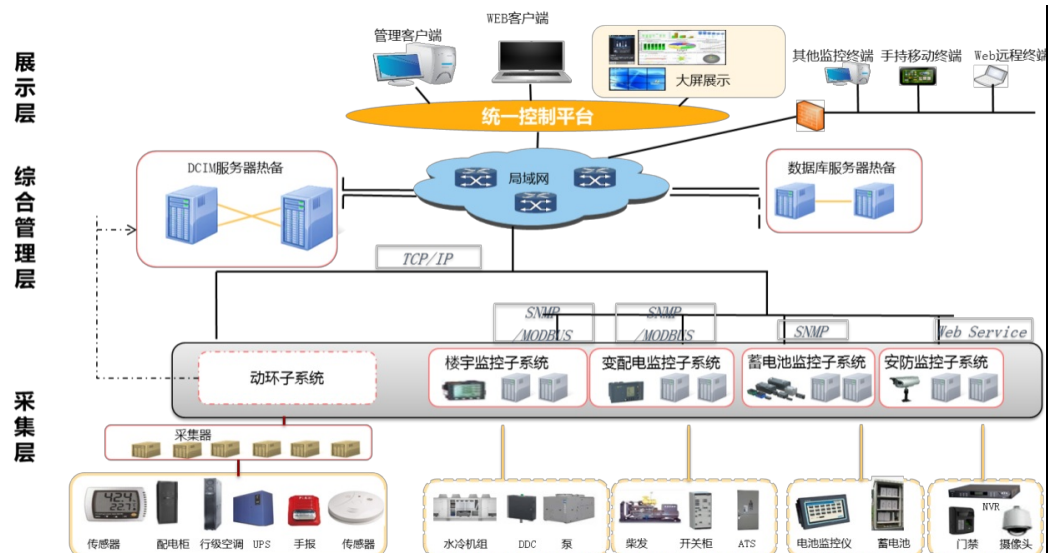
总体系统架构

运维管理系统架构分为：展示层、综合管理层、采集层等。系统架构中各层功能说明如下：

1.采集层：接口模块将各个子系统采集到数据进行协议和信息模型转换，将“事件”、“告警”、“资源”等数据转换成智能化系统可识别的统一的数据模型，接口适配层与上层应用层之间的接口协议采用统一的内部协议。

2.管理层：由服务器和管理软件组成。提供逻辑处理分析、数据存储和应用服务功能，实时接收接口层上传来的数据及告警信息，经过相应的逻辑处理分析后存储数据，并提供向上的应用服务供客户端使用，实现数据存储、记录告警事件，并以各种不同的方式输出告警。

3.展示层：由管理终端、显示终端及告警设备组成。为客户提供人机交互界面，可生成各种报表，实现日志功能及权限管理等功能。



管理系统由管理软件和若干部件组成，共同实现智能微模块各环节、各基础设施的数据采集与管理。一体化监控主机提供微模块内部设备的实时状态、告警信息和配置信息进行管理，提供可视化界面，方便用户运维微模块内部设备。

通过柔性拓展的物理架构和模块化设计的思路，管理系统既能对单个智能微模块基础设施进行管理，也能对多个分地域的智能微模块基础设施进行集中统一管理。

提供WiFi与RF_Z无线组网功能。支持手机移动APP连接至无线接入场景，部分南向部件（天窗执行器、交流执行器、多功能传感器、门禁执行器）同时支持RF_Z无线组网。

管理系统具有良好的可视化界面，根据实际需求可提供全面的管理功能。主要可以监控以下范围的设备：

动力设备：精密空调、精密配电柜、不间断电源（UPS）等。

环境设备：多功能传感器（烟雾、温湿度传感器）、水浸传感器等。

视频设备：摄像机、网络硬盘录像机。

门禁设备：集成标准的门禁管理系统，实现对门状态、刷卡、权限等关键信息的管理和监控。

标准的网管接口：综合管理系统可以向第三方网管系统提供SNMP形式的接口，以满足与第三方系统的信息交互。系统提供多协议扩展机制，满足不同设备的接入。

网络保障

响应国家创新体系整体战略要求，本建设项目原则上从IT底层的基础软硬件到上层的应用软件全产业链的安全、可控，从技术体系引进、强化产业基础、加强保障能力等方面着手，促进国产化产业在本地落地生根。本项目建设的应用系统具备兼容国产化数据库、操作系统、服务器等软硬件环境，满足业务性能需求。

根据实际国产化产业生态整体推进的进展，最新国产化要求的内容，在计算机终端类、服务器、专用产品、通用产品外设、办公软件、操作系统等产品领域都提出相关明确要求。

本项目结合国家国产化产业生态发展的情况以及省市的政策要求和现状，项目建设所涉及到的服务器、网关等均采用国产化产品进行建设，充分考虑未来3~5年国产化情况，做到业务系统可持续稳定运行。

服务器及硬盘扩容改造方案

数据中台服务器扩容方案

依据交管大数据应用特点，以国标、行标作为基准，基于陕西省公安厅交通管理总队数据现状，目前已初步建立交警总队数据标准，按照标准实现数据汇聚、数据处理、数据治理、数据组织、数据服务，通过“标、汇、治、享、用”五个维度提升数据管理能力，支撑上层业务应用、数据挖掘和情报研判，全面服务于群众顺畅出行和交通事故预防，并通过数据研判支撑全省公安交管“减量控大”工作开展，为全省人民提供安全、顺畅的通行环境，为全省公安交通警察提供大数据研判及支撑能力，提升警务效能。本次扩容数据中台建设内容主要包括

数据中台硬件资源扩容采购内容。

数据中台硬件资源

本次项目数据中台业务系统部署在陕西省公安厅交通管理总队公安网内，因业务需要和数据量接入分析对比规模的不断提升，按照业务资源规划项目扩容新增3台通用服务器和3台GPU服务器。具体配置如下配置清单：

服务器配置清单

序号	设备名称	技术参数	数量
1	通用服务器	1、处理器：2颗国产CPU，每颗CPU核数≥32核，每颗CPU主频≥2.6 GHz； 2、内存：≥256GB DDR4； 3、硬盘：≥2*600G SAS，≥2*960G SSD； 4、阵列控制器：≥1个标配SAS RAID阵列卡，支持RAID0/1/5/6/50/60；配置≥2GB缓存，支持缓存数据保护； 5、网卡：≥2*GE，4*10GE； 6、电源：≥2个热插拔冗余电源； 7、服务：三年原厂质保服务，硬盘免回收。	3
2	GPU服务器	1、处理器：2颗国产CPU，每颗CPU核数≥32核，每颗CPU主频≥2.6 GHz； 2、内存：≥768GB DDR4； 3、系统盘：≥2*480G SSD； 4、数据盘：≥6*960G SSD； 5、GPU卡：≥4张国产GPU卡，单卡算力≥140TFLOPS@FP16，单卡显存≥96G； 6、阵列控制器：≥1个标配SAS RAID阵列卡，支持RAID0/1/5/6/50/60；配置≥2GB缓存，支持缓存数据保护； 7、网卡：≥2*GE，4*10GE； 8、电源：≥2个热插拔冗余电源； 9、服务：三年原厂质保服务，硬盘免回收。 10、符合公安交通管理综合应用平台现网大数据平台兼容性要求	3

大数据集群扩容改造方案

扩容设计规划

本次需对大数据集群中Hbase分布式存储系统进行扩容，数据存储节点总需求裸容量为1865TB。扩容方案包括2个部分，首先将现网33个Hbase节点中19块4T盘改造替换为12块8TB存储盘，并将现网14台X86节点改造为国产化节点（按照12块8TB硬盘改造），在按照业务数据规划需求，补充增加扩容Hbase节点，保障业务3-5年的数据安全可靠和系统稳定。

Hbase 扩容节点数量=
$$\frac{1865TB}{12 \times 8TB} - 33 = \text{（向上取整）}$$

Hbase扩容节点数量=

$$\text{存储硬盘改造数量（4TB改造为8TB）} = 19 \text{ 节点} \times 12 \text{ 盘位} = 228 \text{ 盘}$$

硬盘改造新增裸容量为：

$$33(\text{节点数}) \times 12(\text{盘位}) \times (8\text{TB}(\text{硬盘裸容量}) - 4\text{TB}(\text{硬盘裸容量})) = 1584\text{TB}$$

分布式存储扩容节点数为：

$$\frac{1865\text{TB} - 1584\text{TB}}{12(\text{盘位}) \times 8\text{TB}(\text{硬盘裸容量})} \approx 3 \text{ 节点 (向上取整)}$$

同时需要对大数据集群进行软件扩容，当前平台总计3104 VCPU授权，14台现网服务器完成国产化改造后，本次存储扩容改造需要增加4台Hbase节点服务器。

服务器配置清单

序号	设备名称	技术参数	数量
1	改造HBase节点服务器	1、2U 国产品牌机架式服务器； 2、CPU：配置2颗国产ARM架构CPU，单颗CPU 物理核心数≥32核心，主频≥2.6Ghz（基准频率，非超频）； 3、内存：≥配置≥16*32GB 2933MHz DDR4 内存； 4、硬盘：≥配置≥2*480GB SSD、≥12*8TB SATA硬盘； 5、网卡：≥2*GE，4*10GE； 6、Raid卡：≥1个标配SAS RAID阵列卡，支持RAID0/1/5/6/50/60；配置≥2GB缓存，支持缓存数据保护； 7、电源：配置2 块（1+1 冗余）电源，单电源功率≥900W； 8、兼容项及服务要求：符合华为MRS大数据平台兼容性要求（提供华为官网兼容性列表截图证明），提供实际生产厂商3年硬件现场7×24小时服务，硬盘三年免回收； 投标时供应商须出具设备原生产厂商盖章的售后服务承诺函。	14
2	扩容HBase节点服务器	1、2U 国产品牌机架式服务器； 2、CPU：配置2颗国产ARM架构CPU，单颗CPU 物理核心数≥32核心，主频≥2.6Ghz（基准频率，非超频）； 3、内存：≥配置≥16*32GB 2933MHz DDR4 内存； 4、硬盘：≥配置≥2*480GB SSD、≥12*8TB SATA硬盘； 5、网卡：≥2*GE，4*10GE； 6、Raid卡：≥1个标配SAS RAID阵列卡，支持RAID0/1/5/6/50/60；配置≥2GB缓存，支持缓存数据保护； 7、电源：配置2 块（1+1 冗余）电源，单电源功率≥900W； 8、兼容项及服务要求：符合华为MRS大数据平台兼容性要求（提供华为官网兼容性列表截图证明），提供实际生产厂商3年硬件现场7×24小时服务，硬盘三年免回收； 投标时供应商须出具设备原生产厂商盖章的售后服务承诺函。	4
3	改造HBase节点硬盘	1、现网共计19个数据节点，每节点替换12块盘，单盘容量8TB容量，采用SATA盘类型 2、兼容项及服务要求：与现网大数据节点可兼容，提供实际生产厂商3年硬件现场7×24小时服务，硬盘三年免回收；	228

软件SNS续保方案

本次项目建设需要对MRS和DWS软件进行续保，续保时间延续到2028年12月31日，确保在截止期到期间对MRS和DWS进行现网变更和升级扩容操作。同时享受厂家提供的原厂技术支持和软件补丁版本支持服务。

在MRS和DWS软件维保时间延续到2028年12月31日，将享受厂家提供的如下服务：

- （1）提供400电话支持，接到服务请求后，在服务等级规定的响应时间内电话支持现网问题分析、诊断以及定位，提供问题解决方式；
- （2）提供产品知识服务，如原厂网站知识库、产品资料和自助服务工具等资源；
- （3）提供定期巡检服务：在定期巡检中基于MRS巡检工具和日常巡检辅助问题定位，诊断组件存在问题并分析和修复，并提供组件补丁升级服务。

现网存储设备OceanStor 18500F V5、OceanStor 18500 V5 SNS服务到期，本次项目扩容需原厂技术支持保障，需提供以下技术服务保障。

- （1）提供OceanStor 18500F V5、OceanStor 18500 V5 SNS服务；
- （2）OceanStor 18500F V5软件SNS服务截止日期不低于2025年12月31日；
- （3）OceanStor 18500 V5软件SNS服务截止日期不低于2026年12月31日；

SNS服务内容：

序号	服务内容	服务内容描述
1	远程问题处理	24×7覆盖，P1问题：30分钟内响应；P2问题：60分钟内响应；P3问题：2小时内响应；P4问题：NBD响应。
2	版本更新和升级	软件版本更新和升级许可
3	在线自助服务	网站知识库、产品资料和自助服务工具等服务资源共享

软件订阅服务内容：

- 1.提供数据链路看护，及问题辅助定位能力。解决MRS/DWS集群使用过程中的问题。包括问题检查，问题修复。并提供局点组件补丁升级服务。
- 2.日常巡检：基于MRS/DWS/ OceanStor18500的工具提供的巡检能力，对组件相关的问题进行问题分析和修复。
- 3.深入分析MRS/DWS/ OceanStor18500系统运行状态，提供状态评估报告。深度巡检的目的是与ISV深入沟通，了解对平台的述求，帮助其做数据流优化、数据分层等工作。

SNS服务内容

远程问题处理

工程师在接到软件故障申报后，将首先进行远程故障分析与处理，及时排除故障。远程问题处理包括电话支持和远程接入。

1.电话支持

接到服务请求后，将在服务等级规定的响应时间内通过电话支持进行响应，帮助您对问题进行分析、诊断及定位，提供解决问题的方案，并引导您实施。

2.远程接入

对于通过电话支持服务不能解决的故障或问题，在征得您的同意后，通过远程终端登陆到故障产品中调查和收集数据，分析故障原因，提出解决方案，指导您实施，必要时可以提供远程操作。

远程问题处理服务中双方的职责分工：

编号	活动
1	提供问题处理服务申请的途径。
2	在规定的SLA内响应服务请求。
3	将问题单升级到相应的专家支持团队（必要时）。
4	提供问题定位所需的序列号或条码以及产品使用地、故障现象描述以及其他分析问题所需的相关信息，如告警、日志，性能测量，操作记录等。
5	提供远程通道以及临时接入帐号及密码，并授权进行远程接入。
6	确认获得客户授权接入产品并通过远程连接方式处理问题（必要时）。
7	远程进行问题定位和处理。
8	提供临时解决方案，将系统恢复至故障前的状态（必要时）。
9	实施问题解决方案并验证其有效性。
10	确认解决方案的效果并反馈问题的状态。

版本更新和升级

提供软件版本更新和升级下载许可，主要包含软件补丁、软件更新、软件维护版本、软件新特性和软件升级版本，以确保您所购买的软件始终处于最优性能，满足更多应用场景和更高业务需求，持续为您带来收益。

在线自助服务

提供产品和技术资料，如产品手册、配置指南、组网案例、维护经验汇总等，通过开通网站相应权限，使以访问公司网站并下载相关资料，及时掌握最新的维护经验和技巧、获得最新的产品知识；有权登录网站自助服务工具，便捷快速的获取维护相关服务支持。

SnS服务标准

服务内容	服务响应时间	描述	备注
远程问题处理	24×7，P1问题：30分钟内响应；P2问题：60分钟内响应；P3问题：2小时内响应；P4问题：NBD响应。	24×7：周一至周日，00:00～24:00（全天候,节假日无休）	远程问题处理服务响应时间定义：自技术支持中心响应工程师受理客户故障之时算起，直到技术服务工程师首次联系用户开始远程技术支持服务为止。
软件更新和升级	24×7	网站，24×7：周一至周日，00:00～24:00（全天候）	无
在线自助服务	24×7	网站，24×7：周一至周日，00:00～24:00（全天候）	无

系统系统和数据迁移方案

核心应用系统接口对接服务

公安交通管理综合应用平台由公安部交通管理科学研究所研发，分部署改造后上层应用平台接口对接改造

服务，依据《公安交通管理综合应用平台建设指导意见》和《信息系统软硬件运行环境适配情况公示》清单，适配迁移改造分布式大数据节点后的接口对接，数据连通适配服务。完成改造后需要对公安交通管理分布式数据管理服务平台接口对接服务，提供远程基础服务(5*8h)和现场服务，大数据集群扩容改造后，提供分布式数据管理服务平台节点上的目录空间、时间同步、网络拓扑及配置、组件部署等对接服务支持以及性能优化，其中远程基础服务包括运行环境优化支持服务、咨询与处理服务、应急与处置服务、在线软件升级保障服务、分布式数据库表优化服务、数据补录服务、部局业务系统升级支持；现场服务提供不少于2次现场支撑服务（一次5天内），随时响应处理现场分布式数据管理服务平台相关业务问题紧急现场服务

迁移工作量评估

核心应用系统接口对接主要涉及公安交通管理综合应用平台对接以及分布式数据管理服务平台对接，并针对大数据集群改造后的系统联接性能优化。项目具体迁移工作量评估如下：

序号	名称	迁移难度说明	工作量（人月）	备注
1	核心系统接口对接服务	1、公安交通管理综合应用平台分部署改造后上层应用平台接口对接改造服务，依据《公安交通管理综合应用平台建设指导意见》和《信息系统软硬件运行环境适配情况公示》清单，适配迁移改造分布式大数据节点后的接口对接，数据连通适配服务。 2、公安交通管理分布式数据管理服务平台接口对接服务，提供远程基础服务(5*8h)和现场服务，大数据集群扩容改造后，提供分布式数据管理服务平台节点上的目录空间、时间同步、网络拓扑及配置、组件部署等对接服务支持以及性能优化，其中远程基础服务包括运行环境优化支持服务、咨询与处理服务、应急与处置服务、在线软件升级保障服务、分布式数据库表优化服务、数据补录服务、部局业务系统升级支持；现场服务提供不少于2次现场支撑服务（一次5天内），随时响应处理现场分布式数据管理服务平台相关业务问题紧急现场服务	7	

迁移难度等级评估

公安交通管理综合应用平台、分布式数据管理服务平台在与大数据集群节点扩容改造和国产化适配的接口对接服务中，具体迁移工作量中涉及到的所有软、硬件升级必须满足公安部交管局科技研究所（无锡所）接入要求，相关工作要求参考《公安交通综合应用平台实施方案》，根据《陕西省省级政务信息化项目投资编制指南（建设类）（试行）(20230827印发)》标准，参考标准迁移难度等级及工作量如表1，制定本项目集指平台数据和应用迁移难度等级及工作量评估表2，具体如下所示：

表1 迁移难度等级及工作量参考

项目	1级	2级	3级	4级	5级
业务规模（套）	1-5	6-20	21-40	41-120	≥121

系统数据总量（T）	≤1	1<总量≤10	10<总量≤30	30<总量≤100	100<总量
系统关联接口数（个）	≤20	21-50	51-100	101-200	≥121
业务允许中断时长（h）	≤48	≤12	≤8	≤1	≈0
特殊设备	不含	不含	包含	包含	包含
灾备等级	1级，2级	3级	4级	5级	6级
系统改造工作量（人月）	≤1	1<工作量≤3	3<工作量≤8	8<工作量≤17	>17
数据库迁移	数据库平迁	数据库平迁	数据库平迁	数据库升级	数据库改造
工作量（人月/系统）	≤3.3	≤6.6	≤13	≤26	依实际情况

表2 迁移难度及工作量评估表

业务规模（套）	系统数据总量（T）	系统关联接口数（个）	业务允许中断时长（h）	系统改造工作量（人月）
33	100<总量	51-100	≤8	8<工作量≤17
3级	5级	3级	3级	4级

综上，依据公安部交通管理科学研究所与公安部交管局现行标准规范，结合现网公安交通综合应用平台业务情况，整体迁移难度等级评估及工作量合理性分析评估为4级，8<（人月/系统）≤17，依据项目前期分布式改造扩容经验，最低可按照10人月进行规划设计，根据公式迁移费=Σ(工作量×人月费率)，以及系统迁移人月费率参考表B-1软件开发标准人月费率（参考陕西省行业基准数据基准人月费率18000元）；因此本项目迁移迁移费=Σ(工作量10×人月费率18000)，总计180000元，确保满足项目实际需求。

公安交通管理综合应用平台数据迁移

迁移工作量评估

依据《公安交通管理综合应用平台建设指导意见》综合应用平台工作数据库存储设备要进行双活冗余配置，由于现网容量不足，硬件版本停服等影响，需对现网存储进行国产化改造扩容并完成数据迁移工作。为保障整体业务连续性和可靠性，数据迁移严格按照调研评估（信息收集、应用关联分析、风险分析、迁移评估）、规划设计（迁移策略制定、目标架构规划、迁移方案设计、方案预验证）、迁移实施（环境准备、迁移演练、迁移割接）、维护保障（运行监测保障、运行性能评估、持续优化验证）4大步骤14项工作进行实施服务内容共计14人月，其中8人月为针对现网14台消息队列节点（HBase）组件进行国产化硬件数据搬迁，6人月为OceanStor 18500F V5 存储扩容和数据迁移方案。项目具体迁移工作量评估如下：

序号	名称	子项	迁移难度说明	工作量（人月）	备注
（一）	数据迁移费				

				迁移前信息收集和现网调研	现场现网组网梳理，收集设备信息，包含现网存储版本和端口信息、业务主机操作系统型号及版本、业务服务器端口固件版本、数据库版本及使用方式、多路径版本及配置信息。	1	
				迁移方案制定与风险评估	按照收集的信息和现网调研情况，制定迁移方式，识别迁移风险，模拟测试迁移环境，保障迁移方案可执行	1	
			1	HBase 数据节点 迁移 正式数据迁移	<p>新扩容存储空间合理规划，按照31.5TB可用做业务规划，迁移组网构建，完成现网存储的异构接管，现网存储和新扩容存储建立连接，并把待迁移的LUN同时映射给新扩容存储，把现网存储eDevLUN数据迁移到新扩容存储内部LUN，现网存储和新扩容存储断开连接，现网存储退网。</p> <p>规划目标存储配置。按照实际业务需求来规划硬盘域大小、硬盘类型、存储池大小、RAID策略、热备级别等；</p> <p>2、规划光纤网络配置。数据迁移要求源存储和目标存储主机业务和异构链路使用不同的前端端口，在光纤交换机侧异构链路单独规划zone，避免数据迁移链路和主机业务链路共用，迁移过程中影响到主机的性能；</p> <p>3、规划数据迁移路径，接管现网存储 OceanStor 18500 V5 网关，将现网存储LUN映射给新扩容存储节点中；</p> <p>4、新扩容存储节点创建eDevLUN，并添加到 LUN 组；</p> <p>5、新扩容存储节点创建主机，并添加到主机组中。</p> <p>6、新扩容存储节点创建映射视图，将eDevLUN 映射给公安交通管理综合应用平台业务服务器。</p> <p>7、公安交通管理综合应用平台业务服务器磁盘 IO 路径切换。</p> <p>8、迁移现网存储数据到扩容存储，创建 LUN 迁移，新扩容存储接管现网存储。</p> <p>9、现网存储上解除到主机服务器的LUN映射，退出服务。</p> <p>10、检查 Oracle RAC 状态，在新扩容存储节点上重新恢复构建双活机制。</p>	5	
				迁移后的调优	迁移完成后，业务观察，根据业务类型及使用方式，对主机访问存储进行优化，确保最大化利用存储能力。	1	

2	现网存储 数据迁移 服务	迁移前信息收集和现网调研	现场现网组网梳理，收集设备信息，包含现网存储版本和端口信息、业务主机操作系统型号及版本、业务服务器端口固件版本、数据库版本及使用方式、多路径版本及配置信息。	1	
		迁移方案制定与风险评估	按照收集的信息和现网调研情况，制定迁移方式，识别迁移风险，模拟测试迁移环境，保障迁移方案可执行	1	
		正式数据迁移	<p>1、针对现网14台消息队列节点（HBase）组件进行国产化硬件数据搬迁，依据《公安交通管理综合应用平台建设指导意见》和《信息系统软硬件运行环境适配情况公示》清单，将现网3台Kafka节点的数据全部迁移至替代的3台国产化管理节点中，并保障整体业务连续性和可靠性，数据迁移必须按照调研评估、规划设计、迁移实施、维护保障4大步骤逐步迁移方式进行实施服务，对公安交通管理综合应用平台分布式大数据现网集群迁移前必须进行信息收集、应用关联分析、风险分析、迁移评估、迁移策略制定、目标架构规划、迁移方案设计、方案预验证、环境准备、迁移演练、迁移割接、运行监测保障、运行性能评估、持续优化验证等14项工作严格执行数据迁移，并节点迁移中必须严格按照逐台迁移方式进行。</p> <p>2、针对现网19台国产化Hbase数据节点服务器内的4TB SATA硬盘更换为8TB SATA硬盘过程中的数据迁移服务。</p>	3	
		迁移后的调优	迁移完成后，业务观察，根据业务类型及使用方式，确定大数据集群扩容后的数据均衡和性能以及可用容量的有效情况。	1	

迁移难度等级评估

本项目具体迁移工作量中涉及到的所有软、硬件升级必须满足公安部交管局科技研究所（无锡所）接入要求，相关接入要求参考《公安交通管理综合应用平台建设指导意见》，具体工作内容及迁移步骤如下表：

工作内容	序号	步骤	工作量设计方案说明
调研评估	1	信息收集	在实施数据迁移前，需要收集客户现有系统环境中的必要信息，用以支撑项目计划和迁移方案设计，使用工具或业务调研表，需要收集的信息包括且不限于：现场现网组网梳理，收集设备信息，包含源目端存储版本和端口信息、业务主机操作系统型号及版本、业务服务器端口固件版本、数据库版本及使用方式、多路径版本及配置信息。
	2	应用关联分析	根据调研表分析整个业务关联关系及业务中断造成影响,做业务终端风险评估以及具体措施分析
	3	风险分析	根据调研表分析整个迁移风险情况，作为规划设计中的依据

	4	迁移评估	根据业务调研以及分析结果。制定整体的业务迁移策略
规划设计	5	迁移策略制定	制定业务迁移整体计划，对收集的信息经过分析评估的基础上，输出满足迁移性能、容量、安全要求的，可指导实施的解决方案详细设计包括：总体方案设计及评审，分析迁移项目可行性，迁移方案设计，迁移回退、应急方案设计，迁移方案评审及发布，验证迁移方案并输出迁移实施计划。
	6	目标架构规划	根据交警公安交通管理综合应用平台（六合一）平台数据存储双活集群业务场景制定存储双活迁移方案
	7	迁移方案设计	针对整个存储双活迁移风险情况制定相应的应对措施及计划
	8	方案预验证	在后台数据中心部署业务迁移工具，对业务迁移工具进行测试，验证并完善迁移方案，开始正式业务切换宣传
迁移实施	9	环境准备	根据规划设计方案，在目标端完成系统、数据库、存储和网络环境安装配置。测试目标端环境，并测试源端和目标端网络连接通讯成功
	10	迁移演练	迁移前进行一次全面的数据备份，以保证数据的可用性和完整性，按照迁移规划及业务系统、数据库进行数据同步配置。按照迁移计划及方案对业务系统进行迁移切换演练测试
	11	迁移割接	按照迁移计划及方案对业务系统进行正式迁移切换，根据项目要求的系统切换时间和服务窗口，完成指定数据的迁移工作。包括用户角色租户迁移，参数同步，迁移前环境检查，迁移工具部署，历史数据迁移，停机增量数据迁移等
维护保障	12	监控&保障	为了保证迁移后系统的高效稳定运行。必要对迁移后的系统进行一段时间的监控。并对迁移后的系统进行评估优化。保证迁移后，业务持续平稳运行。
	13	性能评估	根据性能基线，评估迁移后存储双活系统运行性能情况，评判是否满足业务运行性能要求。在迁移验收之前进行应用适配及业务上线保障。现场保障存储双活集群稳定及问题处理，存储双活集群问题处理，业务参数优化等
	14	优化&验收	项目验收。如果存在性能问题，进行系统优化确保六合一业务正常使用，最终达到运行性能要求。存储双活集群数据迁移方案实施完成，客户确认业务数据的完整性、一致性。客户数据供业务正常使用。完成迁移实施后总结项目工作，资料移交，账号密码移交等。

根据《陕西省省级政务信息化项目投资编制指南（建设类）（试行）(20230827印发)》标准，参考标准迁移难度等级及工作量如表1，制定本项目集指平台数据和应用迁移难度等级及工作量评估表2，具体如下所示：

表1 迁移难度等级及工作量参考

项目	1级	2级	3级	4级	5级
业务规模（套）	1-5	6-20	21-40	41-120	≥121
系统数据总量（T）	≤1	1<总量≤10	10<总量≤30	30<总量≤100	100<总量

系统关联接口数 (个)	≤20	21-50	51-100	101-200	≥121
业务允许中断时 长 (h)	≤48	≤12	≤8	≤1	≈0
特殊设备	不含	不含	包含	包含	包含
灾备等级	1级, 2级	3级	4级	5级	6级
系统改造工作量 (人月)	≤1	1<工作量≤3	3<工作量≤8	8<工作量≤17	>17
数据库迁移	数据库平迁	数据库平迁	数据库平迁	数据库升级	数据库改造
工作量 (人月/系 统)	≤3.3	≤6.6	≤13	≤26	依实际情况

表2 集指平台迁移难度及工作量评估表

业务规模 (套)	系统数据总量 (T)	系统关联接口数 (个)	业务允许中断 时长 (h)	系统改造工作量 (人月)
4	当前六合一平 台数据50T	≤20	≤8	3<工作量≤8
1级	4级	1级	3级	3级

依据《公安交通管理综合应用平台建设指导意见》相关文件要求，结合现网公安交通管理综合应用平台业务情况，整体迁移难度等级评估分析具体如下：

业务规模:陕西省交警总队六合一平台存储双活系统，共计4套存储，其中2套18500V5做双活网关，一套18500V5存储下挂EMC存储，一套18500V5存储下挂18500Fv5存储。

系统数据总量: 当前共计数据50T。

系统关联接口数: 4套存储共计4个接口对接。

业务允许中断时长: 公安交通管理综合应用平台要求业务不中断，由于本次项目主要针对其业务核心数据库存储进行扩容改造切换，切换过程采用双轨并行，直至数据切换完成后再做整体切割，因此中断时长可确保≤8h，并尽可能保障业务不中断。

系统改造工作量: 4套存储双活数据集群需要整体进行迁移组网构建，完成现网存储的异构接管，现网存储和新扩容存储建立连接，并把待迁移的LUN同时映射给新扩容存储，把现网存储eDevLUN数据迁移到新扩容存储内部LUN，现网存储和新扩容存储断开连接，现网存储退网。

综上本项目集成指挥平台的数据和应用迁移难度等级及工作量参考3级标准设计，根据公式迁移费=Σ(工作量×人月费率)，以及系统迁移人月费率参考表B-1软件开发标准人月费率（参考陕西省行业基准数据基准人月费率18000元）；因此本项目迁移迁移费=Σ(工作量13×人月费率18000)，总计234000元，整体迁移费用设计充分考虑业务连续性和合理性，确保满足项目实际业务情况需要进行规划。

数据迁移实施

规划数据迁移路径

接管现网存储 OceanStor 18500 V5 网关，将现网存储LUN映射给新扩容存储节点中。

建立数据映射关系

在新扩容存储节点创建eDevLUN，并添加到 LUN 组；在新扩容存储节点创建主机，并添加到主机组中。

新扩容存储节点创建映射视图，将eDevLUN 映射给公安交通管理综合应用平台业务服务器。

多路径切换

公安交通管理综合应用平台业务服务器磁盘 IO 路径切换，迁移现网存储数据到扩容存储，创建 LUN 迁移，新扩容存储接管现网存储。现网存储上解除到主机服务器的LUN映射，退出服务。

检查Oracle RAC

检查 Oracle RAC 状态，在新扩容存储节点上重新恢复构建双活机制。

六、建设内容清单

表 6 1硬件设备清单

序号	设备名称	部署位置	设备类型	数量	单位
1	通用服务器	公安网	硬件设备	3	台
2	GPU服务器	公安网	硬件设备	3	台
3	改造HBase节点服务器（核心产品）	公安网	硬件设备	14	台
4	扩容HBase节点服务器	公安网	硬件设备	4	台
5	改造HBase节点硬盘	公安网	硬件设备	228	块
6	堡垒机	公安网	硬件设备	2	台
7	工作站	公安网	硬件设备	5	台

表 6 2机房改造清单

序号	设备名称	部署位置	设备类型	数量
1	45台机柜冷通道封闭组件1套	总队3F机房	硬件设备	1
2	列间空调	总队3F机房	硬件设备	3
3	空调配电箱	总队3F机房	硬件设备	1
4	冷通道动环系统	总队3F机房	硬件设备	1
5	UPS主机	总队3F机房	硬件设备	2
6	电池组	总队3F机房	硬件设备	1
7	监控中心主机	总队3F机房	硬件设备	1
8	3楼视频会议室UPS供电改造	总队3F机房	机房装修	1
9	机房改造装修	总队3F机房	机房装修	1

表 6 3成品软件清单

序号	设备名称	部署位置	设备类型	数量	单位
1	综合应用平台MRS集群软件SNS	公安网	成品软件	1	套
2	综合应用平台DWS集群软件SNS	公安网	成品软件	1	套
3	国产操作系统	公安网	成品软件	24	套

表 6 4数据和应用迁移服务清单

序号	设备名称	设备类型	工作量（人月）
1	核心应用系统接口对接服务	应用迁移	7
2	HBase数据节点迁移	数据迁移	8

3	现网存储数据迁移服务	数据迁移	6
4	暴露面梳理服务	安全服务	2
5	漏洞扫描服务	安全服务	2
6	渗透测试服务	安全服务	1

七、培训要求

1.培训内容

本项目人员培训，是指对系统的使用人员、开发、系统管理人员进行培训。目的是使该项目的受训人员充分具备使业务人员能够熟练使用系统，进行数据的管理维护和业务分析，实现决策、道路交通监管、指挥调度指令发布等操作任务，了解与项目相关的系统软件和操作环境，以及对系统设计及其相关业务的认识，以便更好的开展工作。经过培训，保证贵方人员能够独立进行使用、管理、维护和日常处理，保证系统正常、安全的运行。

使平台操作人员掌握业务系统软件的具体操作方法和步骤，主要是信息的读取、对结果数据的审批等。

使后台管理人员和运维人员，熟悉设备的安装、调试和系统的试运行，掌握故障诊断与排除的技巧，掌握本系统的日常管理和维护方法。

培训的最终目的是使用户能熟练掌握系统的架构、使用技巧以及运维人员进行日常维护和系统扩展等，使系统能在交付使用后，能正常的使用和运维。保证业务数据的准确无误以及车管所业务正常进行，培养技术队伍后期项目建设的技术能力及系统运行维护支持能力。

2.培训的对象

用户单位本系统操作人员、技术人员、系统管理人员。

3.培训计划

本项目培训包括：厂家培训、维护培训、使用操作培训几部分，对平台操作人员、运维人员和管理人员等平台使用人员进行培训。具体内容如下：

培训计划表

序号	培训对象	培训内容	培训时间	培训方式
1	平台操作人员	使平台操作人员熟练相关应用系统的操作，能够处理日常业务。	每周2次（项目实施阶段）	现场指导
2	运维人员和管理人员	1、系统应用软件的日常使用、配置、维护和注意事项培训，使运维人员和后台管理人员（含各单位系统管理员）能够快速熟悉系统功能和性能，完成日常维护工作。 2.系统软、硬件环境、平台及应用软件的安装、调试培训，使管理员能熟练掌握系统安装、平台配置及常见故障处理。	每周3次（系统试运行阶段）	集中授课
3	根据实际需要组织安排 人数不限	针对本次项目建设的应用系统各功能模块进行详细培训以及在线演示、互动。	根据情况而定	网络培训

4.培训方式

系统的培训采用理论和实践相结合的方式。

理论培训主要以集中授课方式进行，上课形式采用座谈或授课的形式，从专业技术理论的角度对系统进行深入浅出的讲解，提高学员的知识水平。

实践操作培训主要以现场指导上机操作和网络培训为主，锻炼学员的动手能力，提升学员对系统的使用和维护能力。

5.培训师力量

配备强大的技术团队，团队内成员具备丰富的项目经验，在本项目培训工作中，安排3名主要负责人及涉及的主要产品厂家培训师2名，提供全方位专业的技术培训。

八、项目验收

1.初步验收

符合初步验收条件之后，项目承建单位向项目单位提交初步验收申请，启动初步验收工作，形成初步验收意见。在系统进行验收前，首先要确保合同要求的全部软件已完成并整个系统通过了试运行，并且，在试运行期发现的问题已全部解决，整个系统运行稳定，性能满足合同要求。系统验收测试方案的编制工作已完成并通过有关方面的评审。系统所有文档资料已经齐套，用户主要培训工作基本完成，通过具有资质的第三方专业机构的软件和符合二级等保要求的信息安全等级保护测评，认为可以进入到系统验收流程。系统验收的依据是：工程承建合同、系统需求说明书、系统总体设计说明书、国家有关行业规范和标准。

（一）初验条件：

- 1、硬件集成类部分，设备安装调试完成、子系统调试(含子系统联调)，均已完成检查合格；
- 2、软件类部分功能完整实现，满足建设的应用要求；
- 3、承建单位进行了自检自查，出具自检合格报告；
- 4、项目单位与承建单位共同进行了联合检查，确认功能实现，系统满足试用条件；
- 5、初验阶段的验收资料（包括图纸资料、技术文件及记录）齐全完整，签章齐备；
- 6、各方同意组织验收。

（二）项目承建单位应提交的资料：

对于软件系统，项目承建单位在提交软件系统验收申请表时，应提供被验收软件系统的合格性测试报告，以及项目建设单位下达的子任务书等文件规定的文档清单和软件系统产品清单等。

（三）被验收软件系统及相关文档的提交

项目承建单位在接到软件系统验收申请的批准通知后，应及时向建设单位提交验收依据所规定的软件系统及相关文档。

2.竣工验收

符合竣工验收条件之后，项目单位向省政务大数据局提交竣工验收申请，启动竣工验收工作，形成竣工验收意见。

（一）基本要求

验收审查计划应包括审查目的、审查范围、审查对象、审查内容、审查准则、审查方法、人员分工、进度安排等。

（二）验收测试和验收审查步骤

- 1、制定验收测试计划和验收审查计划，作好验收测试和验收审查准备；
- 2、进行验收测试和验收审查，建立完整的验收测试记录和验收审查记录；
- 3、编写验收测试报告和验收审查报告。

（三）验收审查内容

应依据验收依据确定验收审查内容。验收审查主要检查项目验收文档的齐全性、完整性和一致性，以及项目建设单位下达的子任务书及相关标准符合性等情况。

（四）性能要求

满足本设计文档的性能需求相关要求。

项目验收不能通过的情况

当存在以下任何情形之一时，项目验收应当不予通过：

- （1）验收文档、资料、数据不真实。
- （2）未完成项目批复的建设内容或未达到批复的建设要求。
- （3）设计或施工不符合合同要求，或未达到国家及省市相关标准要求。
- （4）严重偏离项目目标或擅自修改项目主要建设内容。
- （5）项目实施或试运行过程中出现重大问题，未能解决和做出说明，或存在纠纷尚未解决的。

竣工验收文档清单

序号	材料类别	材料名称
1	申请文档	1.项目单位竣工验收申请函； 2.项目建设总结； 3.数据资源共享报告（包括数据资源目录、共享平台接入、数据共享情况等）； 4.软硬件产品的国产自主可控情况报告等。
2	申报阶段文档	1.项目申报函； 2.项目技术方案（建设类项目可行性研究报告、初步设计和投资概算或实施方案；运维类、服务类项目实施方案）； 3.本部门（单位）研究拟建项目的党委（党组）或办公会议纪要； 4.评审意见。
3	批复阶段文档	1.立项批复材料； 2.重大项目变更批复和三方变更意见。

4	采购阶段 文档	1.采购招标文件； 2.投标（响应）文件（包括各合同包，如软件包、硬件包、第三方软件测试等）； 3.成交通知书（中标通知书）； 4.项目合同（含补充协议）。
5	实施阶段 文档	1.项目实施计划、方案等； 2.变更材料：包含三方变更意见、工程例会纪要、项目单位会议纪要等； 3.到货点验材料：包含到货设备验收单、开箱验收记录、设备产品质量证明文件、第三方软件授权证明、计算机软件著作权登记证书等； 4.设计文档：包含需求说明书、概要设计说明书、详细设计说明书、数据库设计说明书、接口文档、测试报告、系统部署手册、用户使用手册等； 5.移交清单：包含采购的软硬件移交、定制开发的软件系统源代码移交等； 6.实施过程材料：包含工程例会纪要、重大事项记录等； 7.培训材料：包含培训方案、培训手册、培训教材、培训签到表等； 8.项目监理文档：包含开（停、复、返）工令、监理周（月）报等； 9.其他需要的材料。
6	初步验收 文档	适用于建设类（工程类）项目 1.用户使用报告； 2.承建单位实施总结报告； 3.监理单位监理总结报告（仅限实施监理的项目）； 4.项目初步验收意见及验收现场查验记录表； 5.初步验收问题整改报告。
7	试运行与 测试文档	1.试运行方案； 2.试运行记录（附试运行期间业务数据截图）； 3.系统试运行报告； 4.遗留问题处理报告等； 5.第三方软件测评报告（包括代码、功能和性能测评报告）；
8	最终验收 文档	1.用户使用报告； 2.承建单位实施总结报告； 3.监理单位监理总结报告（仅限实施监理的项目）； 4.项目最终验收意见及验收现场查验记录表； 5.最终验收问题整改报告。
9	档案专项 验收文档	1.档案专项验收情况。
10	项目财务 文档	1.财务报告，包含财务基本数据、预算执行情况、财务管理、财务指标分析等； 2.第三方审计报告。

注：根据项目类型，准备竣工验收文档。

九、技术参数

表1硬件设备购置

序号	设备名称	技术参数	数量	说明
(一)	服务器购置			
1	通用服务器	1、处理器：2颗国产CPU，每颗CPU核数≥32核，每颗CPU主频≥2.6GHz； 2、内存：≥256GB DDR4； 3、硬盘：≥2*600G SAS，≥2*960G SSD； 4、阵列控制器：≥1个标配SAS RAID阵列卡，支持RAID0/1/5/6/50/60； 配置≥2GB缓存，支持缓存数据保护； 5、网卡：≥2*GE，4*10GE； 6、电源：≥2个热插拔冗余电源； 7、服务：三年原厂质保服务，硬盘免回收。	3	
2	GPU服务器	1、处理器：2颗国产CPU，每颗CPU核数≥32核，每颗CPU主频≥2.6GHz； 2、内存：≥768GB DDR4； 3、系统盘：≥2*480G SSD； 4、数据盘：≥6*960G SSD； 5、GPU卡：≥4张国产GPU卡，单卡算力≥140TFLOPS@FP16，单卡显存≥96G； 6、阵列控制器：≥1个标配SAS RAID阵列卡，支持RAID0/1/5/6/50/60； 配置≥2GB缓存，支持缓存数据保护； 7、网卡：≥2*GE，4*10GE； 8、电源：≥2个热插拔冗余电源； 9、服务：三年原厂质保服务，硬盘免回收。	3	
3	改造HBase节点服务器（核心产品）	1、处理器：2颗国产CPU，每颗CPU核数≥32核，每颗CPU主频≥2.6GHz； 2、内存：≥配置≥16*32GB，DDR4-2933MHz； 3、硬盘：≥配置≥2*480GB SSD硬盘、配置≥12*8TB SATA硬盘； 4、Raid卡：≥1个标配SAS RAID阵列卡，支持RAID0/1/5/6/50/60；配置≥2GB缓存，支持缓存数据保护； 5、网卡：≥2*GE，4*10GE； 6、电源：≥2个热插拔冗余电源； 7、服务：三年原厂质保服务，硬盘免回收。 8、兼容项及服务要求：符合现网MRS大数据平台兼容性要求，提供实际生产厂商3年硬件现场7×24小时服务，硬盘三年免回收； 投标时供应商须出具设备原生产厂商盖章的售后服务承诺函。	14	

4	扩容HBase节点服务器	1、处理器：2颗国产CPU，每颗CPU核数≥32核，每颗CPU主频≥2.6GHz； 2、内存：≥配置≥16*32GB，DDR4-2933MHz； 3、硬盘：≥配置≥2*480GB SSD硬盘、配置≥12*8TB SATA硬盘； 4、Raid卡：≥1个标配SAS RAID阵列卡，支持RAID0/1/5/6/50/60；配置≥2GB缓存，支持缓存数据保护； 5、网卡：≥2*GE，4*10GE； 6、电源：≥2个热插拔冗余电源； 7、服务：三年原厂质保服务，硬盘免回收。 8、兼容项及服务要求：符合现网MRS大数据平台兼容性要求，提供实际生产厂商3年硬件现场7×24小时服务，硬盘三年免回收； 投标时供应商须出具设备原生产厂商盖章的售后服务承诺函。	4	
5	改造HBase节点硬盘	1、现网共计19个HBase数据节点，每节点替换12块盘，单盘容量8TB容量，采用SATA盘类型 2、兼容项及服务要求：与现网大数据节点可兼容，硬盘三年免回收； 3、含硬盘实施服务	228	
(二)	其他硬件设备购置			
6	堡垒机	1、硬件参数：双电源，128G SSD ,8T硬盘，8*千兆电口,4*千兆光口，2个接口扩展插槽，2* USB，硬件国密加密卡，符合国密要求。 2、性能参数：最大字符并发数4500，最大图形并发数2500。 3、软件授权：配置授权管理500台设备和3个 SDP 远程接入授权，配合国密算法功能模块，符合国密要求。 4、维保：硬件产品从激活起前三年服务包，包含：①产品系统升级授权；②远程支持服务；③产品保修服务；④硬件故障上门支持。	2	
7	工作站	处理器：CPU主频3.5GHz；内存：16GB；配置1TB硬盘 显存：6GB 配置一机双屏显示器 屏幕大小：≥27英寸 分辨率≥2560*1440	5	
8	机房整改	见后表2机房购置	1	

表2机房购置

序号	名称	数量	单位	备注
一、冷通道改造				
1	双开自动滑动门	1	套	1组冷通道配置前后2个门，采用2.0mm厚优质冷轧钢板制作；框架式大面积通透防火玻璃结构；带自动闭门装置；门与机架缝隙有密闭措施每个门均配置1个自动滑动门（含闭门器），颜色：黑色，通道宽度1200mm
2	翻转玻璃天窗（600）	24	个	1200mm宽，每2个相对的柜子用一单元，与机柜对应的上方翻转式天窗，高于机柜顶部300mm安装；采用1.5mm冷轧钢板+防火玻璃制作
3	固定功能天窗（600）	2	个	1200mm宽，每2个相对的柜子用一单元，与机柜、空调对应的上方固定式天窗，高于机柜顶部300mm安装；采用1.5mm冷轧钢板+防火玻璃制作。注意：为了强度，冷通道的最前面和最后面配置的为固定天窗

4	非标玻璃固定订天窗	1	个	1200mm宽，每2个相对的柜子用一单元，与机柜、空调对应的上方固定式天窗，高于机柜顶部300mm安装；采用1.5mm冷扎钢板+防火玻璃制作。用于放置机柜外空挡处
5	翻转天窗控制器	1	个	含控制器，开关电源，继电器，用于給翻转天窗门极供电用；
6	顶部围板（600）	52	套	注意：一套天窗用一套
7	侧面封板4件（1200）	4	套	600宽机柜使用，用于安装在机柜顶部，保持冷通道美观统一（含列头柜、立柱间隔位置）
8	非标封堵	1	套	机柜侧板，1200mm深度机柜使用
9	机柜	2	个	600*1200标准机柜
10	氛围灯	26	套	填补通道
二、列间空调				
1	精密空调	3	台	40KW制冷量
2	铜管	350	米	国标
3	外机电源线	280	米	
4	内机电源线	160	米	RVV5*10mm²
5	市电电缆	160	米	YJV4*75+1*35
6	配电箱	1	套	
7	给排水连接	3	套	
8	制冷剂	15	罐	R410A
9	外机支架	3	套	
10	延长组件、冷冻油	3	套	
三、冷通道动环系统				
A	列头柜监测（监测5台列头柜）			
1	精密配电柜监控软件	1	项	
B	精密空调监测（监测3台精密空调）			
1	智能空调监控软件	7	项	
C	非定位漏水检测（接点式）			
1	水浸传感器	3	个	
2	不定位感应绳	3	根	
3	开关量采集模块	1	个	
4	漏水监测接口软件	1	项	
D	温湿度监测（安装于冷通道内）			

1	温湿度传感器	8	个	
2	温湿度监测接口软件	1	项	
E	消防烟雾报警监测			
1	探测器（烟感）	6	个	
2	开关量采集模块	1	个	
3	消防报警监测接口软件	1	项	
F	冷通道天窗控制/LED灯带联动控制			
1	控制模块	2	个	
2	控制监测接口软件	1	项	
G	门禁系统			
1	门禁一体机	2	个	
2	电源	2	个	
3	指纹门禁系统软件	1	项	
H	视频系统			
1	半球摄像机	2	个	
2	8口POE交换机	1	个	
3	联网视频监控软件	1	项	
I	辅材			
1	电源	1	个	
2	信号采集箱	1	个	
3	线缆、管材及辅材	1	批	
J	监控中心			
1	工控机	1	台	
2	21.5寸触摸屏	1	台	
3	串口服务器	1	台	
4	语音卡	1	个	
5	数据中心综合管理组态软件V1.0	1	套	
6	安之源电话语音报警系统	1	项	
7	声光报警器	1	个	

K	原有动环系统兼容调试	1	项	
四、UPS				
1	UPS	2	台	
2	蓄电池	240	节	
3	电池架	6	台	
4	电池汇流盒	1	台	
5	电池开关盒	6	台	
6	电池连铜排	240	条	
7	电池组至UPS电源线	24	米	
五、设备承重加固、机房局部装修及其他				
1	承重加固及机房局部装修	1	项	
2	精密空调风道制作安装	1	项	
3	部分机柜电线电缆	1	项	
4	部分机柜通讯线缆改造	1	项	
六、3楼视频会议室UPS供电改造				
1	配电柜U电改造	3	处	三楼会议室端三处配电柜/箱供电改造
2	UPS输入输出配电箱	1	台	定制
3	UPS输出电缆	150	米	ZR-YJV5*16mm2
4	UPS输出电缆	150	米	ZR-YJV5*10mm2
5	UPS输出电缆	150	米	ZR-RVV3*6mm2
6	辅材	1	批	监测线、端子、空开、电缆、插座、桥架、阻燃管等，根据现场环境灵活配置

表3成品软件购置

序号	系统名称	技术参数	数量	说明
(一)	基础软件购置			

1	综合应用平台 MRS集群软件 SNS	(1) 提供现网MRS软件3104VCPU已永久授权软件的SNS服务； (2) 软件SNS服务截止日期不低于2028年12月31日； (3) 提供400电话支持，接到服务请求后，在服务等级规定的响应时间内电话支持现网问题分析、诊断以及定位，提供问题解决方式； (4) 提供产品知识服务，如原厂网站知识库、产品资料和自助服务工具等资源； (5) 提供定期巡检服务：在定期巡检中基于MRS巡检工具和日常巡检辅助问题定位，诊断组件存在问题并分析和修复，并提供组件补丁升级服务。	1	
2	综合应用平台 DWS集群软件 SNS	(1) 提供现网DWS软件192VCPU已永久授权软件的SNS服务； (2) 软件SNS服务截止日期不低于2028年12月31日； (3) 提供400电话支持，接到服务请求后，在服务等级规定的响应时间内电话支持现网问题分析、诊断以及定位，提供问题解决方式； (4) 提供产品知识服务，如原厂网站知识库、产品资料和自助服务工具等资源； (5) 提供定期巡检服务：在定期巡检中基于DWS巡检工具和日常巡检辅助问题定位，诊断组件存在问题并分析和修复，并提供组件补丁升级服务。	1	
3	国产操作系统	1、操作系统应当符合安全可靠测评要求，在中国信息安全测评中心《安全可靠测评结果公告》名单中； 2、满足《操作系统政府采购需求标准（2023年版）》（财库[2023]34号）中“*”指标，如政府采购需求标准更新，以合同签订的最新政府采购需求标准为主； 通过中国信息安全测评中心和国家保密科技测评中心联合认证的安全测评； 3、基于国内自主可控的开源社区内核，支持国产CPU类型，包括但不限于C86、ARM等架构； 4、支持国家自主研发的数据加密算法SM2、SM3、SM4等。提供对操作系统的安全加固工具，支持在OS首次启动时进行自动化加固； 5、兼容国内主流厂商服务器整机（超聚变、浪潮、宝德、华启等）； 6、软件兼容常用数据库（达梦、高斯等）、中间件（东方通、宝兰德等）软件；	24	

表4数据和应用迁移

序号	名称	迁移难度说明	工作量 (人月)	备注
(一)	数据和应用迁移			

1	核心应用系统接口对接服务	<p>1、公安交通管理综合应用平台分部署改造后上层应用平台接口对接改造服务，依据《公安交通管理综合应用平台建设指导意见》和《信息系统软硬件运行环境适配情况公示》清单，适配迁移改造分布式大数据节点后的接口对接，数据连通适配服务。</p> <p>2、公安交通管理分布式数据管理服务平台接口对接服务，提供远程基础服务(5*8h)和现场服务，大数据集群扩容改造后，提供分布式数据管理服务平台节点上的目录空间、时间同步、网络拓扑及配置、组件部署等对接服务支持以及性能优化，其中远程基础服务包括运行环境优化支持服务、咨询与处理服务、应急与处置服务、在线软件升级保障服务、分布式数据库表优化服务、数据补录服务、部局业务系统升级支持；现场服务提供不少于2次现场支撑服务（一次5天内），随时响应处理现场分布式数据管理服务平台相关业务问题紧急现场服务</p>	7	
	HBase数据节点迁移	<p>1、针对现网14台消息队列节点（HBase）组件进行国产化硬件数据搬迁，依据《公安交通管理综合应用平台建设指导意见》和《信息系统软硬件运行环境适配情况公示》清单，将现网3台Kafka节点的数据全部迁移至替代的3台国产化管理节点中，并保障整体业务连续性和可靠性，数据迁移必须按照调研评估、规划设计、迁移实施、维护保障4大步骤逐步迁移方式进行实施服务，对公安交通管理综合应用平台分布式大数据现网集群迁移前必须进行信息收集、应用关联分析、风险分析、迁移评估、迁移策略制定、目标架构规划、迁移方案设计、方案预验证、环境准备、迁移演练、迁移割接、运行监测保障、运行性能评估、持续优化验证等14项工作严格执行数据迁移，并节点迁移中必须严格按照逐台迁移方式进行。</p> <p>2、针对现网19台国产化Hbase数据节点服务器内的4TB SATA硬盘更换为8TB SATA硬盘过程中的数据迁移服务。</p>	8	
	现网存储数据迁移服务	<p>依据《公安交通管理综合应用平台建设指导意见》综合应用平台工作数据库存储设备要进行双活冗余配置，由于现网容量不足，硬件版本停服等影响，需对现网存储进行国产化改造扩容并完成数据迁移工作。为保障整体业务连续性和可靠性，数据迁移严格按照调研评估（信息收集、应用关联分析、风险分析、迁移评估）、规划设计（迁移策略制定、目标架构规划、迁移方案设计、方案预验证）、迁移实施（环境准备、迁移演练、迁移割接）、维护保障（运行监测保障、运行性能评估、持续优化验证）4大步骤14项工作进行实施服务。</p> <p>（1）迁移前信息收集和现网调研：现场现网组网梳理，收集设备信息，包含现网存储版本和端口信息、业务主机操作系统型号及版本、业务服务器端口固件版本、数据库版本及使用方式、多路径版本及配置信息。</p> <p>（2）迁移方案制定与风险评估：按照收集的信息和现网调研情况，制定迁移方式，识别迁移风险，模拟测试迁移环境，保障迁移方案可执行。</p> <p>（3）正式迁移：新扩容存储空间合理规划，按照50TB可用做双活规划，迁移组网构建，完成现网存储的异构接管，现网存储和新扩容存储建立连接，并把待迁移的LUN同时映射给新扩容存储，把现网存储eDevLUN数据迁移到新扩容存储内部LUN，现网存储和新扩容存储断开连接，现网存储退网。</p>	6	
	（二）数据安全服务			

1	暴露面梳理服务	<p>根据《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》等法律法规及标准对互联网侧的各类资产开展全面的暴露面梳理。内容包括但不限于：</p> <p>1、发现暴露在互联网中的资产，建立资产信息库，缩小暴露面，包括但不限于域名IP、端口、服务等互联网资产信息；其中域名资产要素包括，域名名称、标题（应用名称）、注册机构、备案机构、证书信息；IP资产要素，包括IP地址、端口、服务、组件、组件信息、证书信息等；</p> <p>2、对存在的移动端资产进行普查，主要涉及公众号、小程序、APP等相关内容，发现移动端资产信息；</p> <p>3、梳理与用户存在关联的违规资产、影子资产详情，包括但不限于web页面、h5页面、微信公众号、小程序等关联页面；</p> <p>4、对发现的资产进行安全扫描和人工分析，发现存在的典型安全问题，对单位外部安全状态进行评估；</p> <p>5、每次服务结束后出具《互联网暴露面排查服务报告》《互联网资产清单及敏感信息排查清单》，提供整改方案并配合实施。</p> <p>重要要求：1、服务周期内提供一套SaaS化资产暴露面测绘平台配合用户日常运维使用，提供工具证明材料；</p>	2	
2	漏洞扫描服务	<p>对互联网侧所有在用软硬件信息资产和业务系统，包括服务器、网络设备及办公终端、操作系统、数据库、中间件、Web应用、应用软件等的安全漏洞、脆弱性进行全面扫描检测。内容包括但不限于：</p> <p>1、通过扫描等手段对指定的远程或者本地计算机系统的安全脆弱性进行检测，发现可利用漏洞，查找应用系统、主机服务器存在的安全漏洞；</p> <p>2、通过智能遍历规则库和多种扫描选项组合的手段，深入准确的检测出系统和网站中存在的漏洞和弱点；</p> <p>3、根据扫描结果，提供漏洞扫描用例来辅助验证漏洞的准确性；</p> <p>4、安全服务工程师对扫描出的漏洞进行人工验证后，同时提供整改方法和建议，帮助用户修补漏洞，全面提升整体安全性（内容包括：具体的漏洞细节描述；安全修复建议等）；</p> <p>5、每次服务结束后出具《XXX系统漏洞扫描报告》。</p>	2	

			<p>对互联网侧信息系统进行深度渗透测试，全面验证被测试信息系统的安全漏洞问题及安全防护能力。内容包括但不限于：</p> <p>1、针对进行渗透测试的每一个信息系统，严格遵循相关政策规范，明确区分各项服务内容的关联和边界，合理的资源投入，确保服务内容质量，保证服务的具体内容和工作方法应贴合本行实际需求和具体要求，并符合相关规定；</p> <p>2、要求对所有开放的端口，应用，中间件漏洞等进行测试，对所有目标系统的身份认证方式以及认证的安全性进行渗透检查，测试内容包括但不限于：身份鉴别，自主访问控制，强制访问控制，可信路径，越权访问，会话验证绕过，弱口令等；</p> <p>3、要求测试内容包括但不限于基本信息测试、身份认证测试、客户端安全测试、动账管理测试、日志审计测试、查询功能测试、参数管理测试、平台及应用组件测试、上传下载测试等方面；</p> <p>4、要求采用书面文字、关键截图、以及视频录相多种方式做记录，直观的、更真实的反映渗透测试全过程，并根据渗透测试的过程文档撰写《XX信息系统安全渗透测试报告》，详细描述渗透测试的过程和结果，并对发现的问题提出解决方案；</p> <p>6、要求根据渗透测试的结果，以及漏洞情况，提供漏洞问题的加固整改协助，提供漏洞整改后的复测验证，针对严重缺陷漏洞的整改，指派专人在现场办公，确保漏洞问题被正确合理的修复；</p> <p>7、服务结束后输出《XX信息系统安全渗透测试报告》。</p>	1	
--	--	--	--	---	--

采购包2：

标的名称：公安交管信息系统软硬件更新升级项目密码改造部分

序号	参数性质	技术参数与性能指标																																																
		<div>一、项目概况</div> <div>公安交管信息系统软硬件更新升级项目密码改造部分。</div> <div>★1、安全认证网关；2、签名验签服务器；3、时间戳服务器；4、数据库加密网关；5、国密智能密码钥匙；6、国密门禁系统；7、国密浏览器 等所有密码类产品符合信创要求，并具有商用密码检测认证中心颁发的《商用密码产品认证证书》。</div> <div>二、建设内容</div> <div>1.硬件设备</div> <div>建设内容表</div> <table><tr><th>序号</th><th>设备名称</th><th>部署位置</th><th>设备类型</th><th>数量</th><th>单位</th></tr><tr><td>1</td><td>安全认证网关（核心产品）</td><td>公安网、互联网</td><td>硬件设备</td><td>2</td><td>台</td></tr><tr><td>2</td><td>签名验签服务器</td><td>公安网、互联网</td><td>硬件设备</td><td>2</td><td>台</td></tr><tr><td>3</td><td>时间戳服务器</td><td>公安网、互联网</td><td>硬件设备</td><td>2</td><td>台</td></tr><tr><td>4</td><td>数据库加密网关</td><td>公安网、互联网</td><td>硬件设备</td><td>2</td><td>台</td></tr><tr><td>5</td><td>国密智能密码钥匙</td><td>公安网、互联网</td><td>硬件设备</td><td>20</td><td>个</td></tr><tr><td>6</td><td>国密门禁系统</td><td>公安网、互联网</td><td>硬件设备</td><td>2</td><td>套</td></tr></table> <div>2.成品软件</div> <div>建设内容表</div> <table><tr><th>序号</th><th>设备名称</th><th>部署位置</th><th>设备类型</th><th>数量</th><th>单位</th></tr></table>	序号	设备名称	部署位置	设备类型	数量	单位	1	安全认证网关（核心产品）	公安网、互联网	硬件设备	2	台	2	签名验签服务器	公安网、互联网	硬件设备	2	台	3	时间戳服务器	公安网、互联网	硬件设备	2	台	4	数据库加密网关	公安网、互联网	硬件设备	2	台	5	国密智能密码钥匙	公安网、互联网	硬件设备	20	个	6	国密门禁系统	公安网、互联网	硬件设备	2	套	序号	设备名称	部署位置	设备类型	数量	单位
序号	设备名称	部署位置	设备类型	数量	单位																																													
1	安全认证网关（核心产品）	公安网、互联网	硬件设备	2	台																																													
2	签名验签服务器	公安网、互联网	硬件设备	2	台																																													
3	时间戳服务器	公安网、互联网	硬件设备	2	台																																													
4	数据库加密网关	公安网、互联网	硬件设备	2	台																																													
5	国密智能密码钥匙	公安网、互联网	硬件设备	20	个																																													
6	国密门禁系统	公安网、互联网	硬件设备	2	套																																													
序号	设备名称	部署位置	设备类型	数量	单位																																													

1	国密浏览器	公安网、互联网	成品软件	20	套
---	-------	---------	------	----	---

三、现状分析

1.密码应用安全现状分析

总队3楼科技数据中心

在安全物理环境方面，机房严格按照B类机房标准进行建设实施，所在场地具有防震、防风和防雨能力。建设在所在建筑的三楼，未建设在顶楼或地下室，机房出入口已安装门禁系统，通过指纹+刷卡方式进行人员校验，出入记录保存180天以上。机房主要设备通过螺丝固定在机柜中，并配置了不易去除的机打标识。机房当前设置了13台视频系统，可无死角监视机房运行情况，并接入了动环系统，如监控设备故障或发生入侵事件时可进行报警。机房上方当前设置了多个烟感传感和温度传感，并配置了柜式七氟丙烷气体灭火装置，在检测到火情时自动报警并自动灭火，也可手动启动喷洒按钮。机房当前配备了艾默生精密空调对机房进行温湿度调节，能够防止水蒸气结露。机房当前已铺设防静电地板，并通过地线对设备机柜产生的静电安全接地。机房当前配备了4组具有稳压保护功能的UPS装置，预计可提供4小时电力供应，在供电线路上为机房提供稳压保护。

在安全通信网络方面，系统接入交换机CPU使用率15%，内存占用率56%；互联网核心交换机CPU使用率3%，内存占用率40%；互联网出口防火墙CPU使用率16%，内存占用率40%，能够满足业务高峰期需要。平台网络区域划分为出口链路安全防护区和数据库区，并对不同的网络区域划分了地址。被测系统重要区域为数据库区，未部署在网络边界，在系统与互联网边界处部署了互联网出口防火墙，已根据业务需求配置访问控制策略，在出口链路安全防护区和数据库区之间通过核心交换机ACL进行访问控制。主要设备在远程管理时均采用密码技术保证通信过程中数据的完整性和保密性。

在安全区域边界方面，在系统与互联网边界处部署了互联网出口防火墙，已根据业务需求配置访问控制策略，确保跨越访问和数据流均通过边界设备提供的受控接口进行通信。当前仅科技管理处3台终端可访问内部网络。已在互联网出口防火墙中限制系统内未授权终端的外联功能，在出口路由中添加黑白名单，并在办公区域严禁插入外部U盘或访问外部网络。互联网出口防火墙可记录源安全域、源地址、目的安全域、目的地址、用户、服务、应用、防护状态、命中数；在出口链路安全防护区和数据库区之间通过交换机ACL进行访问控制。对进出网络的信息内容进行过滤，可以实现对应用层协议命令级的控制。其中集成了入侵防御和防病毒模块，能够有效防止从外部发起的网络攻击行为。对安全攻击和病毒进行防护和记录，能够记录攻击源IP、攻击类型、攻击目标、攻击时间等信息，并提供报警。安全审计功能已开启，对攻击检测行为进行记录，审计覆盖到每个用户。互联网出口防火墙设备审计记录由系统管理员定期下载保存至管理终端并出具保存记录，保存时间可追溯至6个月以上。

在安全计算环境方面，网络设备对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，具有登录处理功能及超时退出等措施，远程管理时，通过SSH协议进行登录管理，能够防止信息在网络传输过程中被窃听。设置特权用户、查看用户两个级别，不同级别管理人员分别使用不同的用户进行管理，无默认账户，无多余、过期、共享用户的存在，网络设备均开启了安全审计功能；审计访问覆盖到每个系统用户；能够对重要用户行为和事件进行审计。当前仅指定的运维终端可访问管理，并定期对设备进行漏洞扫描。设备采用AES256加密方式存储鉴别数据，能够保证在存储过程中的完整性和保密性。设备配置数据已在管理终端保存，配置数据发生变更将重新备份。

安全设备对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，具有登录处理功能及超时退出等措施，远程管理时，通过HTTPS协议进行管理，能够防止信息在网络传输过程中被窃听。设置不同级别管理人员分别使用不同的用户进行管理，无多余、过期、共享用户的存在，设备均开启了安全审计功能；审计访问覆盖到每个系统用户；能够对重要用户行为和事件进行审计。当前仅指定的运维终端可访问管理，并定期对设备进行漏洞扫描。设备采用HTTPS协议进行登录，使用SSL协议安全密码

套层，能够保证重要鉴别数据在传输过程中的完整性和保密性。设备配置数据已在管理终端保存，配置数据发生变更将重新备份。

操作系统通过用户名+口令的方式进行身份鉴别，且身份标识具有唯一性，不存在空口令账户，管理口令由大、小字母、数字、特殊字符组成，长度超过8位，42天定期更换口令。连续登录失败5次锁定30分钟，超时默认5分钟自动退出操作界面，在对服务器进行远程时，鉴别数据传输过程中开启了远程（RDP）连接要求使用指定的安全层，策略启用为协商，可以防止鉴别信息在网络传输过程中被窃听。不同的用户具有不同的权限。设置的有系统管理员、安全管理员、审计管理员、普通用户，可以实现管理用户的权限分离。操作系统均开启审核功能，可以对每个用户以及重要的用户行为和安全事件进行审核。审计记录为本地保存，并配置定期备份策略，设置日志保存时间大于六个月；设备日志除系统管理员外均无法进行修改，遵循最小安装的原则，仅安装需要的组件和应用程序；仅能通过交警总队内网登录。每月定期通过安全监管平台的漏洞扫描模块进行漏洞扫描，部署的有瑞星杀毒软件、互联网安全服务助手，特征库均为最新，能够及时发现恶意代码，并将其阻断。通过HASH加密存储鉴别信息，保证鉴别信息在存储过程中的完整性和保密性。操作系统为分布式部署，可以实现系统的高可用性。可以保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除，存有敏感数据的存储空间被释放或重新分配前得到完全清除。

数据库对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换，具有登录失败处理功能及超时退出功能，远程数据库使用PL/SQL工具进行安全连接，需要输入账号密码，可以防止鉴别信息在网络传输过程中被窃听。对登录的用户分配账户和权限，无多余、共享、过期账户。设置审计管理员以及安全管理员、审计管理员来实现管理用户的权限分离以及三权分离。对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问，启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计，审计记录定期备份，审计进程能够受到保护，定期进行漏洞扫描，重要业务数据和身份鉴别数据都使用数据库进行透明加密，加密算法为基于PBKDF2的SHA512哈希算法，保证数据在存储过程中的完整性和保密性。数据库为Oracle-RAC集群技术，可以保证系统的高可用性，可以保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除，可以保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

应用系统使用网页通过用户名+口令方式进行登录，用户的身份标识具有唯一性，由大小写字母、数字、特殊符号组成，口令定期90天进行更换，应用系统已开启口令复杂度检测，具体设置为口令必须包含数字、大小写字母、特殊符号，长度不得小于8位。具有登录失败处理功能及超时退出功能，对登录的用户分配账户和权限，离职用户人力资源部门会进行相关账户禁用。设置的有系统管理员、安全管理员、审计管理员，普通用户，可以实现管理用户的权限分离。管理员账户进行相关资源配置，包括新建用户、配置资源等。系统启用安全审计功能，审计范围覆盖到每个用户。可以对重要的用户行为及重要安全事件进行记录，审计记录仅系统管理员可以查看，审计进程受到保护，系统具有数据有效性检验功能，系统已通过数据有效性检测功能，仅允许特定的格式输入以及对恶意代码进行拦截等；应用系统经过使用安恒漏洞检查工具漏洞扫描后，未发现高危漏洞。应用系统在管理员退出登录后，不保存用户名和口令，清除session和鉴别信息所在的存储空间。

重要业务数据每周全量备份至存储系统，且经测试备份数据可恢复。定期上传至公安部交通管理局进行存储。在退出登录切换用户后，其余用户无法查看当前退出登录用户的敏感信息。仅采集和保存业务必需的用户个人信息。已禁止未授权访问和非法使用用户个人信息。

在安全管理中心方面，平台通过运维终端作为安全管理中心，通过用户名+口令的方式登录系统管理员账号，使用特定的命令或操作对系统进行操作管理，操作存在日志记录。可以对系统的资源和运行进行配置、控制和管理。通过用户名+口令的方式登录审计管理员可以查看所有用户的登录日志、系统操作日志。审计管理员登录后可以对日志记录通过系统报表功能对审计记录进行分析、查询等。网络中已划分出出口链路安全防护区对安全设备和组件进行管理，与数据库区通过交换机ACL策略进行地址划分。网络中的安全设备远程管理时均只开启了HTTPS协议，关闭了不安全的HTTP和TELNET管理协议。系统内安全设备报警功能已开启，数据库

审计对异常文件和数据库操作进行记录并告警；F5负载均衡能够在服务器带宽到达峰值时弹窗报警。

密码系统现状分析

目前，陕西省公安厅交通管理总队尚未依据相关国家、行业标准针对信息系统密码应用进行过相关建设，在网络和通信、设备和计算、应用和数据等层面，对于身份鉴别、通信数据完整性、远程管理通道安全、重要数据传输机密性等方面，个别环节如用户身份验证使用了密码技术，但所使用的密码技术不合规或机制不正确；另对于通信数据机密性、网络边界访问控制信息完整性、系统资源访问控制信息完整性、日志记录完整性、重要信息资源安全标记完整性、重要数据传输机密性、重要数据存储机密性和完整性、不可否认性等方面，都未使用符合标准和要求的密码技术，存在较大安全风险。

陕西省公安厅交通管理总队也未依据《信息安全技术 信息系统密码应用基本要求》中的安全管理要求，制定密码相关管理制度，尚未开展过密码应用安全性评估。

本次项目针对当前密码应用现状，将以统一的密码资源管理、统一的密码接口规范、统一的密码策略配置、统一的密码安全应用配置为原则进行密码应用规划建设，以满足密码应用需求并符合“密码应用安全性评估”安全合规要求。

四、需求分析

密码应用安全需求分析

技术方面

物理和环境安全

陕西省公安厅交通管理总队主楼三楼数据中心机房应按照GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》标准要求，需部署取得商用密码产品型号证书的门禁系统，使用国密算法实现门禁卡的“一卡一密”，并基于国密算法对人员身份进行鉴别，同时，复用现有的国密视频系统，通过门禁系统和视频系统完成人员出入记录的完整性保护。需采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理具体风险分析表如下：

表 41 风险分析表

序号	威胁类别	问题描述	风险分析
1	身份鉴别	机房未采用密码技术进行物理访问身份鉴别，无法保证重要区域进入人员身份的真实性。	存在非授权人员进入机房，对软硬件设备和数据进行直接破坏的风险，可能对系统的安全稳定运行造成影响。
2	电子门禁记录数据存储完整性	机房未采用密码技术保证电子门禁系统进出记录数据的存储完整性。	未使用密码技术的完整性功能来保证电子门禁系统进出记录的完整性，存在物理进出记录遭到非授权篡改和掩盖非授权人员进出情况的风险。
3	视频记录数据存储完整性	机房未采用密码技术保证视频监控音像记录数据的存储完整性。	机房的监控视频数据若遭受破坏或恶意篡改删除，导致无法对安全事件进行追溯。

根据以上风险分析，陕西省公安厅交通管理总队机房需部署符合 GM/T 0036-2014 标准要求的电子门禁系统对进出机房人员进行身份鉴别。复用现有的视频系统，对门禁进出记录和视频监控数据进行完整性保护。

网络和通信安全

陕西省公安厅交通管理总队信息系统在网络和通信层面主要涉及以下三类通信信道：

表 42通信信道表

序号	网络传输链路
1	各应用系统业务终端与系统的通信信道
2	运维终端与堡垒机的通信信道
3	总队各类应用系统与省公安厅的通信信道

以下分别对各类通道进行风险和密码应用需求进行分析。

本期项目通信网络主要依托陕西省公安厅交通管理总队内部网络，按照国家标准GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》应在通信前基于密码技术对通信双方进行身份认证，使用密码技术的机密性和真实性功能来实现防截获、防假冒和防重用，保证传输过程中鉴别信息的机密性和网络设备实体身份的真实性。

表 43网络和通信安全需求分析表

序号	威胁类别	问题描述	风险分析
1	身份鉴别	未对通信实体进行身份鉴别。未采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。	通信身份未进行有效的认证手段，存在身份假冒、重放攻击、数据包被截获、恶意设备接入等安全风险。
2	通信数据完整性	用户使用当前系统时,未建立安全的数据传输通道，不能保证通信数据的完整性。	存在通信数据被非授权截取、蓄意地删除、篡改、伪造、乱序、重放、插入等破坏和丢失以及无法对安全事件进行追溯的风险。
3	通信过程中重要数据的机密性	用户使用当前系统时，未对通信实体进行身份鉴别。未采用密码技术对通信实体进行身份鉴别，保证通信实体身份的机密性。	存在通信数据报文被窃听、截获的风险。
4	网络边界访问控制信息完整性	防火墙等网络边界设备未使用密码技术保护网络边界访问控制信息的完整性	存在边界访问控制列表等信息被截取、篡改、删除等安全风险。
5	安全接入认证	未采用密码技术对从外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。	存在外部未知设备和人员为经过合法认证，恶意接入内部网络的风险。

公安信息网业务终端与系统的通信信道：本单位内部相关工作人员（PC端）访问陕西省公安厅交通管理总队应用系统的通信通道，通过部署符合密码相关国家、行业标准要求的安全认证网关，在通信前实现对服务端的通信实体身份鉴别，保证通信数据的传输完整性和机密性，同时可对边界的访问控制信息进行完整性保护。

运维终端与堡垒机的通信信道：运维终端与堡垒机之间的通信信道，通过部署符合密码相关国家、行业标准要求的运维安全认证网关，在通信前实现对运维安全认证网关的通信实体身份鉴别，保证通信数据的传输完整性和机密性。

设备和计算安全

未使用密码技术对登录的运维人员及用户进行身份标识和鉴别，身份标识具有唯一性；在远程管理时，未

使用密码技术的机密性功能来实现鉴别信息的防窃听；未使用密码技术的完整性功能来保证系统资源访问控制信息的完整性；未使用密码技术的完整性功能来保证重要信息资源敏感标记的完整性；未采用可信计算技术建立从系统到应用的信任链，实现系统运行过程中重要程序或文件完整性保护；未使用密码技术的完整性功能来对日志记录进行完整性保护。

表 44 设备和计算安全需求分析表

序号	威胁类别	问题描述	风险分析
1	身份鉴别	未采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性。	登录设备的用户未进行有效的认证手段，存在身份假冒、重放攻击、数据包被截获、恶意设备接入等安全风险。
2	远程管理通道安全	远程管理设备时，未采用密码技术建立安全的信息传输通道	存在远程管理设备被未授权访问，影响系统正常运行。
3	系统资源访问控制信息完整性	未采用密码技术保证系统资源访问控制信息的完整性	存在系统资源访问控制信息被截取、篡改、删除等安全风险。
4	重要信息资源安全标记完整性	未采用密码技术保证设备中的重要信息资源安全标记的完整性。	采用安全操作系统，不存在安全标记，无需实现完整性保护。
5	日志记录完整性	运维人员通过堡垒机对网络设备、相关服务器进行统一管理，操作日志并未使用密码技术保护其完整性。	目前本系统应用服务器、数据库服务器等设备日志均明文存储，未使用密码技术进行完整性保护，存在设备日志记录被非授权篡改风险。
6	重要可执行程序完整性、重要可执行程序来源真实性	未采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证。	系统中使用的密码产品需要通过检测认证，具备相应的安全防护能力。

本项目新增安全认证网关已经过商密认证机构检测合格，登录设备的身份鉴别符合相关要求，为登录上述密码设备的用户配发智能密码钥匙，内置密钥，采用SM2数字证书+口令的双因子的方式进行身份认证；对登录堡垒机的用户采用缓解性措施：使用ukey+口令+SM2数字证书的方式对登录运维安全认证网关的用户进行身份鉴别，再通过用户名+静态口令的方式登录堡垒机；对于通用设备登录用户的身份鉴别，采用缓解性措施：使用ukey+口令+SM2数字证书的方式对登录运维安全认证网关的用户进行身份鉴别，再通过用户名+静态口令的方式登录堡垒机，且堡垒机只能通过该运维安全认证网关进行登录，最后再通过用户名+静态口令的方式登录通用设备。

远程管理运维安全认证网关时采用国密SSL协议，然后通过运维安全认证网关访问其他密码设备时，采用国密HTTPS协议。访问堡垒机和通用设备采用缓解措施：访问堡垒机时使用HTTPS协议（TLS 1.2），通过堡垒机对通用设备进行运维时采用SSH 2.0登录，并且通过合规的运维安全认证网关建立专用的集中管理通道降低风险。

本系统在设备和计算安全层面无重要信息资源安全标记，该测评单元不适用。

应用和数据安全

应用和数据安全保护对象需要保护的重要数据分为3类：

1.登录应用系统的用户名和口令；

2.系统数据中出现的个人信息：如住址、电话号、身份证等，这个是《个人信息保护法》要求的；

上述2类信息是刚性需求，和业主方无关，只要涉及，必须按照39786要求做加密、完整性等；

未使用密码技术对登录的用户进行身份标识和鉴别，实现身份鉴别信息的防截获、防假冒和防重用，保证应用系统用户身份的真实性；未使用密码技术的完整性功能来保证业务应用系统访问控制策略、数据库表访问控制信息和重要信息资源敏感标记等信息的完整性；

未采用密码技术保证重要数据在传输过程中的机密性，包括但不限于鉴别数据、重要业务数据和重要用户信息等；

未采用密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要用户信息等；应使用密码技术的完整性功能来实现对日志记录完整性的保护；

未采用密码技术对重要应用程序的加载和卸载进行安全控制，采用符合GM/T 0028的三级及以上密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密钥管理。

表 45应用和数据安全需求分析表

序号	威胁类别	问题描述	风险分析
1	身份鉴别	目前用户访问系统使用用户名+口令方式进行登录，未采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性。	登录系统的用户未进行有效的认证手段，存在身份假冒、重放攻击、数据包被截获、恶意设备接入等安全风险。
2	访问控制信息完整性	未采用密码技术保证信息系统应用的访问控制信息的完整性。	存在远程管理设备被未授权访问，影响系统正常运行。
3	重要信息资源安全标记完整性	未采用密码技术保证设备中的重要信息资源安全标记的完整性。	系统未采用强制访问控制机制，未对重要信息资源设置安全标记，无重要信息资源安全标记完整性保护需求。
4	重要数据传输机密性	未采用密码技术保证信息系统应用的重要数据在传输过程中的机密性。	存在重要数据在通信过程中被窃听、截获、伪造的风险。
5	重要数据存储机密性	未采用密码技术保证信息系统应用的重要数据在存储过程中的机密性。	重要数据明文存储，存在被窃取、替换、篡改、伪造的风险。
6	重要数据传输完整性	未采用密码技术保证信息系统应用的重要数据在传输过程中的完整性。	重要数据在通信过程中存在被非授权截取、蓄意地删除、篡改、嗅探、劫持的风险。

7	重要数据存储完整性	未采用密码技术保证信息系统应用的重要数据在存储过程中的完整性。	重要数据明文传输，存在被非授权截取、蓄意地删除、篡改、伪造、乱序、重放、插入的安全风险。
8	不可否认性	在可能涉及法律责任认定的应用中，未采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性。	关键数据操作和交换过程中存在接收和发送不一致和抵赖的安全风险。

对PC端业务人员、管理员配发智能密码钥匙，使用SM2数字证书+口令的方式登录系统，实现登录用户的身份鉴别。

部署符合密码相关国家、行业标准要求的签名验签服务器，对用户访问控制权限列表计算HMAC，实现访问控制信息的完整性保护，保护访问控制权限列表不被篡改，防止非授权的访问。

基于应用系统现状，在应用层实现重要数据的传输机密性、完整性难度较大，因此采用缓解措施：通过网络边界处部署的安全认证网关，实现基于GMTLS的安全接入，建立基于SSL协议的安全数据传输通道，实现数据传输机密性和完整性保护。

部署符合密码相关国家、行业标准要求的签名验签服务器，系统已补充调用数据加解密服务，采用SM4算法对重要数据进行加密运算，实现数据的加密存储。同时调用HMAC-SM3服务，实现重要数据存储的完整性保护。

1.用户身份鉴别

根据以上风险分析，陕西省公安厅交通管理总队应用系统需与统一数字证书系统进行对接，通过统一数字证书系统实现基于密码技术的用户身份鉴别。统一数字证书系统及配套数据库加密网关采用符合国家密码管理局要求的商用密码技术，产品获得商用密码产品认证证书。

2.访问控制信息完整性保障

根据以上风险分析，陕西省公安厅交通管理总队应用系统需通过与签名验签服务器进行对接，通过调用签名验签服务器完整性保护接口，采用符合国家密码管理局要求的商用密码技术对其访问控制信息进行完整性保护。

3.重要数据传输机密性保障

本项目涉及的专网区业务用户及管理用户在访问应用系统时，可能会涉及到资产、漏洞、网络安全事件、指挥公文等重要数据，目前该过程已经通过“网络和通信安全”层面采用基于SM4算法的安全认证网关加密隧道对重要数据传输通道进行了机密性保护，有效降低了重要数据传输过程遭窃取的风险。

4.重要数据存储机密性保障

根据以上风险分析，应用系统需实现与数据库加密网关对接，重要数据在进行存储时通过调用数据库加密网关数据加密接口，采用了符合国家密码管理局要求的SM4商密技术对重要数据进行了加密保护。

5.重要数据传输完整性保障

需通过“网络和通信安全”层面采用基于HMAC-SM3算法的安全认证网关加密隧道对重要数据传输通道进行了完整性保护，有效降低重要数据传输过程遭篡改的风险。

6.重要数据存储完整性保障

需与签名验签服务器对接，重要数据在进行存储时，通过调用签名验签服务器实现数据完整性保护。

关联系统需求分析

密码应用软硬件系统建设完成后，将对接密码及相关的各个业务子系统的密码改造及密码评测。

根据关联系统需求分许，我们知道密码系统建设需要关联整合多个子系统，根据对接的系统应用要求，接口可以采用中间库或者rest接口方式。具体的接口数据包含组织接口数据、人员接口数据、功能调用接口数据、其他接口数据。

具体对接的接口需求如下：

表46系统接口需求表

序号	系统 /小程序	对接内容	主要接口
1	安全认证网关服务	身份鉴别、重要数据传输完整性/机密性	业务系统登录模块
2	数据库加密网关	重要数据存储完整性、访问控制信息完整性	业务系统重要数据、数据库访问控制列表
3	签名验签服务	数据原发行为不可否认行、日志记录完整性	业务系统电子签章模块、业务系统及数据库日志记录
4	数据库加密网关	重要数据存储机密性	业务系统重要数据、数据库表
5	时间戳服务	重要业务时间抗抵赖、篡改	业务系统时间信息
6	协同签名服务	移动端身份鉴别、移动端重要数据传输完整性/机密性	业务系统移动端登录模块、移动客户端SDK包

根据对接的系统，以上密码软硬件基础资源提供接口，各个业务系统适配开发。

合规性方面

信息安全合规性要求是指密码系统运行所需的机房运行环境安全，以及主机、存储和网络等设备的安全。

1.机房运行环境安全，承载密码系统平台的物理机房应满足 GB 50174-2017 《数据中心设计规范》中的A类机房建设要求。

2.主机安全，密码系统平台的物理主机应满足GB/T 22239-2019《网络安全等级保护基本要求》主机安全三级（含）以上防护要求。

3.存储安全，密码系统平台的存储应满足GB/T 22239-2019《网络安全等级保护基本要求》三级（含）以上数据安全与备份恢复要求。

4.网络安全，密码系统平台的网络应满足GB/T 22239-2019《网络安全等级保护基本要求》网络安全三级（含）以上防护要求。

安全可控性方面

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等相关标准，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等四个方面提出了密码应用技术要求，具体如下表：

表47 GB/T 39786密码应用技术要求表

指标体系			第一级	第二级	第三级	第四级
	物理和环境安全	身份鉴别	可	宜	宜	应
		电子门禁记录数据存储完整性	可	可	宜	应
		视频监控记录数据存储完整性			宜	应

技术 要求		密码服务	应	应	应	应
		密码产品		一级及以上	二级及以上	三级及以上
	网络和通信 安全	身份鉴别	可	宜		
		通信数据完整性	可	可	宜	应
		通信过程中也要数据的机密性	可	宜	应	应
		网络边界访问控制信息的完整性	可	可	宜	应
		安全接入认证			可	宜
		密码服务	应	应	应	应
		密码产品		一级及以上	二级及以上	三级及以上
	设备和计算 安全	身份鉴别	可	宜	应	应
		远程管理通道安全			应	应
		系统资源访问控制信息完整性	可	可	宜	应
		信息资源安全标记完整性			宜	应
		日志记录完整性	可	可	宜	应
		重要可执行程序完整性、重要可执行程序来源真实性			宜	应
		密码服务	应	应	应	应
		密码产品		一级及以上	二级及以上	三级及以上
	应用和数据 安全	身份鉴别	可	宜	应	应
		访问控制信息完整性	可	可	宜	应
		重要信息资源安全标记完整性			宜	应
		重要数据传输机密性	可	宜	应	应
		重要数据存储机密性	可	宜	应	应
		重要数据传输完整性	可	宜	宜	应
		重要数据存储完整性	可	宜	宜	应
		不可否认性			宜	应
		密码服务	应	应	应	应
		密码产品		一级及以上	二级及以上	三级及以上

在密码管理要求方面从管理制度、人员管理、建设运行、应急处置等提出了密码应用管理要求，具体如下

表48 GB/T 39786密码应用管理要求表

指标体系	第一级	第二级	第三级	第四级
------	-----	-----	-----	-----

管理要求	管理制度	具备密码应用安全管理制度	应	应	应	应
		密钥管理规则	应	应	应	应
		建立操作规程		应	应	应
		定期修订安全管理制度			应	应
		明确管理制度发布流程			应	应
		制度执行过程记录留存			应	应
	人员管理	了解并遵守密码相关法律法规和 密码管理制度	应	应	应	应
		建立密码应用岗位责任制度		应	应	应
		建立上岗人员培训制度		应	应	应
		定期进行安全岗位人员考核			应	应
		建立关键岗位人员保密制度和调离制度	应	应	应	应
	建设运行	制定密码应用方案	应	应	应	应
		制定密钥安全管理策略	应	应	应	应
		制定实施方案	应	应	应	应
		投入运行前进行密码应用安全性评估	可	宜	应	应
		定期开展密码应用安全性评估及攻防对抗演习			应	应
	应急处置	应急策略	可	应	应	应
		事件处置			应	应
		向有关主管部门上报处置情况			应	应

管理方面

管理制度及人员管理

未制定密码应用安全管理制度；未制定密码应用方案建立相应的密钥管理制度；未对管理人员或操作人员执行的日常管理操作建立操作规程；未定期对密码应用安全管理制度和操作规程的合理性适用性进行论证和审定，对存在不足或需要改进之处进行修订；未明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；不具有密码应用操作规程的相关执行记录，安全管理制度不完善，管理流程不健全，执行不到位，职责不明确，存在密钥泄漏、数据泄漏等风险。

需制定密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度；需根据密码应用方案建立相应的密钥管理制度；需对管理人员或操作人员执行的日常管理操作建立操作规程；需定期对密码应用安全管理制度和操作规程的合理性适用性进行论证和审定，对存在不足或需要改进之处进行修订；需明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制；需具备密码应用操作规程的相关执行记录并妥善保存。

相关人员对密码相关法律法规、密码应用安全管理制度等不了解；未建立密码应用岗位责任制度，未明确各岗位在安全系统中的职责和权限；未建立上岗人员培训制度，对于涉及密码的操作和管理的人员未进行专门培训，未确保其具备岗位所需专业技能；未定期对密码应用安全岗位人员进行考核；未建立关键人员保密制度和调离制度、签订保密合同、承担保密义务。

本项目依据密码相关国家、行业标准，制定密码应用方案，规划建设密码保障系统，并依据《密码应用基本要求》中的安全管理要求，规划制定密码相关管理制度，在本系统中落实密码相关国家政策要求，发挥密码在信息系统安全中的基础支撑作用。

运行机制及应急处置

陕西省公安厅交通管理总队信息系统当前未根据密码相关标准和密码应用需求，制定密码应用方案；未根据密码应用方案，确定系统设计的密钥种类及生存周期环节；未按照密码应用方案实施建设；未在投入运行前进行并通过密码应用安全性评估；在运行过程中，未严格执行既定的密码应用安全管理制度，未定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。未制定密码应用应急预案，未做好应急资源准备。

在项目建设过程中需根据密码相关标准和密码应用需求，制定密码应用方案；需根据密码应用方案，确定系统设计的密钥种类及生存周期环节；需按照密码应用方案实施建设；需在投入运行前进行并通过密码应用安全性评估；在运行过程中，需严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及攻防对抗演习，并根据评估结果进行整改。

在项目建设过程中需制定密码应用应急预案，做好应急资源准备，当密码应用安全事件发生时，需立即启动应急处置措施，结合实际情况及时处置；事件发生后，需及时向信息系统主管部门进行报告；事件处置完成后，需及时向信息系统主管部门及归属的密码管理部门报告事件发生的情况及处置情况。

密钥管理

依据《密码应用基本要求》，陕西省公安厅交通管理总队应制定相关的密钥管理措施，包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程。

表 49 密码应用需求分析清单

通用要求		密码应用基本要求（第三级）		不适用说明
物理和环境安全	身份鉴别	宜	宜采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性；	无
	电子门禁记录数据存储完整性	宜	宜采用密码技术来保证电子门禁系统进出记录的存储完整性；	无
	视频监控记录数据存储完整性	宜	宜采用密码技术来保证视频监控音像记录的存储完整性；	有（复用）
	密码产品	二级及以上	以上采用的密码产品，应达到GB/T 37092二级及以上安全要求。	无
	身份鉴别	应	应采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性；	无
	通信数据完整性	宜	宜采用密码技术保证通信过程中数据的完整性；	无
	通信过程中重要数据的机密性	应	应采用密码技术保证通信过程中的重要数据的机密性；	无
	网络边界访问控制信息的完整性	宜	宜采用密码技术来保证网络边界访问控制信息的完整性；	无

网络和 通信安 全				
	安全接入认证	可	不适用：根据《密码应用基本要求》对等级保护第三级信息系统的密码应用技术要求，安全接入认证项应用要求为“可”，同时接入系统的设备无安全接入认证需求，本指标不纳入标准符合性判定范围。	不适用
	密码产品	二级及以上	以上采用的密码产品，应达到GB/T 37092二级及以上安全要求。	无
设备和 计算安 全	身份鉴别	应	应采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；	无
	远程管理通道安全	应	远程管理时，应采用密码技术建立安全的信息传输通道；	无
	系统资源访问控制信息完整性	宜	宜采用密码技术来保证系统资源访问控制信息的完整性；	无
	重要信息资源安全标记完整性	宜	不适用	本系统无重要信息资源敏感标记
	日志记录完整性	宜	宜采用密码技术来保证日志记录的完整性；	无
	重要可执行程序完整性、重要可执行程序来源真实性	宜	宜采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证；	无
	密码产品	二级及以上	以上采用的密码产品，应达到GB/T 37092二级及以上安全要求。	无
应用和 数据安	身份鉴别	应	应采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；	有（复用）
	访问控制信息完整性	宜	应采用密码技术来保证应用系统访问控制信息的完整性；	无
	重要信息资源安全标记完整性	宜	不适用	本系统无重要信息资源敏感标记
	重要数据传输机密性	应	应采用密码技术保证信息系统应用的重要数据传输的机密性；	无
	重要数据存储机密性	应	应采用密码技术保证信息系统应用的重要数据存储的机密性；	无

全	重要数据传输完整性	宜	宜采用密码技术保证信息系统应用的重要数据传输的完整性；	无
	重要数据存储完整性	宜	宜采用密码技术保证信息系统应用的重要数据存储的完整性；	无
	不可否认性	宜	不适用	系统中不涉及法律责任认定类应用场景
	密码产品	二级及以上	以上采用的密码产品，应达到GB/T 37092二级及以上安全要求。	无

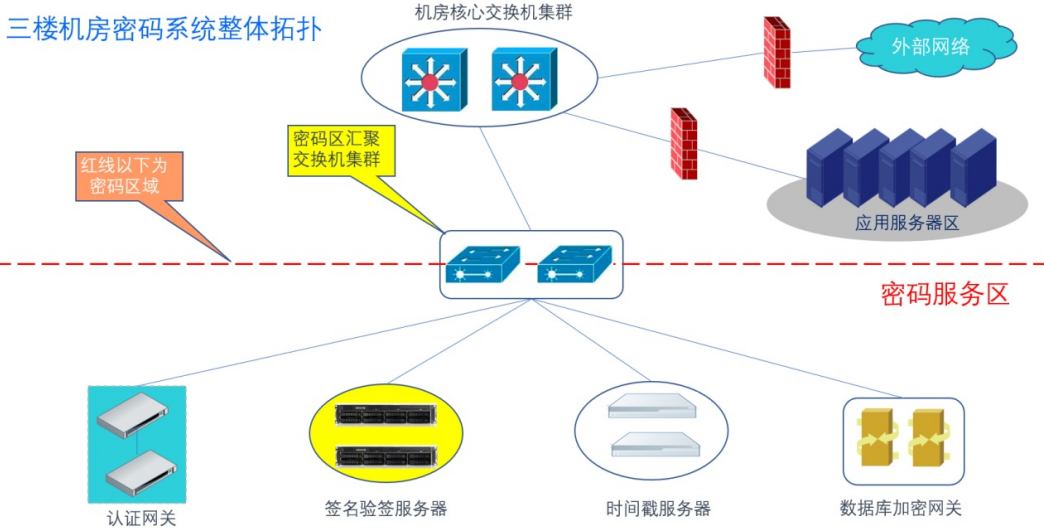
五、建设方案

密码应用安全建设方案

架构设计

总体架构

本项目密码系统建设总体架构如下：



注：指挥中心机房密码设备数量与部署方式和三楼机房相同

图5-1 总体架构图

按照密评整改建议及实际需求，本次需要的密码组件为：安全认证网关、签名验签服务器、时间戳服务器、数据库加密网关、服务器密码机、数据库加密网关、国密门禁系统、Ukey（含数字证书）、国密客户端；

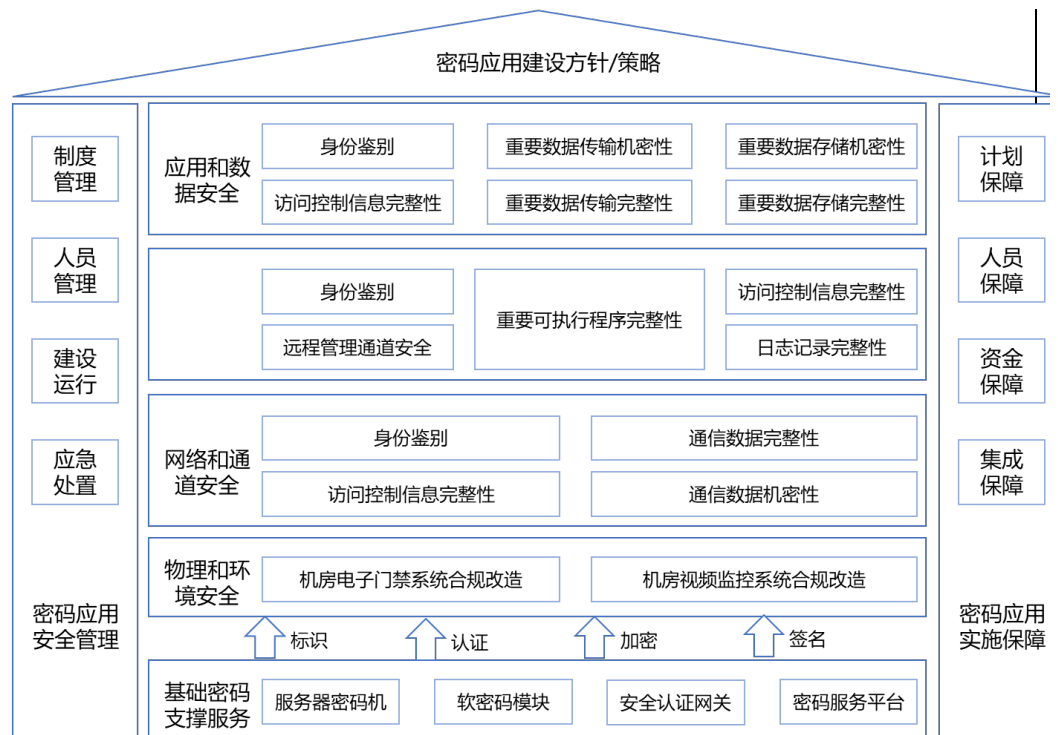
其中国密门禁系统为机房基础设施，独立部署，不涉及应用系统的对接；Ukey（含数字证书）、国密客户端为PC终端设备；

安全认证网关、签名验签服务器、时间戳服务器、数据库加密网关、服务器密码机都建议按照双机配置；

上图为本次密码产品部署的逻辑示意图，在本次的网络中设置一块密码服务子区，把本次新建的密码设备都放置在该区域中，按需进行路由配置。

技术架构

依据《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021），对陕西省公安厅交通管理总队进行商用密码应用安全性设计，满足系统对密码的适应性建设需求。密码应用建设框架设计如下：



本密码应用方案应用场景、保护对象如下：

- 1.应用系统用户登录安全。通过移动业务端APP、PC业务端登录业务系统用户的安全身份鉴别，防止非授权人员登录。
- 2.运维人员管理系统安全。通过终端软件密码模块和接入认证网关之间建立SSL VPN 加密通道，实现身份鉴别和机密性保护。
- 3.服务器接口安全。通过数据库加密网关提供签名验签API接口，对访问控制信息进行签名，确保数据的完整性和保密性。
- 4.应用系统数据传输机密性和完整性。通过终端密码模块和接入认证网关之间建立SSL VPN加密通道，实现数据完整性和机密性保护。
- 5.应用系统数据存储机密性和完整性。通过数据库加密网关签名验签API接口，实现敏感数据存储的机密性、完整性保护。

密码应用设计

总体方案

从总体功能架构设计，密码应用系统包括密码应用软硬件设施和配套支撑设施两部分组成，为各类警务业务系统提供符合商用密码应用安全性评估要求的身份认证、传输安全、存储安全等密码服务，基于密码技术支撑信息系统的安全升级改造。

设计目标及原则

设计目标

本项目严格按照《中华人民共和国密码法》及商用密码有关规范，以落实《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）、密码测评等相关标准为原则，搭建密码应用平台。本次陕西省公安厅交通管理总队从安全计算环境、安全区域边界、安全通信网络和集中安全管理等方面，通过国产商用密码产品和技术，实现基础密码服务资源、密码资源弹性扩展、密文计算、数据溯源等功能，解决传统密码服务性能低、密钥安全风险高、数据隐私泄漏等安全问题，实现密码资源的高效利用，提供统一的密码管理服务。

设计原则与依据

陕西省公安厅交通管理总队密码应用设计应遵循以下原则：

1.总体性原则。通过从整体层面，对陕西省公安厅交通管理总队的云平台及重要系统的密码服务开展顶层设计，明确密码应用需求和预期目标，并与本系统网络安全保护等级相结合，通过系统的设计形成涵盖技术、管理、实施保障的整体方案，为在陕西省公安厅交通管理总队系统中落实密码应用相关要求奠定基础。

2.完备性原则。围绕陕西省公安厅交通管理总队系统实际业务应用（包含云平台）与安全保护等级，站在整体角度，通过自上而下的体系化设计，综合考虑物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等多个层面密码应用需求，设计陕西省公安厅交通管理总队系统密码改造方案。

3.经济性原则。结合陕西省公安厅交通管理总队系统规模，在合理、够用的前提下，设计满足《基本要求》的密码应用改造方案，确保本系统密码应用改造投资合理，规模适度，避免资金浪费和过度保护。

4.可行性原则。针对陕西省公安厅交通管理总队密码应用方案设计需进行可行性论证，在保证云平台及信息系统业务正常运行的同时，综合考虑公安行业信息系统的复杂性、兼容性、及时性及其他保障措施等因素，保证方案切合实际、合理可行。要科学评估密码应用解决方案和实施方案，可采取整体设计、分期建设、稳步推进的策略，结合实际情况制订项目组织实施计划。

在国家信息化、公安部信息化建设指导思想与方针政策上，设计方案编制过程中，应该遵循现行标准规范。

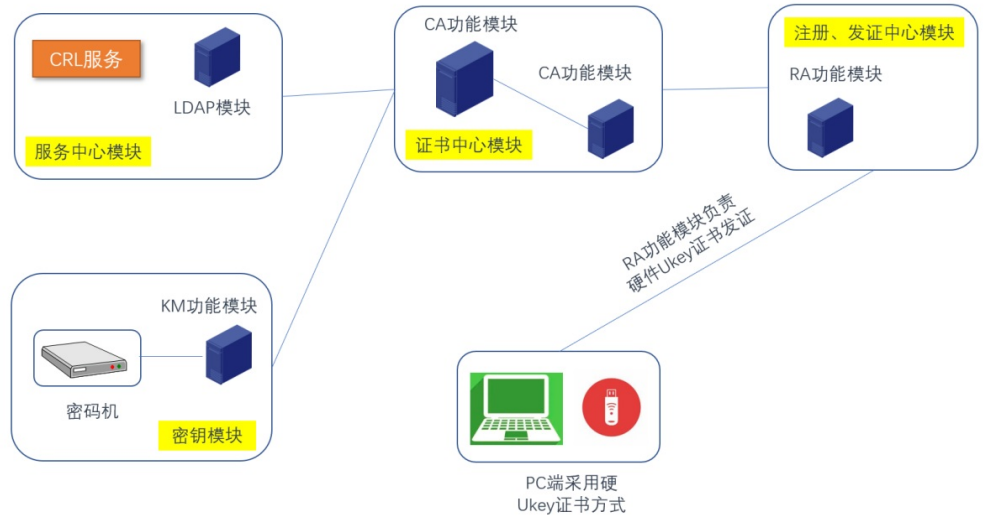
密码应用等级

根据GB/T 39786-2021中的密码应用等级一般由网络安全等级保护的级别确定，根据GB/T 22240-2020《信息安全技术网络安全等级保护定级指南》确定等级保护级别时，同步对应确定密码应用等级。即等保定级为第一级的网络与信息系统应遵循GB/T 39786-2021第一级密码应用基本要求，等保定级为第二级的网络与信息系统应遵循GB/T 39786-2021第二级密码应用基本要求，等保定级为第三级的网络与信息系统应遵循GB/T 39786-2021第三级密码应用基本要求；因此，根据陕西省公安厅交通管理总队中的业务系统等保等级定级情况，共有20个等级保护三级信息系统，但其中陕西省公安厅交通管理总队全省视频会议研判系统主要为视频会议类应用，目前不适宜进行密码应用改造，以及满分学习教育平台部署在公有云之上，受公有云平台的环境限制，目前也不适宜进行密码应用改造，故建议在本次项目中主要针对18个三级信息系统进行密码应用安全建设。

组件调用情况

数字证书流程介绍

数字证书服务拓扑架构



数字证书系统为本次密码建设的基础和核心，几乎所有的密码应用都会围绕数字证书开展。

数字证书的发放和终端类型相关，本次终端类型分为PC。

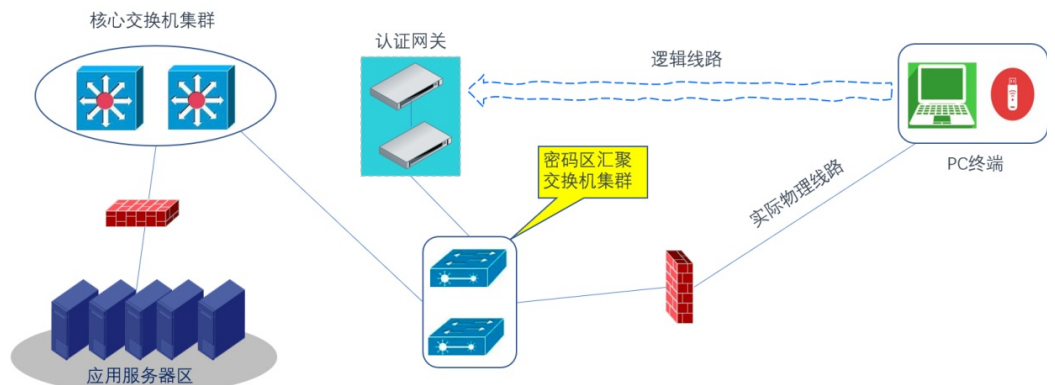
对于PC终端，本次项目采用硬件Ukey方式，数字证书发放到硬件Ukey中，当业务系统需要验证终端证书时，由终端程序调用硬件Ukey中的证书后，再将该证书传至证书认证网关。

如上图所示，数字证书服务组件由证书中心、注册中心、密钥中心、服务中心四部分构成。证书中心提供数字证书的生成功能；注册中心提供相关人员、机构的信息审核功能并且负责发放证书至相应介质载体；密钥中心提供公钥密钥对的生成；服务中心提供证书查询、验证功能。

数字证书的来源分为自建CA系统和从警务系统申请，按照警务系统的要求，使用警务系统发放数字证书（含Ukey）即可，本次项目无需建设；

客户端登陆示意拓扑及说明

客户端登陆示意拓扑

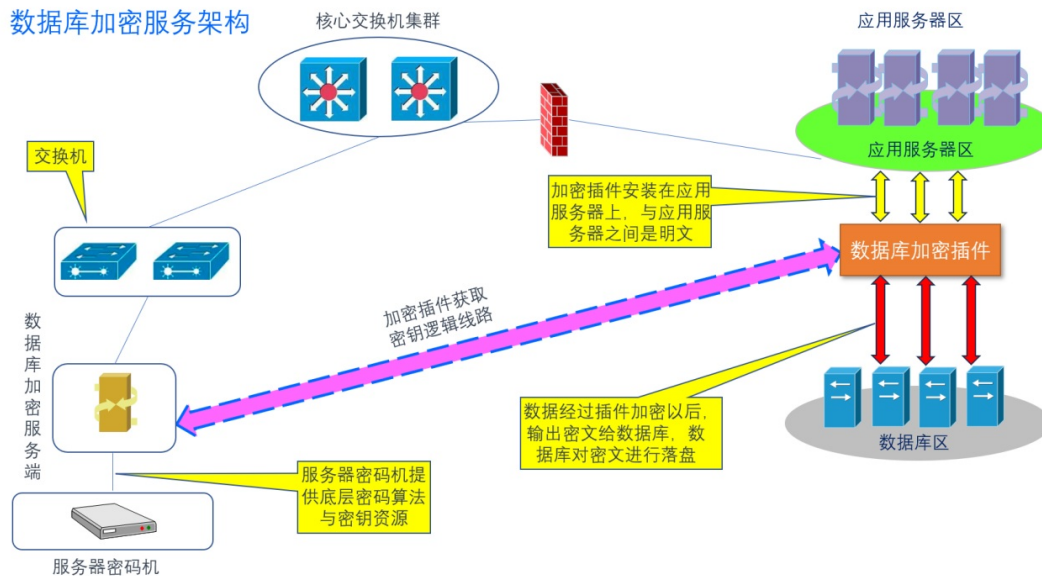


完成本次建设后，PC端使用硬Ukey证书登陆，整个证书完整的公私钥都存在于硬件Ukey中，公钥存在于证书中，私钥无法导出Ukey；对应的网关是认证网关；

认证网关对业务服务器做反向代理，根据客户端提交的证书由判断客户端身份，从而给予客户端相应访问权限；

数据库加密系统架构及描述

数据库加密服务架构



数据库加密系统分为服务端和客户端插件，客户端插件安装在数据库服务器上，应用服务器从数据库读写数据时会经过该插件，当应用服务器给数据库写数据时，明文数据传递到数据库服务器上，此时该插件对数据进行加密，然后输出密文落盘；当应用服务器从数据库读取数据时候，该插件对密文数据进行解密，然后把明文传递给应用服务器；数据库加密系统对于各个应用系统（数据库系统）会生成一个用户主密钥CMK，该用户主密钥位于密钥管理系统，该用户主密钥标识CMK-id会传递给应用系统或数据库系统。

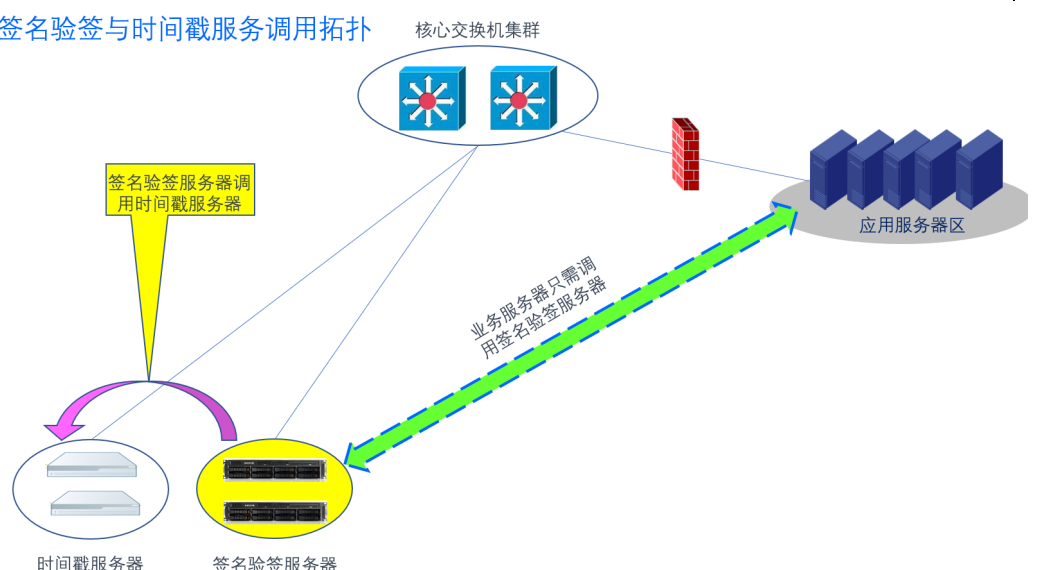
确定用户主密钥以后，数据库加密系统会生成一个数据密钥DEK，并且用CMK对该DEK进行加密，生成一个密文的DEK。把明文DEK和密文DEK都发送给应用系统（数据库系统），明文DEK和密文DEK在密钥管理系统上都是临时的，不落盘，发送以后，就从内存中清除；应用系统收到后，使用明文DEK加密数据，然后把数据密文、密文DEK和CMK-id一同存储下来，明文DEK不落盘，直接从内存中清除。整个过程，只有密文的DEK落盘在业务系统（数据库系统中）。

读取过程：应用系统读取数据密文、数据密钥密文和用户主密钥标识CMK-id。向密钥管理系统提交数据密钥密文和用户主密钥标识CMK-id，得到数据密钥DEK明文。使用数据密钥解密数据密文，得到数据明文。

综上所述，本次项目的数据库加密改造无需改动应用服务器和应用程序代码，所有工作在数据库服务器上以安装插件方式完成，方便快捷，无需任何二次代码开发；

签名验签与时间戳服务器拓扑

签名验签与时间戳服务调用拓扑

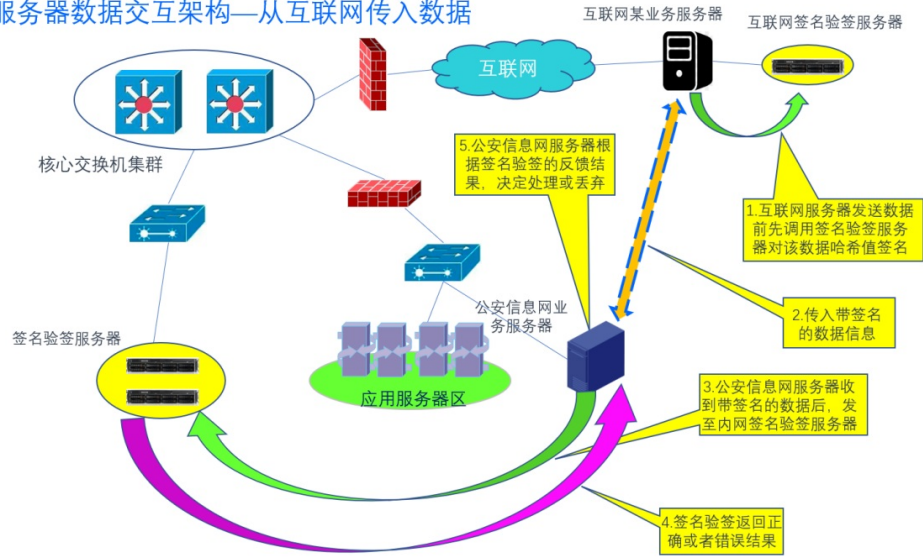


对于应用服务器，无需分别调用签名验签与时间戳，程序只需要调用签名验签服务器，对于有时间戳要求的应用程序，时间戳服务器的调用由签名验签服务器完成，对于应用程序为一次接口调用。

如果不需要时间戳，则没有签名验签和时间戳直接的接口调用，签名验签完成任务后，直接给应用服务器反馈结果。

与互联网服务网的数据交互---从互联网传入

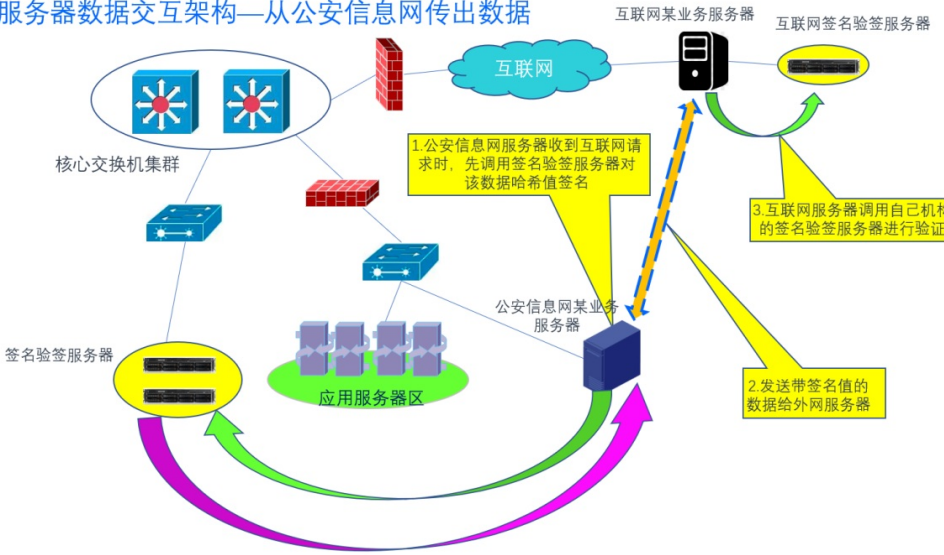
互联网服务器数据交互架构—从互联网传入数据



公安信息网和互联网的签名验签服务器先互备双方单位的公钥证书，当互联网某台业务服务器要想给公安信息网对应的业务服务器发送数据时，先调用自身签名验签服务器对该数据的哈希值进行签名，随后将该数据和签名发送至公安信息网服务器，公安信息网服务器收到数据后先不做业务处理，先发至公安信息网签名验签服务器进行数据完整性、不可抵赖性验证，等待签名验签服务器返回正确或错误结果后，再进行下一步处理或者丢弃。

与互联网服务网的数据交互---从公安信息网传出

互联网服务器数据交互架构—从公安信息网传出数据



通信双方签名验签服务器先互备双方单位的公钥证书，当公安信息网某台业务服务器收到来着其他的数据请求时，先调用公安信息网的签名验签服务器或时间戳服务器对该数据的哈希值进行签名或加盖时间戳，随后将该数据和时间戳发送至互联网服务器，互联网中对应的业务服务器调用自己单位的签名验签服务器进行验证。

密码应用技术方案

本项目密码应用的技术方案，包含密码应用技术框架、物理和环境安全、网络和通信安全、设备和计算安

全、应用和数据安全、密钥管理、密码应用部署、安全与合规性分析内容，具体设计如下：

物理和环境安全

密码保护对象

密码保护对象本次为陕西省公安厅交通管理总队，包括机房访问者身份真实性、电子门禁记录数据存储完整性、视频系统音像记录数据的存储完整性。

采用的密码措施

通过在陕西省公安厅交通管理总队一楼西区信息机房新建国密门禁系统，利用对称密钥分散和对称加解密技术，基于SM4算法进行密钥分散的CPU卡验证身份真实性，实现一卡一密，对人员进出记录逐条签名，确保人员身份的真实性，保证人员进出记录的完整性。

复用现有的国密视频系统，采用SM3+HMAC技术，实现视频录像的完整性保护。

国密门禁与视频监控

陕西省公安厅交通管理总队尚未建设密码设备，在本项目中，将按照政策要求，增加密码设备，业务系统需要调用密码设备确保达到GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，考虑新建国密门禁系统，复用现有国密视频系统，实现一门一控制，确保人员出入有记录。

经过前期现场勘察，需安装4个国密门禁，50张国密用户卡。安装位置如下：

- 1.陕西省公安厅交通管理总队主楼一楼西区信息机房部署3个门禁，其中2个入户，1个设备区。
- 2.在陕西省公安厅交通管理总队主楼一楼东电池间部署1个入户门禁。

门禁部署位置如下图：

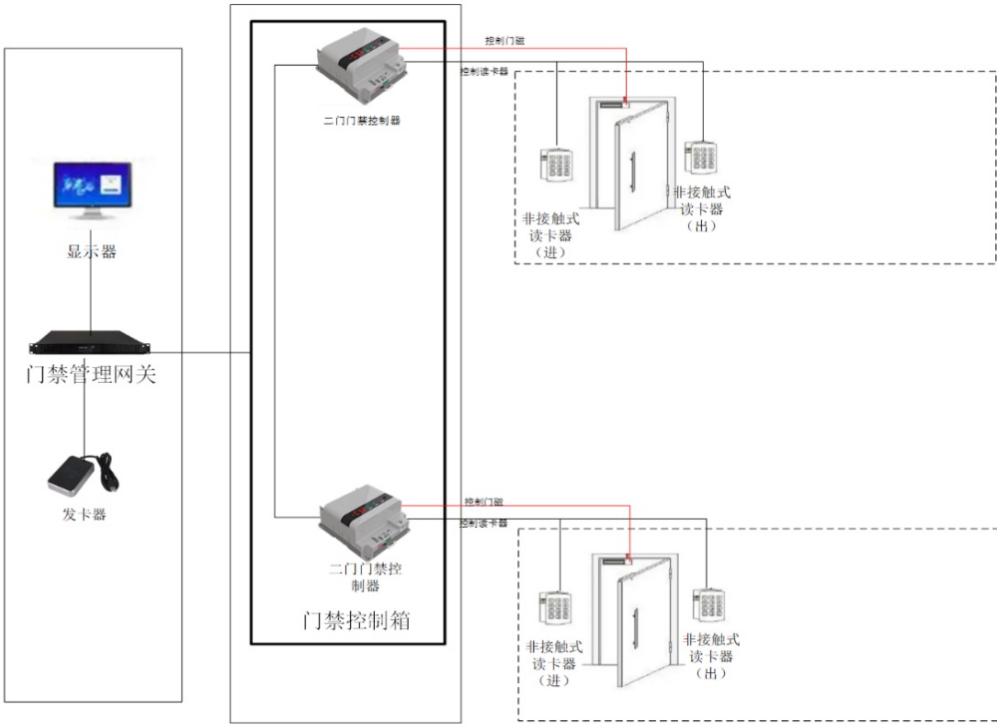


图 54 门禁部署位置示意图

通过在前端部署替换的国密非接触式读卡器和读卡器，在进行身份鉴别时，门禁读卡器发送一个内部认证命令给到门禁卡，门禁卡用卡内密钥对认证命令进行国密SM1加密，并返回给门禁读卡器，门禁读卡器对卡片进行身份鉴别，并根据鉴别结果来控制门禁功能的执行。

网络和通信安全

密码保护对象

网络和通信安全保护的对象是陕西省公安厅交通管理总队系统与外部实体之间网络通信的安全，包括通信

实体身份的真实性、通信数据的机密性和完整性、以及网络边界访问控制信息的完整性。

采用的密码措施

1.密码应用设计

（1）采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。

针对以上通道，通过在主楼一楼西信息中心机房部署安全认证网关（包含SSL VPN功能），前端设备/应用客户端集成软件密码模块，实现身份标识、双向认证，实现通信实体的身份鉴别。

（2）采用密码技术保证通信过程中数据的完整性。

针对以上通道，通过在主楼一楼西信息中心机房部署安全认证网关（包含SSL VPN功能），前端设备/应用客户端集成软件密码模块。两端基于SSL协议 建立安全通信链路，采用SM3算法保证通信数据完整性。

（3）采用密码技术保证通信过程中重要数据的机密性。

针对以上通道，通过在主楼一楼西信息中心机房部署安全认证网关（包含SSL VPN功能），前端设备/应用客户端集成软件密码模块。两端基于SSL协议建立安全通信链路，进行会话密钥协商，并以SM4算法保证通信过程中重要数据的机密性。

（4）采用密码技术保证网络边界访问控制信息的完整性。

针对以上通道，通过在主楼一楼西信息中心机房部署安全认证网关（包含SSL VPN功能），网关设备内置访问控制功能，保证网络边界访问控制信息的完整性。

网络和通信安全层面使用的密码算法、密码技术、密钥管理由符合《SSL VPN 网关产品规范》（GM/T 0025-2014）、《安全认证 网关产品规范》（GM/T0026-2014）、《密码模块安全技术要求》（GM/T 0028-2014）的数据库加密网关实现。

2.密码应用工作流程

通信传输主要采用 SM2、SM3、SM4国密算法，遵循《安全认证网关产品规范》（GM/T0026-2014）、《SSL VPN 技术规范》(GM/T 0024)规范。

数字证书

依托省厅的数字证书平台，在前期信息化建设中，已经建立了全警种使用的Ukey方式的数字证书系统。本项目通过复用现有的数字证书系统，实现对应用和数据访问人员身份的认证和控制。

数字证书系统详细拓扑架构如下：

数字证书系统详细拓扑架构

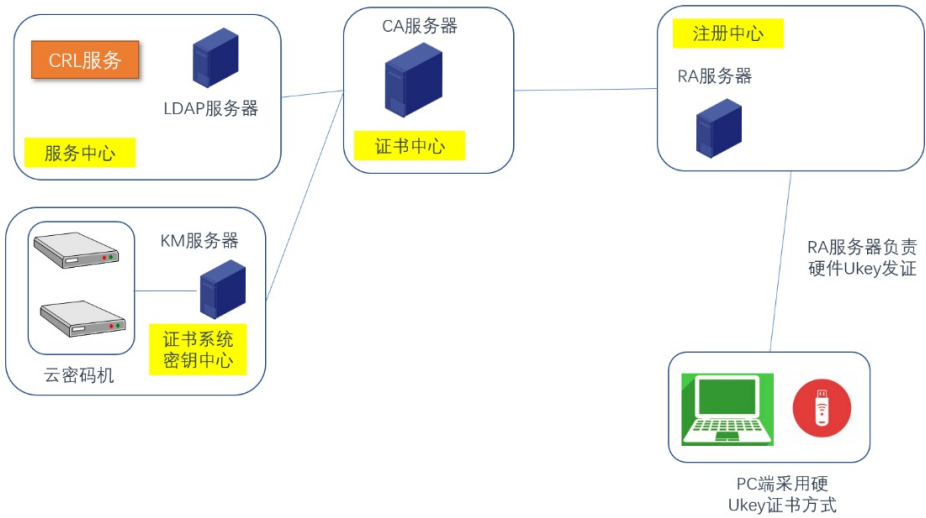


图 55数字证书系统详细拓扑架构

如上图所示，数字证书服务组件由证书中心、注册中心、密钥中心、服务中心四部分构成。证书中心提供数字证书的生成功能；注册中心提供相关人员、机构的信息审核功能并且负责发放证书至相应介质载体；密钥中心提供公钥密钥对的生成；服务中心提供证书查询、验证功能。

数字证书系统为密码建设的基础和核心，几乎所有的密码应用都会围绕数字证书开展。

设备和计算安全

密码保护对象

设备和计算安全保护的对象是用于承载交警总队信息系统的各类设备和计算环境的安全防护，包括保障计算设备的身份鉴别、日志记录完整性等。

采用的密码措施

1.密码应用设计

针对设备使用时身份鉴别的需求，通过密码模块与设备指纹进行绑定，设备使用人员采用动态令牌方式进行登录认证。

在安全管理区部署服务器密码机和数据库加密网关，服务器密码机、数据库加密网关提供基于HMAC_SM3的数据签名接口，通过接口调用对业务服务器、数据库服务器、堡垒机等设备的访问控制信息进行完整性保护。系统中使用的密码产品经商用密码认证机构认证合格，具备相应的安全防护能力。

日志记录完整性，日志审计系统通过调用服务器密码机或数据库加密网关的HMAC_SM3签名接口，对日志进行完整性保护。安全管理员在执行完整性检查时，可通过计算和原有摘要值进行比对并判断日志文件是否被篡改过。

设备和计算安全层面使用的密码算法、密码技术、密钥管理由符合《SSL VPN 网关产品规范》（GM/T 0025-2014）、《安全认证网关产品规范》（GM/T0026-2014）、《密码模块安全技术要求》（GM/T 0028-2014）的数据库加密网关实现。

运维人员管理

密码建设完成后，运维人员通过Ukey证书登录运维通道的网关，经过网关后，到达运维堡垒机（含数据库审计），确保运维人员登录的合法合规，采用密码技术认证身份，及建立SSL通道。

运维人员登陆示意如下图：

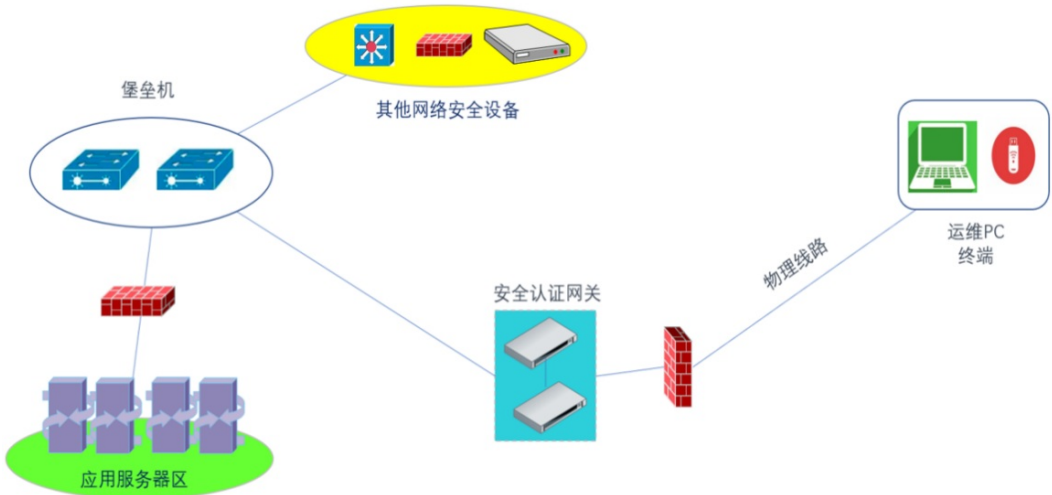


图 56运维人员登录示意拓扑图

应用和数据安全

密码保护对象

应用和数据安全场景主要包括用户登录身份验证、用户信息访问、数据传输、数据存储全场景的数据安全服务。对数据安全要求包括保护数据的完整性和机密性。涉及的重要数据包括所有用户的登录密码、权限信息、重要的配置信息和业务基础数据等。

重要关键数据密码保护分析如下：

表 5-1数据情况说明表

序号	类别	对象	描述	安全需求
1	重要数据	鉴别数据	用户的登录口令、密钥	机密性 完整性
2		用户信息	用户的身份证号码、手机号码等信息	机密性 完整性
3		访问控制信息	系统访问控制策略、数据库表访问控制信息等	完整性
4		日志数据	系统运行日志、业务操作日志等	完整性
5		重要业务数据	业务数据，比如：涉及在逃人员、涉毒人员、刑事案件、案件嫌疑人、民航进港数据、110接警数据、110派警数据、110处警数据、重要情报送数据、情报线索数据、重点人预警数据、重点人预警处置数据、临时布控预警数据和云控预警及处置数据等重点数据等；	机密性 完整性
6		密钥	对称密钥、非对称密钥，涉及密钥的生成、存储、分发、使用、更新、归档、撤销、备份、恢复、销毁等全生命周期	机密性 完整性
7	实体身份	系统管理员	对系统进行维护和管理，对系统的使用和业务分析提供技术支持。	真实性
8		设备和应用	签名验签服务器等设备和应用系统身份	真实性
9		决策领导	查看系统信息	真实性
10		值守人员	对系统进行维护	真实性
11	关键操作行为	管理操作	系统登录、合同签署、安全审计、支付类交易等行为	不可否认性

采用的密码措施

通过调用密码应用软硬件系统中相关组件，如签名验签、数据库加解密系统、安全认证网关、服务器密码机、数据库加密网关等设备，实现信息系统的身份鉴别、访问控制信息完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性。

通过调用密码应用软硬件系统中的数据库加密服务组件，可实现现有业务系统的数据加密解密。业务系统通过调用 SDK，实现对现有数据的加密或解密。并可结合数字签名技术，判断发送或接收方的身份真实性，已经数据是否经过篡改，从而保证数据的机密性和完整性。业务系统将待加解密的数据传输至服务器密码机或数据库加密网关。服务器密码机或数据库加密网关接收到加解密请求后，调用存储于密码设备的加密密钥执行加解密运算。业务流程如下图所示：

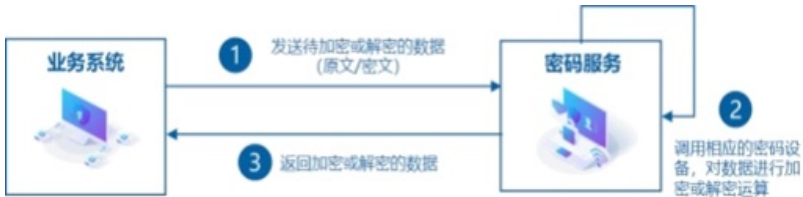


图 57数据加解密流程图

本层面调用密码安全服务主要包括以下密码业务实现功能：

1.使用密码技术来实现用户身份鉴别

在访问系统时，PC端用户通过配发智能密码钥匙，配合服务端安全认证网关，实现基于数字证书的身份认

证，对登录用户进行身份标识和鉴别，且保证用户名的唯一性。移动端用户通过协同签名客户端（密码模块），配合服务端协同签名系统，实现基于数字签名技术的“挑战—响应”机制登录。

“智能密码钥匙”主要是用作基于公钥体系的数字证书和私钥的安全载体，并能在硬件中进行加密运算。采用“硬件 + PIN 码”的双因子认证，保证数字证书和私钥的合法使用。符合《GM/T 0016-2012 智能密码钥匙 密码应用接口规范》、《GM/T 0017-2012 智能密码钥匙 密码应用接口数据格式规范》，存储用户的私钥以及数字证书，使用 USB 接口与 PC 机连接，然后 PC 机通过 USB 接口存储和读取智能密码钥匙中的密钥、证书等数据和信息，保证了用户认证的安全性，自带了安全校验机制，包括 PIN 码等方式。

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；

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。

采用SM2数字签名算法实现身份鉴别后才能访问相应系统或资源。

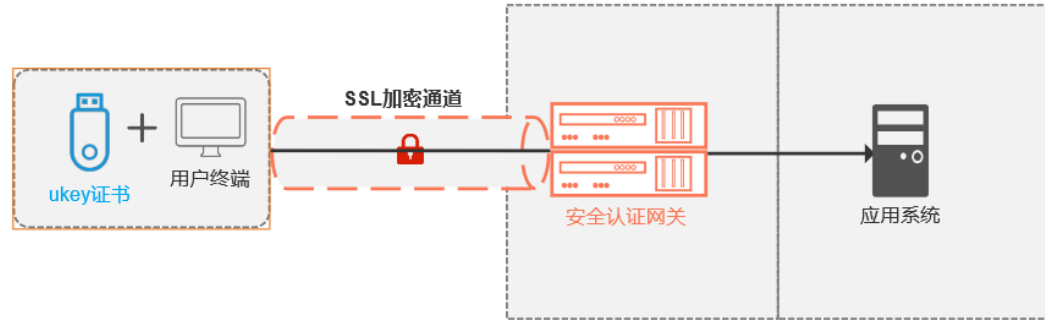


图 58 用户身份鉴别业务技术框架图

2.访问控制信息完整性

调用密码应用软硬件系统中的签名验签服务组件，使用数字签名技术对系统用户访问权限控制列表信息进行完整性保护，系统用户登录平台时校验权限信息的完整性，防止应用资源被非授权用户获取，只有通过权限完整性校验，才能访问相关业务和资源。

3.重要数据存储机密性

对系统中数据资源，由硬件密码机提供 SM2、SM4 等算法运算，调用即可实现数据本身的加密、签名，从根本上实现数据安全防护。对重要身份鉴别信息、用户信息、重要信息进行机密性保护。

即使数据被监听、窃取，因为数据加密，也不会导致泄密。通过数据签名验签，保证数据在传输、存储过程中不会被篡改，也认证了数据发送方的真实身份，实现抗抵赖。

数据库加密系统支持数据库的透明化加解密处理，文件加密系统支持文件的透明化加解密处理。

4.重要数据存储完整性

用户访问系统时，在通信层面通过安全认证网关通道调取服务，保证了数据传输过程中的完整性。

对系统资源，通过调用服务器密码机或数据库加密网关，使用HMAC-SM3算法，对重要数据进行完整性保护，并在数据查询、使用过程中进行检。

数据传输机密性和完整性

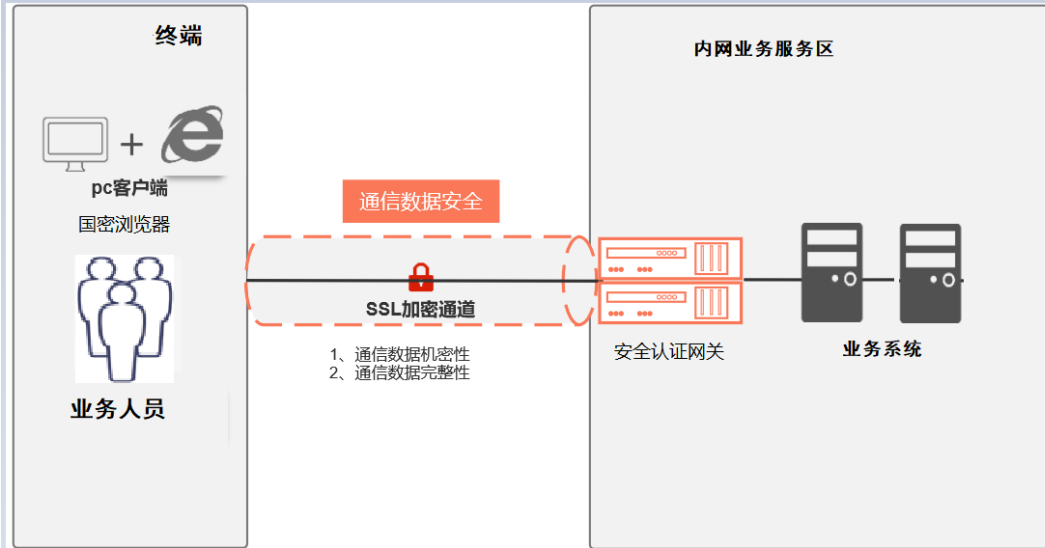


图 59 数据传输机密性和完整性技术框架图

用户访问系统时，在通信层面通过安全认证网关通道调取服务，保证了数据传输过程中的机密性和完整性。其次，在应用层，对少量的重要业务数据，如口令，采用SM2加密算法，客户端利用服务端公钥对数据进行传输前的加密，并在服务端进行解密。

对系统资源，通过调用服务器密码机或数据库加密网关，使用HMAC-SM3算法，对重要数据进行完整性保护，并在数据查询、使用过程中进行检测。

5. 数据库敏感字段加密

基于国密算法（支持 SM2/3/4）和安全的密钥管理，以保留格式加密技术为核心，实现安全可控、可管理的数据库敏感字段加密，支持特定字段加密、全库加密，支持密文查询检索，支持数据加密后的还原和安全共享交换，可以保障在数据库DBA密码泄漏、拖库、监守自盗等情况下数据仍然不会外泄。

密码应用工作流程

身份认证流程

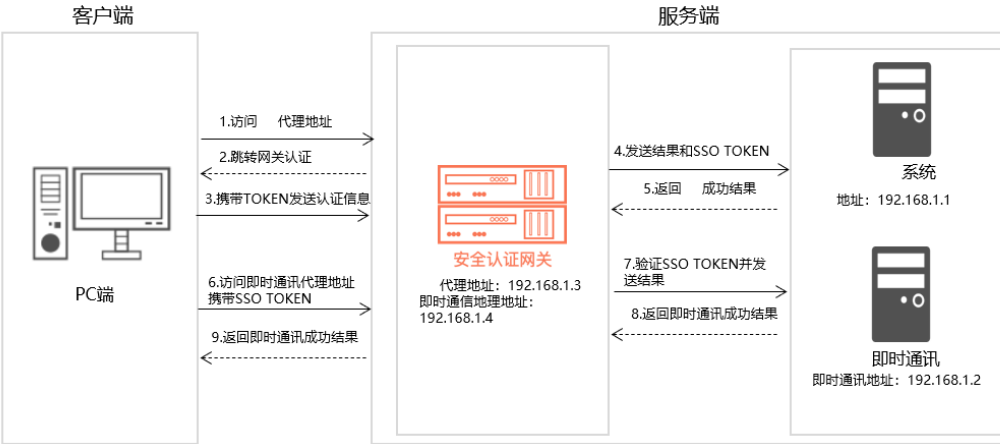


图 510 身份认证流程图

配置业务系统的代理地址和Ukey认证功能，包括客户侧受信CA证书，需要用于认证的Ukey根证书以及证书吊销列表。

访问代理地址时，会先打开网关自带的认证页面，完成Ukey认证后，网关将用户信息提交给代理的业务系统。

重要数据传输机密性、重要数据传输完整性密码应用工作流程详见网络和通信。

结构化数据存储机密性/完整性密码应用工作流程：

对关键数据使用SM4密码算法进行加密保护，对于关键信息的数据写入操作，在写入数据库前，调用国产密码算法，对数据进行加密处理，再执行写入操作，以密文形式存储在数据库中。对于关键信息的数据读取操作，在从数据库读取后，调用国产密码算法，对数据进行解密处理，将明文数据返回给上层接口。

- 1.在应用系统中部署密码中间件；
- 2.应用系统向服务器密码机或数据库加密网关申请数据加解密密钥，生成加解密密钥，返回加解密密钥至数据库加解密系统；
- 3.在数据库加解密系统中设置数据加解密策略，并下发加解密策略和加解密密钥至密码中间件；
- 4.应用系统发起加密请求，调用密码中间件中的加解密密钥，对明文数据进行加密后密文存储；
- 5.应用系统发起解密请求，调用密码中间件中的加解密密钥，对密文数据进行解密后明文展示。

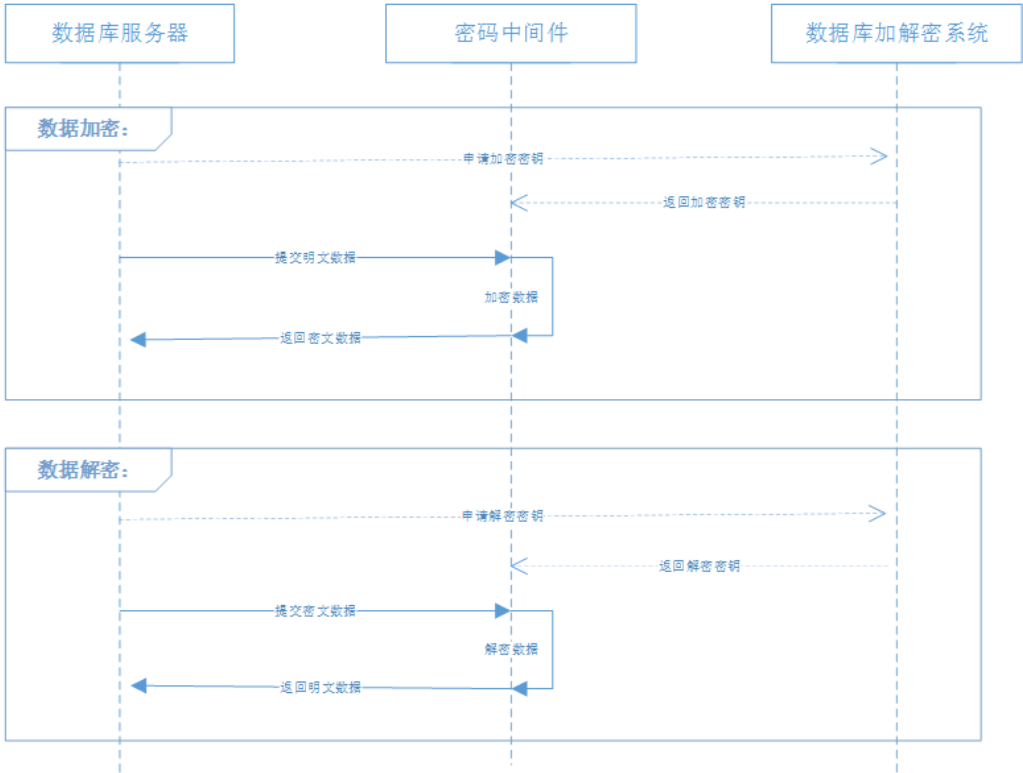


图 511结构化数据存储机密性/完整性密码应用流程图

密钥1		密钥2		密钥n	
字段1	字段2	字段3	字段4	字段.....	字段n
张三	330314558850	18928345799	男		广东省深圳市
刘石	450224355809	13309285778	男		广东省深圳市
陈娜	442243525517	15899221468	女		广东省广州市

↓

字段1	字段2	字段3	字段4	字段.....	字段n
张三	ED3C6BCC8BF28A0500D615BA43FC20C7	B3E2773C5DD1EF033EAC9C8C02803C5E	男		DE248B1AC7902FFE7DC402A7A35508CE
刘石	E03DACFF245E40B93AE8C750D2FD1C37	4E89C874F6E542CE545D60C8CA05E36F	男		DE248B1AC7902FFE7DC402A7A35508CE
陈娜	2DD5CB9E3762F8A2A91DDA80F711B0AC	C9D108341030E68B993F923118DCF8A5	女		8FCB9ED2417330C0A5A0D1E183F96AD2

图 512结构化数据加密效果图

- 1.密码应用设计
 - (1) 身份鉴别认证

本密码应用中，用户通过软密码模块设备绑定结合PIN码的方式进行应用登录身份辨别认证。USBkey，移动软证书服务，按照公安部和省公安厅标准进行集成对接。
 - (2) 访问控制信息完整性实现

访问控制信息完整性实现包括数字签名和签名验签两个过程。

数字签名：本次新建签名验签服务器提供数字签名服务，实施时按照公安部和省公安厅统一的标准流程和接口进行服务调用。系统管理员每次授权完成，系统通过调用数据库加密网关，使用SM3杂凑算法和SM2非对称

称密码算法，对系统访问控制信息进行签名，并将访问控制列表及其数字签名值同时存储，保证其完整性。

访问控制信息的完整性保护工作流程如下：

系统管理员打开系统的授权模块；

系统管理员进行授权，并保存；

系统存储访问控制信息；

系统将访问控制信息提交数据库加密网关，申请数字签名；

数据库加密网关使用**SM3**杂凑算法，计算访问控制信息的摘要值；

数据库加密网关调用系统的签名私钥，对摘要值做数字签名，形成签名值；

数据库加密网关将签名值返回系统；

如果系统没有接收到签名值，在终端页面显示访问控制信息完整性保护失败；

如果系统接收到签名值，存储访问控制信息及其签名值；

在终端页面显示访问控制信息完整性保护成功。

签名验签：用户/平台管理员每次登录时，系统通过调用数据库加密网关，使用**SM3**杂凑算法和 **SM2**非对称密码算法，验证访问控制信息的数字签名，及时发现篡改行为。

访问控制信息的完整性保护工作流程如下：

用户/平台管理员通过身份认证；

系统提取当前访问控制信息和最近的访问控制信息的数字签名，发送数据库加密网关，申请签名验证；

数据库加密网关获取当前访问控制信息和最近的访问控制信息的数字签名；

数据库加密网关调用系统的签名公钥，解密最近的访问控制信息的数字签名，获取最近访问控制信息的摘要值；

数据库加密网关使用**SM3**杂凑算法，计算当前访问控制信息的摘要值；

数据库加密网关比较当前访问控制信息的摘要值与最近访问控制信息的摘要值，是否一致，并向系统返回结果；

如果两个摘要值一致，说明访问控制信息未被篡改，系统根据用户权限信息推送应用内容；

如果两个摘要值不一致，说明访问控制信息已经被篡改，系统通知系统管理员处理；并在终端提示。

数据存储机密性实现：系统中的个人信息等数据属于重要数据，需要实现存储机密性保护。存储的机密性保护包括两个部分：数据录入时，使用**SM4**对称密码算法，对重要数据进行加密，防止相关信息泄漏；访问读取时，使用**SM4**对称密码算法，对重要数据进行解密。

对重要数据进行加密存储：数据录入人员录入重要数据时，系统调用数据库加密网关，使用**SM4**对称密码算法，对录入的重要数据进行加密。加密流程图如下：

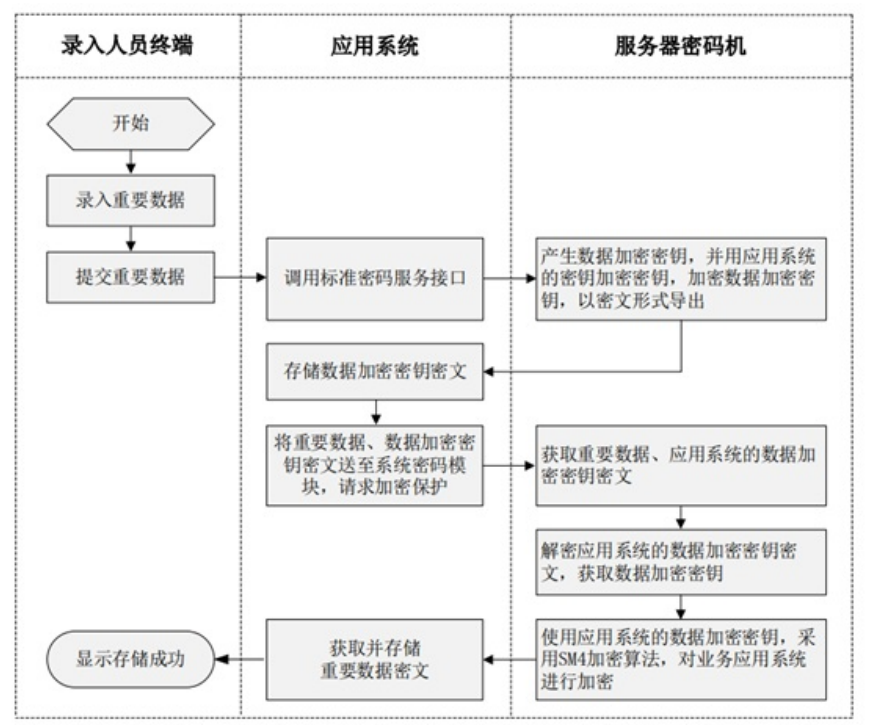


图 513重要数据加密流程图

本次新建的密码应用软硬件系统提供数据加密服务，实施时按照公安部和省公安厅统一的标准流程和接口进行服务调用。

录入重要数据的加密存储工作流程如下：

用户向系统输入重要数据后，并提交；

系统获取录入的重要数据，调用标准密码服务接口申请数据加密密钥；

数据库加密网关产生系统的数据加密密钥，并用系统的密钥加密密钥，加密数据加密密钥，以密文形式导出；

系统存储数据加密密钥密文，将录入的重要数据加密密钥密文送数据库加密网关，请求加密保护；

数据库加密网关获取录入的重要数据加密密钥密文；解密系统的数据

加密密钥密文，获取系统的数据加密密钥；

数据库加密网关使用系统的数据加密密钥，采用SM4加密算法，对录入的重要数据进行加密；

系统获取并存储录入重要数据的密文；

用户终端显示存储成功；

对重要数据进行解密访问。

访问系统中的加密重要数据时，系统自动调用数据库加密网关，使用SM4对称密码算法，对加密的重要数据进行解密。

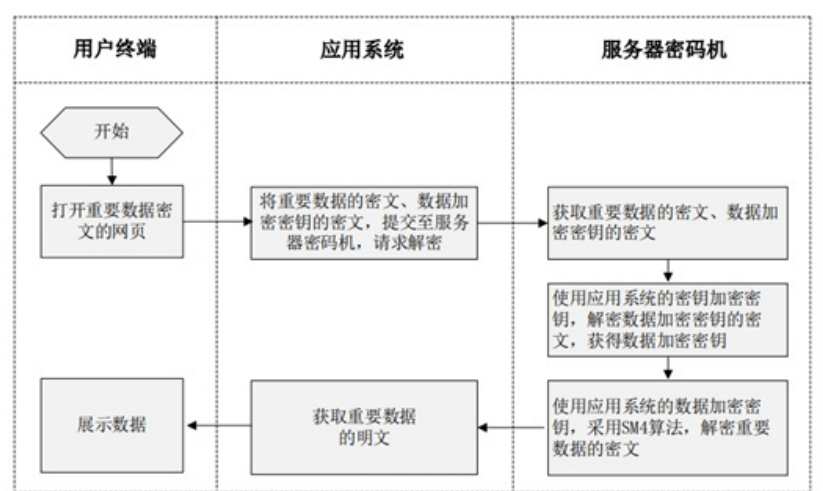


图 514重要数据解密流程图

本项目密码应用软硬件系统提供数据加密服务，实施时按照公安部和省公安厅统一的标准流程和接口进行服务调用。

访问人员点击已加密存储的重要数据页面；

系统将重要数据的密文、数据加解密密钥的密文，提交至数据库加密网关，请求解密；

数据库加密网关获取重要数据的密文、数据加解密密钥的密文；

数据库加密网关使用系统的密钥加解密密钥，解密数据加解密密钥密文，获得数据加解密密钥；

数据库加密网关调用系统的数据加解密密钥，采用SM4加密算法，解密重要数据的密文，获得重要数据明文，送回系统；

系统获得重要数据的明文，向终端展现数据。

数据传输完整性和机密性实现：通信传输使用安全认证网关主要采用SM2、SM3、SM4 算法，遵循《SSL VPN 网关产品规范》（GM/T 0025-2014）、《安全认证网关产品规范》（GM/T0026-2014）。本方案中采用国密SSL安全网关完成，SSL安全网关作为应用层代理设备，通过建立国密SSL加密通道，实现对数据传输过程的机密性和完整性进行保护。

数据存储完整性实现：系统中的个人信息和配置数据等属于重要数据，需要进行完整性保护。重要数据的完整性保护包括两个部分：平台发布重要信息时，对数据的相关关键信息做MAC运算；用户每次访问时，验证公开数据相关关键信息的MAC值。

签名签章：对涉及的关键电子文书、电子证照需要进行数字签名，确保文件的完整性、有效性。

密码应用集成方案

重要数据分析

1.密码保护对象

应用和数据安全保护对象是陕西省公安厅交通管理总队，包括系统的登录用户、系统管理员、访问控制信息、重要关键数据。确保数据的真实性、数据传输的机密性和完整性、数据存储的机密性和完整性等。

表 5-2陕西省公安厅交通管理总队密码保护对象详情

序号	类别	对象	描述
1	实体身份	系统管理员	系统管理、权限配置、日志审计
2		省市县管理用户（审批用户）	系统的审核人员
3		一般用户（部门用户）	应用系统的普通用户
4	访问控制信息	用户账号权限	系统用户所属的角色的权限表
5	重要数据	个人信息	用户身份证号、手机号、账号等个人信息
6		业务数据	警员基本信息（手机号、身份证等）；机构信息；警务数据信息、随访结果数据等。
7	日志数据	登录日志和操作日志	应用系统操作日志、用户操作行业日志、服务器等日志记录信息。

2.采用的密码措施

通过密码应用软硬件系统提供的数据库加解密服务、身份认证服务、安全接入服务等功能，实现业务系统的身份鉴别、访问控制信息完整性、重要数据传输机密性、重要数据存储机密性、重要数据传输完整性、重要数据存储完整性。

(1) 身份鉴别

PC端用户通过配发智能密码钥匙（Ukey）+数字证书，配合服务端身份认证网关，实现基于数字证书的身份认证。

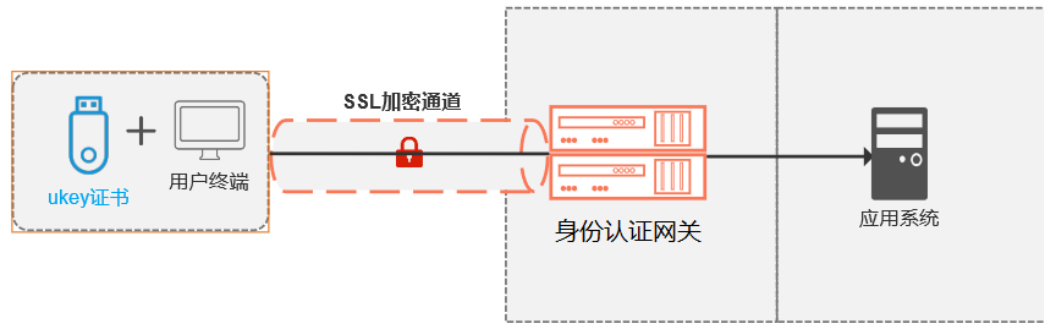


图 515 身份鉴别示意图

(2) 访问控制信息完整性

调用服务器密码机或数据库加密网关接口，对访问控制策略、数据库表访问控制信息等使用SM3算法进行单向散列函数构造消息认证码（HMAC）实现数据的完整性。

(3) 重要数据存储机密性/完整性

警员信息（手机号、身份证等）、机构信息、业务数据信息等重要业务数据存储通过数据库加解密系统，使用SM4算法的对称加密保护数据机密性，使用SM3算法进行单向散列函数构造消息认证码（HMAC）实现数据完整性。

非结构化数据存储通过调用服务器密码机或数据库加密网关接口，使用SM4算法的对称加密保护数据机密性，使用SM3算法进行单向散列函数构造消息认证码（HMAC）实现数据完整性认证。

(4) 数据传输机密性和完整性

数据传输机密性和完整性，通过安全接入网关、身份认证网关和国密浏览器实现。

3. 密码应用工作流程

(1) 身份认证流程

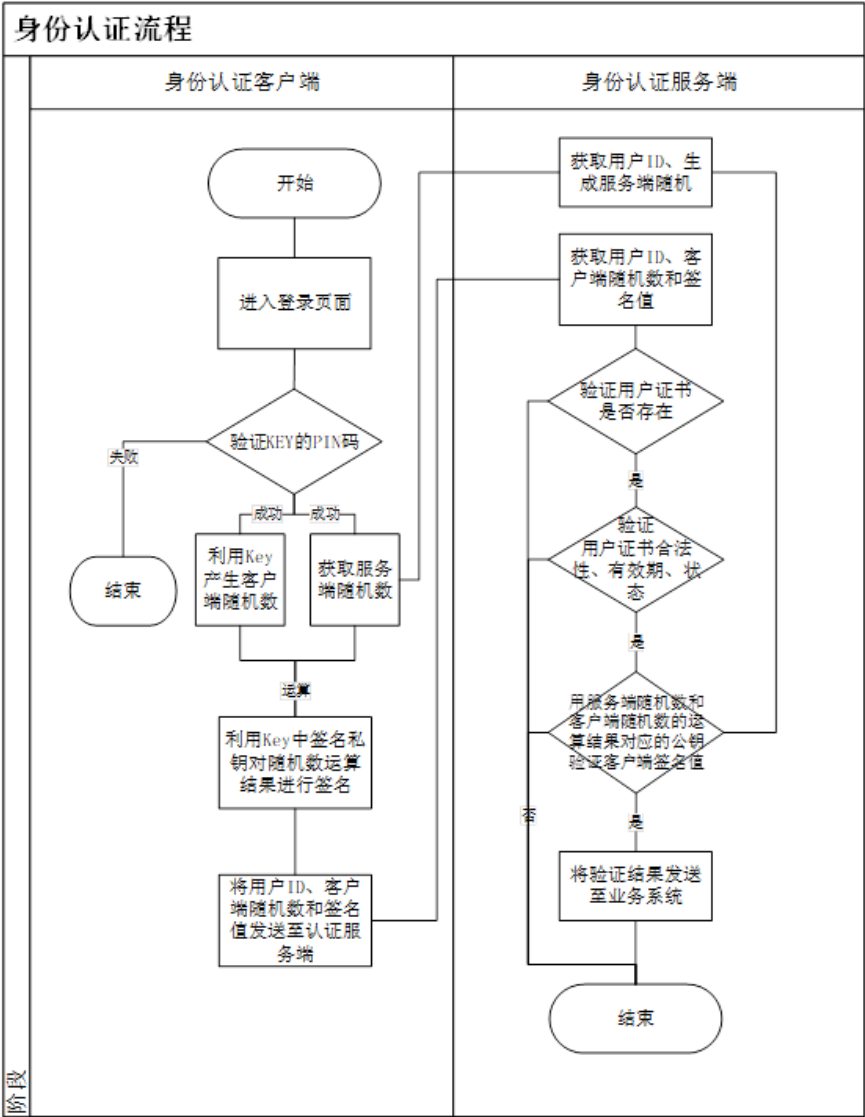


图 516 身份认证加密流程图

用户进入登录页面；

用户插入智能密码钥匙（Ukey），输入智能密码钥匙（Ukey）验证口令的正确性，口令验证失败则认证失败，否则进入下一步；

客户端获取服务端提供的随机数；

客户端使用智能密码钥匙（Ukey）产生客户端随机数，同时与服务端提供的随机数进行运算；

系统用户利用智能密码钥匙（Ukey）中的签名私钥对随机数运算结果进行签名，生成签名值；

将用户ID、客户端随机数、签名值传给认证服务端；

服务器端根据获取的用户ID，从数据库获取用户签名证书，验证用户证书是否存在、证书有效性、有效期、是否已经被注销。成功进行下一步；

服务器端根据获取的用户ID，从数据库获取服务端随机数，与客户端随机数进行运算，根据运算结果和客户端签名值进行验签。从而确定该登录用户，验证用户身份，将验证结果发送至业务系统；

完成身份认证，流程结束。

（2）重要数据传输机密性、重要数据传输完整密码应用工作流程

与网络和通信安全流程一致，详见“网络和通信安全”章节。

（3）数据存储机密性、完整性保护流程

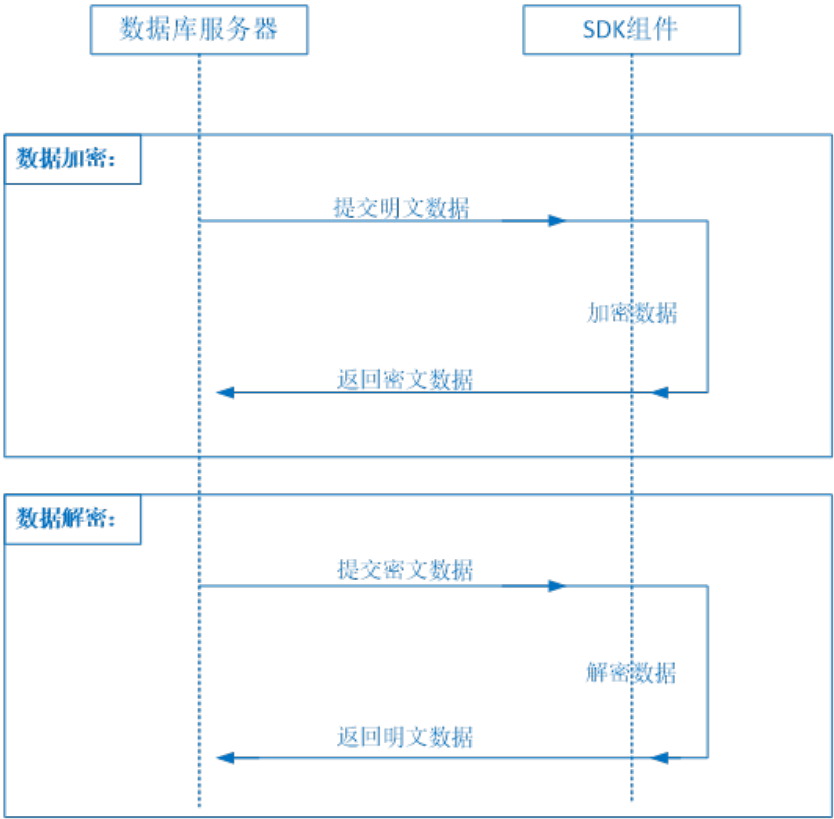


图 517密码机加密过程示意图

创建SDK加密插件加解密时所需要的凭证和口令，并由密码机运算生成对应的密钥；

SDK从签名验签协同签名策略同步申请；

用户端触发SQL操作，触发业务系统的SDK，SDK根据SQL解析、查询、执行等操作进行加解密策略匹配，达到重要数据存储机密性的安全保护。

4.密码算法配置

表 5-3密码算法配置表

实施保护层面	应用环节	配用的密码算法	承载算法的密码系统
应用和数据安全	身份鉴别	SM2/3	安全接入网关
	访问控制信息完整性	SM2/3	密钥管理系统
	重要数据传输机密性	SM4	服务器密码机
	重要数据存储机密性	SM4	数据库加密网关
	重要数据传输完整性	SM4	加解密系统
	重要数据存储完整性	SM3	数据库加密网关

数据库加密服务

本项目的数据库加密服务通过组件的方式来实现。

数据库加密服务架构如下图所示：

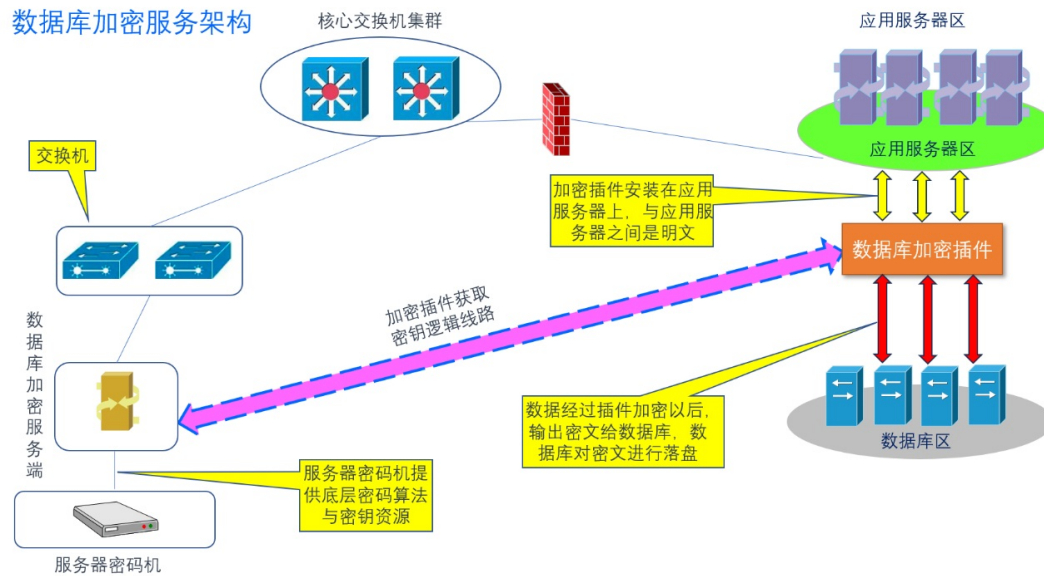


图 518 数据库加密服务架构图

数据库加密服务组件分为服务端和客户端插件，客户端插件安装在数据库服务器上，应用服务器从数据库读写数据时会经过该插件，当应用服务器给数据库写数据时，明文数据传递到数据库服务器上，此时该插件对数据进行加密，然后输出密文落盘；当应用服务器从数据库读取数据时候，该插件对密文数据进行解密，然后把明文传递给应用服务器；数据库加密服务组件对于各个应用系统（数据库系统）会生成一个用户主密钥CMK，该用户主密钥位于密钥管理系统，该用户主密钥标识CMK-id会传递给应用系统或数据库系统。

确定用户主密钥以后，数据库加密服务组件会生成一个数据密钥DEK，并且用CMK对该DEK进行加密，生成一个密文的DEK。把明文DEK和密文DEK都发送给应用系统（数据库系统），明文DEK和密文DEK在密钥管理系统上都是临时的，不落盘，发送以后，就从内存中清除；应用系统收到后，使用明文DEK加密数据，然后把数据密文、密文DEK和CMK-id一同存储下来，明文DEK不落盘，直接从内存中清除。整个过程，只有密文的DEK落盘在业务系统（数据库系统中）。

读取过程：应用系统读取数据密文、数据密钥密文和用户主密钥标识CMK-id。向密钥管理系统提交数据密钥密文和用户主密钥标识CMK-id，得到数据密钥DEK明文。使用数据密钥解密数据密文，得到数据明文。

综上所述，本次项目的数据库加密改造中，服务端内置于数据库加密网关中，无需改动应用服务器和应用程序代码，所有工作在数据库服务器上以安装客户端插件方式完成，方便快捷，无需任何二次代码开发；

签名验签服务

对于应用服务器，按照密评要求，需要进行数据完整性保护，通过调用签名验签服务组件对数据进行签名和验签。

如后续业务涉及时间戳组件，则无需分别调用签名验签与时间戳，程序只需要调用签名验签组件，对于有时间戳组件要求的应用程序，时间戳组件的调用由签名验签组件完成，对于应用程序为一次接口调用。

本项目签名验签服务组件调用拓扑如下图所示：

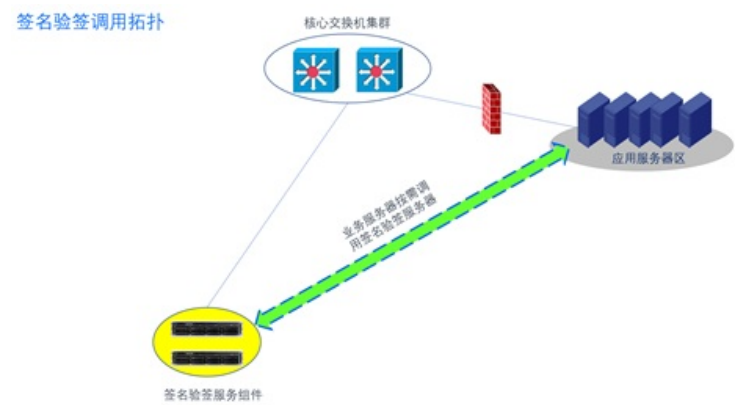


图 519 密码验签调用拓扑图

与互联网的数据交互

通信双方签名验签服务器先互备双方单位的公钥证书，当互联网某台业务服务器要想给公安信息网对应的业务服务器发送数据时，先调用自身签名验签服务组件对该数据的哈希值进行签名，随后将该数据和签名发送至公安信息网服务器，公安信息网服务器收到数据后先不做业务处理，先发至公安信息网签名验签服务组件进行数据完整性、不可抵赖性验证，等待签名验签服务组件返回正确或错误结果后，再进行下一步处理或者丢弃

数据交互架构如下图所示：

互联网服务器数据交互架构—从互联网传入数据

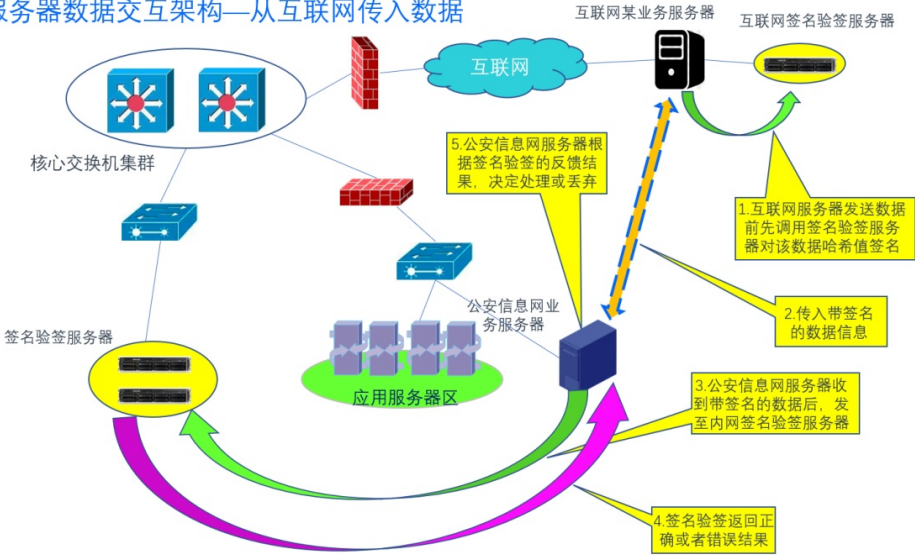


图 520 与互联网服务器数据交互架构图

密钥管理

本项目平台及系统选用符合要求的安全认证服务、软件密码模块、数据库加密网关、等商用密码产品，并提供密钥管理方案，保证密钥的管理和存储安全，并严格遵照该方案进行使用和实施。

密钥管理是包括了密钥生成、分发、存储、使用、更新、归档、备份、恢复和销毁等全生命周期的管理。简述如下：

密钥生成：专用硬件密码卡/设备生成，并同步记录密钥关联信息，包括密钥种类、长度、拥有者、使用起始时间、使用终止时间等。

密钥分发：对称密钥和非对称密钥的分发，对称密钥分发采用密钥分散或真随机生成的形式进行安全下发，非对称密钥主要采用数字证书形式分发。

密钥存储：密钥以密文方式存储，防止被非授权的访问或篡改，支持密钥外部加密存储。

密钥使用：提供可靠的身份认证机制，确定服务使用者身份及访问权限，可防止服务使用者的数据被恶意访问、篡改、外泄等。服务使用者的密钥数据采用不同的加密密钥保护存储，支持密钥数据逻辑隔离，确保用户在安全 的环境中使用密钥，确保一个用户的信息泄漏不会影响到其他用户，支持根据用户密钥更换周期要求更换密钥。

密钥更新：密钥超过使用期限、已泄漏或存在泄漏风险时，支持根据密钥更新策略进行密钥更新。

密钥归档：对系统历史密钥、被注销密钥进行归档，并对归档密钥进行加密处理再存储。归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息。

密钥备份：执行密钥备份后，同步生成审计信息，包括备份的主体、备份的时间等。

密钥恢复：执行密钥恢复后，同步生成审计信息，包括恢复的主体、恢复的时间等。

密钥销毁：具备用户密钥由于某些原因(暂时不使用、怀疑泄密等)进行密钥销毁。销毁过程不可逆，即无

	<p>法从销毁结果中恢复原密钥。</p> <p>对称密码算法和非对称密码算法由密码机提供对外支持服务，所有的密码运算均在密码机中进行。对称密码在密码机内有相应的索引号和唯一标识，使用时满足密码机的运算操作权限。非对称密码同样有相应的索引号和唯一标识，满足密码机的运算操作权限要求。</p> <p>对于长期保存的密钥，密码机应具备相应的备份/恢复功能。本次项目中采用密码机进行密钥存储和备份，密钥恢复操作只能在密码机中完成。当密钥失效或被泄漏时，密码机可以对指定密钥进行销毁。</p> <p style="text-align: center;">密码服务</p> <p>概述</p> <p>为了保障的信息安全，网络安全和密码安全是建设过程中不可或缺部分，且须通过计算机等级保护和商用密码应用安全性评估三级才能正式交付上线。</p> <p>密码应用软硬件系统的主要作用是为网络中应用或终端用户提供密码服务，如数据加密/解密、签名/验证、摘要运算等通用密码服务，同时结合政策法规、行业要求、安全服务理念，提供如安全认证、时间戳、电子签章、数据加密等更直接、可用的场景化密码应用服务。</p> <p>密码服务功能</p> <p>本项目密码应用建设，严格按照国家《GB/T 39786-2021信息安全技术信息系统密码应用基本要求》中的要求，采用密码技术的数字证书技术，从身份鉴别、数据传输安全、数据存储安全、访问控制信息完整性保护等方面，通过部署安全网关、签名验签服务器、数据库加密网关、服务器密码机、数据库加密网关等密码应用软硬件系统，对云平台和各业务系统进行全面保护。</p> <p>在陕西省公安厅交通管理总队用户域云平台国产化资源池上部署的业务系统均使用密码技术完成应用安全防护。</p> <p>用户使用业务系统使用的密码保护的应用场景，包括身份鉴别、访问控制信息完整性、传输机密性和完整性、存储机密性、存储完整性、不可否认性等。</p> <p>（1）采用密码技术的数字证书、密码模块或者其他认证方式提供身份鉴别服务和访问控制服务；</p> <p>（2）通过密钥管理和数据和文件加密系统，使用SM4算法对存储的重要数据提供安全加解密服务；</p> <p>（3）通过签名验签服务、密码模块等保障重要数据的传输机密性和完整性；通过数字签名服务器和时间戳系统保障操作行为的不可否认性。</p> <p style="text-align: center;">身份鉴别</p> <p>业务系统身份鉴别方式为PC端USBKEY登录业务系统。完成身份鉴别。</p> <p>PC 端登录身份鉴别：</p> <p>PC端用户登录主要包括使用USBKEY和扫码认证进行登录，USBKEY和移动安全中间件分别向CA系统，申请个人数字证书，登录时进行电子签名的身份鉴别；</p> <p>PC端USBKEY登录，PC端使用USBKEY身份认证流程，具体流程图如下：</p>
--	---

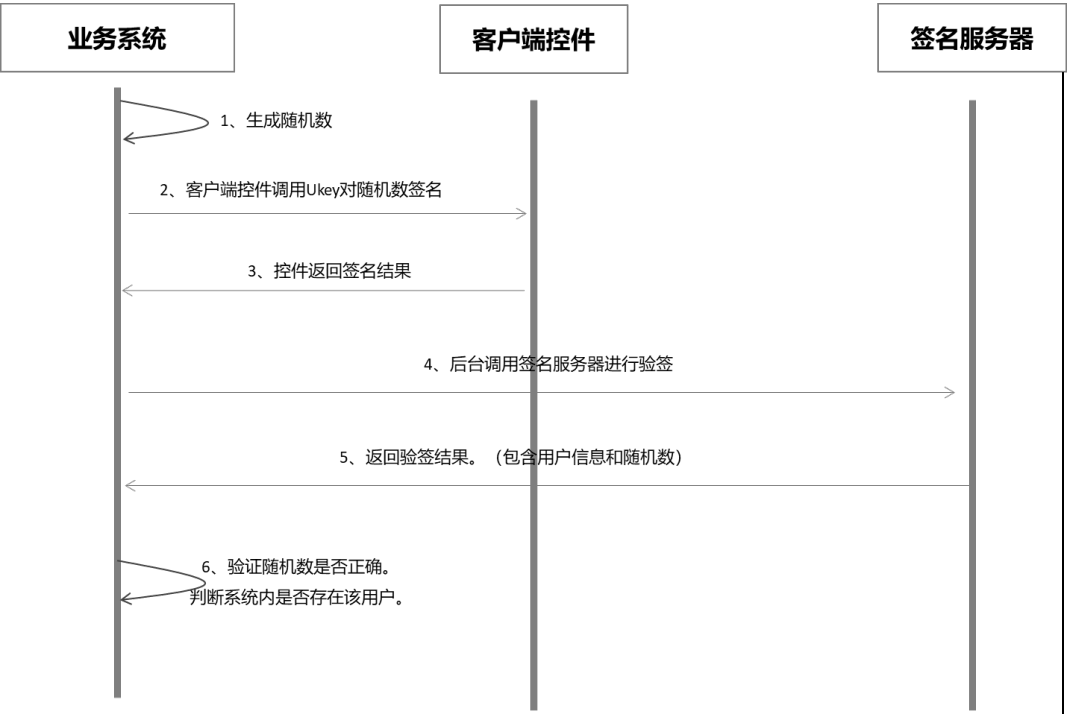


图 521 身份认证流程图

对接流程：

- 1.业务系统登陆页面生成随机数。
- 2.业务系统调用客户端签名控件，通过签名接口调用key对随机数签名。
- 3.签名控件返回签名值。
- 4.业务系统提交签名值给签名服务器进行验签。
- 5.签名服务器返回验签结果。
- 6.业务系统检验用户信息和随机数，一致则跳转登入系统。

访问控制信息完整性

针对业务系统中对重要业务数据在存储的完整性保护方面的需求，提供数据完整性保护服务。系统涉及到的重要数据包括：日志信息以及访问控制信息等，由签名验签服务器提供（HMAC-SM3）算法和基于数字签名的完整性保护算法，保护信息免受非授权实体的篡改或替代。对外提供数据完整性保护服务接口，业务系统可以通过服务接口方式调用服务器密码机数据完整性保护服务。

业务系统

签名验签服务

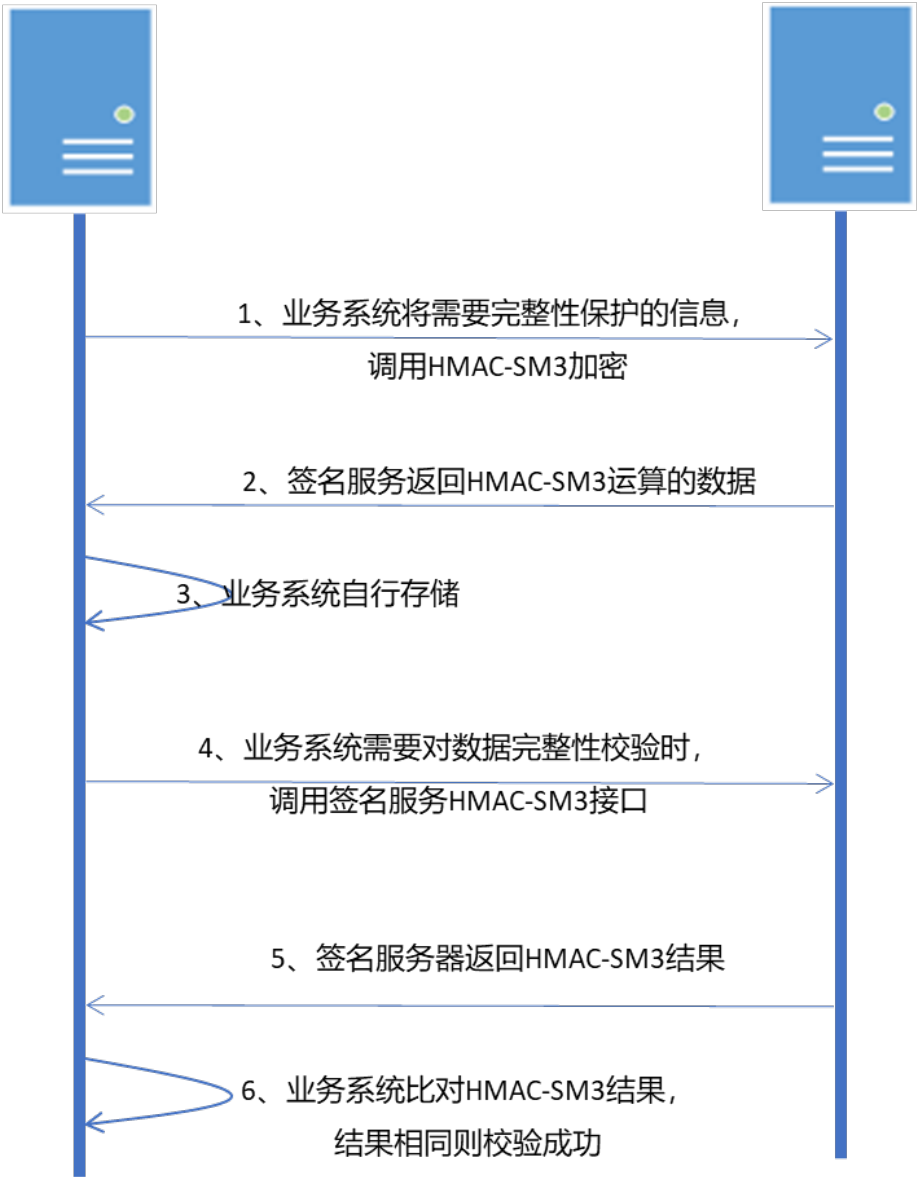


图 522 签名验签流程图

对接流程:

- 1、业务系统调用签名验签服务HMAC-SM3接口对重要数据进行完整性保护，返回的消息鉴别码存入数据库。
- 2、业务系统需要验证重要信息完整性时，调用签名验签服务HMAC-SM3接口对重要数据生成消息鉴别码。
- 3、比对新生成的消息鉴别码和数据库中的值，相同则校验通过。

传输机密性和完整性

在业务应用和数据层，需要对传输数据进行机密性和完整性保护，主要包括身份鉴别信息、访问控制信息、业务敏感信息、个人隐私信息等信息重要信息。在客户端访问时，通过密码模块在本地对敏感数据进行加密保护，上传至后端，服务端的数据通过密码机完成数据解密，这样保障数据传输的机密性和完整性保护。

PC端WEB端数据安全传输工作流程如下：

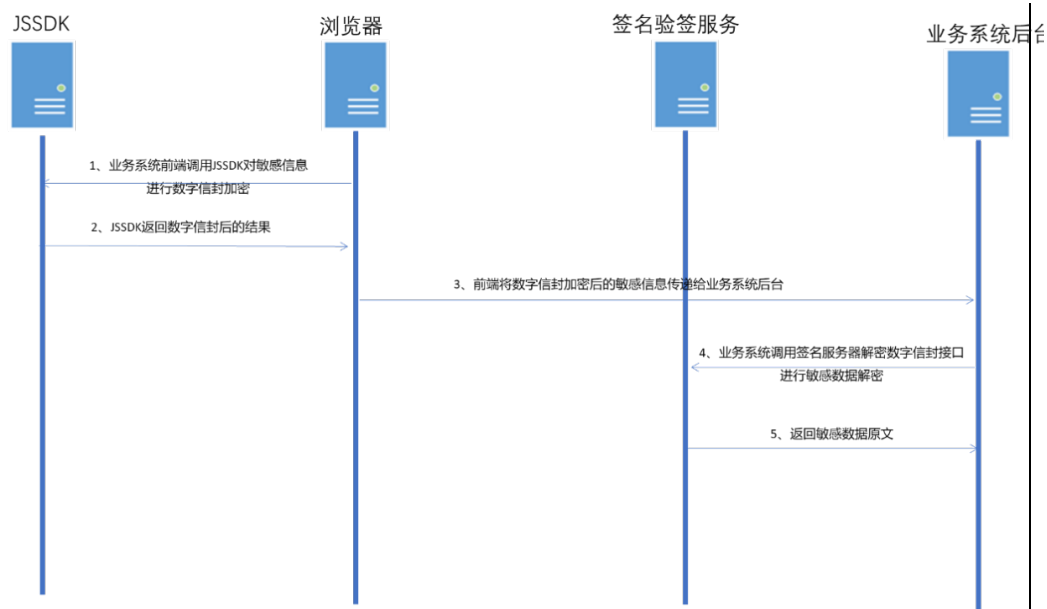


图 523 安全传输工作流程图

具体业务流程如下：

- 1.业务系统前端调用JSSDK对需要传输到后台的敏感数据进行数字信封加密。
- 2.业务系统前端将数字信封加密后的敏感数据传递给业务系统后台。
- 3.业务系统后台调用签名验签服务器进行数字信封解密。

存储机密性

业务系统重要数据存储保护，通过数据加解密服务实现，业务系统应用服务端调用加解密接口，使用基于SM4算法的高性能加解密，对重要关键数据如：敏感公文信息、用户隐私信息、机构信息、重要的文件材料等敏感信息在存储过程中的机密性、完整性保护，防止拖库、被篡改等风险事件发生。

对存储在数据库中的敏感数据如个人敏感信息（姓名、身份证号码等）、警务重要数据等都可通过数据加解密系统实现存储的机密性，防止拖库、被篡改等风险事件发生。

业务系统

数据加解密服务

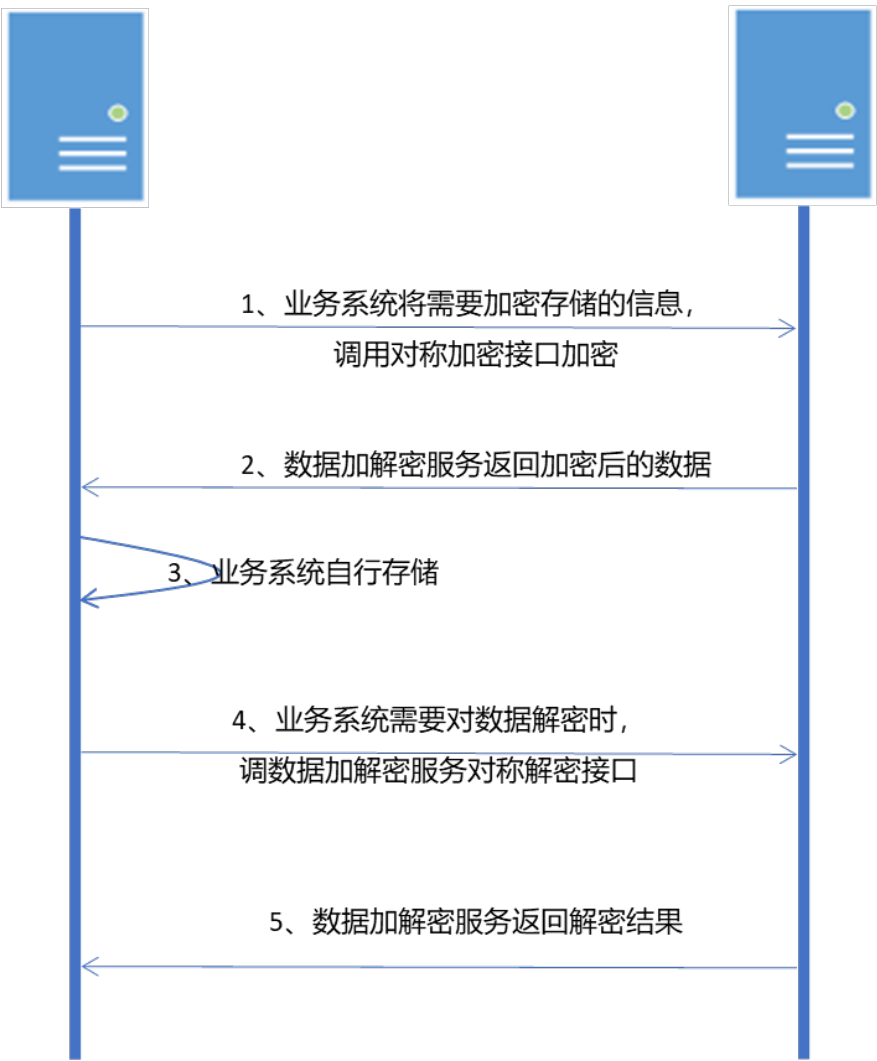


图 524 数据加密流程图

对接流程：

- 1.业务系统调用数据加解密服务对称加密接口对重要数据进行加密存储。
- 2.业务系统需要获取重要数据明文信息时，调用数据加解密系统对称解密接口对重要数据进行解密。

存储完整性

针对业务系统中对重要业务数据在存储的完整性保护方面的需求，提供数据完整性保护服务。系统涉及到的重要数据包括：日志信息以及访问控制信息等，由签名验签服务器提供（HMAC-SM3）算法和基于数字签名的完整性保护算法，保护信息免受非授权实体的篡改或替代。对外提供数据完整性保护服务接口，业务系统可以通过服务接口方式调用服务器密码机数据完整性保护服务。

业务系统

签名验签服务

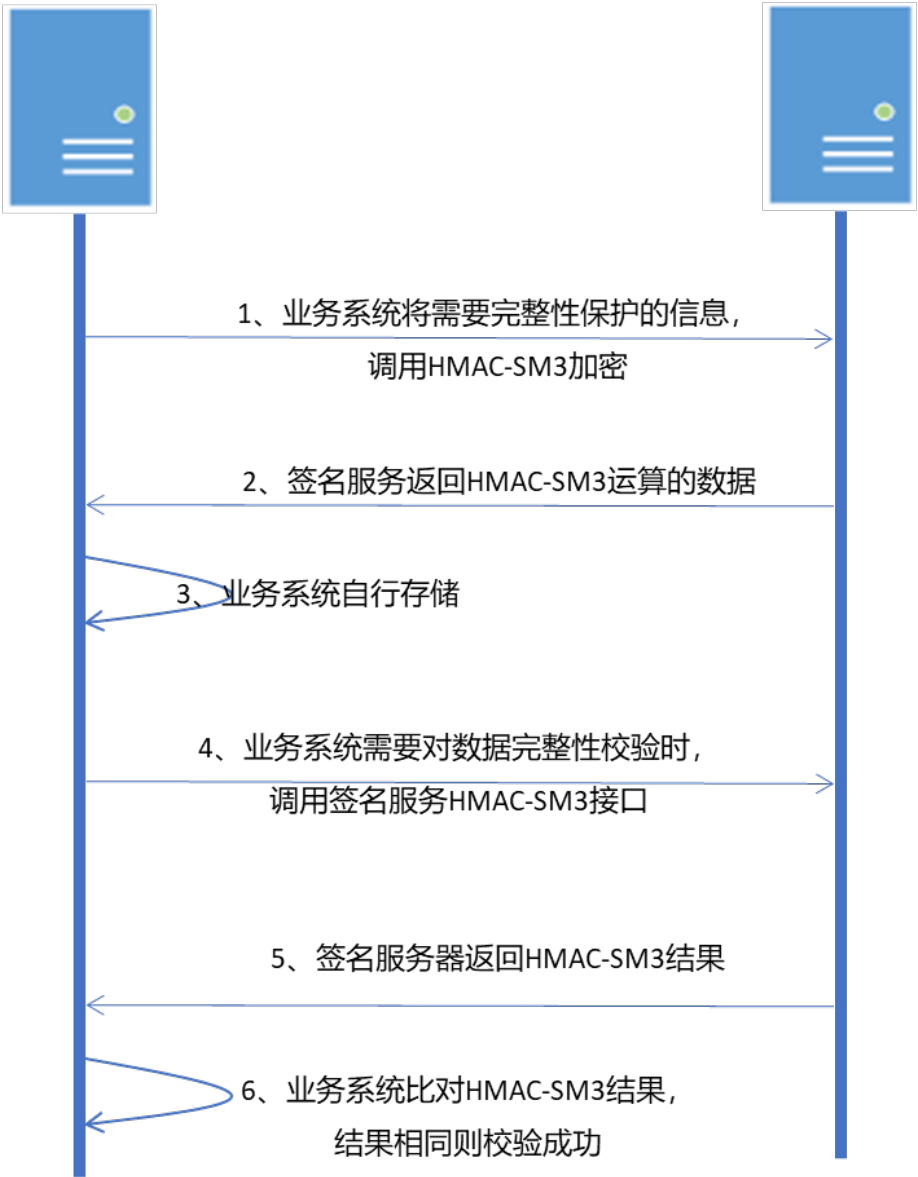


图 525 签名验签流程图

对接流程：

- 1.业务系统调用签名验签服务HMAC-SM3接口对重要数据进行完整性保护，返回的消息鉴别码存入数据库。
- 2.业务系统需要验证重要信息完整性时，调用签名验签服务HMAC-SM3接口对重要数据生成消息鉴别码。
- 3.比对新生成的消息鉴别码和数据库中的值，相同则校验通过。

不可否认性

数字签名

应用系统需要客户端对关键业务数字签名，防止操作被抵赖，应采用签名验签服务，流程如下图所示：

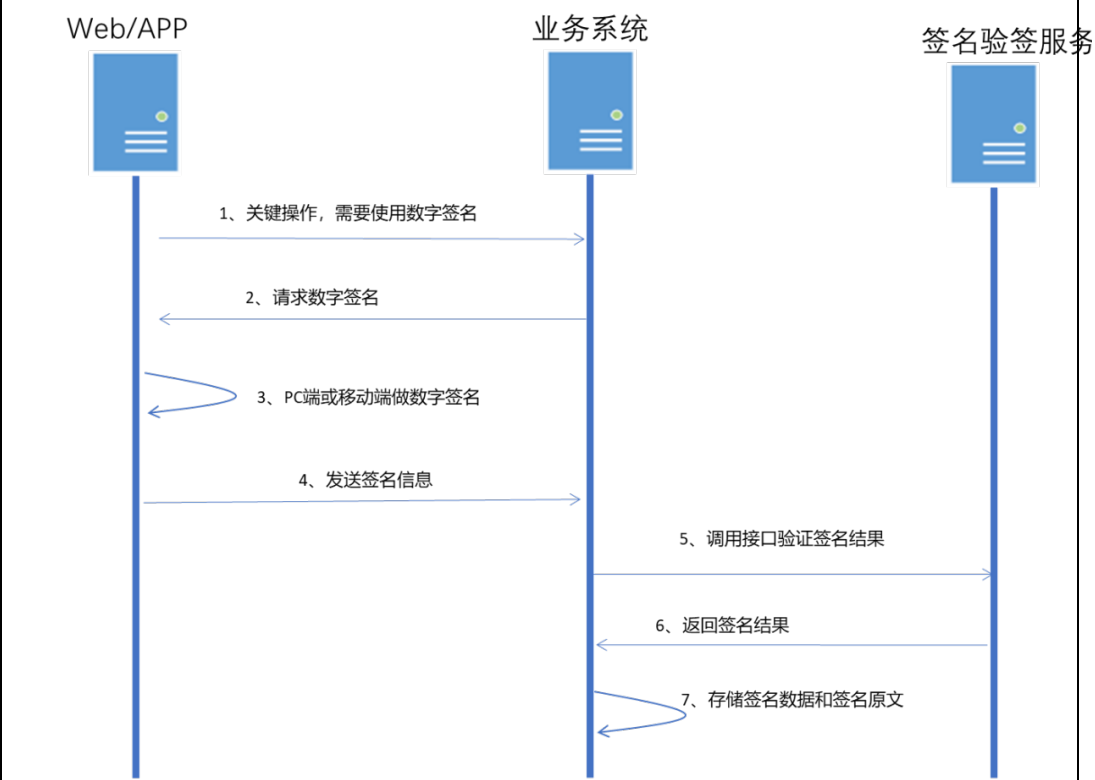


图 526 签名验签流程图

- 1.用户登录业务系统，进行业务操作；
- 2.业务系统判断当前操作是否为关键操作，如果为关键操作，则要求客户端对当前操作产生的关键数据做数字签名；
- 3.客户端调用USBKEY或移动端数字证书对关键数据做数字签名；
- 4.应用系统接收客户端签名数据，并发送到签名验签服务系统进行验证；
- 5.签名验签服务系统对签名数据进行验证，并将验证结果返回给应用系统；
- 6.应用系统根据返回的验证结果，确认客户端的签名是否有效。如果有效，将签名后数据、验证结果存入数据库；如果签名无效，则将错误信息返回给客户端，进行下一步业务处理。

安全与合规性分析

根据政策法规、标准规范，针对本项目安全需求的满足情况进行分析自查，情况如下：

表 5-4密码应用合规性对照表

指标要求	密码技术应用点	采取措施	标准符合性 (符合/不适用)	说明（针对不适用项说明原因及替代性措施）
	身份鉴别	在机房部署符合要求的国密安全电子门禁系统，实现门禁卡的“一卡一密”，实现人员的身份鉴别，并实现对电子门禁进出记录数据的完整性保护。	符合	无

	物理和环境安全	电子门禁记录数据完整性	在机房部署符合要求的数据库加密网关，提供SM2/SM3 签名验签服务对电子门禁系统数据进行完整性保护。	符合	无
		视频记录数据完整性	在机房部署符合要求的数据库加密网关，提供SM2/SM3签名验签服务对视频系统数据进行完整性保护。	符合	有
		密码模块实现	采用的密码产品达到GB/T 37092二级的安全要求。	符合	无
	网络和通信安全	身份鉴别	在手机、电脑、平板等业务端采用国密软件密码模块，完成移动业务端APP、PC业务端登录业务系统用户的安全身份鉴别，防止非授权人员登录。	符合	无
		安全接入认证	在电脑或移动客户端安装国密软件密码模块，完成设备接入认证和VPN通道加密功能，完成接入认证和准入控制	符合	无
		访问控制信息完整性	通过签名验签服务器提供签名验签API接口，对访问控制信息进行签名，确保数据的完整性。	符合	无
		通信数据完整性	在电脑或移动客户端安装国密软件密码模块，建立安全传输通道，实现通信数据的机密性和完整性；	符合	无

		通信数据机密性	在电脑或移动客户端安装国密软件密码模块，建立安全传输通道，实现通信数据的机密性和完整性；	符合	无
		集中管理通道安全	在电脑或移动客户端安装国密软件密码模块，建立安全传输通道，	符合	无
		密码模块实现	采用的密码产品达到GB/T 37092二级的安全要求。	符合	无
	设备和计算安全	身份鉴别	终端设备安装国密软件密码模块完成设备自身认证，实现用户身份鉴别	符合	无
		远程管理身份鉴别信息机密性	通过终端软件密码模块和接入认证网关之间建立SSL VPN 加密通道，实现身份鉴别和机密性保护	符合	无
		访问控制信息完整性	通过签名验签服务器提供签名验签API接口，对访问控制信息进行签名，实现数据的完整性。	符合	无
		敏感标记的完整性	通过签名验签服务器提供签名验签API接口，对敏感标记信息进行签名，实现数据的完整性。	符合	无
		日志记录完整性	通过签名验签服务器提供签名验签API接口，对日志记录信息进行签名，实现数据的完整性。	符合	无
		重要程序或文件完整性	通过签名验签服务器提供签名验签API接口，对重要程序和文件完整性信息进行签名，确保数据的完整性	符合	无

		密码模块实现	采用的密码产品达到GB/T 37092二级的安全要求。	符合	无
		身份鉴别	在手机、电脑、平板等业务端采用国密软件密码模块，完成移动业务端APP、PC业务端登录业务系统用户的安全身份鉴别，防止非授权人员登录。	符合	有（复用）
		访问控制信息和敏感标记完整性	通过签名验签服务器提供签名验签API接口，对访问控制信息和敏感标记进行签名，确保数据的完整性	符合	无
		数据传输机密性	通过终端软件密码模块和接入认证网关之间建立SSL VPN 加密通道，实现身份鉴别和机密性保护	符合	无
		数据存储机密性	部署签名验签服务器和服务器密码机，提供SM4 加密服务、密钥管理服务，对存储数据进行加密	符合	无
	应用和数据安全	数据传输完整性	通过终端软件密码模块和接入认证网关之间建立SSL VPN加密通道，实现数据完整性保护	符合	无
		数据存储完整性	通过云签名验签服务器签名验签API接口，实现敏感数据存储的机密性、完整性保护	符合	无
		日志记录完整性	通过云签名验签服务器签名验签API接口，实现日志记录数据存储的完整性保护	符合	无

重要应用程序的加载和卸载	通过签名验签服务器 签名验签API接口，对 重要程序进行签名保 护	符合	无
抗抵赖	密码签名验签服务器 提供签名验签服务， 实现数据的不可否认 性。	符合	无
密码模块实现	采用的密码产品达到G B/T 37092 二级的安 全要求。	符合	无

密码应用对接方案

登录现状

B/S架构登录现状

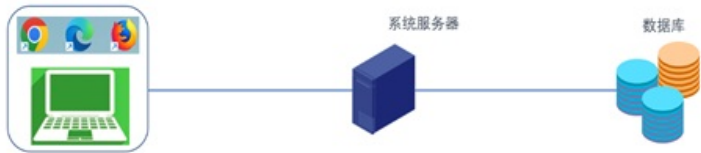


图 527 登录现状图

如图所示，对于B/S架构的信息系统，当前PC客户端（浏览器）采用“用户名+口令”方式登录。

系统网关对接

按照密评要求，应用系统登录方式需采用数字证书登录方式，所以“用户名+口令”的登录方式需要做改变

应用系统登录方式改造

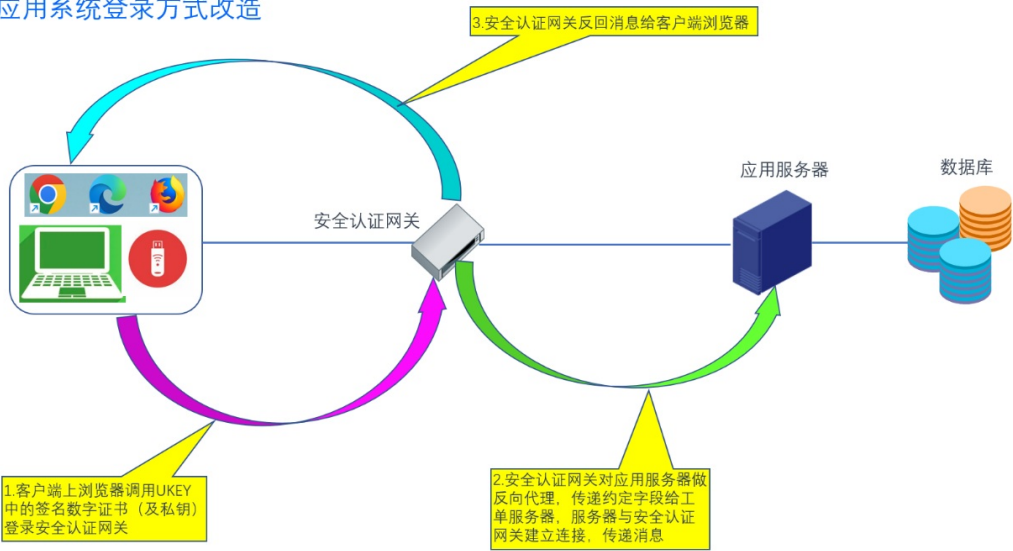


图 五27 应用系统登录方式改造图

在应用服务器前部署一台安全认证网关，后续PC客户端（浏览器）都需要通过该安全认证网关登录应用服务器；

对接网关后，应用服务器推送PC客户端（浏览器）的登录界面不再是“用户名+口令”的方式，而是让选择数字证书的方式，对接前后举例如下：

对接前登录



图 529 对接前登录界面

对接后登录



图 530 对接后登录界面

网关识别数字证书并确认合法后，给服务器发送登录指令，服务器收到登录指令后，建立与网关的连接，登录步骤如下：

1. 客户端上浏览器调用UKEY中的签名数字证书（及私钥）登录安全认证网关；Ukey插入PC机，会安装驱动，告诉操作系统和浏览器，数字证书的存储位置；
2. 安全认证网关对应用服务器做反向代理，传递约定字段给各应用系统，各应用系统与安全认证网关建立连接，传递消息；
3. 安全认证网关返回消息给客户端；

结构化数据加密与完整性保护

签名验签服务对接

结构化数据完整性改造

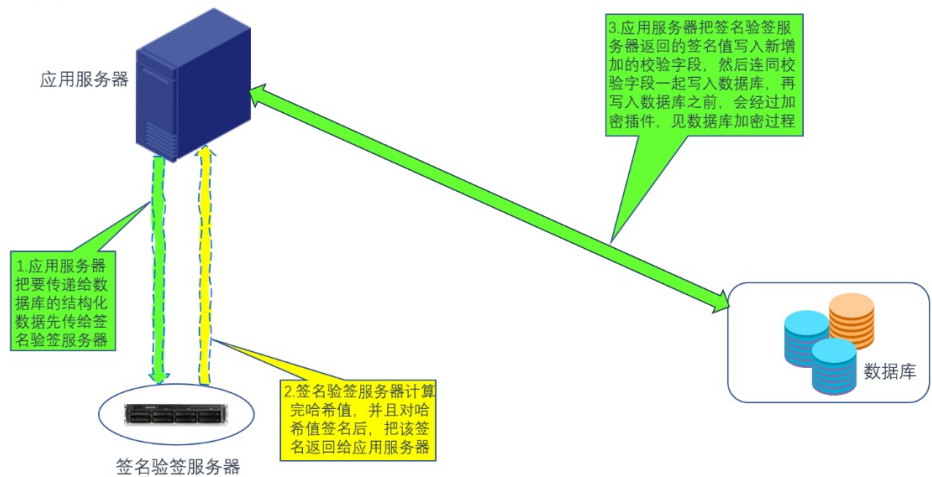


图 531 结构化数据完整性改造图

在本次密码建设中，签名验签服务组件主要完成关键数据完整性保护，本系统的关键数据都是数据库中的结构化数据，假设一张人员信息表，举例说明如下：

表有6个字段：

表 5-5 人员信息举例表

序号	姓名	性别	信箱	身份证	电话号
1	张三	男	123@qq	610.....2121	1390.....
2	李四	女	345@qq	610.....1212	1380.....

如果张三的信息被非法篡改，系统是无法感知的，纵使对数据库磁盘、整库、整表或者某字段进行加密，仍无法阻止信息的篡改：把上表中内容都加密，虽然非法入侵无法识别具体内容，但不妨碍对密文进行篡改，或者把李四的电话号和张三互调等动作。

对接签名验签服务后增加一个校验值字段：

表 5-6 校验后字段表

序号	姓名	性别	信箱	身份证	电话号	校验字段
1	张三	男	123@qq	610.....2121	1390.....	\$&)>?~!3
2	李四	女	345@qq	610.....1212	1380.....	%)?>8rt&

合规途径：每次对张三信息进行修改时，都会调用签名验签服务器，把张三整行（或者定义好的某几个字段）的信息传入签名验签服务组件，签名验签服务组件会对整行信息进行哈希运算得出一个哈希值，接着签名验签服务器会对此哈希值进行加密（加密后的内容称为签名），再把该签名值返回给应用系统；应用系统把签名值填入张三的校验字段；

下次读取张三信息时，应用系统从数据库拿到张三这一行的数据，把除校验字段外的整行信息传入签名验签服务组件，和上述步骤一样，签名验签服务组件做完哈希和加密，把签名值返回应用系统，应用系统会用返回的签名值和检验字段现有的签名值比对，如果一致则继续下一步；如果不一致，则说明张三的信息被非法篡改过，可以给出提示；

总结如下：

通过应用系统合法的新增行或者对现有行的数据修改，按照程序设定都会执行调用签名验签服务器的动作，并且在校验字段填入校验值（就是签名验签服务器返回的签名值），读取的时候也会有相应的动作，确保数据完整性；

如果非法入侵数据库直接修改张三的信息，就无法触发应用系统调用签名验签服务器的动作，虽然把张三

的手机号修改了，但校验字段无法获得，后续系统在读取张三信息时候，就会发现错误。

注：纵使人工把张三的信息全部拿出，计算哈希也没用，因为无法获得签名验签服务器的私钥，就无法对这个哈希值进行合法加密，用其他密钥加密，等应用系统按照流程读取张三信息时，签名验签服务器就会发现不是自己的私钥加密的数值，从而报错。

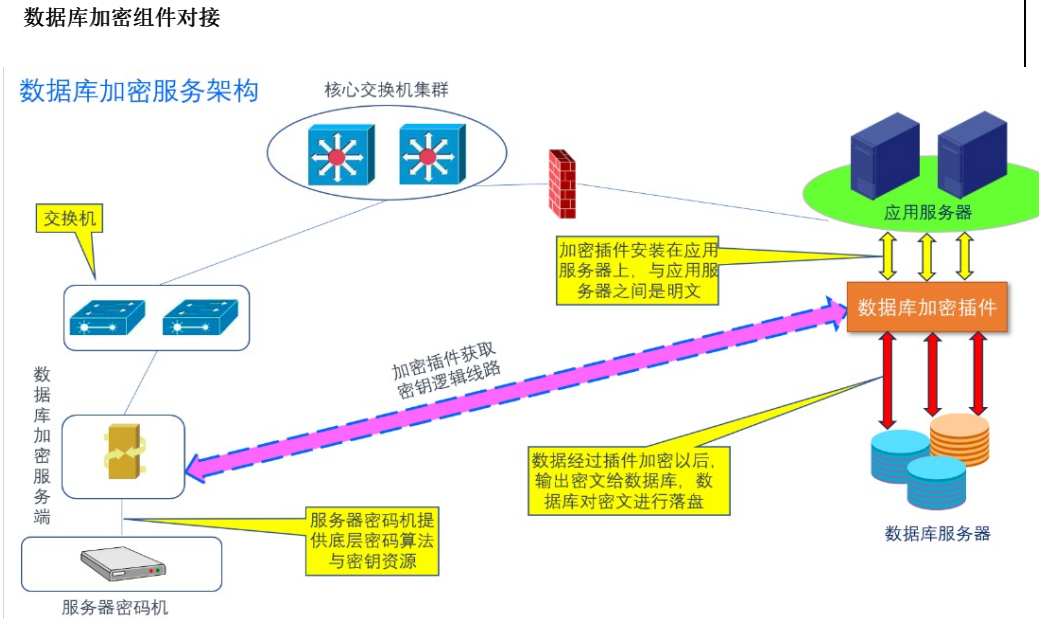


图 532 数据库加密服务架构图

在应用服务器上安装数据库加密插件，该插件先于JDBC捕获SQL语句，然后根据事先的定义进行判断，对需要加密的字段进行加密，加密过程对应用系统是透明的；

读取数据时所有数据也会经过数据库加密插件，根据事先定义的规则进行判断，明文直接放行，密文进行解密后放行。

非结构化数据加密对接

文件加密组件会在服务器上虚拟出一个磁盘（假设盘符为H），H盘是虚拟盘（无真正存储空间），需要和服务器本地一个磁盘关联，假设为F盘；无论以前非结构化数据存储的位置在哪里，对接后要把以前的非结构化数据存储存储在虚拟的H盘中，只要进入H盘的任何数据都会被文件加密网关自动加密并且落入F盘，如此完成对接和调用，就相当于对非结构化数据进行了加密，如下图所示：

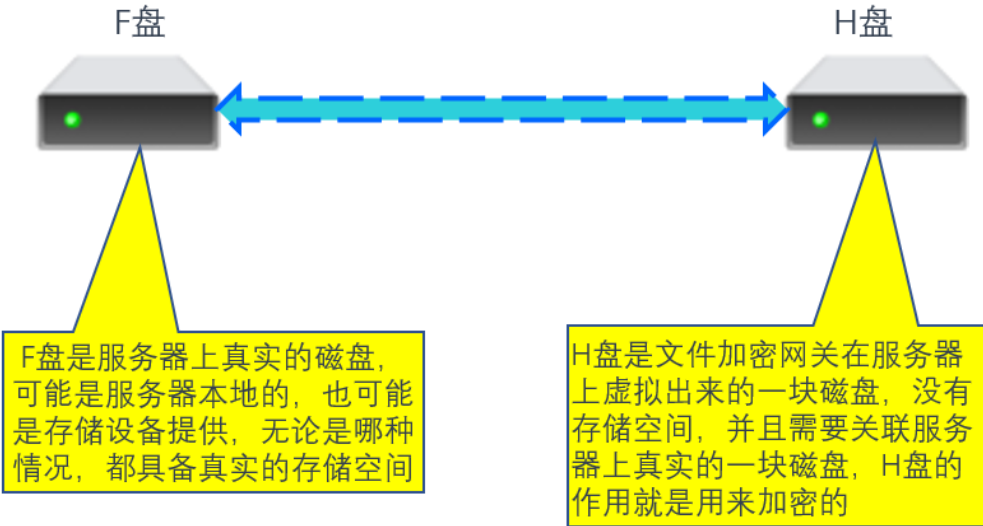


图 533 非结构化数据加密对接图

对应某个文件，如果拷入F盘，就和正常情况一样，就是明文；如果拷入H盘，虽然最终还是存储在F盘中

，但此时从F盘看到的就是加密后的文件，从F盘无法正常读取；只有从H盘读取，才会有解密过程，才能看到明文。

安全管理方案

管理组织架构

密码安全小组

依据《信息安全技术 信息系统密码应用基本要求》GB/T 39786-2021 中对密码管理以及人员的要求，建立密码安全管理小组，密码安全管理组依托于本机关内安全管理小组进行人员的重新设定、复用等建立。建立人员组织框架如下：

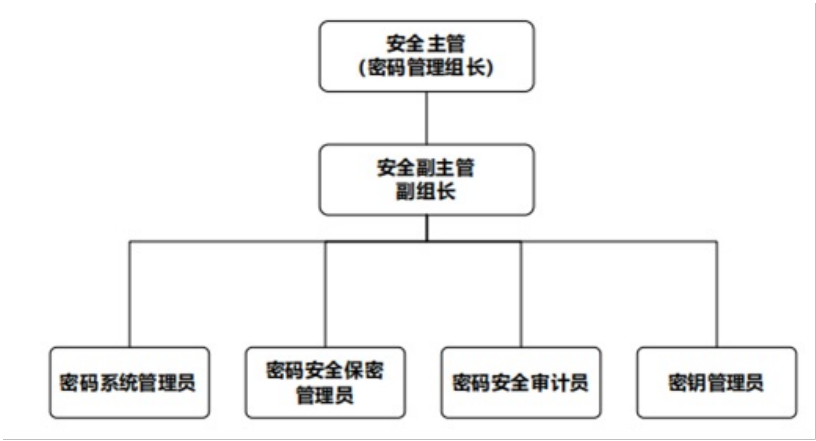


图 534 密码安全小组

管理组织职责

管理组织职责如下：本管理小组主要负责设密码项目的规划建设(包括方案设计、组织专家评估等)、密码评估配合、密码设备维护、密码人员职责设定和人员管理等职能。

管理岗位设定

密码小组人员职责如下：

密码系统管理员职责：制定严格的规章制度并认真执行。建立完善的变更管理审核和批准制度，对任何可能影响系统正常运行的密码软硬件变更，包括更改设置、软硬件升级等，应及时登记报备。

密码安全保密管理员职责：负责系统密码安全策略的制定与配置；负责定期进行安全检查，检查内容包括系统正常运行、系统漏洞和数据备份等情况；安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

密码安全审计员职责：负责定期对系统管理员、安全管理员、业务操作员等的操作行为进行安全审计和监督检查，及时发现违规行为等。

密钥管理人员职责：负责对应应用系统密钥的保管、监督、变更、撤销等操作，包括对密钥的生成、存储、分发、导入导出、使用、备份恢复、归档、销毁等全生命周期的管理。

管理制度体系

商用密码安全管理制度

总则

为了加强密码设备管理工作，确保安全使用密码，根据《中华人民共和国密码法》、《密码管理条例》、《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）等国家有关法规规定，制定本制度。单位涉及密码管理、使用和运维等相关人员均需遵守本规定。

第一章 密码建设要求

信息系统密码建设应符合密码相关法律与行业相关政策要求进行建设。

	<p>统筹系统密码应用，应与业务系统统一设计，同步规划、同步建设、同步运行密码保障系统并定期进行评估。</p> <p>信息系统规划阶段，依据相关标准，制定密码引用方案， 组织专家进行评审，评审意见作为项目规划立项重要材料。通过专家审定后的方案应作为建设、验收和测评的重要依据。</p> <p>对未及时开展密码建设的系统， 应逐步完成密码建设的备案、整改、测评等工作。</p> <p>密码建设产品应当采用符合国家密码管理部门核准的密码产品、许可的密码服务，产品应具备最新商用密码产品型号证书的产品。</p> <p>第二章 密码运行要求</p> <p>信息系统投入前，应经过密码测评机构进行安全性评估，评估通过方可投入正式运行。</p> <p>信息系统投入运行后，本单位主管责任人应委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；如若有重大安全隐患，应停止系统运行，制定整改方案，整改完成并通过后方可投入运行。</p> <p>第三章 密码人员管理要求</p> <p>结合系统分析、风险分析和安全需求分析的结果，明确安全管理人员。</p> <p>结合系统建设具体现状明确本管理机构内密码管理人员组成与职能，明确管理责任，做到责任到部门责任到人。</p> <p>根据密码管理政策、数据安全保密政策， 结合本组织实际情况，设立密钥管理员、密码系统管理员、密码安全保密管理员，以及密码安全审计员。</p> <p>相互制约相互监督，关键设备的管理和使用账号不得多人共用。</p> <p>建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度。</p> <p>建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训。</p> <p>建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。</p> <p>第四章 密码使用责任要求</p> <p>密码使用单位应当建立密码管理责任人，落实信息系统密码应用工作。</p> <p>密码使用单位应严格遵循相关要求使用密码技术完善系统的安全保护功能，因密码使用不当导致信息泄密、数据破坏的，追究相关单位密码管理部门和管理人员责任，并按要求整改。</p> <p>本单位应当严格遵守相关保密制度，保管好个人数字证书，不得出借或使用他人证书登录信息系统平台。</p> <p>个人数字证书介质一旦丢失，应立即进行挂失，并按规定流程到证书发放机构申请新的证书和介质。</p> <p>第五章 密码设备维护规定</p> <p>密码设备维护人员需经过培训，取得相关资质才能上岗，并需严格按照设备维护规范和使用说明开展维护工作。</p> <p>密码设备应当按照要求定期完成设备巡检、升级和维保工作，至少每半年集中检查一次，密码设备操作必须经过授权，且不得接入互联网访问。</p> <p>建立密码设备故障和应急保障机制，定期开展应急演练，确保设备发生故障能及时上报、恢复。事件处理完成后及时向同级密码负责人报告事件发生情况和处理办法。</p> <p>加强密码设备的日常监控，评估系统安全风险，及时进行扩容和升级。</p> <p>商用密码人员管理制度</p> <p>依据本机关《商用密码安全管理制度》设立本管理制度，主要用于对人员的相关合规性要求、培训、奖惩制度的说明和建立。</p> <p>第一章 总章</p> <p>第一条 密码人员应了解并遵守密码相关法律法规。</p> <p>第二条 在岗密码人员应能够正确、合理使用密码产品。</p> <p>第二章 密码人员岗位与职责</p>
--	--

第三条 结合系统分析、风险分析和安全需求分析的结果，明确安全管理人员。

第四条 结合系统建设具体现状明确本管理机构内密码管理人员组成与职能，明确管理责任，做到责任到部门责任到人。

第五条 建立密码系统管理员、密码安全保密管理员，以及密码安全审计员，并制定规范边界任务。

第六条 密码系统管理员职责。

制定严格的规章制度并认真执行。建立完善的变更管理审核和批准制度，对任何可能影响系统正常运行的密码软硬件变更，包括更改设置、软硬件升级等，应及时登记报备。

第七条 密码安全保密管理员职责。

负责系统密码安全策略的制定与配置；负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等。

第八条 密码安全审计员职责。

负责定期对系统管理员、安全管理员、业务操作员等的操作行为进行安全审计和监督检查，及时发现违规行为等。

第九条 密钥管理人员职责。

负责对应用系统密钥的保管、监督、变更、撤销等操作，包括对密钥的生成、存储、分发、导入导出、使用、备份恢复、归档、销毁等全生命周期的管理。

第三章 密码人员培训规范

第十条 制定密码人员学习管理制度。

制定密码人员学习、培训档案 管理、培训考核等相关制度要求。

第十一条 培训管理。

定期参与陕西省密码管理局开展的密码培训会议。建立本机关内密码培训工作档案，记录包括培训范围、培训方式、培训内容、培训人数、培训时间和其他情况。

第十二条 人员档案管理。

建立针对密码管理人员建立员工培训档案，接受培训的具体情况和培训结果应详细记录备案，包括培训时间、培训地点、培训内容、培训目的以及培训效果。

第十三条 培训档案管理。

应对培训过程进行记录保存，培训资料应以纸质、电子文档、录音、录像等形式记录保存， 并通过口令或专用加密软件加密保存至专用存储设备(如 U 盘、移动硬盘、NAS 服务器等，纸质应单独文件柜) 统一管理，培训档案留存时间应保存五年，五年后可销毁。

第十四条 日常工作应用。

针对密码人员的日常工作进行评估，针对培训填写“课程评估调查表”，对商用密码管理人员是否具备工作改善成果或方案进行调查。

第四章 密码人员考核与奖惩

第十五条 依托本机关人员绩效考核管理制度，制定密码人员考核管理办法。

第十六条 依据测评机构、省密码管理局、国家密码管理局的定期检查、抽查结果作为基本考核单元。对重大隐患、系统测评问题应及时上报处理、备案。

第十七条 定期针对业务系统开展密码使用情况年度自查，并纳入责任单位相关人员考核。

第十八条 在当年密码应用考核中被处理的，原则上取消当年评优评先资格。

第十九条 在当年密码应用考核中表现突出的，依托本机关人员绩效考核管理制度酌情予以表彰、评优评先。

密钥管理制度

本单位依据《商用密码安全管理制度》设定对密钥管理的相关管理制度。管理内容包括对密钥的生成、存

储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理和策略制定的全过程。

《密钥管理制度》

第一条 密钥生成

本单位所使用的密钥生成使用的随机数均符合《GM/T 0005》要求，密钥均在符合 GM/T 0028 的密码模块中产生；密钥均在密码模块内部产生，不会以明文方式出现在密码模块之外；密码模块均具备检查和剔除弱密钥的能力。

第二条 密钥存储

本单位所使用的密钥均采用加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥均存储在符合 GM/T 0028 的二级及以上密码模块中。

第三条 密钥分发

本单位在密钥分发时均采取身份鉴别、数据完整性、数据机密性等安全措施，均能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

第四条 密钥导入与导出

本单位已采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

第五条 密钥使用

本单位在密钥使用时已明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前均对其进行验证；均有安全措施防止密钥的泄漏和替换；密钥泄漏时，立即停止使用，并启动相应的应急处理和响应措施。密钥使用时均按照密钥更换周期要求更换密钥；已采取有效的安全措施，保证密钥更换时的安全性。

第六条 密钥备份与恢复

本单位已制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

第七条 密钥归档

本单位已采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

第八条 密钥销毁

本单位已具有在紧急情况下销毁密钥的措施。

密码安全操作规范

《密码安全操作规范》

第一章 密码设备安全操作规范

第一条 认真执行岗位责任制和相关规章制度

第二条 严格遵守安全操作规程，保证密码设备的安全运行。

第三条 及时准确地填写各项原始记录和统计报表，并及时反馈密码设备存在的问题。

第四条 密码设备操作人员必须经过培训，并留存培训记录。

第五条 密码设备操作应由密码操作人员进行，禁止任何非专业人员对机房设备进行任何操作。

第六条 密码设备操作应严格遵守相关规章制度和操作规范。

第七条 密码设备操作应由两人或两人以上互相监督操作运行，确保操作正确。

第八条 密码设备操作前应检查，操作后应查看策略，确保业务能够正常运行。

第九条 对于可能影响业务的操作，操作前需要提前进行测试，或在专业人员配合下操作，确保安全后方可执行。

第十条 严禁在各密码设备或管理客户端上安装一切与操作无关的软件。

第十一条 严禁将来历不明的移动存储介质(含光盘、磁盘、优盘等)在密码设备、管理客户端上使用。

第十二条 操作时若需要连接笔记本电脑操作，应制定操作密码专用笔记本进行操作，专用笔记本应由专人保管，并设置复杂度较高的口令，由操作人员进行管理。设备应严禁安装与操作无关的任何软件等。操作专用笔记本禁止连接外网；专用笔记本电脑应当安装防病毒软件并定期更新，更新时应使用优盘通过补丁进行更新，确保系统安全。

第十三条 厂家人员操作，应用相关技术人员全程陪同监督。

第十四条 若需要远程操作，应由相关人员提出申请，经审批后方可执行。厂家人员远程操作，应确保两人及以上同时进行远程操作，同时由相关技术人员陪同并得到证实。

第二章 密码口令类

第十五条 密码设置应具有安全性和保密性，不得使用设备初始密码。不得使用名字、生日，重复、顺序、规律数字等容易猜测的数字和字符串。

第十六条 系统维护密码应至少由两人共同设置、保管和使用，不得记录在可容易获取到的位置，如不能防止在客户端电脑、笔记本上。

第十七条 系统维护密码应定期修改，时间间隔不得超过三个月，如发现或怀疑密码遗失或泄漏应立即修改，并详细记录用户名、修改时间、修改人等。

第十八条 禁止非工作人员操作网关系统主机，不使用网关时，应注意锁屏。

第十九条 重要系统或设备的用户应设置不同权限，超级管理员(可定义用户修改、查看权限等)、一般管理员(只能修改、操作或查看权限等)。超级管理员应指定专人管理，确保系统安全性。新增管理员应经过领导或密码小组批准方可执行。

第二十条 所有密码不得外泄。

第二十一条 系统密码人员调离工作岗位后，应立即更改密码。

第三章 密码证书类

第二十二条 在申请数字证书时应提供真实、完整、准确的身份信息和其他相关信息，并在这些信息变更时及时到与密码小组管理员沟通变更手续。

第二十三条 获取数字证书时，应当使用安全的工具产生并存储私钥及证书，比如使用 USB Key 来存储数字证书；使用完 USB Key 后应立即将其从电脑上拔出，不要将 USB Key 长时间留在电脑上；不使用已被证实产生弱私钥的工具来产生私钥。

第二十四条 设置密码时，避免设置与个人资料相关的简单密码，如身份证号码、出生日期、电话号码等，应定期更改密码。

第二十五条 务必妥善保管数字证书使用密码及存储数字证书的 USB Key 设备，防止机密信息泄漏或被他人窃取；如果数字证书遗失，或者发现相关的密码泄漏，务必及时到申请网点办理挂失手续并按照规定重新办理证书和/或设置密码。

第二十六条 避免在公共场所或他人计算机上使用数字证书。

第二十七条 在使用数字证书的电脑上要及时安装操作系统和浏览器的最新安全补丁，提高系统安全性；安装个人防火墙，防止他人的非法访问和恶意攻击；安装并定期更新防病毒软件，防止受到新病毒的侵害；切勿在使用数字证书的电脑上随意登录不明网站，下载、安装不明软件或运行不明程序。

管理流程设计

密码管理流程

密码管理流程如下图所示：

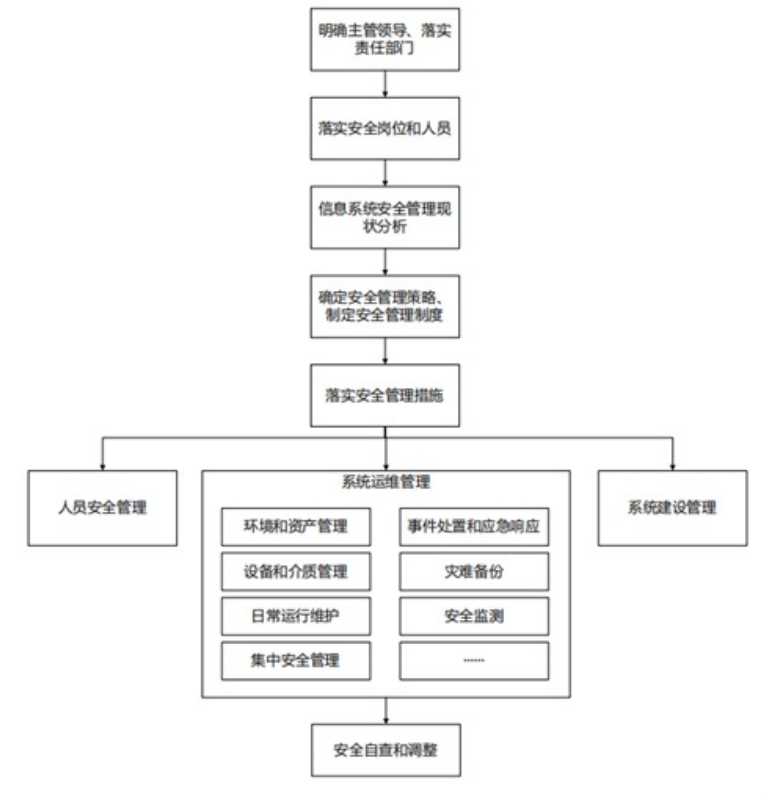


图 535密码管理流程

密码系统建设流程

表 5-7密码系统建设流程表

序号	建设过程	描述
1.	项目启动	在密码管理组长的指导下，确定项目建设目标和项目组织结构，并确定项目里程碑计划及交付物后，召开项目启动会议，填写项目启动申请表，完成项目启动。
2.	项目过程管理	项目启动后，实施过程中实行日报制度，对每个自然天内的工作情况进行记录；每周实行周报制度，对本周内的工作进行记录、总结、分析，提出需要外部协调解决的问题。每两周召开一次周例会，对本阶段的项目工作进行总结，对资源、风险、问题、质量等项目情况进行分析，形成周例会会议纪要；每月底召开一次月例会，总结本月内工作完成情况，进度控制情况，并对本月内所有的风险和问题处理情况进行统计，并与主管部门、建设单位进行沟通。
3.	项目问题管理	项目组对发现的风险和问题，由项目经理协调解决，项目经理持续关注项目风险和问题的状态，每周更新《项目周报》中的风险与问题跟踪表，每月底更新《项目计划与跟踪表》中的风险和问题管理信息。
4.	项目文档管理	项目文档参照 CMMI3 级标准编写，项目文档在评审完成后，及时进行归档，待项目完成时统一进行提交。
5.	方案设计	在对业务系统充分调研的基础上，梳理系统在终端、网络接入、应用系统和运维管理方面的安全问题和需求，完成密码应用解决方案，该方案需要通过专家评审。
6.	系统开发	根据方案设计，完成涉及到的密码应用需求的功能、中间件开发。

7.	工程实施	完成涉及到的密码设备的部署与安装
8.	联调	完成密码设备与试点应用系统联调工作
9.	测试验收	第三方测试单位对系统进行安全性测试，并出具安全性测试报告； 制定验收方案并完成系统验收工作；
10.	系统交付	制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，对系统运行维护技术人员进行相应的 技能培训，并按照管理规定的要求完成系统交付工作；
11.	等级测评	在系统运行过程中，选择具有国家相关技术资质和安全资质的 测评单位进行等级测评，至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；在系统发生变 更时及时对系统进行等级测评，发现级别发生变化的及时调整 级别并进行安全改造，发现不符合相应等级保护标准要求的及 时整改。

密码实施流程

表 5-8密码实施流程

序号	工作内容	任务分工	实施主体	责任单位	阶段交付物
1	密码产品和软件采购	密码产品采购	项目实施方	项目实施方	采购合同
2	密码产品到货验收	安全认证网关、服务器 密码机等密码应用软硬件设备到货验收 其他设备到货验收	项目实施方	国密厂商	到货验收单
3	密码产品部署	安全认证网关安装部署 签名验签、数据库加密 网关、密码机安装部署 相关密码应用软件系统 安装部署 其他设备安装部署	国密厂商 项目实施方	项目实施方	《密码产品实施手册》、《密码产品开发对接手册》
4	系统集成	各密码产品配置	项目实施方	项目实施方	各产品配置信息
5	综合调试	综合系统调试	项目实施方	项目实施方	《联调测试报告》
6	上线试运行	上线试运行	项目实施方	项目实施方	《试运行报告》
7	项目验收	项目验收	项目实施方	项目实施方	《项目验收报告》

密码应急响应流程

密码应急响应流程如下图所示：

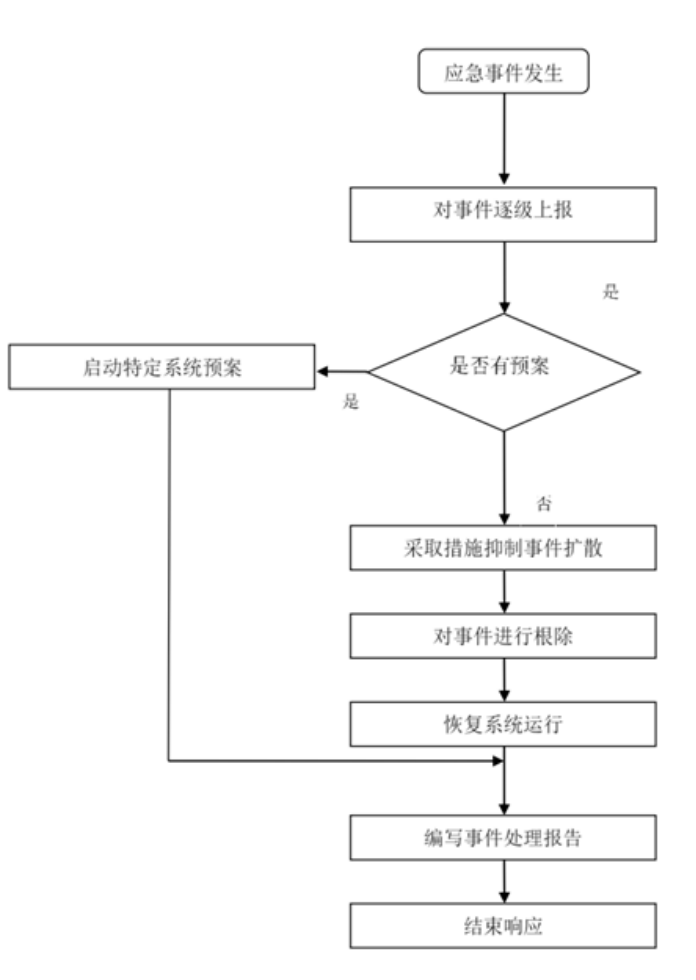


图 536 密码应急响应流程

人员管理流程

人员管理流程如下图所示：

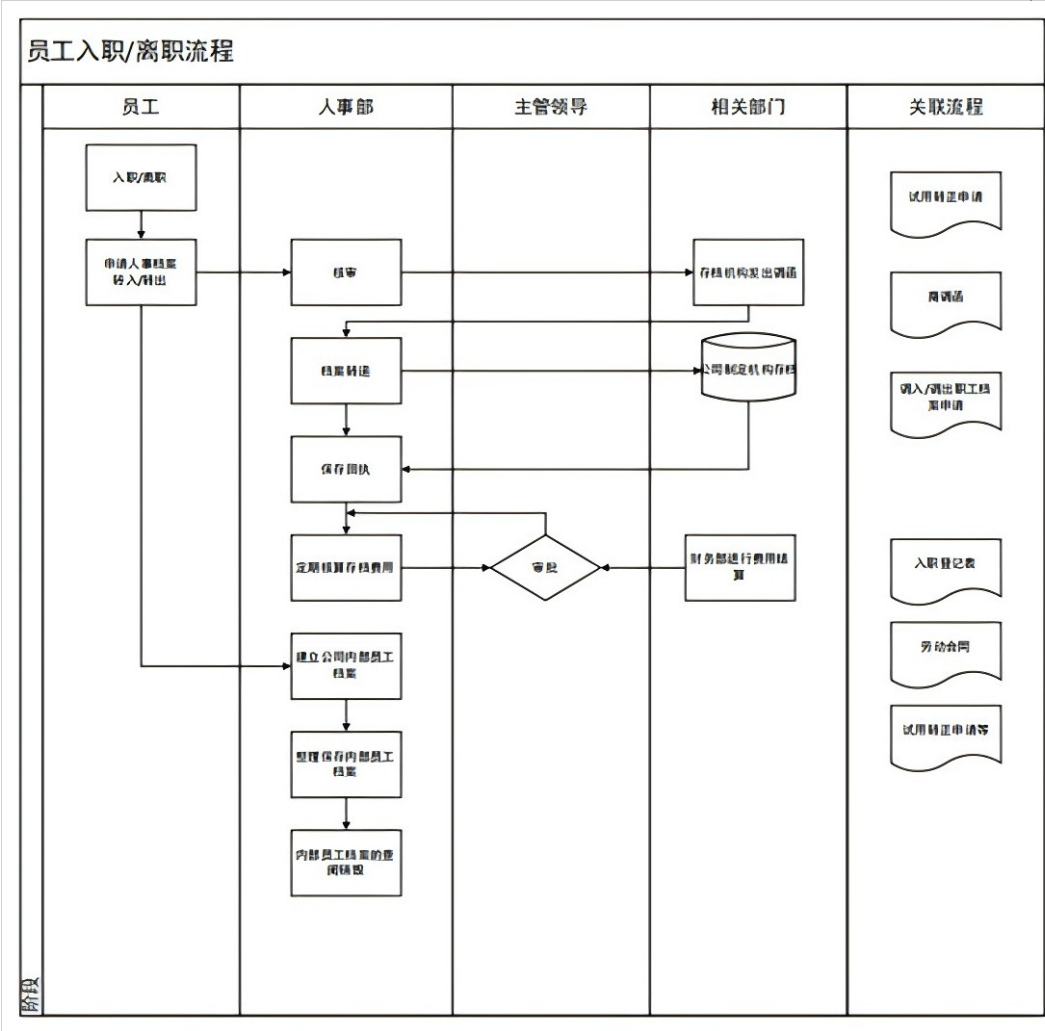


图 537人员管理流程

密码管理制度发布流程

密码安全管理小组负责各管理制度的制定和发布，其主要流程如下：

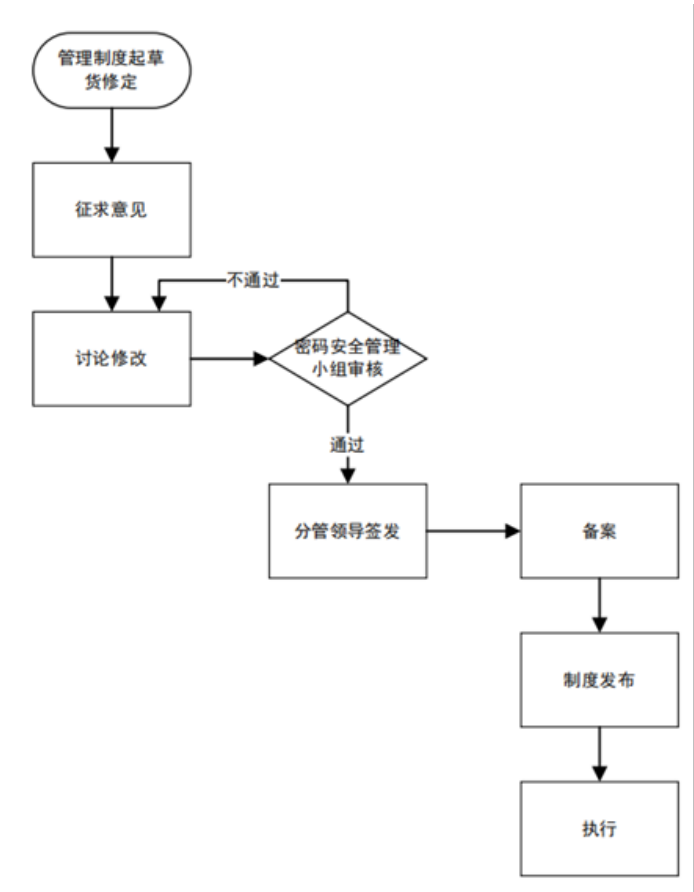


图 538管理制度发布流程

系统建设管理流程

1.项目启动

在密码管理组长的指导下，确定项目建设目标和项目组织结构，并确定项目里程碑计划及交付物后，召开项目启动会议，填写项目启动申请表，完成项目启动。

2.项目过程管理

项目启动后，实施过程中实行日报制度，对每个自然天内的工作情况进行记录；每周实行周报制度，对本周内的工作进行记录、总结、分析，提出需要外部协调解决的问题。

每两周召开一次周例会，对本阶段的项目工作进行总结，对资源、风险、问题、质量等项目情况进行分析，形成周例会会议纪要；每月底召开一次月例会，总结本月内工作完成情况，进度控制情况，并对本月内所有的风险和问题处理情况进行统计，并与主管部门、建设单位进行沟通。

3.项目问题管理

项目组对发现的风险和问题，由项目经理协调解决，项目经理持续关注项目风险和问题的状态，每周更新《项目周报》中的风险与问题跟踪表，每月底更新《项目计划与跟踪表》中的风险和问题管理信息。

4.项目文档管理

项目文档参照CMMI3级标准编写，项目文档在评审完成后，及时进行归档，待项目完成时统一进行提交。

5.方案设计

在对业务系统充分调研的基础上，梳理系统在终端、网络接入、应用系统和运维管理方面的安全问题和需求，完成密码应用解决方案，该方案需要通过专家评审。

6.系统开发

根据方案设计，完成涉及到的密码应用需求的功能、中间件开发。

7.工程实施

完成涉及到的密码设备的部署与安装。

8.联调

完成密码设备与系统联调工作。

9.测试验收

第三方测试单位对系统进行安全性测试，并出具安全性测试报告；制定验收方案并完成系统验收工作。

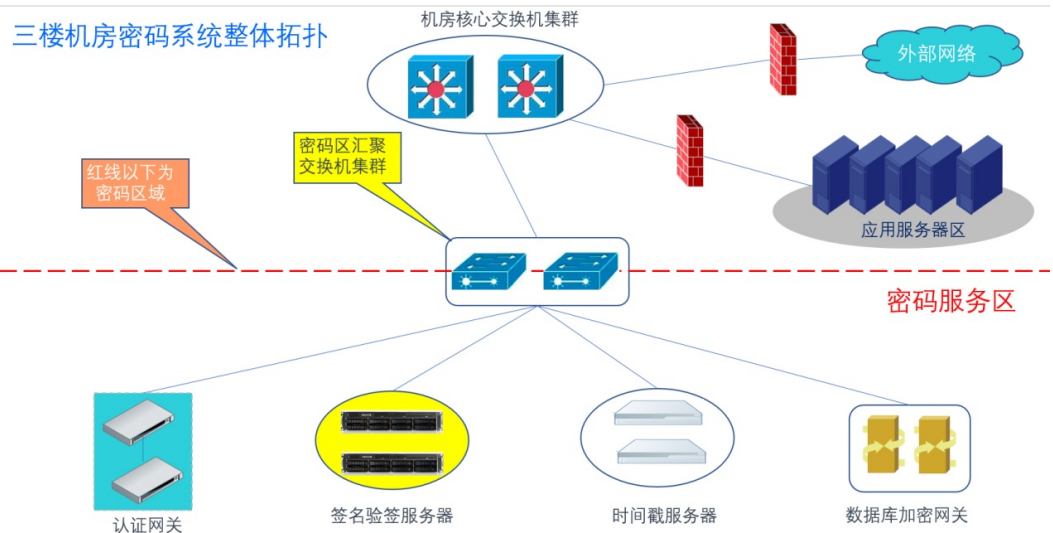
10.系统交付

制定详细的系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点，对系统运行维护技术人员进行相应的技能培训，并按照管理规定的要求完成系统交付工作。

11.密码应用测评

在系统运行过程中，选择具有国家相关技术资质和安全资质的测评单位进行密码应用测评，发现不符合相应标准要求的及时整改；在系统发生变更时及时对系统进行测评，级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级标准要求的及时整改。

本项目密码系统建设总体架构如下：



注：指挥中心机房密码设备数量与部署方式和三楼机房相同

图5-1 总体架构图

按照密评整改建议及实际需求，本次需要的密码组件为：安全认证网关、签名验签服务器、时间戳服务器、数据库加密网关、服务器密码机、数据库加密网关、国密门禁系统、Ukey（含数字证书）、国密客户端；

其中国密门禁系统为机房基础设施，独立部署，不涉及应用系统的对接；Ukey（含数字证书）、国密客户端为PC终端设备；

安全认证网关、签名验签服务器、时间戳服务器、数据库加密网关、服务器密码机都建议按照双机配置；

上图为本次密码产品部署的逻辑示意图，在本次的网络中设置一块密码服务子区，把本次新建的密码设备都放置在该区域中，按需进行路由配置。

安全建设方案

拟采购两台全国产化堡垒机产品，每台500设备资产授权，分别部署到互联网和公安网中，以满足运维人员的接入与管理功能。

通过本项目的实施，预计可实现以下目标：

大幅提升信息系统运维安全性；

通过堡垒机集中管控运维入口，强制实施动态身份鉴别与访问控制，降低密码泄露、越权操作等风险。

部署入侵检测与漏洞扫描联动机制，实时发现并阻断异常会话，有效防范APT攻击和数据泄露。

完善运维管理体系，提高合规能力；

内置符合等保2.0标准的审计模板，自动生成操作日志、权限变更记录等报表，满足《网络安全法》《数据安全法》的合规审查要求。

支持三权分立管理（系统管理员、审计员、操作员），实现权限最小化分配与操作留痕。

提升审计效率和应急响应能力；

全量记录运维操作指令及图形会话录像，支持按时间戳、用户IP等多维度检索，5分钟内定位异常操作节点。

建立高危命令实时阻断规则（如rm -rf、系统服务重启命令），同步触发短信告警至安全管理员。

为总队后续信息安全体系建设打下坚实基础。

提供标准化API接口，支持与现有网络平台、安全系统设备对接，实现安全事件统一处置与威胁情报共享。

预留40%性能冗余，支持后续扩展至1000+设备资产规模，适应未来业务增长需求。

建设内容清单

硬件设备清单

序号	设备名称	部署位置	设备类型	数量	单位
1	安全认证网关（核心产品）	公安网	硬件设备	2	台
2	签名验签服务器	公安网	硬件设备	2	台
3	时间戳服务器	公安网	硬件设备	2	台
4	数据库加密网关	公安网	硬件设备	2	台
5	智能密码钥匙	公安网	硬件设备	20	台
6	国密门禁系统	公安网	硬件设备	2	套

成品软件

序号	设备名称	部署位置	设备类型	数量	单位
1	国密浏览器	公安网、互联网	成品软件	20	套

七、技术参数

表1硬件设备购置

序号	设备名称	技术参数	数量	说明
1	安全认证网关（核心产品）	安全认证网关支持SSL代理，VPN隧道，高强度数据链路加密服务；支持HT TP、HTTPS的B/S应用，支持C/S应用，无限用户数；2U机架设备，千兆网口 ≥ 6个，千兆光口 ≥ 4 个，万兆光口 ≥ 2 个，冗余电源。	2	
2	签名验签服务器	支持签名验签和加密解密功能，可用做身份认证和重要数据完整性保护项目中。支SM2、SM3、SM4等国产密码算法。无限用户数。2U机架设备，千兆网口 ≥ 6个，冗余电源。	2	
3	时间戳服务器	用于对时间敏感的业务场景，时间戳策略OID的配置；ASN.1时间戳请求签发；通过原文摘要直接签发时间戳；支持对时间戳中证书、原文摘要、策略OID、签名时间等信息的解析及获取，无限用户数。2U机架设备，千兆网口 ≥ 6个，配置授时卡，冗余电源。	2	
4	数据库加密网关	支持Mysql、Oracle、DB2、Sql Server、达梦、人大金仓等多种数据库；支持国密算法SM4；多级密钥体系，敏感数据发现能力，提供可视化的敏感数据发现，支持自定义发现算法，支持敏感数据变化跟踪；无限用户数。2U机架设备，千兆网口 ≥ 6个，千兆光口 ≥ 4 个，万兆网卡 ≥ 2 个，冗余电源。	2	
5	国密智能密码钥匙	20个密码钥匙，高安全性网络身份认证设备。具有加密、解密、签名、验签功能，支持警用证书颁发及存储，Pin 码修改等辅助功能。	1	
6	国密门禁系统	对进入机房人员进行身份鉴别，包含门禁管理软件、密钥管理软件、国密发卡器、国密读卡器、双门控制器、50张国密用户卡。	2	

表2成品软件购置

序号	系统名称	技术参数	数量	说明
1	国密浏览器	建国密SS1加密通道，管控中心1套和客户端20个，支持授权管理、管理系统设置、浏览器基础功能模块	1	

采购包3:

序号	参数性质	技术参数与性能指标
		<p>一、监理技术规格要求</p> <p>1.1. 监理基本原则</p> <p>1.1.1 监理服务应遵守的基本准则</p> <p>1.1.1.1 遵照国家《信息技术服务监理》（GB/T 19668.1）参照监理服务各阶段内的具体监理工作，以“守法、诚信、公正、科学”的准则执业，维护建设单位与承建单位的合法权益。</p> <p>1.1.1.2 执行有关项目建设的国家法律、法规、规范、标准和制度，履行监理合同规定的义务和职责；</p> <p>1.1.1.3 不得泄露所监理项目各方认为需要保密的事项；</p> <p>1.1.1.4 遵守国家的法律和政府的有关条例、规定和办法等；</p> <p>1.1.1.5 坚持公正、公平、公开、独立地处理有关项目各方的争议；</p> <p>1.1.1.6 坚持科学的态度和实事求是的原则；</p> <p>1.1.1.7 在坚持按监理合同的规定向建设单位提供技术服务的同时，帮助承建单位完成所担负的建设任务。</p> <p>1.2 服务依据</p> <p>设计方案</p> <p>监理合同</p> <p>《信息技术服务监理第1部分：总则》 GB/T19668.1- 2014</p> <p>《信息技术服务监理第2部分：基础设施工程监理规范》 GB/T19668.2- 2017</p> <p>《信息技术服务监理第3部分：运行维护监理规范》 GB/T19668.3- 2017</p> <p>《信息技术服务监理第4部分：信息安全监理规范》 GB/T19668.4- 2017</p> <p>《信息技术服务监理第5部分：软件工程监理规范》 GB/T19668.5- 2018</p> <p>《信息技术服务监理第6部分：应用系统数据中心工程监理规范》GB/T 19668.6-2019</p> <p>2. 监理范围</p> <p>2.1 监理范围</p> <p>监理范围主要为本项目采购包1公安交管信息系统软硬件更新升级及采购包2公安交管信息系统软硬件更新升级项目密码改造部分。</p> <p>2.2 监理基本内容：</p> <p>A. 准备阶段</p> <p>(1) 严格按照设备招标文件、承建单位的投标文件及施工合同对承建单位提供的所有设备进行验收，确认设备品目、型号、配置、数量、性能。</p> <p>(2) 审核系统承建单位的集成方案，确保系统承建单位按照其投标文件所做的承诺执行集成工作。</p> <p>B. 施工阶段</p> <p>(1) 审批施工方案，确认开工报告，签发开工指令。</p> <p>(2) 每天检查施工现场和施工的安全防护设施及工作情况。</p> <p>(3) 检查承建单位的施工组织、施工技术方案和进度计划，检查计划执行情况实际进度与计划进度对比分析，纠正进度计划偏离，审查有关技术合同附件，确保工程在合同规定期限内完成。</p> <p>(4) 检查承建单位的管理规范与质量控制体系是否符合要求。严格监督与管理督促承建单位按规范、设计方案及工艺标准施工，确保工程按质按量完成。</p> <p>(5) 对项目的各个分项分部及单位工程质量控制及检查验收把关，各分项、隐蔽工程自检，签发子系统检验认可书，进行质量事故分析，监督事故处理方案执行。</p>

(6) 当质量有问题时,分析查明原因并及时提出要求,若工程需变更,提出变更的参考意见,并督促承建单位返修返工。

(7) 督促履行工程合同,协助调解合同有关问题,检查工程质量,督促工程进度。

C. 试运行阶段

(1) 检查系统调试和试运行情况,做出试运行检测报告。

(2) 对于运行系统中出现的质量问题,写出质量分析报告,督促承建单位负责解决。

(3) 按合同要求督促完成培训工作,建立运行规章制度。

D.验收阶段

(1) 按项目招标文件、承建单位投标文件和合同中的技术指标做出详细的检测报告,配合对各系统进行验收测试。

(2) 监督督促承建单位整理并提交工程相关的技术资料和提交验收的材料。

(3) 完成工程竣工验收的准备工作,并参与工程验收,编写竣工验收评估报告。

项目建设运维期间,监理单位需要随时关注相关安全及运维管理工作进展,配合建设单位方完成对承建单位管理工作。

3.监理工作责任

3.1 本项目的监理应该严格按照有关规定开展工作,对项目的进度、质量进行有效的控制和管理,督促、检查承建单位落实安全及质量保证措施,做好组织协调工作,为建设单位提供技术、经济和法律等方面的咨询服务,协助建设单位实现预定的合理建设目标,帮助承建单位实现合同所规定的目标、公正维护各方的合法权益。

3.2 未经建设单位同意,不得泄露任何与本工程项目有关的资料。

3.3 若承建单位在工程施工中不符合工程规范和质量要求,监理单位要监督承建单位停工整改或返工。若遇到确实需要变更设备或施工方案的情况时,在确保工程建设质量的前提下,监理单位须提出合理建议并报建设单位批准后方可执行。

3.4 承建单位违反合同规定的完工时限,监理单位需协助建设单位追究有关承建单位的责任。

3.5 由于监理单位监督不力,造成建设单位经济损失的,需扣除相应监理费(该费用协商解决);如由于承建单位的责任造成建设单位的经济损失,监理单位必须负责配合追究承建单位,赔偿给建设单位造成的全部经济损失。

3.6 监理单位使用建设单位提供的设备和物品属建设单位所有,在监理工作完成或终止时,应将设备和剩余物品在合同规定的时间和方式移交给建设单位。

3.7 监理单位不得对监理工程进行分包或转包,否则建设单位有权终止合同,监理单位要承担由此造成的一切经济损失。

3.8 监理单位不得在工程监理期间对投标文件中已经明确的监理人员进行更换,如遇特殊情况须经建设单位同意;如现场监理人员工作不力时,建设单位有权提出更换监理人员,更换后的监理人员必须及时到达监理现场。

4.监理工作质量要求

监理单位应该在质量控制、投资控制、进度控制、信息管理、合同管理/组织协调等几个方面对监理工程采取必要和完善的监督、控制和管理措施,保证所监理的工程能够按时、按质、按量竣工。

监理单位必须每周定期向建设单位通报工程进展情况及工程实施过程中所遇到的问题。

监理工作的质量控制目标:达到国家规定的质量评定标准。

监理工作的计划控制目标:工程工期必须在合同工期内完成。

监理工作的投资控制目标:工程总投资必须严格控制在批复概算范围以内。

5.监理人员要求

针对本项目技术含量高，施工涉及面多，实施工期长、建设内容多等特点，监理单位应成立专门项目监理工作组，该项目组由具有类似监理业绩、丰富监理经验和过硬的专业理论与实践知识的人员组成。监理组成员将严格遵循“守法、公平、公正、独立”的监理原则，对建设项目的全过程进行科学、公正、公平的质量跟踪监控、协调与处理，并以良好的职业道德，遵纪守法，以丰富的实践经验来作好本项目的监理工作。总监理工程师对本项目的实施全面负责，管理项目部的日常工作，对本项目的监理工作提供参考意见和技术咨询指导；总监代表组织信息系统监理工程师负责现场的“四控三管一协调”工作，实施现场监理。

监理人员必须全程到位，监理单位必须保证按照建设单位通知要求，能及时委派负责本项目的总监及专职监理工程师及时到位参与各项工作。同时保证，在项目承建单位进场日期开始至项目竣工验收完毕之日，有不少于*名的项目监理人员常驻施工现场，对整个项目建设全程作现场监理。

监理人员的人身安全及劳务关系等由监理单位负责。本监理项目的费用包括监理人员在采购人驻地外开展工作时的全部费用，包括因为本项目产生的差旅费用；监理人员由于项目工作需要产生的加班，值班等工作不另外计费。监理单位应充分考虑响应报价，所有监理人员一切费用均包含在项目报价中。

三、监理的工作内容及要求

本次项目监理工作需按照国家信息化工程监理的国标（GB/T 196681 《信息技术服务监理》）针对各项目分别开展信息系统工程监理，工作应按照“四控、三管、一协调”的监理基本原则进行，即对项目进度、质量、投资、变更进行控制，对项目对合同执行情况、资料编制及整理情况、施工安全进行管理，并协调建设方、供应商、业务部门等干系人，对参与的各方进行沟通协调。同时，监理单位为采购人提供项目建设全过程的技术咨询服务，对项目建设中的技术难点、问题及风险为建设单位提供全方位的解答和咨询服务

监理工作内容包括项目施工阶段、验收阶段、运维阶段和工程缺陷期的全过程监理。按照相关国家标准，监理工作包括至少以下内容及要求：

1.质量控制

1.1质量控制目标

监理单位应正确处理项目进度、费用、质量三大控制目标之间的关系，对项目实施全过程中所有影响质量的活动进行恰当有效连续监控，使影响工程质量的技术、管理和人的因素处于受控状态，预防和减少质量问题的发生，以及质量事故纠正，保证项目各个阶段、各个过程的每一项活动都符合质量要求

1.2质量控制的方法

1.2.1质量的事前控制

1）在设计方案会审前总监理工程师组织专业监理工程师熟悉设计文件，并对设计方案中存在的问题提出书面意见，总监理工程师负责组织设计方案会审汇总或指定人员汇总。

2）总监理工程师组织专业监理工程师审查承建单位报送的施工组织设计方案及专项方案，签认后交建设单位。

3）监理工程师审查承建单位现场项目质量管理、技术管理和质量保证的组织机构；质量管理、技术管理制度；专职管理人员和特种作业人员的资格证、上岗证。

4）监理工程师对工程所需原材料、半成品及设备的质量控制，对工程所用材料、半成品严格审核其出厂证明、技术合格证或质保证书。对试验材料，必须按规定进行抽检或试验，送样实行监理现场见证。所有设备在安装前必须按其技术说明书进行质量验收。

5）监理工程师及时审查承建单位报送的工程开工报审资料并签署意见。

6) 参加由建设单位主持召开的第一次工地会议, 介绍项目监理机构、人员分工; 建设单位宣布对监理授权, 建设单位、承建单位介绍开工前的准备情况, 总监对施工准备情况的意见与要求, 介绍监理规划的内容、监理程序, 制定工地共同遵守的会议制度及其监理过程中各方配合协调事宜。

1.2.2 质量的事中控制

1) 施工工艺过程质量控制

按照国家规范及实际设计方案的要求, 采用巡视、旁站、检测、试验等手段检查施工过程, 确保施工质量。严格施工工艺的质量控制。监理工程师对施工工艺过程的各个质量控制点, 施工各工序进行跟班巡视和检查, 对施工重点部位、关键部位进行旁站监督施工, 现场发现质量问题及时要求施工人员整改。

监理工程师将编写《监理细则》时应明确旁站监理范围。

2) 工序交接检查

坚持上道工序不经检查验收不准进行下道工序的原则, 上道工序完成后, 先由承建单位进行自检、专职检, 认为合格后再通知现场监理工程师到现场会同检验, 检验合格后签署认可方能进行下道工序。

3) 隐蔽工程检查验收

隐蔽工程完成后, 先由承建单位自检、专职检, 初验合格后填报隐蔽工程报验单。监理、建设单位、承建单位现场联合检验, 确认合格后隐蔽。

4) 工程质量事故处理

包括质量事故原因、责任分析; 质量事故处理措施的商定; 批准处理工程质量事故的技术措施或方案; 处理措施效果的检查。

5) 行使监理质量监督权, 出现问题时下达停工指令。

6) 建立质量监理日记, 现场质量监理工程师及质量检验人员应逐日记录有关工程质量动态及影响因素的情况。

7) 组织现场工程例会及专题会议

现场工程例会由总监理工程师或总监代表主持。会议将讨论质量及工程的其他事宜, 解决施工遇到的各种问题。会后形成会议纪要。

8) 定期向建设单位报告有关工程质量动态情况

现场监理组每月在《监理月报》中向建设单位报告有关工程质量方面的情况。重大质量事故及其它质量方面的重大事宜则及时提出报告。

1.2.3 质量的事后控制

1) 每一检验批、分项、分部工程完成后, 必须先经承建单位自行检查并进行验收, 再经监理工程师复验达标并签认后, 方可进行后续工程的施工。

2) 审核竣工资料, 对工程质量进行竣工预验收。工程完工后, 由承建单位提出工程验收申请, 并提交全部工程技术资料, 质量自评报告及与质量有关的技术文件, 经监理工程师(总监)审核后, 组织有关各方进行初验, 对初验提出的问题, 要求承建单位限期内进行整改。

3) 单位、单项工程竣工验收

初验合格后, 建设单位主持竣工验收, 监理协助建设单位作好竣工验收、备案工作。

4) 承担保修期的监理工作时, 监理单位应安排监理人员对建设单位提出的工程质量缺陷进行检查和记录, 对承建单位进行修复的工程质量进行验收, 合格后予以签认。

1.3 质量控制措施

1.3.1 质量控制的组织措施

1) 明确职责分工。监理及施工均制定质量管理体系和质量保证体系并接受监督管理。

2) 监理单位领导定点联系制度, 监理单位领导对各项监理部定期巡视检查, 解决项目部内部及施工

中遇到的各项问题以提高监理能力及水平

3) 监理单位实行定期到监理工地进行质量检查制度, 及时发现和解决存在问题, 提高监理水平, 加大对质量监理力度。

4) 督促和审查承建单位建立健全质量管理体系和质量保证体系, 落实人员, 完善措施和制度。

1.3.2 质量控制的技术措施

1) 材料设备供应阶段, 通过实地考察、现场抽样, 审查供应厂家的资质证、准销证、产品合格证等各种手段, 确保材料达到设计和规范要求。

2) 施工阶段严格事前、事中和事后的质量控制

(1) 事前控制: 监理工程师应熟悉质量控制的技术依据, 并对施工现场、施工机械、施工队伍资质、进场材料进行检查验收, 审查施工组织设计和施工方案的技术可靠性和质量保证措施。

(2) 事中控制: 监理工程师在质量检查中, 用观察、量测、测量、试验等手段按规范要求完成施工工艺过程的质量控制, 做好工序交接和隐蔽工程检查验收, 做好工程变更、质量事故的监理工作方法 & 措施

(3) 事后控制: 检验批验收或分项验收时严格设计文件及相关标准验收, 发现问题及时纠正整改, 保证在上道工序合格的基础上进行下道工序施工。监理工程师要做好单位、单项及项目竣工验收, 审核竣工图及其它技术文件资料, 整理工程技术文件资料并编目建档。

1.3.3 质量控制的经济措施及合同措施

1) 监理工程师在质量检查和验收中, 严格按合同规定的质量要求, 对承建单位不符合要求的拒付工程款。

2) 根据施工合同, 对可能的违约行为提出警告。

3) 按合同条款, 对造成损失一方进行经济处罚。

2. 进度控制

2.1 进度控制目标

运用先进的项目进度控制与管理技术, 对项目的设计、采购、施工、安装、调试直至投产等工作中所有影响项目建设进度的因素进行连续的、全过程的监控、测量、分析和预测, 在确保项目质量及费用在受控的状态下, 快速推进项目建设, 保证项目优质、高效、快速建成。

2.2 进度控制方法

2.2.1 进度的事前控制

进度的事前控制, 即为工期预控, 主要工作内容有:

1) 审批项目实施总进度计划

监理工程师审批承建单位编制的总进度计划;

2) 审核承建单位提交的施工进度计划

审核是否符合总工期控制目标的要求; 审核施工进度计划与施工方案的协调性和合理性等。

3) 审核承建单位提交的施工方案

审核保证工期, 充分利用时间的技术组织措施的可行性、合理性。

4) 制定由建设单位供应材料、设备的需用量及供应时间参数, 编制有关材料、设备部分的采供计划。

2.2.2 进度的事中控制

1) 建立反映工程进度的监理日志

逐日如实记载每日形象部位及完成的实物工程量。同时, 如实记载影响工程进度的内、外、人为和自然的各种因素。

2) 工程进度的检查

审核承建单位每月、周提交的工程进度报告，审核的要点：

- (1) 计划进度与实际进度的差异。
- (2) 形象进度、实物工程量与工作量指标完成情况的一致性。
- (3) 按合同要求，及时进行工程计量验收。
- (4) 有关进度、计量方面的签证。

进度、计量方面的签证是支付工程进度款、计算索赔、延长工期的重要依据。

- (5) 工程进度的动态管理

实际进度与计划进度发生差异时，分析产生的原因，并提出进度调整的措施和方案，并相应调整施工进度计划及设计、材料设备、资金等进度计划；必要时调整工时目标。

3) 需要时组织现场协调会

4) 在监理月报中向建设单位报告有关工程进度和所采取进度控制措施的执行情况，并提出合理预防由建设单位原因导致的工期及其相关费用索赔的建议。

2.2.3 进度的事后控制

当实际进度与滞后于计划进度时，专业监理工程师书面通知承建单位，在分析原因的基础上采取纠偏措施，并监督实施：

- 1) 制定保证总工期不突破的对策措施。

——技术上：如缩短工艺时间、减少技术间歇期、实行平行流水立体交叉作业等；

——组织上：如增加作业队数、增加工作人数、工作班次等；

——经济上：如实行包干资金、提高计件单价、资金水平等；

——其它配套措施：如改善外部配合条件、改善劳动条件、实施强有力调度等。

- 2) 制定总工期突破后的补救措施。

- 3) 调整相应的施工计划、材料设备、资金供应计划等，在新的条件下组织新的协调和平衡。

2.3 进度控制措施

2.3.1 进度控制的组织措施

1) 落实进度控制的责任，由总监理工程师（或总监代表）负责工程进度的整体控制，解决进度控制的重大问题，并指定一个监理工程师做进度控制的具体工作。

2) 进度监理工程师根据建设工期总目标要求，编制监理项目的控制进度和各阶段的控制工期，实行项目分解。并审查施工承建单位的单项工程施工进度计划与年、季、月的施工计划，并将结果报总监理工程师和建设单位。

3) 建立进度监理协调制度，建立反映工程进度状况的监理日志，每周工程例会均进行工程进度目标实现分析，承建单位、监理单位、建设单位负责进度人员均应到会，每月按时将工程进度情况和进度分析意见报建设单位和采购人。

4) 总监理工程师（或总监代表）负责为工程进度款签署进度和计量方面的认证意见。

2.3.2 进度控制的技术措施

1) 在施工进行阶段监理工程师应认真审核施工进度计划与施工方案的协调性和合理性，审核施工方案能否保证工期，保证“全天候”施工的技术组织措施的可行性、合理性，审核施工总平面图与施工进度计划的协调性，审核材料、设备的采、供计划的用量和时间参数。

2) 审核承建单位每月提交的工程进度报告，检查计划进度与实际进度的差异，当实际进度与计划进度发生差异时，应提出调整措施和方案，技术上采取缩短工艺时间，减少技术间歇，实行平行立体交叉作业，配合相应的组织经济措施补救。

2.3.3 进度控制的经济措施和合同措施

按合同要求及时协调有关各承建单位的进度，以确保项目的形象进度要求，确保合同工期的实现，执

行对工期提前或拖后者的奖罚制度。

2.4进度变更控制

审查进度计划

监理工程师要实际检查、审查进度计划草案，了解项目最初的进度期望值，把握可能出现的变更，并分析、记录。

进度计划的实际检查

通过现场旁站、项目干系人会议、审查项目文档等获取取有关项目进展方面的信息。了解项目中各项活动为什么遵守或没有遵守进度计划，并采取预防性措施。当出现进度的严重冲突时，监理工程师首先会同承建单位提出更改计划和措施，报请总监理工程师审核、签字，然后报客户单位批准。若总监理工程师或客户单位未批准，则由监理人员协助承建单位根据返回的意见对变更计划和措施进行修改或重新制定。

2.5进度计划调整

项目进度计划调整过程是进度监测过程的后续工作过程。当工程进度出现偏差并且客户单位审核批准《信息工程建设延期审批表》后，监理工程师启动该过程对进度计划实施调整。

3.投资控制

3.1投资控制的目标

投资控制的主要目标是在保证实现项目质量、进度的前提下，以降低工程投资为出发点，按照批准的投资计划，建立有效的费用控制、跟踪、分析系统，使项目全体工作人员提高费用控制的意识，在项目实施的全过程中对所有影响工程费用的活动进行恰当而连续的有效控制，将工程项目投资控制在批准的项目初步设计概算内，为项目建成投产后能够取得良好的经济效益奠定基础。

3.2投资控制的方法

3.2.1投资事前控制

投资事前控制，监理单位依据施工合同有关条款、施工图，对工程项目造价对策，目标进行工程风险预测，并采取相应的防范性对微量，尽量减少承建单位提出索赔的可能。

3.2.2投资事中控制

- 1) 按合同规定，及时答复承建单位提出的问题及配合要求，避免造成违约和对方索赔的条件。
- 2) 监理工程师应从造价、功能要求、质量、工期等方面审查工程变更方案，并宣布工程变更实施前与建设单位、承建单位协商确定工程变更的价款。
- 3) 按合同规定，及时对已完工程量进行计量。
- 4) 监督承建单位按合同规定，及时申报工程量，监理工程师及时审批进度款，避免延误工期违约造成索赔。
- 5) 定期、不定期地进行工程费用超支分析，并提出控制工程费用突破的方案和措施。

3.2.3投资事后控制

- 1) 审核承建单位提交的工程结算书。
- 2) 公正处理双方单位提出的索赔申请。

3.3投资控制措施

3.3.1投资控制的组织措施

建立健全监理组织，完善职责分工及有关制度，落实投资控制的责任。

- 1) 由驻现场监理工程师通过工程量支付来控制合同价款，工程承建单位按约定的时间向监理工程师提交已完工工程报告，监理工程师核实已完工程数量，并由承建单位、监理工程师共同参与计量，承建单位无正当理由不参与计量，由监理工程师自行进行，计量仍然有效，作为工程价款支付依据。

2) 由驻现场监理工程师核实签字后, 须经总监理工程师 (或总监代表) 审核签字, 才作为有效的凭证。

3) 项目监理部每月应以规范的格式向监理单位报告工程投资情况。

3.3.2 投资控制的技术措施

1) 材料设备供应阶段, 监理工程师根据建设单位的要求, 对材料提出自己的建议。

2) 施工阶段, 监理工程师督促承建单位采用先进合理的施工组织设计和施工方案, 合理编排工期, 避免不必要的赶工费用。

3.3.3 投资控制的经济措施

1) 驻现场监理工程师每月定期进行计划费用与实际费用的比较分析, 并提出控制工程费用突破的方案和措施。经总监理工程师 (或总监代表) 审查签字后, 报监理单位。经主管领导审批后报建设单位。

2) 驻现场监理工程师应预测和防范可能发生的索赔, 及时向建设单位和上级报告可能发生的索赔, 并制定对策, 减少向建设单位索赔的发生。

3) 鼓励监理工程师对原设计或施工方案提出合理化建议, 如合理化建议被采用并对工程产生的投资节约, 应按合同予以一定的奖励。

3.3.4 投资控制的合同措施

1) 监理单位应协助建设单位如期向承建单位提供施工现场, 如期、保质、保量供应由建设单位负责的材料、设备, 及时提供设计方案等技术资料, 不违约, 不造成索赔条件。

2) 监理单位应按合同条款经审核支付工程款, 但防止过早、过量的现金支付。

4. 变更控制

4.1 变更控制的原则

- (1) 对变更申请快速响应
- (2) 任何变更都要得到三方确认
- (3) 明确界定项目变更的目标
- (4) 防止变更范围的扩大化
- (5) 三方都有权提出变更
- (6) 加强变更风险以及变更效果的评估
- (7) 及时公布变更信息
- (8) 选择冲击最小的方案

4.2 变更控制的流程

4.2.1 了解变化

在项目实施过程中, 监理工程师与项目组织者要发现和把握变化, 认真分析变化的性质, 确定变化的影响, 适时地进行变化一的描述, 监理工程是要对整个项目的执行情况做到心中有数。

4.2.2 接受变更申请

变更申请单位向监理工程师提出变更要求或建议, 提交书面工程变更建议书。工程变更建议书主要包括以下内容: 变更的原因及依据; 变更的内容及范围; 变更引起的合同总价增加或减少; 变更引起的合同工期提前或缩短; 为审查所提交的附件及计算资料等。工程变更建议书应在预计可能变更的时间之前14天提出。在特殊情况下, 工程变更可不受时间的限制。

4.2.3 变更的初审

项目监理机构应了解实际情况和收集与项目变更有关的资料, 首先明确界定项目变更的目标, 再根据收集的变更信息判断变更的合理性和必要性。对于完全无必要的变更, 可以驳回此申请, 并给出监理意见; 对于有必要的变更, 可以进一步进行变更分析。

4.2.4 变更分析

把项目变化融入项目计划中是一个新的项目规划过程，只不过这规划过程是以原来的项目计划为框架，在考察项目变化的基础上完成的。通过与新项目计划的对比，监理工程师可以清楚地看到项目变化对项目预算、进度、资源配置的影响与冲击。把握项目变化的影响和冲击是相当重要的，否则就难以做出正确的决策，做出合理的项目变更。

4.2.5确定变更方法

三方进行协商和讨论，根据变更分析的结果，确定最优变更方案。做出项目变更时，力求在尽可能小的变动幅度内对主要因素进行微调。根据变更方案下达变更通知书并进行变更公布，并把变更实施方案告知有关实施部门和实施人员，为变更实施做好准备。

4.2.6监控变更的实施

变更后的内容作为新的计划和方案，可以纳入正常的监理工作范围，监理工程师对变更部分的内容要密切注意，项目变更控制是一个动态的过程，在这一过程中，要记录这一变化过程，充分掌握信息，及时发现变更引起的超过估计的后果，以便及时控制和处理。

4.2.7变更效果评估

在变更实施结束后，要对变更效果进行分析和评估。整个变更控制流程如图所示。

5.合同管理

5.1合同管理的原则

合同管理的原则是指监理单位在信息工程监理过程中针对各类合同的管理须遵循的宗旨，贯穿合同管理的全过程，包括：事前预控原则、实时纠偏原则、充分协商原则和公正处理原则。

5.2合同管理的主要内容

本项目合同管理的工作内容包括：

拟定信息系统的合同管理制度，其中应包括合同草案的拟定、会签、协商、修改、审批、签署、保管等工作制度及流程；

协助建设单位拟定信息工程合同的各类条款，参与建设单位和承建单位的谈判活动；

及时分析合同的执行情况，并进行跟踪管理；

协调建设单位与承建单位的有关索赔及合同纠纷事宜。

归纳起来，监理单位在合同管理中的主要内容由三部分组成，即合同的签订管理、合同的档案管理和合同的履行管理。

5.3合同的签订管理

合同的签订管理是指监理协助建设单位与承建单位、设备材料供应单位等各方之间的各种合同进行分析、谈判、协商、拟定、签署等。

合同分析是合同签订中最重要的内容和环节，是合同签订的前提。监理工程师应对工程承建、共同承担风险的合同条款、法律条款分别进行仔细的分析解释。同时也要对合同条款的更换、延期说明、投资变化等事件进行仔细分析。合同分析和项目检查等工作要与其联系起来。

监理工程师在订立合同的过程中要按条款逐条分析，如果有对建设单位产生风险较大的条款，要增加相应的抵御条款。要详细分析哪些条款与建设单位有关、与承建单位有关、与项目检查有关、与工期有关等，分门别类地分析各自责任和相互联系的关联要素，做到一清二楚，心中有数。

5.4合同的履行管理

合同的履行管理是指监理工程师对合同各方关于合同约定的工期、质量和费用、争议解决及索赔处理等工作的管理。

1)履约管理的方式—合同控制

合同控制指为保证合同所约定的各项义务的全面完成及各项权利的实现，以合同分析的成果为基准，

监理对整个合同实施过程的全面监督、检查、对比、引导及纠正的管理活动。

合同控制的首要内容是对合同实施情况进行追踪，追踪的对象包括：

具体的合同事件。包括项目的质量、工期、成本。

承建单位的工作。对承建单位的项目缺陷提出意见，提出警告，责成他们改进。

建设单位是否及时下达命令，做出答复，及时支付项目款项。

总体情况，如整体项目的秩序如何，已完项目是否通过验收，有无大的项目事故，进度是否出现拖期，计划和实际成本有无大的偏差等。

2) 履约管理的保证—合同监督

合同监督就是要对合同条款经常与实际实施情况进行比对，以便根据合同来掌握项目的进展。保证设计、开发、实施的精确性，并符合合同要求。合同监督的另一个重要的内容是检查解释双方来往的信函和文件，以及会议记录、建设单位指示等，因为这些内容对合同管理是非常重要的

5.5 合同档案的管理

合同档案的管理，也即合同文件管理，是整个合同管理的基础。所有与合同有关的文件都是重要的文字依据，合同管理人员必须及时填写并妥善保存经有关方面签证的文件和单据，并建立合同档案数据库，以免在合同履行中发生纠纷时缺少有关的文字根据。

6. 安全管理内容

审核工程信息安全方案，监督信息安全策略的实施；审核施工组织安全管理措施，监督安全制度的落实，确保施工安全。

7. 信息管理

7.1 项目信息的划分

项目信息应划分为：

1) 投资控制信息

投资控制信息包括：费用规划信息，如投资计划、投资估算、工程预算等；实际费用信息，如各类费用支出凭证、工程变更情况、工程结算签证，以及物价指数、人工、软件环境、硬件设备等市场价格等；投资控制的分析比较信息，如费用的历史经验数据、现行数据、预测数据及经济与财务分析的评价数据等。

2) 进度控制信息

进度控制信息包括：信息工程项目进度规划，如总进度计划、分目标进度计划、各实施阶段的进度计划、单项工程及单位工程实施进度计划、资金及物资供应计划、劳动力及设备的配置计划等；工程实际进度的统计信息，如项目日志、实际完成工程量、实际完成工作量等；进度控制比较信息，如工期定额、实现指标等。

3) 质量控制信息

质量控制信息包括：信息工程项目实体质量信息，如质量检查、测试数据、隐蔽验收记录、质量事故处理报告，以及材料、设备质量证明及技术验证单等；信息工程项目的功能及使用价值信息，如有关标准和规范，质量目标指标，设计文件、资料、说明等；信息工程项目的工作质量信息，如质量体系文件，质量管理工作制度，质量管理的考核制度，质量管理工作的组织制度等。

4) 合同管理信息

合同管理信息包括：合同管理法规，如招标投标法、经济合同法等；信息系统工程合同文本，如设计合同、实施合同、采购合同等；合同实施信息，如合同执行情况、合同变更、签证记录、工程索赔等。

5) 组织协调信息

组织协调信息包括：工程质量调整及信息工程项目调整的指令；工程建设合同变更及其协议书；政府

及主管部门对工程项目建设过程中的指令、审批文件；有关信息系统工程有关的法规及技术标准。

6) 其他用途的信息

其他用途的信息是除上述五类用途的信息外，对信息系统工程项目建设决策提供辅助支持的某些其他信息，如工程中往来函件等。

7.2 目信息管理的方法

7.2.1 文档管理过程应该注意事项

文档的格式应该统一。

文档版本的管理。新的版本出来后，旧的版本应该进行相应的改变，同时彻底从管理库中清除，以保持文档版本的统一。

关于文档的存档标准。文档的存档标准是指某一类型的文档究竟应该保存多长时间，这个问题应该由监理单位根据国家档案管理相关的要求，统一进行规定。

7.2.2 监理工程师在归集监理资料时注意事项

监理资料应及时整理、真实完整、分类有序；

监理资料的管理应由总监理工程师负责，并指定专人具体实施；

监理资料应在各阶段监理工作结束后及时整理归档；

监理档案的编制及保存应按有关规定执行。

7.3 监理机构文档管理的职责

监理单位对文档工作的支持。监理单位应为编写文档的人员提供指导和实际鼓励，并使各种资源有效地用于文档开发。

监理单位的主要职责：

建立编制、登记、出版、分发系统文档和软件文档的各种策略；

把文档计划作为整个开发工作的一个组成部分；

建立确定文档质量、测试质量和评审质量的各种方法的规程；

为文档的各个方面确定和准备各种标准和指南；

积极支持文档工作以形成在开发工作中自觉编制文档的团队风气；

不断检查已建立起来的过程，以保证符合策略和各种规程并遵守有关标准和指南。

8. 项目协调

8.1 协调的原则

在协调项目实施过程中项目进度、工程质量与合同支付等合同目标之间的矛盾时，遵循以下原则：

8.1.1 在确保项目质量的条件下，促进项目实施进展；

8.1.2 在寻求建设单位更大投资效益的基础上，正确处理合同目标之间的矛盾；

8.1.3 在维护建设单位合同权益的同时，实事求是的维护承建单位地合法权益。

8.2 监理协调内容

8.2.1 工程项目内部需求关系协调

1) 监理过程中抓计划环节，平衡人员、材料、设备、能源动力的需求，要注意抓住期限的及时性，规格上的明确性，数量上的准确性，质量上的规定性，体现计划的严肃性，发挥指导作用。

2) 指导承建单位对施工力量的平衡，要抓住瓶颈环节，发现瓶颈环节，要通过资源力量的调整，集中力量打攻坚战。抓关键、抓主要矛盾、运用网络计划技术的关键线路法是有效的工具。

3) 对专业工种配合，要抓住调度环节，项目施工中需要机械化施工、土建、机电安装等专业工种交替配合进行，交替进行抓好衔接问题，配合进行抓好步调问题，就是抓好调度协调工作。

4) 施工准备阶段的协调：

作好施工准备是顺利组织施工的先决条件。满足开工的条件是：有完善有效的施工设计方案；有政府

		<p>管理部门签发的施工许可证；财务和材料渠道已落实，能按工程进度需要拨款、供料；施工组织设计已经批准；加工订货和设备已基本落实；施工准备工作已基本完成，现场已“五通一平”。监理工程师应协助落实上述开工条件，保持建设单位与承建单位的信息沟通，协商办事，督促双方严格按合同执行。建设单位和承建双方对施工准备工作应有明确的约定和分工，以便协调。</p> <p>5) 施工阶段的协调：</p> <p>包括解决进度、质量、中间计量与支付、合同纠纷等一系列问题。</p> <p>进度问题有两项有效协调工作应作好，一是建设单位和承建单位双方商定工程计划方案，并双方负责人在上面签字，作为工程承包合同附件；二是设立进度考核规范，按工程计划节点考核，分期预付。</p> <p>质量问题的协调：实行监理工程师质量签字认可，对没有出厂证明，不符合使用要求的原材料、设备和构件，不准使用，对不合格的工程部位不予验收签证，也不予计算工程量，不予支付进度款。</p> <p>合同争议的协调：合同纠纷，应协商解决，不能协调解决时再向合同管理机关申请调解或仲裁。</p> <p>6) 交工验收阶段的协调：</p> <p>对交工验收中建设单位提出的问题，承建单位应根据技术文件、合同、中间验收签证及验收规范作出解释，对不符合要求应督促其采取补救措施，使其达到设计、合同、规范要求，而后办理竣工结算。</p>
--	--	---

3.4商务要求

3.4.1交货时间

- 采购包1：
合同签订之日起9个月交货并完工。
- 采购包2：
合同签订之日起90日历日交货并完工。
- 采购包3：
完成公安交管信息系统软硬件更新升级及密码改造部分项目的监理工作。

3.4.2交货地点

- 采购包1：
陕西省公安厅交通管理总队指定地点。
- 采购包2：
陕西省公安厅交通管理总队指定地点。
- 采购包3：
陕西省公安厅交通管理总队指定地点。

3.4.3支付方式

- 采购包1：
分期付款
- 采购包2：
分期付款
- 采购包3：
分期付款

3.4.4支付约定

- 采购包1： 付款条件说明： 合同签订之日起，达到付款条件起 20 日内，支付合同总金额的 50.00%。
- 采购包1： 付款条件说明： 设备全部到货后，达到付款条件起 20 日内，支付合同总金额的 40.00%。
- 采购包1： 付款条件说明： 项目完成并通过验收后，达到付款条件起 20 日内，支付合同总金额的 10.00%。
- 采购包2： 付款条件说明： 合同签订之日起，达到付款条件起 20 日内，支付合同总金额的 50.00%。

采购包2：付款条件说明：设备全部到货后，达到付款条件起 20 日内，支付合同总金额的 40.00%。

采购包2：付款条件说明：项目完成并通过验收后，达到付款条件起 20 日内，支付合同总金额的 10.00%。

采购包3：付款条件说明：合同签订之日起，达到付款条件起 20 日内，支付合同总金额的 40.00%。

采购包3：付款条件说明：项目完成并通过验收后，达到付款条件起 20 日内，支付合同总金额的 60.00%。

3.4.5验收标准和方法

采购包1：

达到验收标准后，供应商向采购人申请验收，采购人收到验收申请后组织验收，验收时中标人应无条件予以配合并提供验收所需的全部资料，若中标人不配合或者未按合同要求提供服务的，采购人将拒绝验收,验收须以合同、招标文件、澄清、及国家相应的标准、规范等为依据。

采购包2：

达到验收标准后，供应商向采购人申请验收，采购人收到验收申请后组织验收，验收时中标人应无条件予以配合并提供验收所需的全部资料，若中标人不配合或者未按合同要求提供服务的，采购人将拒绝验收,验收须以合同、招标文件、澄清、及国家相应的标准、规范等为依据。

采购包3：

达到验收标准后，供应商向采购人申请验收，采购人收到验收申请后组织验收，验收时中标人应无条件予以配合并提供验收所需的全部资料，若中标人不配合或者未按合同要求提供服务的，采购人将拒绝验收,验收须以合同、招标文件、澄清、及国家相应的标准、规范等为依据。

3.4.6包装方式及运输

采购包1：

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

采购包2：

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

采购包3：

涉及的商品包装和快递包装，均应符合《商品包装政府采购需求标准（试行）》《快递包装政府采购需求标准（试行）》的要求，包装应适应于远距离运输、防潮、防震、防锈和防野蛮装卸，以确保货物安全无损运抵指定地点。

3.4.7质量保修范围和保修期

采购包1：

质保期三年。

采购包2：

质保期三年。

采购包3：

质保期三年。

3.4.8违约责任与解决争议的方法

采购包1：

（1）按《中华人民共和国民法典》中合同部分的相关条款执行。（2）未按合同要求提供产品或产品质量不能满足技术要求，采购人有权终止合同，并保留追究供应商违约责任的权利。

采购包2：

（1）按《中华人民共和国民法典》中合同部分的相关条款执行。（2）未按合同要求提供产品或产品质量不能满足技术要求，采购人有权终止合同，并保留追究供应商违约责任的权利。

采购包3:

(1) 按《中华人民共和国民法典》中合同部分的相关条款执行。(2) 未按合同要求提供产品或产品质量不能满足技术要求, 采购人有权终止合同, 并保留追究供应商违约责任的权利。

3.5其他要求

1.为保证服务质量和效率, 本项目按照“兼投不兼中”的原则确定中标人, 即: 每个投标人最多只能中标一个包。若同一投标人在不同标包中综合得分排名第一时, 确定其为包号顺序靠前一包的中标人, 其他相关包推荐综合得分排名第二的投标人为该包的中标人。2.知识产权 即供应商应保证采购人不承担任何涉及知识产权法律诉讼的责任。3.投标保证金 (1) 投标保证金退还: A. 未中标供应商: 自中标通知书发出之日起5个工作日内退还未中标供应商的投标保证金, 无需亲自前来办理; B. 中标供应商: 自采购合同签订之日起5个工作日内退还中标供应商的投标保证金。(须携带合同原件或合同复印件(加盖单位鲜章)各一份, 同时将合同扫描件发送至联系人邮箱), 但因中标供应商自身原因导致无法及时退还的除外。(2) 有下列情况之一的, 采购代理机构不予退还其交纳的投标保证金; 情节严重的, 由财政部门将其列入不良行为记录名单, 在一至三年内禁止参加政府采购活动, 并予以通报: A. 开标后在招标文件规定的投标有效期内, 投标供应商撤回其所投投标文件的; B. 中标供应商无正当理由不与采购人签订合同的; C. 中标供应商将中标项目转让给他人, 或者在投标文件中未说明, 且未经采购人同意, 将中标项目分包给他人的; D. 中标供应商拒绝履行合同义务的; E. 中标供应商未按时缴付中标服务费的; F. 由于中标供应商的原因导致中标无效的。4.报价包括产品的供应费及所发生的运输费、杂费(含保险)、商检费、搬运费、安装调试费、培训费等, 包括从产品供应地点到交货地点所包含的一切费用, 报价不可变更, 不受市场价变化的影响, 不受实际数量变化的影响。5.供应商需要在线提交所有通过电子化交易平台实施的政府采购项目的投标文件, 同时, 线下提交纸质投标文件贰份; 若电子投标文件与纸质投标文件不一致的, 以电子投标文件为准; 投标文件装订成册密封(在书脊处标明项目名称、供应商名称(机打或手写均可), 逐页标注连续页码), 在封口处加盖供应商公章; 纸质投标文件递交截止时间与线上开评标时间一致; 纸质投标文件可邮寄递交, 应于递交投标文件截止时间前邮寄到代理机构(地点: 西安市高新区丈八一路1号汇鑫中心D座2206陕西德勤招标有限公司)。6.如提交保函, 建议至少提前一个工作日将保函正本送至采购代理机构, 如提供电子保函, 应将电子保函发送至代理机构指定邮箱deqinlh@126.com。7.供应商需要在线提交所有通过电子化交易平台实施的政府采购项目的响应文件, 同时, 线下提交纸质响应文件正本壹份、副本贰份; 若电子响应文件与纸质响应文件不一致的, 以电子响应文件为准; 响应文件正、副本分别各自装订成册密封(在书脊处标明项目名称、供应商名称(机打或手写均可), 逐页标注连续页码), 在封口处加盖供应商公章; 纸质响应文件递交截止时间与线上开评标时间一致; 纸质响应文件可邮寄递交, 应于递交响应文件截止时间前邮寄到代理机构。

第四章 资格审查

资格审查由采购人或代理机构组建的资格审查小组依据法律法规和招标文件的规定，对投标文件中的资格证明等进行审查，以确定投标人是否具备投标资格，并出具资格审查报告。

资格审查标准及要求如下：

4.1一般资格审查

采购包1：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料
3	单位负责人为同一人或者存在直接控股、管理关系的不同供应商不得参加同一合同项下的政府采购活动； 为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函

采购包2：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料
3	单位负责人为同一人或者存在直接控股、管理关系的不同供应商不得参加同一合同项下的政府采购活动； 为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函

采购包3：

序号	资格审查要求概况	评审点具体描述	关联格式
1	供应商应具备《中华人民共和国政府采购法》第二十二条规定的条件	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函 投标人应提交的相关资格证明材料
2	供应商应提供健全的财务会计制度的证明材料；	供应商需在项目电子化交易系统中按要求上传相应证明文件并进行电子签章。	投标人应提交的相关资格证明材料

3	单位负责人为同一人或者存在直接控股、管理关系的不同供应商不得参加同一合同项下的政府采购活动； 为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。	供应商需在项目电子化交易系统中按要求填写《投标函》完成承诺并进行电子签章。	投标函
---	--	---------------------------------------	-----

4.2特殊资格审查

采购包1:

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照等主体资格证明文件	提供营业执照/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料
2	财务状况报告	提供2024年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
3	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关文件证明。	投标人应提交的相关资格证明材料
4	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据，凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
5	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法
6	控股管理关系	提供直接控股和管理关系清单。若与其他投标供应商存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系
7	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务。	书面声明
8	信用记录	供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）。	投标人应提交的相关资格证明材料

9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件（附在资格证明文件中）；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供法人给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明

采购包2:

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照等主体资格证明文件	提供营业执照/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料
2	财务状况报告	提供 2024 年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
3	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关文件证明。	投标人应提交的相关资格证明材料
4	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据，凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
5	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法
6	控股管理关系	提供直接控股和管理关系清单。若与其他投标供应商存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系
7	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、监理、检测等服务。	书面声明

8	信用记录	供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）。	投标人应提交的相关资格证明材料
9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件（附在资格证明文件中）；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供法人给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明

采购包3:

序号	资格审查要求概况	评审点具体描述	关联格式
1	营业执照等主体资格证明文件	提供营业执照/事业单位法人证书/专业服务机构执业许可证/民办非企业单位登记证书。	投标人应提交的相关资格证明材料
2	财务状况报告	提供 2024 年度经审计的财务报告（成立时间至提交投标文件截止时间不足一年的可提供成立后任意时段的资产负债表），或其开标前三个月内基本开户银行出具的资信证明，或信用担保机构出具的投标担保函（以上三种形式的资料提供任何一种即可）。	投标人应提交的相关资格证明材料
3	社保缴纳证明	提供递交投标文件截止之日前一年内任意一个月的社会保障资金缴存单据或社保机构开具的社会保险参保缴费情况证明。依法不需要缴纳社会保障资金的投标供应商应提供相关文件证明。	投标人应提交的相关资格证明材料
4	税收缴纳证明	提供递交投标文件截止之日前一年内任意一个月的依法缴纳税收的相关凭据，凭据应有税务机关或代收机关的公章或业务专用章。依法免税或无须缴纳税收的投标供应商，应提供相应证明文件。	投标人应提交的相关资格证明材料
5	近三年无重大违法、违纪书面声明	提供《近三年无重大违法、违纪书面声明》。	近三年无重大违法
6	控股管理关系	提供直接控股和管理关系清单。若与其他投标供应商存在单位负责人为同一人或者存在直接控股、管理关系的，则投标无效。	控股管理关系

7	书面声明	提供书面声明，包括声明具有履行合同所必需的设备和专业技术能力；未为本项目提供整体设计、规范编制或者项目管理、检测等服务。	书面声明
8	信用记录	供应商未被列入“信用中国”网站记录的“失信被执行人”或“重大税收违法案件当事人”名单；不处于“中国政府采购网”记录的“政府采购严重违法失信行为记录名单”中的禁止参加政府采购活动期间。（以采购人或采购代理机构开标当天查询结果为准）。	投标人应提交的相关资格证明材料
9	法定代表人授权委托书	法定代表人参加投标的，须提供本人身份证复印件（附在资格证明文件中）；法定代表人授权他人参加投标的，须提供法定代表人授权委托书。招标文件中凡是需要法定代表人盖章之处，非法人单位的负责人均参照执行。法人的分支机构参与投标时，除提供《法定代表人授权委托书》外，还须同时提供法人给分支机构出具的授权书。	法定代表人授权书
10	本项目不接受联合体投标，不允许分包	投标供应商应提供《非联合体不分包投标声明》，视为独立投标，不分包。	非联合体不分包投标声明

4.3 落实政府采购政策资格审查

采购包1:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包2:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

采购包3:

序号	资格审查要求概况	评审点具体描述	关联格式
无			

第五章 评标办法

5.1总则

一、根据《中华人民共和国政府采购法》《中华人民共和国政府采购法实施条例》《政府采购货物和服务招标投标管理办法》《陕西省政府采购评审专家管理实施办法》等法律规章，结合采购项目特点制定本评标办法。

二、评标工作由代理机构负责组织，具体评标事务由采购人或代理机构依法组建的评标委员会负责。评标委员会由采购人代表和评审专家组成。

三、评标工作应遵循公平、公正、科学及择优的原则，并以相同的评标程序和标准对待所有的投标人。

四、本项目采取电子评标，通过项目电子化交易系统完成评标工作。评标委员会成员、采购人、代理机构和投标人应当按照本招标文件规定和项目电子化交易系统操作要求开展或者参加评标活动。

五、评标过程中的书面材料往来均通过项目电子化交易系统传递，投标人通过互认的证书及签章加盖其电子印章后生效。出现无法在线签章的特殊情况，评标委员会成员可以线下签署评标报告，由代理机构对原件扫描后以附件形式上传。

六、评标过程应当独立、保密，任何单位和个人不得非法干预评标活动。投标人非法干预评标活动的，其投标文件将作无效处理；代理机构、采购人及其工作人员、采购人监督人员非法干预评标活动的，将依法追究其责任。

5.2评标委员会

一、评审专家是采取随机方式在政府采购平台的专家库系统（以下简称专家库系统）抽取/由采购人根据《陕西省政府采购评审专家管理实施办法》（陕财办采〔2018〕20号）的规定，报主管部门同意后自行选定。

二、评标委员会成员应当满足并适应电子化采购评审的工作需要，使用已身份认证并具备签章功能的证书，登录项目电子化交易系统进入项目评审功能模块确认身份、签到、推荐评标委员会组长。采购人代表可以使用采购人代表专用签章确认评审意见。

三、评标委员会成员获取解密后的投标文件，开展评标活动。出现应当回避的情形时，评标委员会成员应当主动回避；代理机构按规定申请补充抽取评审专家；无法及时补充抽取的，采购人或者代理机构应当封存供应商投标文件，按规定重新组建评标委员会，解封投标文件后，开展评标活动。

四、评标委员会按照招标文件规定的评标程序、评标方法和标准进行评标，并独立履行下列职责：

- （一）熟悉和理解招标文件；
- （二）审查供应商投标文件等是否满足招标文件要求，并作出评价；
- （三）根据需要要求采购组织单位对招标文件作出解释；根据需要要求供应商对投标文件有关事项作出澄清、说明或者更正；
- （四）推荐中标候选人供应商，或者受采购人委托确定中标供应商；
- （五）起草评标报告并进行签署；
- （六）向采购组织单位、财政部门或者其他监督部门报告非法干预评审工作的行为
- （七）法律、法规和规章规定的其他职责。

5.3 评标方法

采购包1：综合评分法

采购包2：综合评分法

采购包3：综合评分法

5.4评标程序

5.4.1熟悉和理解招标文件和停止评标

一、评标委员会正式评审前，应当对招标文件进行熟悉和理解，内容主要包括招标文件中供应商资格资质性要求、采购项目

技术、服务和商务要求、评审方法和标准以及可能涉及签订政府采购合同的内容等。

二、本招标文件有下列情形之一的，评标委员会应当停止评标：

- （一）招标文件的规定存在歧义、重大缺陷的；
- （二）招标文件明显以不合理条件对供应商实行差别待遇或者歧视待遇的；
- （三）采购项目属于国家规定的优先、强制采购范围，但是招标文件未依法体现优先、强制采购相关规定的；
- （四）采购项目属于政府采购促进中小企业发展的范围，但是招标文件未依法体现促进中小企业发展相关规定的；
- （五）招标文件规定的评标方法是综合评分法、最低评标价法之外的评标方法，或者虽然名称为综合评分法、最低评标价法，但实际上不符合国家规定；
- （六）招标文件将投标人的资格条件列为评分因素的；
- （七）招标文件有违反国家其他有关强制性规定的情形。

出现上述应当停止评标情形的，评标委员会应当通过项目电子化交易系统向采购组织单位提交相关说明材料，说明停止评审的情形和具体理由。除上述情形外，评标委员会不得以任何方式和理由停止评标。

出现上述应当停止评标情形的，采购组织单位应当通过项目电子化交易系统书面告知参加采购活动的供应商，并说明具体原因，同时在陕西省政府采购网公告。采购组织单位认为评标委员会不应当停止评标的，可以书面报告采购项目同级财政部门依法处理，并提供相关证明材料。

5.4.2 符合性审查

评标委员会依据本招标文件的实质性要求，对符合资格的投标文件进行审查，以确定其是否满足本招标文件的实质性要求。本项目符合性审查事项，必须以本招标文件的明确规定的实质性要求作为依据。

在符合性审查过程中，如果出现评标委员会成员意见不一致的情况，按照少数服从多数的原则确定，但不得违背政府采购基本原则和招标文件规定。

符合性审查标准见下表（按以下顺序审查）：

采购包1：

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	<p>1.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细陈述。</p> <p>2.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单

2	投标文件语言及有效期	投标文件语言及有效期符合招标文件要求。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
3	投标文件封面、投标函、法定代表 人授权委托书三处的项目名称、项 目编号、包号(如有)	三处均无遗漏，且与所投项目名称、项目编号、 包号(如有)一致。	投标函 投标文件封面 法定代表人授权书
4	投标文件签署、盖章	均按招标文件要求签章(评分标准中要求提供的证 明材料除外)。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
5	开标一览表	(1)投标报价符合唯一性要求；(2)开标一览表填 写符合要求；(3)计量单位、报价货币均符合招 标文件要求；(4)未超出采购预算或招标文件规 定的最高限价。	开标一览表 标的清单
6	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
7	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函

8	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
---	-----------------------	---------------------------	---

采购包2:

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	<p>1.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细描述。</p> <p>2.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单

2	投标文件语言及有效期	投标文件语言及有效期符合招标文件要求。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
3	投标文件封面、投标函、法定代表 人授权委托书三处的项目名称、项 目编号、包号(如有)	三处均无遗漏，且与所投项目名称、项目编号、 包号(如有)一致。	投标函 投标文件封面 法定代表人授权书
4	投标文件签署、盖章	均按招标文件要求签章(评分标准中要求提供的证 明材料除外)。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
5	开标一览表	(1)投标报价符合唯一性要求；(2)开标一览表填 写符合要求；(3)计量单位、报价货币均符合招 标文件要求；(4)未超出采购预算或招标文件规 定的最高限价。	开标一览表 标的清单
6	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
7	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函

8	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
---	-----------------------	---------------------------	---

采购包3:

序号	符合审查要求概况	评审点具体描述	关联格式
1	不正当竞争预防措施（实质性要求）	<p>1.在评标过程中，评标委员会认为投标人报价明显低于其他实质性响应的投标人报价，有可能影响产品质量或者不能诚信履约的，评标委员会应当要求其在合理的时间内提供成本构成书面说明，并提交相关证明材料。书面说明应当按照国家财务会计制度的规定要求，逐项就投标人提供的货物、工程和服务的主营业务成本（应根据投标人企业类型予以区别）、税金及附加、销售费用、管理费用、财务费用等成本构成事项详细描述。</p> <p>2.投标人提交的相关说明和证明材料，应当加盖投标人（法定名称）电子印章，在评标委员会要求的时间内通过项目电子化交易系统进行提交，否则提交的相关证明材料无效。投标人不能证明其投标报价合理性的，评标委员会应当将其投标文件作为无效处理。</p>	开标一览表 标的清单

2	投标文件语言及有效期	投标文件语言及有效期符合招标文件要求。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
3	投标文件封面、投标函、法定代表 人授权委托书三处的项目名称、项 目编号、包号(如有)	三处均无遗漏，且与所投项目名称、项目编号、 包号(如有)一致。	投标函 投标文件封面 法定代表人授权书
4	投标文件签署、盖章	均按招标文件要求签章(评分标准中要求提供的证 明材料除外)。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
5	开标一览表	(1)投标报价符合唯一性要求；(2)开标一览表填 写符合要求；(3)计量单位、报价货币均符合招 标文件要求；(4)未超出采购预算或招标文件规 定的最高限价。	开标一览表 标的清单
6	商务条款响应	完全理解接受招标文件商务条款。	商务应答表
7	投标保证金	保证金交纳符合招标文件要求。	保证金汇款声明函

8	无其他招标文件或法规明确规定响应无效的事项	没有不符合招标文件规定的被视为无效响应的其他条款。	开标一览表 投标方案 保证金汇款声明函 分 项报价表 中小企业声 明函 商务应答表 控股 管理关系 法定代表人 授权书 投标人应提交 的相关资格证明材料 产品技术参数表 投标 函 残疾人福利性单位 声明函 标的清单 非联 合体不分包投标声明 投标文件封面 近三年 无重大违法 书面声明 监狱企业的证明文件
---	-----------------------	---------------------------	---

以上实质性要求全部响应并满足采购需求的，则通过符合性审查；如有任意一项未响应或不满足采购需求的，则按无效投标文件处理。如果评标委员会认为投标人有任意一项不通过的，应在符合性审查表中载明不通过的具体原因。

5.4.3解释、澄清有关问题

一、评标过程中，评标委员会认为招标文件有关事项表述不明确或需要说明的，可以提请代理机构书面解释。代理机构的解释不得改变招标文件的原义或者影响公平、公正，解释事项如果涉及投标人权益的以有利于投标人的原则进行解释。

二、对投标文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，评标委员会应当要求投标人作出必要的澄清、说明或更正，并给予投标人必要的反馈时间。投标人应当按评标委员会的要求进行澄清、说明或者更正。投标人的澄清、说明或者更正不得超出投标文件的范围或者改变投标文件的实质性内容。澄清、说明或者更正不影响投标文件的效力，有效的澄清、说明或者更正材料是投标文件的组成部分。

三、投标人的澄清、说明或者更正需进行电子签章，应当不超出投标文件的范围、不实质性改变投标文件的内容、不影响投标人的公平竞争、不导致投标文件从不响应招标文件变为响应招标文件的条件。下列内容不得澄清：

- （一）投标人投标文件中不响应招标文件规定的技术参数指标和商务应答；
- （二）投标人投标文件中未提供的证明其是否符合招标文件资格、符合性规定要求的相关材料。
- （三）投标人投标文件中的材料因印刷、影印等不清晰而难以辨认的。

四、投标文件报价出现下列情况的，按以下原则处理：

- （一）投标文件中开标一览表（报价表）内容与投标文件中相应内容不一致的，以开标一览表（报价表）为准；
- （二）大写金额和小写金额不一致的，以大写金额为准，但大写金额出现文字错误，导致金额无法判断的除外；
- （三）单价金额小数点或者百分比有明显错位的，以开标一览表总价为准，并修改单价；
- （四）总价金额与按单价汇总金额不一致的，以单价金额计算结果为准。

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

五、对不同语言文本投标文件的解释发生异议的，以中文文本为准。

六、代理机构宣布评标结束前，投标人应通过项目电子化交易系统随时关注评标消息提示，及时响应评标委员会发出的澄清、说明或更正要求。投标人未能及时响应的，自行承担不利后果。

评标委员会应当积极履行澄清、说明或者更正的职责，不得滥用权力。

5.4.4比较与评价

评标委员会应当按照招标文件规定的评标细则及标准，对符合性检查合格的投标文件进行商务和技术评估，综合比较和评

价。

5.4.5复核

评分汇总结束后，评标委员会应当进行复核，对拟推荐为中标候选人、报价最低、投标文件被认定为无效等进行重点复核。

评标结果汇总完成后，评标委员会拟出具评标报告前，代理机构应当组织不少于2名工作人员，在采购监督人员的监督之下，依据有关的法律制度和招标文件对评标结果进行复核，出具复核报告。

评标结果汇总完成后，除下列情形外，任何人不得修改评标结果：

- （一）分值汇总计算错误的；
- （二）分项评分超出评分标准范围的；
- （三）评标委员会成员对客观评审因素评分不一致的；
- （四）经评标委员会认定评分畸高、畸低的。

评标报告签署前，经复核发现存在以上情形之一的，评标委员会应当当场修改评标结果，并在评标报告中记载；评标报告签署后，采购人或者代理机构发现存在以上情形之一的，应当组织原评标委员会进行重新评标，重新评标改变评标结果的，书面报告本级财政部门。

5.4.6确定中标候选人名单

采购包1：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包2：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

采购包3：按投标人综合得分从高到低进行排序，确定3名中标候选人。综合得分相同的，按投标报价由低到高顺序排列；得分且投标报价相同的，按投标人提供的优先采购产品认证证书数量由多到少顺序排列；得分且投标报价且提供的优先采购产品认证证书数量相同的并列。投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。

5.4.7编写评标报告

评标报告是评标委员会根据全体评标成员签字的评标记录和评标结果编写的报告，其主要内容包括：

- 一、招标公告刊登的媒体名称、开标日期和地点；
- 二、投标人名单和评标委员会成员名单；
- 三、评审方法和标准；
- 四、开标记录和评审情况及说明，包括投标无效供应商名单及原因；
- 五、评标结果，确定的中标候选人名单或者经采购人委托直接确定的中标人
- 六、其他需要说明的情况，包括评标过程中投标人根据评标委员会要求进行的澄清、说明或者补正，评标委员会成员的更换等；
- 七、报价最高的投标人为中标候选人的，评标委员会应当对其报价的合理性予以特别说明。

评标委员会成员应当在评标报告中签字或加盖电子签章确认，对评标过程和结果有不同意见的，应当在评标报告中写明并说明理由。签字但未写明不同意见或者未说明理由的，视同无意见。拒不签字或加盖电子签章又未另行说明其不同意见和理由的，视同同意评标结果。

5.5评标争议处理规则

评标委员会在评标过程中，对于符合性审查、对投标人文件作无效投标处理及其他需要共同认定的事项存在争议的，应当以少数服从多数的原则作出结论，但不得违背法律法规和招标文件规定。持不同意见的评标委员会成员应当在评标报告上签署不同意见及理由，否则视为同意评标报告。持不同意见的评标委员会成员认为认定过程和结果不符合法律法规或者招标文件规定的，应当及时向采购人或代理机构书面反映。采购人或代理机构收到书面反映后，应当书面报告采购项目同级财政部门依法处理

5.6评标细则及标准

一、评标委员会只对通过资格审查的投标文件，根据招标文件的要求采用相同的评标程序、评分办法及标准进行评价和比较。

二、评标委员会成员应依据招标文件规定的评分标准和方法独立评审。

5.6.1评分办法

若采用综合评分法的，由评标委员会各成员对通过资格检查和符合性审查的投标人的投标文件进行独立评审。 投标报价得分=（评标基准价 / 投标报价）×100

评标总得分=F1×A1+F2×A2+.....+Fn×An

F1、F2.....Fn分别为各项评审因素的得分；

A1、A2、.....An 分别为各项评审因素所占的权重（A1+A2+.....+An=1）。

评标过程中，不得去掉报价中的最高报价和最低报价。

因落实政府采购政策进行价格调整的，以调整后的价格计算评标基准价和投标报价。

5.6.2评分标准

采购包1:

评审因素		评审标准			
分值构成		详细评审70.00分 报价得分30.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式
	技术指标	投标人所投产品的技术指标，参数完全满足招标文件规定相应技术指标、参数的得20分；低于招标文件规定相应技术指标、参数的证明材料无法提供的不得分；技术指标不满足的招标文件要求的，每有一项扣1分，扣完为止。 注：部分满足该技术指标的按不满足处理。	20.0000	客观	产品技术参数表 商务应答表 投标方案
	业绩	投标人提供2020年1月1日至今同类项目业绩，每提供一个得1分，最高得5分。 注：需提供合同（包含合同首页、关键内容页及签署页）复印件并加盖本单位公章有效证明文件。不符合上述要求或未按要求提供有效证明文件的业绩在评审时不得分。	5.0000	客观	产品技术参数表 商务应答表 投标方案

详细评审	项目实施方案	<p>投标人针对本项目的实施方案，包括：1、提供具体可行的实施方案，具体的供货组织安排；2、详细的人员、调配、运输、派送措施及设备到货后验收；3、实施进度及保证措施设备安装；4、人员组成及人员调配、安装调试等。</p> <p>1.方案完整全面，实施方案组织合理，调配运输方案清晰明确，进度保障措施先进可靠，能够切实保障项目时效性的，得 20 分；2.方案基本完整，实施方案组织较合理，调配运输方案基本清晰，进度保障措施具备一定可靠性，得 15 分；3.方案完整性一般，实施方案组织存在一定不合理性，调配运输方案清晰度不足，进度保障措施可靠性一般，得 10 分；4.方案完整性差，实施方案组织混乱，调配运输方案不清晰，进度保障措施不可靠，对项目时效性无法保障得 5 分；6.未响应不得分。</p>	20.0000	主观	产品技术参数表 商务应答表 投标方案
	售后服务	<p>针对本项目提供售后服务方案，内容包含：1、为本项目配备的售后服务团队；2、为本项目提供的后期运维及提升等服务承诺；3、可提供增值服务；4、保修期的保修范围和维护期的服务范围等。</p> <p>1.方案描述详尽清晰，可行性高，内容完整无缺项漏项，能充分满足本项目售后服务需求的，得 12 分；2.方案描述较详尽，可行性较好，内容基本完整无缺项，得 9 分；3.方案描述清晰度一般，可行性一般，内容完整性不足，基本能满足项目基础售后服务需求的，得 6 分；4.方案描述模糊，可行性差，内容完整性差，不能满足项目售后服务需求的，得 3 分；5.未响应不得分。</p>	12.0000	主观	产品技术参数表 商务应答表 投标方案

	培训方案	针对本项目有具体的培训方案，内容包含：1、培训地点及时间安排；2、培训内容安排，内容至少应包括：所提供产品的原理和技术性能、操作维护方法、安装调试、排除故障等各个方面；3、现场及远程培训方案；4、拟派培训人员团队。1. 方案描述详尽清晰，可行性高，内容完整无缺项漏项，能全面覆盖培训需求且可直接落地执行的，得12分；2.方案描述较详尽，可行性较好，内容基本完整无缺项，得9分；3.方案描述清晰度一般，可行性一般，内容完整性不足，仅能满足基础培训需求的，得6分；4.方案描述模糊，可行性差，内容完整性差，不能支撑正常培训开展的，得3分；5.未响应不得分。	12.0000	主观	产品技术参数表 商务应答表 投标方案
	保密	投标人应承诺不得泄露采购单位一切敏感信息，包括但不限于技术情报、技术资料、商业秘密和商业信息等，提供保密措施方案，内容应包括：（1）保密管理制度和规章制度；（2）人员保密规划；（3）保密应急三个方面分别阐述。内容全面、符合本项目要求得1分；内容简单、不完全符合或有缺失不得分。	1.0000	主观	产品技术参数表 商务应答表 投标方案
价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算：投标报价得分=(评标基准价 / 投标报价) ×100计算分数时四舍五入取小数点后两位。	30.0000	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件
---	-----------------------	--------------------	--------	--	--

采购包2:

评审因素		评审标准			
分值构成		详细评审70.00分 报价得分30.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式
	技术指标	投标人所投产品的技术指标，参数完全满足招标文件规定相应技术指标、参数的得10分；低于招标文件规定相应技术指标、参数的证明材料无法提供的不得分；技术指标不满足的招标文件要求的，每有一项扣1分，扣完为止。注：部分满足该技术指标的按不满足处理。	10.0000	客观	产品技术参数表 商务应答表 投标方案

其他要求	<p>（1）安全认证网关：通过国家网络与信息系统安全产品质量检验检测中心的漏洞覆盖测试，提供《信息技术产品安全测试证书》；具有IPv6 Ready logo认证证书；具备信创产品认证证明；支持用户信息绑定为应用提供身份凭据，使用HMAC-SM3 算法保护信息真实性和完整性。提供相关证明材料，并加盖公章。全部满足得2.5分。（2）签名验签服务器：通过国家网信安检中心的漏洞覆盖测试，获得《信息技术产品安全测试证书》；具有IPv6 Ready logo认证证书；具备信创产品认证证明；支持CMac、HMac、条形码生成、二维码生成、上传证书、获取随机数等接口；支持对数据和文件进行签名验签，最大签名数据或文件不小于1G。提供相关证明材料，并加盖公章。全部满足得2.5分。（3）时间戳服务器：具备国家版权局颁发的《计算机软件著作权登记证书》；具备CNAS中国认可检测机构出具的软件测试报告；提供相关信创软件的适配和认证证明，支持包括但不限于南大通用、翰高、人大金仓、达梦等数据库，支持包括但不限于金蝶、东方通等中间件产品。提供相关证明材料，并加盖公章。全部满足得2.5分。</p> <p>（4）数据库加密网关：支持字段级的机密性和完整性保护，支持对不同的数据字段项设置不同的密钥和加密算法；对配置了加密字段作为查询条件时，对条件值进行加密后进行查询，且支持对姓名、身份证、手机号码等密文数据进行模糊查询。提供相关证明材料，并加盖公章。全部满足得2.5分。</p>	10.0000	客观	产品技术参数表 商务应答表 投标方案
------	---	---------	----	--------------------------

详细评审	业绩	投标人提供2020年1月1日至今同类项目业绩，每提供一个得1分，最高得6分。注：需提供合同（包含合同首页、关键内容页及签署页）复印件并加盖本单位公章有效证明文件。不符合上述要求或未按要求提供有效证明文件的业绩在评审时不得分。	6.0000	客观	产品技术参数表 商务应答表 投标方案
	项目实施方案	投标人针对本项目的实施方案，包括：1、提供具体可行的实施方案，具体的供货组织安排；2、详细的人员、调配、运输、派送措施及设备到货后验收；3、实施进度及保证措施设备安装；4、人员组成及人员调配、安装调试等。1.方案完整全面，实施方案组织合理，调配运输方案清晰明确，进度保障措施先进可靠，能够切实保障项目时效性的，得 20 分；2.方案基本完整，实施方案组织较合理，调配运输方案基本清晰，进度保障措施具备一定可靠性，得 15 分；3.方案完整性一般，实施方案组织存在一定不合理性，调配运输方案清晰度不足，进度保障措施可靠性一般，得 10 分；4.方案完整性差，实施方案组织混乱，调配运输方案不清晰，进度保障措施不可靠，对项目时效性无法保障得 5 分；6.未响应不得分。	20.0000	主观	产品技术参数表 商务应答表 投标方案

售后服务	<p>针对本项目提供售后服务方案，内容包含：1、为本项目配备的售后服务团队；2、为本项目提供的后期运维及提升等服务承诺；3、可提供增值服务；4、保修期的保修范围和维护期的服务范围等。</p> <p>1.方案描述详尽清晰，可行性高，内容完整无缺项漏项，能充分满足本项目售后服务需求的，得 12 分；2.方案描述较详尽，可行性较好，内容基本完整无缺项，得 9 分；3.方案描述清晰度一般，可行性一般，内容完整性不足，基本能满足项目基础售后服务需求的，得 6 分；4.方案描述模糊，可行性差，内容完整性差，不能满足项目售后服务需求的，得 3 分；5.未响应不得分。</p>	12.0000	主观	产品技术参数表 商务应答表 投标方案
培训方案	<p>针对本项目有具体的培训方案，内容包含：1、培训地点及时间安排；2、培训内容安排，内容至少应包括：所提供产品的原理和技术性能、操作维护方法、安装调试、排除故障等各个方面；3、现场及远程培训方案；4、拟派培训人员团队。</p> <p>1.方案描述详尽清晰，可行性高，内容完整无缺项漏项，能全面覆盖培训需求且可直接落地执行的，得 12 分；2.方案描述较详尽，可行性较好，内容基本完整无缺项，得 9 分；3.方案描述清晰度一般，可行性一般，内容完整性不足，仅能满足基础培训需求的，得 6 分；4.方案描述模糊，可行性差，内容完整性差，不能支撑正常培训开展的，得 3 分；5.未响应不得分。</p>	12.0000	主观	产品技术参数表 商务应答表 投标方案

价格分	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算：投标报价得分= $(\text{评标基准价} / \text{投标报价}) \times 100$ 计算分数时四舍五入取小数点后两位。	30.0000	客观	开标一览表 标的清单
-----	-----	--	---------	----	---------------

价格扣除

序号	情形	适用对象	比例	说明	关联格式
1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）;监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	开标一览表 中小企业声明函 残疾人福利性单位声明函 标的清单 监狱企业的证明文件

采购包3:

评审因素		评审标准			
分值构成		详细评审100.00分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式

	项目理解	根据对本项目的业务需求和系统建设进行需求分析： 1.分析清晰、合理、深入、准确的，得10分； 2.分析基本合理、存在部分内容理解不够准确的，得6分； 3.分析没有针对性或业务流程掌握不准确、分析与业务需求有较大偏差的，得3分。 4.未响应不得分。	10.0000	主观	产品技术参数表 商务应答表 投标方案
	重点难点分析	对本项目关键点把控和重点难点分析符合项目实际情况： 1.分析清晰、合理、深入、准确的，得10分； 2.分析基本合理、存在部分内容理解不够准确的，得6分； 3.分析没有针对性或业务流程掌握不准确、分析与业务需求有较大偏差的，得3分。 4.未响应不得分。	10.0000	主观	产品技术参数表 商务应答表 投标方案
	合理化建议分析	对本项目关键点把控和重点难点分析提出的合理化建议，具有针对性与可行性： 1.符合项目实际情况的，得10分； 2.提出的建议可行性一般或不完全符合项目实际情况的，得6分； 3.提出的建议针对性较差的，得3分。 4.未响应不得分。	10.0000	主观	产品技术参数表 商务应答表 投标方案
	质量控制方法和措施	1.质量控制原则，描述内容详细完整，控制原则有针对性、切实可行，得3分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 2.质量控制总思路，描述内容有完整，有详细的质量控制组织框架，得3分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 3.质量控制方法，描述内容详细完整，质量控制方法科学、切实可行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 4.质量控制措施，描述内容详细完整，质量控制措施完善、有针对性且可执行，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。	10.0000	主观	产品技术参数表 商务应答表 投标方案

详细评审	进度控制方法和措施	1.进度控制原则，描述内容详细完整，进度控制原则符合项目需求，方案合理可行，得4分；方案基本合理，内容基本完整，得2分；内容不合理或未响应不得分； 2.进度控制方法，描述内容详细完整，进度控制方法科学、可执行，得3分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 3.进度控制措施，描述内容详细完整，质量控制措施完善、有针对性且可执行，得3分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。	10.0000	主观	产品技术参数表 商务应答表 投标方案
	投资控制方法和措施	1.投资控制原则，描述内容详细完整，投资控制原则规范、合理可行，得4分；方案基本合理，内容基本完整，得2分；内容不合理或未响应不得分； 2.投资控制方法，描述内容详细完整，投资控制方法符合项目控制目标，针对性强，得3分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分； 3.投资控制措施，描述内容详细完整，质量控制措施完善、有针对性且可执行，得3分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。	10.0000	主观	产品技术参数表 商务应答表 投标方案

项目安全、合同、变更、信息管理方案	1.项目安全管理方案目标明确、措施方法合理可行，且具有针对性，符合本项目实际需求，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。 2.项目合同管理方案目标明确、措施方法合理可行，且具有针对性，符合本项目实际需求，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。 3.项目变更管理方案目标明确、措施方法合理可行，且具有针对性，符合本项目实际需求，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。 4.项目信息管理方案目标明确、措施方法合理可行，且具有针对性，符合本项目实际需求，得2分；方案基本合理，内容基本完整，得1分；内容不合理或未响应不得分。	8.0000	主观	产品技术参数表 商务应答表 投标方案
组织协调方法和措施	协调难点分析准确，协调工作程序和会议制度等明确，措施方法合理可行，且具有针对性，得6分；方案基本合理，内容基本完整，得3分；内容不合理或未响应不得分。	6.0000	主观	产品技术参数表 商务应答表 投标方案
项目实施和风险控制措施	监理工作的组织实施与计划安排细致、周全、合理、详尽风险控制措施有力，得10分； 监理工作的组织实施与计划安排较细致、较周全、较合理、较详尽，风险控制措施较有力，得6分； 监理工作的组织实施与计划安排一般，风险控制措施一般，得3分； 未提供项目实施进度计划和安排的不得分。	10.0000	主观	产品技术参数表 商务应答表 投标方案

	业绩	投标人提供 2021年1月1日 至今（以合同签订时间为准）同类项目业绩，每提供一个得 2分 ，最多得 6分 。 投标人需提供项目案例合同关键页（包括但不限于合同封面页、合同双方、服务内容、签字盖章、生效时间等）复印件或扫描件并加盖公章，否则不得分。	6.0000	客观	产品技术参数表 商务应答表 投标方案
	价格分	价格分统一采用低价优先法计算，即满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标供应商的价格分统一按照下列公式计算：投标报价得分= $(\text{评标基准价} / \text{投标报价}) \times 100$ 计算分数时四舍五入取小数点后两位。注：对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予 10% 的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予 10% 的价格扣除，即：评标价= $\text{最后报价} \times (1-10\%)$ ；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	10.0000	客观	开标一览表 标的清单

价格扣除

序号	情形	适用对象	比例	说明	关联格式
----	----	------	----	----	------

1	小型、微型企业，监狱企业，残疾人福利性单位	投标人或联合体成员均为小型、微型企业	10.00%	对于经主管预算单位统筹后未预留份额专门面向中小企业采购的采购项目，以及预留份额项目中的非预留部分采购包，对符合《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）规定的小微企业报价给予C1的扣除，用扣除后的价格参加评审。承接本项目的供应商符合相应条件时，给予C1的价格扣除，即：评标价=最后报价×（1-C1）；监狱企业与残疾人福利性单位视同小型、微型企业，享受同等价格扣除，当企业属性重复时，不重复价格扣除	中小企业声明函 残疾人福利性单位声明函 监狱企业的证明文件
---	-----------------------	--------------------	--------	--	-------------------------------

说明：

- 1、评分的取值按四舍五入法，保留小数点后两位；
- 2、评分标准中要求提供复印件的证明材料须清晰可辨。

若采用最低评标价法的，投标文件满足招标文件全部实质性要求，且投标报价最低的投标人为中标候选人。采用最低评标价法评标时，除了算术修正和落实政府采购政策需进行的价格扣除外，不能对投标人的投标价格进行任何调整。

5.7废标

本次政府采购活动中，出现下列情形之一的，予以废标：

- 一、符合专业条件的投标人或者对招标文件作实质响应的投标人不足三家的；
- 二、出现影响采购公正的违法、违规行为的；
- 三、投标人的报价均超过了采购预算，采购人不能支付的；
- 四、因重大变故，采购任务取消的；

废标后，代理机构将在“陕西省政府采购网”上公告。对于评标过程中废标的采购项目，评标委员会应当对招标文件是否存在不合理条款进行论证，并出具书面论证意见。

5.8定标

5.8.1 定标原则

采购人在评标报告确定的中标候选人名单中按顺序确定1名中标人。中标候选人并列的，由采购人采取随机抽取的方式确定中标人。

5.8.2定标程序

- 一、评标委员会在项目电子化交易系统中编制评标情况，生成评标报告。

二、代理机构在评标结束之日起2个工作日内将评标报告送采购人。

三、采购人在收到评标报告后5个工作日内，按照评标报告中推荐的中标候选人顺序确定中标供应商。逾期未确认的，又不能说明合法理由的，视同按评标报告推荐的顺序确定排名第一的中标候选人为中标供应商。

四、根据确定的中标供应商，代理机构在陕西省政府采购网上发布中标结果公告，通过项目电子化交易系统向中标供应商发出中标通知书。

5.9评审专家在政府采购活动中承担以下义务

- （一）遵守评审工作纪律；
- （二）按照客观、公正、审慎的原则，根据采购文件规定的评审程序、评审方法和评审标准进行独立评审；
- （三）不得泄露评审文件、评审情况和在评审过程中获悉的商业秘密；
- （四）及时向监督管理部门报告评审过程中的违法违规情况，包括采购组织单位向评审专家作出倾向性、误导性的解释或者说明情况，供应商行贿、提供虚假材料或者串通情况，其他非法干预评审情况等；
- （五）发现采购文件内容违反国家有关强制性规定或者存在歧义、重大缺陷导致评审工作无法进行时，停止评审并通过项目电子化交易系统向采购组织单位书面说明情况，说明停止评审的情形和具体理由；
- （六）配合答复处理供应商的询问、质疑和投诉等事项；
- （七）法律、法规和规章规定的其他义务。

5.10评审专家在政府采购活动中应当遵守以下工作纪律

- （一）遵行《中华人民共和国政府采购法》第十二条和《中华人民共和国政府采购法实施条例》第九条及财政部关于回避的规定。
- （二）评审前，应当将通讯工具或者相关电子设备交由采购组织单位统一保管。
- （三）评审过程中，不得与外界联系，因发生不可预见情况，确实需要与外界联系的，应当在监督人员监督之下办理。
- （四）评审过程中，不得干预或者影响正常评审工作，不得发表倾向性、引导性意见，不得修改或细化采购文件确定的评审程序、评审方法、评审因素和评审标准，不得接受供应商主动提出的澄清和解释，不得征询采购人代表的意见，不得协商评分，不得违反规定的评审格式评分和撰写评审意见，不得拒绝对自己的评审意见签字确认。
- （五）在评审过程中和评审结束后，不得记录、复制或带走任何评审资料，除因配合答复处理供应商的询问、质疑和投诉等事项外，不得向外界透露评审内容。
- （六）服从评审现场采购组织单位的现场秩序管理，接受评审现场监督人员的合法监督。
- （七）遵守有关廉洁自律规定，不得私下接触供应商，不得收受供应商及有关业务单位和个人的财物或好处，不得接受采购组织单位的请托。

第六章 投标文件格式

采购包1:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：投标人应提交的相关资格证明材料

详见附件：产品技术参数表

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：保证金汇款声明函

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：近三年无重大违法

详见附件：控股管理关系

详见附件：书面声明

详见附件：投标方案

采购包2:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：投标人应提交的相关资格证明材料

详见附件：产品技术参数表

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：保证金汇款声明函

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：近三年无重大违法

详见附件：控股管理关系

详见附件：书面声明

详见附件：投标方案

采购包3:

分册名称：投标响应文件分册

详见附件：投标文件封面

详见附件：投标函

详见附件：中小企业声明函

详见附件：残疾人福利性单位声明函

详见附件：监狱企业的证明文件

详见附件：投标人应提交的相关资格证明材料

详见附件：产品技术参数表

详见附件：商务应答表

详见附件：开标一览表

详见附件：标的清单

详见附件：保证金汇款声明函

详见附件：法定代表人授权书

详见附件：非联合体不分包投标声明

详见附件：分项报价表

详见附件：近三年无重大违法

详见附件：控股管理关系

详见附件：书面声明

详见附件：投标方案

第七章 拟签订合同文本

详见附件：拟签订合同文本.docx

