

磋商文件

(服务类)

采购项目名称：西安市全民健康信息平台升级建设项目密码应用改造

采购项目编号：**SDZC2024-282**

西安市卫生统计信息中心

陕西上德招标有限公司共同编制

2024年11月20日

第一章 竞争性磋商邀请

陕西上德招标有限公司（以下简称“代理机构”）受西安市卫生统计信息中心委托，拟对西安市全民健康信息平台升级建设项目密码应用改造采用竞争性磋商采购方式进行采购，兹邀请供应商参加本项目的竞争性磋商。

一、项目编号：SDZC2024-282

二、项目名称：西安市全民健康信息平台升级建设项目密码应用改造

三、磋商项目简介

西安市全民健康信息平台升级建设项目密码应用改造

四、邀请供应商

本次采购采取公告征集邀请磋商的供应商。

公告征集：本次竞争性磋商在“陕西省政府采购网（www.ccgp-shaanxi.gov.cn）”上以公告形式发布，兹邀请符合本次采购要求的供应商参加本项目的竞争性磋商。

五、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：

落实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、提供投标人合法注册的法人或其他组织的营业执照/事业单位法人证书/非企业专业服务机构执业许可证/民办非企业单位登记证书；提供投标人合法注册的法人或其他组织的营业执照/事业单位法人证书/非企业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：财务状况报告：提供具有财务审计资质单位出具的2022年或2023年度财务报告（成立时间至开标时间不足一年的可提供成立后任意时段的资产负债表）或开标前六个月内其基本账户银行出具的资信证明或政府采购信用担保机构认可的担保函；

3、税收缴纳证明：税收缴纳证明：提供截止至开标时间前六个月内任意一个月的缴纳凭据；（增值税、企业所得税至少提供一种，依法免税的供应商应提供相关文件证明）；

4、社会保障资金缴纳证明：社会保障资金缴纳证明：提供截止至开标时间前六个月内任意一个月的社保缴纳凭据或社保机构开具的社会保险参保缴纳情况证明；（依法不需要缴纳社会保障资金的供应商应提供相关证明）；

5、提供具有履行本合同所必需的设备和专业技术能力的说明及承诺：提供具有履行本合同所必需的设备和专业技术能力的说明及承诺（提供书面说明及承诺，加盖供应商公章）；

6、提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明：提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明（提供书面声明，加盖供应商公章）；

7、法定代表人授权委托书：法定代表人授权委托书（附法定代表人身份证复印件及被授权人身份证复印件）；法定代表人直接参加磋商只须提供法定代表人资格证明书（附法定代表人身份证复印件）；采购文件凡是法定代表人之处，非法人单位的负责人均参照执行（式样见响应文件格式）；

8、信用信息查询：不得为“信用中国”网站(<http://www.creditchina.gov.cn>)列入“失信被执行人（页面跳转至“中国执行

信息公开网”<http://zxgk.court.gov.cn/shixin/>)、重大税收违法失信主体、政府采购严重违法失信行为记录名单”的供应商；不得为中国政府采购网(<http://www.ccgp.gov.cn>)“政府采购严重违法失信行为记录名单”中的供应商。（根据财库【2019】38号文规定，此项在磋商截止日当天在“信用中国”网站和中国政府采购网站进行查询，截图留档；如网站无供应商信息的，供应商须提供相关证明资料或书面声明）；

9、控股关系：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。（根据财库【2019】38号文规定，此项在磋商截止日当天在“国家企业信用信息公示系统”进行查询，截图留档；如网站无供应商信息的，供应商须提供相关证明资料或书面声明）。

六、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

七、竞争性磋商文件获取时间、方式及地址

（一）磋商文件获取时间：详见采购公告或邀请书。

（二）在磋商文件获取开始时间前，采购人或代理机构将本项目磋商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磋商文件。成功获取磋商文件的，供应商将收到已获取磋商文件的回执函。未成功获取磋商文件的供应商，不得参与本次采购活动，不得对磋商文件提起质疑。

成功获取磋商文件后，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响应文件编制的，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磋商文件，供应商应当重新获取磋商文件；澄清或者修改后的磋商文件发布日期距提交响应文件截止日期不足5日的，采购人或代理机构顺延提交响应文件的截止时间。供应商未重新获取磋商文件或者未按照澄清或者修改后的磋商文件编制响应文件进行响应的，自行承担不利后果。

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

八、首次响应文件提交截止时间及开启时间、地点、方式

(一) 提交首次响应文件截止时间及开启时间：详见采购公告或邀请书。

(二) 响应文件提交方式、地点：供应商应当在提交首次响应文件截止时间前，通过项目电子化交易系统提交响应文件。成功提交的，供应商将收到已提交响应文件的回执函。

九、磋商方式

本项目磋商小组与供应商通过项目电子化交易系统以在线方式进行磋商。磋商会议由磋商小组在线主持，供应商代表在线参加。供应商应随时关注项目电子化交易系统信息，及时参与在线磋商。供应商登录项目电子化交易系统，与磋商小组进行在线磋商、提交供应商响应表，供应商响应表应加盖供应商（法定名称）电子印章。

十、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，凭项目成交结果、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。

十一、联系方式

采购人：西安市卫生统计信息中心

地址：西安市未央区凤城八路109号

邮编：710000

联系人：孟圆伟

联系电话：029-86787930

代理机构：陕西上德招标有限公司

地址：西安市经开区凤城八路正尚国际金融广场A座7层703（张家堡转盘东南角）

邮编：710000

联系人：李艳洁（4号工位）、王涛

联系电话：029-86673953、86518381转8004

采购监督机构：西安市财政局政府采购管理处

联系人：杜新星

联系电话：029-89821846

第二章 供应商须知

2.1 供应商须知前附表

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1：1,370,000.00元</p> <p>供应商采购包报价高于采购包采购预算的，其响应文件将按无效处理。</p>
2	最高限价（实质性要求）	<p>详见第三章。</p> <p>供应商的采购包响应报价高于最高限价的，其响应文件将按无效处理。</p>
3	评审方法	综合评分法(详见第六章)。
4	是否接受联合体	<p>采购包1：不接受</p> <p>如以联合体响应的，联合体各方均应当具备本磋商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磋商项目必备的条件，如相应的人力、物力、资金等。</p> <p>（2）磋商文件对供应商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/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，否则作无效响应处理。</p> <p>3.本项目采购的/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/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）	<p>（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）根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46号）第九条和《关于进一步加大政府采购支持中小企业力度的通知》（财库〔2022〕19号）的规定。</p> <p>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六章。</p> <p>（其他情形）不适用。</p>

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>提供相同品牌产品且通过资格审查、符合性审查的不同供应商参加同一合同项下采购活动的，按一家供应商计算，评审后得分最高的同品牌供应商获得成交供应商推荐资格；最后评审得分相同的，由采购人或者采购人委托磋商小组采取随机抽取方式确定一个供应商获得成交供应商推荐资格，其他同品牌供应商不作为成交候选人。</p> <p>核心产品清单详见第三章。</p> <p>在符合性审查、有效报价环节提供核心产品品牌不足3个的，视为有效响应供应商不足3家。</p>
8	不正当竞争预防措施（实质性要求）	<p>在磋商过程中，磋商小组认为供应商报价明显低于其他通过符合性审查供应商的报价，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在合理的时间内通过项目电子化交易系统书面说明，必要时提交相关证明材料。供应商提交的书面说明和相关证明材料，应当加盖供应商公章，在磋商小组要求的时间内通过项目电子化交易系统进行提交，否则提交的相关材料无效，视为不能证明其响应报价合理性。供应商不能证明其响应报价合理性的，磋商小组应当将其响应文件作为无效处理。</p>
9	磋商保证金	缴交方式：否
10	标书费信息	免费获取
11	履约保证金（实质性要求）	采购包1：不缴纳
12	响应有效期（实质性要求）	提交首次响应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）	本项目不收取代理服务费
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	成交通知书	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成交供应商发出成交通知书；成交供应商通过项目电子化交易系统获取成交通知书。
16	政府采购合同公告、备案	<p>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；</p> <p>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。</p>
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
19	特殊情况	<p>出现下列情形之一的，采购人或者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：</p> <p>（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；</p> <p>（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；</p> <p>（三）其他无法保证电子化交易的公平、公正和安全的情况。</p> <p>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终止采购活动。</p>

2.2总则

2.2.1适用范围

一、本磋商文件仅适用于本次竞争性磋商采购项目。

二、本磋商文件的最终解释权由西安市卫生统计信息中心和陕西上德招标有限公司享有。对磋商文件中供应商参加本次政府采购活动应当具备的条件，磋商项目技术、服务、商务及其他要求，评审细则及标准由西安市卫生统计信息中心负责解释。除上述磋商文件内容，其他内容由陕西上德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。本次磋商的采购人是西安市卫生统计信息中心。

二、“供应商”是指在按照磋商公告规定获取磋商文件，拟参加响应和向采购人提供货物、工程或服务的法人、其他组织或自然人。

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上德招标有限公司。

四、“网上开启”是指供应商通过项目电子化交易系统在线完成签到、响应文件解密后，采购人或者采购代理机构通过项目电子化交易系统在线完成已解密响应文件的开启工作。

五、“电子评审”是指通过项目电子化交易系统在线完成资格审查小组、磋商小组组建，开展资格和符合性审查、比较与评价、出具磋商报告、推荐成交候选供应商等活动。

2.2.3响应费用（实质性要求）

供应商应自行承担参加竞争性磋商采购活动的全部费用。

2.3磋商文件

2.3.1磋商文件的构成

一、磋商文件是供应商准备响应文件和参加响应的依据，同时也是评审的重要依据。磋商文件用以阐明磋商项目所需的资质、技术、服务及报价等要求、磋商程序、有关规定和注意事项以及合同草案条款等。本磋商文件包括以下内容：

- （一）竞争性磋商邀请；
- （二）供应商须知；
- （三）磋商项目技术、服务、商务及其他要求；
- （四）资格审查；
- （五）磋商过程中可实质性变动的内容；
- （六）磋商办法；
- （七）响应文件格式；
- （八）拟签订采购合同文本。

二、供应商应认真阅读和充分理解磋商文件中所有的事项、格式条款和规范要求。供应商没有对磋商文件全面作出实质性响应所产生的风险由供应商承担。

2.3.2磋商文件的澄清和修改

一、在提交首次响应文件截止时间前，采购人或者代理机构可以对已发出的磋商文件进行必要的澄清或者修改。

二、澄清或者修改的内容为磋商文件的组成部分，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，供应商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。更正内容可能影响响应文件编制的，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磋商文件，供应商应依据更正后的磋商文件编制响应文件。若供应商未按前述要求进行响应的，自行承担不利后果。

2.4响应文件

2.4.1响应文件的语言

一、供应商提交的响应文件以及供应商与磋商小组在磋商过程中的所有来往书面文件均须使用中文。响应文件中如附有外

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，磋商小组将其视为无效材料。

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供应商的不利后果，由供应商承担。

2.4.2 计量单位

除磋商文件中另有规定外，本项目均采用国家法定的计量单位。

2.4.3 响应货币

本次项目均以人民币报价。

2.4.4 知识产权

一、供应商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，如存在前述情形，由供应商承担所有相关责任。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、供应商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，供应商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、如采用供应商所不拥有的知识产权，则在报价中必须包括合法使用该知识产权的相关费用。

四、构成本磋商文件的各组成部分，未经采购人书面同意，供应商不得擅自复印或用于非本磋商项目所需的其它目的。

2.4.5 响应文件的组成（实质性要求）

供应商应按照磋商文件的规定和要求编制响应文件。

响应文件具体内容详见第七章。

2.4.6 响应文件格式

一、供应商应按照磋商文件第七章中提供的“响应文件格式”填写相关内容。

二、对于没有格式要求的响应文件由供应商自行编写。

2.4.7 响应报价（实质性要求）

一、供应商的报价是供应商响应磋商项目要求的全部工作内容的价格体现，包括供应商完成本项目所需的一切费用。

二、响应文件报价出现前后不一致的，按照磋商文件第六章磋商办法规定予以修正，修正后的报价经供应商通过项目电子化交易系统进行确认，并加盖供应商（法定名称）电子印章，供应商逾时确认的，其响应无效。

2.4.8 响应有效期（实质性要求）

响应有效期详见第二章“供应商须知前附表”，响应文件未明确响应有效期或者响应有效期小于“供应商须知前附表”中响应有效期要求的，其响应文件按无效处理。

2.4.9 响应文件的制作、签章和加密

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、供应商应按照客户端操作要求，对应磋商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磋商文件对应项的要求的，其响应文件作无效处理。

三、供应商完成响应文件编制后，应按照响应文件第1章明确的签章要求，使用互认的证书及签章对响应文件进行电子签章和加密。

四、磋商文件澄清或者修改的内容可能影响响应文件编制的，代理机构将重新发布澄清或者修改后的磋商文件，供应商应重新获取澄清或者修改后的磋商文件，按照澄清或者修改后的磋商文件进行响应文件编制、签章和加密。

2.4.10 响应文件的提交（实质性要求）

一、供应商应当在提交首次响应文件截止时间前，通过项目电子化交易系统完成响应文件提交。

二、在提交首次响应文件截止时间后，代理机构不再接受供应商提交响应文件。供应商应充分考虑影响响应文件提交的各

种因素，确保在提交首次响应文件截止时间前完成提交。

2.4.11响应文件的补充、修改（实质性要求）

响应文件提交截止时间前，供应商可以补充、修改或者撤回已成功提交的响应文件；对响应文件进行补充、修改的，应当先行撤回已提交的响应文件，补充、修改后重新提交。

供应商响应文件撤回后，视为未提交过响应文件。

2.5开启、资格审查、磋商和确定成交供应商

2.5.1磋商开启程序

一、本项目为竞争性磋商项目。网上开启的开始时间为响应文件提交截止时间。成功提交或解密电子响应文件的供应商不足3家的，不予开启，采购人或代理机构将终止采购活动。

二、磋商开启准备工作

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、解密响应文件（实质性要求）

响应文件提交截止时间后，成功提交响应文件的供应商符合响应文件规定数量的，代理机构将启动响应文件解密程序，解密时间为30分钟；供应商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交易系统进行响应文件解密。供应商未在规定的解密时间内完成解密的，按无效响应处理。

开启过程中，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。供应商对开启过程和开启记录有疑义，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供应商提出的询问或者回避申请应当及时处理。

2.5.2查询及使用信用记录

开启结束后，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，查询供应商在响应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，以一个供应商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

详见磋商文件第四章。

2.5.4磋商

详见磋商文件第六章。

2.5.5成交通知书

一、采购人或者磋商小组确认成交供应商后，代理机构在陕西省政府采购网发布成交结果公告、通过项目电子化交易系统发出成交通知书，成交供应商通过项目电子化交易系统获取成交通知书。

二、成交通知书是采购人和成交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、规章制度规定的成交无效情形的，将以公告形式宣布发出的成交通知书无效，成交通知书将自动失效，并依法重新确定成交供应商或者重新开展采购活动。

三、成交通知书对采购人和成交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、采购人应在成交通知书发出之日起三十日内与成交供应商签订采购合同。

二、采购人和成交供应商签订的采购合同不得对磋商文件确定的事项以及成交供应商的响应文件作实质性修改。

2.6.2合同分包和转包（实质性要求）

2.6.2.1合同分包

一、供应商根据磋商文件的规定和采购项目的实际情况，拟在成交后将成交项目的非主体、非关键性工作分包的，应当在响应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，必须与成交的一致。

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，不属于成交供应商的主要合同义务。

三、采购合同实行分包履行的，成交供应商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。履行分包项目事项应当具备法定资质规定要求的，分包供应商应当具备相应资质。

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。

2.6.2.2合同转包

一、严禁成交供应商将本采购项目采购合同转包。本项目所称转包，是指成交供应商签订政府采购合同后，不履行合同约定的责任和义务，将其全部工程转给他人或者将其全部工程肢解以后以分包的名义分别转给其他单位承包的行为。

二、成交供应商转包的，视同拒绝履行政府采购合同，将依法追究法律责任。

2.6.3合同公告

采购人应当自政府采购合同签订（双方当事人均已完成盖章）之日起2个工作日内，在陕西省政府采购网公告本项目采购合同，但合同中涉及国家秘密、商业秘密的内容除外。

2.6.4合同备案

采购人自政府采购合同签订（双方当事人均已完成盖章）之日起7个工作日内，将本项目采购合同通过报同级财政部门备案。

2.6.5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、工程或者服务的，在不改变合同其他条款的前提下，可以与成交供应商协商签订补充合同，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。

2.6.6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。

2.6.7履约验收方案

采购包1：

1.项目建设完毕后，由采购方、使用单位组织项目总监及相关人员按照国家行业规范标准和文献资料进行审核、考评。2.采购人应按照政府采购合同约定的技术、服务、安全标准组织对供应商每一项技术、服务、安全标准的履约情况进行验收，并出具验收书。

2.6.8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磋商活动纪律要求

采购人、代理机构应保证磋商活动在严格保密的情况下进行，采购人、代理机构、供应商和磋商小组成员应当严格遵守政府采购法律法规规章制度和本项目磋商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磋商过程和结果。

对各供应商的商业秘密，磋商小组成员应予以保密，不得泄露给其他供应商。

2.7.2 供应商不得具有的情形（实质性要求）

供应商参加响应不得有下列情形：

一、有下列情形之一的，视为供应商串通响应：

- （一）不同供应商的响应文件由同一单位或者个人编制；
- （二）不同供应商委托同一单位或者个人办理磋商事宜；
- （三）不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；
- （四）不同供应商的响应文件异常一致或者响应报价呈规律性差异；
- （五）不同供应商的响应文件相互混装。

二、提供虚假材料谋取成交；

三、采取不正当手段诋毁、排挤其他供应商；

四、与采购人或代理机构、其他供应商恶意串通；

五、向采购人或代理机构、磋商小组成员行贿或者提供其他不正当利益；

六、在磋商过程中与采购人或代理机构进行协商磋商；

七、成交后无正当理由拒不与采购人签订政府采购合同；

八、未按照磋商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。

供应商有上述情形的，按照规定追究法律责任，具有前述一至十一条情形之一的，其响应文件无效，或取消被确认为成交供应商的资格或认定成交无效。

2.7.3 采购人员及相关人员回避要求

政府采购活动中，采购人员及相关人员与供应商有下列利害关系之一的，应当回避：

- （一）参加采购活动前3年内与供应商存在劳动关系；
- （二）参加采购活动前3年内担任供应商的董事、监事；
- （三）参加采购活动前3年内是供应商的控股股东或者实际控制人；
- （四）与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；
- （五）与供应商有其他可能影响政府采购活动公平、公正进行的关系。

供应商认为采购人员及相关人员与其他供应商有利害关系的，可以向代理机构书面提出回避申请，并说明理由。代理机构将及时询问被申请回避人员，有利害关系的被申请回避人员应当回避。

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，供应商对采购文件中采购需求的询问、质疑由 陕西上德招标有限公司 负责答复；供应商对除采购需求外的采购文件的询问、质疑由陕西上德招标有限公司 负责答复；供应商对采购过程、采购结果的询问、质疑由 陕西上德招标有限公司 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、不影响响应文件的编制的情形）。

四、供应商认为磋商文件、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）质疑函正本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（针对磋商文件提出的质疑，需提交从项目电子化交易系统获取的磋商文件回执单）。

接收质疑函方式：书面形式。

答复主体：代理机构

联系人：李艳洁（4号工位）

联系电话：029-86673953、86518381转8004

地址：西安市经开区凤城八路正尚国际金融广场A座7层703（张家堡转盘东南角）

邮编：710000

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磋商文件、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 磋商项目技术、服务、商务及其他要求

（注：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。）

3.1 采购项目概况

西安市全民健康信息平台升级建设项目密码应用改造

3.2 服务内容及服务要求

3.2.1 服务内容

采购包1：

采购包预算金额（元）：1,370,000.00

采购包最高限价（元）：1,370,000.00

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	西安市全民健康信息平台升级建设项目密码应用改造	1.00	1,370,000.00	项	软件和信息技术服务业	否	否	否	否

3.2.2 服务要求

采购包1：

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

标的名称：西安市全民健康信息平台升级建设项目密码应用改造

参数性质	序号	技术参数与性能指标
		<p>1.背景</p> <p>密码是保障网络与信息安全的核心技术和基础支撑，国产密码算法是我国自主研制完成的密码算法，并经过国密局严格评定，具有较高安全性，是我国信息安全的重要保障。</p> <p>随着信息化快速发展，网络与信息系统安全事件呈现快速增长趋势，密码作为保护网络与信息系统安全的重要手段，在身份识别、信息加密、完整性保护和抗抵赖性等方面发挥着不可替代的重要作用。</p> <p>网络运营者应当按照国家网络安全等级保护制度，使用密码保护网络安全。</p> <p>按照《中华人民共和国密码法》有关法律法规及《国家政务信息化项目建设管理办法（国办发〔2019〕57号）》等文件的相关要求，应在政务信息系统建设中同步规划、同步建设、同步运行密码保障系统。</p>

为保障全民健康信息平台安全，应通过对系统现状和密码应用需求进行分析，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称《基本要求》），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、管理制度、人员管理、建设运行、应急处置及密钥生命周期管理9个层面，设计密码应用的技术方案、安全管理方案和实施保障方案，以实现对系统密码应用安全和管理安全的提升。

系统概述

系统基本情况

系统名称：西安市全民健康信息平台

系统上线运行时间：--

完成等保备案时间：--

网络安全保护等级：三级

系统用户情况：本系统服务于西安市卫生健康委员会、西安市各医疗机构、居民，用户为管理员用户、平台的内部用户、医疗机构的用户、第三方应用的用户和上下级、平级部门的用户。

本次“西安市全民健康信息平台”主要分为政务外网服务区、互联网服务区及互联网区。

西安市全民健康信息平台中的基础平台、惠民应用系统、惠民支撑应用、助医应用系统、辅政应用系统等系统在政务外网进行部署，系统部署所需的硬件设施、网络设备、服务器等基础设施将统一依托市政务云平台。

互联网服务区主要提供移动端，使得移动网用户进行登录操作。

关键用户及数据

序号	用户类别	安全防护需求	是否为重要用户	描述
1	系统管理员	身份鉴别	是	系统管理员能够查看所有用户信息，属于重要用户，需要进行身份鉴别改造。
2	业务用户	身份鉴别	是	
3	维护人员（互联网）	身份鉴别	是	
4	维护人员（政务外网）	身份鉴别	是	

序号	数据类别	安全防护需求	是否为重要数据	描述
1	身份鉴别数据	完整性、机密性	是	登录系统用户的身份数据，包括用户名口令等

2	核心业务数据	完整性、机密性	是	门诊诊断编码、门诊诊断名称、住院诊断编码等
3	日志数据	完整性	是	系统的登录日志、操作日志和重要系统运行日志等
4	可公开数据	完整性	否	

管理制度

本单位根据等保**2.0** 管理要求，制定有通用的“信息安全管理^{制度}汇编”，该安全管理制度汇编内容涉及安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等**5**个方面的安全管理要求。密码应用需求分析

本系统为新建系统，根据项目规划系统的用户在政务外网、互联网环境中通过移动端、PC端浏览器进行系统访问。移动端、PC访问系统时，采用HTTPS协议建立数据传输通道。同时，软件系统的运维人员通过堡垒机对系统进行远程运维。以上的HTTPS、SSL通道协议均采用国际算法RSA2048和AES等。现根据GB/T 39786等进行相应的密码应用建设。

风险控制需求

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的第三级标准以及GM/T 0115-2021《信息系统密码应用测评要求》、《信息系统密码应用高风险判定指引》，分别从物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面对本系统进行风险分析，得出本系统密码应用需求并做出分析。

一、信息系统中使用的密码算法应符合法律、法规的规定和密码相关国家标准、行业标准的有关要求，避免出现以下安全问题：

- 1) 采用存在安全问题或安全强度不足的密码算法对重要数据进行保护，如MD5、DES、SHA-1、RSA（不足2048比特）等密码算法；
- 2) 采用安全性未知的密码算法，如自行设计的密码算法、经认证的密码产品中未经安全性论证的密码算法。

二、信息系统中使用的密码技术应遵循密码相关国家标准和行业标准，避免出现以下安全问题：

- 1) 采用存在缺陷或有安全问题警示的密码技术，如SSH 1.0、SSL 2.0、SSL 3.0、TLS 1.0等；
- 2) 采用安全性未知的密码技术，如未经安全性论证的自行设计的密码通信协议、经认证的密码产品中未经安全性论证的密码通信协议等。

三、信息系统中使用的密码产品、密码服务应符合法律法规的相关要求，避免出现以下安全问题：

- 1) 采用自实现且未提供安全性证据的密码产品；
- 2) 采用存在高危安全漏洞的密码产品，如存在Heartbleed漏洞的OpenSSL产品；
- 3) 密码产品的使用不满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件；
- 4) 选用的密码服务提供商不具有相关资质；
- 5) 存在密钥管理相关安全问题。

物理和环境安全

保护对象

物理和环境安全层面的保护对象为信息系统所在的物理机房，具体为物理机房的电子门禁和视频监控系統。

风险分析

（1）目前本系统所在机房使用ID卡对进入机房人员进行身份鉴别，未使用密码技术对进入机房人员进行身份鉴别，存在非授权人员进入物理环境，对软硬件设备和数据进行直接破坏的风险；

（2）目前本系统所在机房人员进出记录明文存储在门禁管理系统数据库中，视频监控音像数据明文存储在磁盘阵列中，未使用密码技术进行存储完整性保护，存在物理进出记录和视频监控记录遭到非授权篡改，以掩盖非授权人员进出情况的风险。

密码应用需求

在本系统所在机房部署符合GM/T 0036-2014 标准要求的国密电子门禁系统对进出机房人员进行身份鉴别，通过国密电子门禁和国密视频监控系统内配置的密码卡并对门禁进出记录及视频记录数据进行完整性保护。

不适用与替代措施

本层面无不适用项与替代措施。

网络和通信安全

保护对象

本方案中涉及的网络通信类型包括互联网服务区、政务外网服务区。而涉及的客户端包括：移动端、业务人员PC端、软件系统运维人员PC端和设备层运维PC端。

风险分析

（1）目前本系统网络通信通道，都采用国际密码算法或者未采用密码算法，存在算法漏洞、后门和中间人攻击等安全风险。这些通道通信前未使用密码技术对通信双方身份信息进行验证，未使用密码技术对传输数据进行机密性和完整性保护，通信数据在信息系统外部被非授权截取、非授权篡改风险。

（2）目前本系统未使用密码技术对网络边界访问控制信息进行完整性保护，存在网络边界（即放置于网络边界处的网络设备）内规则信息、策略信息、ACL信息等被篡改风险，从而导致未经授权的流

量进出。

密码应用需求

（1）本系统应通过调用国密VPN设备通过 TLS 协议基于国密算法实现单向身份鉴别，防止设备被非授权人员登录、身份鉴别数据被非授权截取或非授权使用等风险等。

（2）本系统通信的网络通道应调用国密VPN设备通过 SSL 协议基于国密算法实现数据传输通道的机密性。摄像头通过运营商互联网专线接入系统前端的通道应采用专用的硬件密码设备实现基于国密算法和协议的数据传输机密性。

（3）本系统通信的网络通道应调用国密VPN设备通过 SSL 协议基于国密算法实现数据传输通道的完整性。摄像头通过运营商互联网专线接入系统前端的通道应采用专用的硬件密码设备实现基于国密算法和协议的数据传输完整性。

（4）本系统通信的网络通道所依赖的网络设备和网络安全设备都应该确保其内部访问控制信息的完整性。

注：本系统网络边界处的防火墙、交换机等设备的访问控制信息完整性需要采用密码技术进行保护。但是考虑到上述设备通常为网络厂商和网络安全厂商生产和制造，本身缺乏密码技术的应用。同时作为成熟的量产产品，后期改造难度较大，因此目前不考虑此类边界访问控制信息完整性。

不适用与替代措施

系统不涉及外部网络接入的设备，安全接入认证作为不适用项。

设备和计算安全

保护对象

设备和计算层面的保护对象为信息系统所涉及的通用设备（及其操作系统、数据库管理系统）、网络及安全设备、密码设备、各类虚拟机设备及各类虚拟设备以及提供相应密码功能的密码产品。

风险分析

（1）目前本系统的运维主要分为两大部分，软件系统和服务器等设备。软件系统层面的运维主要是系统管理员用户通过VPN+堡垒机服务，接入政务外网区的系统，使用用户名口令登录堡垒机。另外，服务器等设备的运维由西安市政务云平台侧代为运维，该运维终端和通道均在西安市政务云内部，且通过堡垒机进行运维。总体而言，未使用密码技术对管理员登录进行身份鉴别，未使用合规的密码技术对管理员远程管理设备时的信息传输通道进行传输机密性和完整性保护，存在设备被非授权人员登录、身份鉴别数据被非授权获取或非授权使用等风险。

（2）目前本系统应用服务器和数据库服务器中的访问控制信息未使用密码技术进行完整性保护，使用或读取这些访问控制信息时存在被非授权篡改的风险。

（3）目前本系统应用服务器中所有重要可执行程序未使用密码技术进行完整性保护，使用这些重要可执行程序时。对其来源进行真实性验证，存在重要程序被非授权篡改、来源不可信风险。

(4) 目前本系统应用服务器中未进行数据资产的分级标注，不存在重要信息资源安全标记的篡改问题。

(5) 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。

密码应用需求

(1) 本系统需要对租户侧和西安市政务云平台侧所使用各类设备进行基于密码技术的身份鉴别改造，通过采用堡垒机和国密VPN设备，并采用基于SM2的数字证书实现登录人员的身份鉴别。

(2) 本系统租户侧和西安市政务云平台侧的设备的远程运维管理，需要采用合规的密码算法、技术和协议，以及产品实现远程管理通道的安全。即需要调用国密VPN设备，对远程管理设备时的信息传输通道进行机密性和完整性保护，防止管理数据等被非授权窃取。

(3) 本系统租户侧和西安市政务云平台侧的设备系统资源访问控制信息完整性需要采用合规的密码算法和密码产品实现。这些设备包括数据库虚拟机、应用虚拟机、网络设备和网络安全设备等。

(4) 本系统租户侧和西安市政务云平台侧的设备日志记录完整性需要采用合规的密码算法和密码产品实现。这些设备包括数据库虚拟机、应用虚拟机、网络设备和网络安全设备等。

(5) 本系统租户侧和西安市政务云平台侧的设备重要可执行程序完整性和来源真实性需要采用合规的密码算法和密码产品实现。这些设备包括数据库虚拟机、应用虚拟机、网络设备和网络安全设备等。

注：因为本系统涉及的各类设备均为量产的各类品牌产品，客观上对于访问控制信息完整性、重要可执行程序的来源真实性和自身程序完整性、日志数据完整性等具备很大的改造难度。因此本方案采用其他安全手段去缓解系统的相关密码安全需求。

不适用与替代措施

本系统中不涉及重要信息的敏感性标记，作为不适用项。

应用和数据安全

保护对象

应用和数据安全层面的保护对象为信息系统所涉及的业务应用及鉴别数据、重要业务数据、重要审计数据、个人敏感信息以及法律规定的其他重要数据类型。

风险分析

(1) 目前本系统用户和管理员采用移动端应用、浏览器等基于用户名/口令进行人员身份鉴别。均未使用密码技术对登录用户进行身份鉴别，存在应用被非授权人员登录风险；

(2) 目前本系统未使用密码技术对本系统用户访问权限控制列表进行完整性保护，存在应用资源被非授权用户获取的风险；

(3) 目前本系统中未进行数据资产的分级标注，不存在重要信息资源安全标记的篡改问题。

（4）目前本系统应用中所有重要数据在传输和存储均未使用合规的密码技术对其进行机密性和完整性的保护，存在被非法篡改和非法截获的风险；

（5）目前本系统不涉及与其他系统进行数据交互的场景，因此不涉及数据收发行为的抵赖风险。

密码应用需求

（1）在本系统中调用西安市政务云平台（采用密码服务平台）提供的杂凑密码服务（HMAC_SM3）或者非对称密码服务（SM2），对应用系统的访问权限控制列表进行完整性保护，防止应用资源被非授权用户获取；

（2）在本系统中调用西安市政务云平台（采用密码服务平台）提供的合规对称密码服务（SM4和SM1）、合规杂凑密码服务（HMAC-SM3）或者合规非对称密码服务（SM2），对应用中所有重要数据的传输和存储进行机密性和完整性的保护，实现所有重要数据防窃取和防篡改的保护。

不适用与替代措施

（1）本系统中不涉及重要信息的敏感性标记、不可否认性，作为不适用项。

安全管理

风险分析

本系统在系统建设阶段，未依据密码相关国家、行业标准，制定密码应用方案，规划建设密码保障系统，系统上线前未开展过密码应用安全性评估，未依据《基本要求》中的安全管理要求，制定密码相关管理制度，不利于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。

密码应用需求

依据《基本要求》，制定本系统密码应用改造方案，并委托密评机构对密码应用改造方案进行评估，评估通过后，建设密码保障系统，制定密码相关的管理制度，系统改造完成后，依据密码应用改造方案对本系统进行密码应用安全性评估，评估通过后上线运行。

设计目标及原则

设计目标

本方案依托于《中华人民共和国密码法》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，依托对现有等级保护建设的基础上，按照等级保护三级对现有整改信息系统进行符合商用密码应用安全性评估改造设计。通过对现有信息系统中增加、部署独立的、可替换的商用密码产品，采用网络或应用升级改动较小的方式，完成信息系统密码应用改造，满足本单位对密码的适应性建设

需求。符合国家对商用密码应用安全性评估的要求，达成系统“密码安全可靠”的建设。

设计原则

- (1)总体性原则。通过从整体层面，对本系统的密码应用开展顶层设计，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，为在本系统中落实密码应用相关要求奠定基础。
- (2)完备性原则。围绕本系统实际业务应用与安全保护等级，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，设计本系统密码改造方案。
- (3)经济性原则。结合本系统规模，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)合规性原则。密码产品中应配置使用SM系列商用密码算法，如SM2、SM3、SM4等。实现密码保护所使用的密码算法应为商用密码算法，严禁使用MD5、SHA-1、RSA1024等已经明确为高风险的密码算法。信息系统中应采用国家密码主管部门核准的密码产品，达到GB/T 37092二级及以上安全要求。在本次项目中，密码产品均取得商用密码产品认证证书。系统中使用的密码技术应遵循密码相关国家标准和行业标准，例如云服务器密码机应遵循《GM/T 0104-2021 云服务器密码机技术规范》。系统中所使用的密码服务，如数字证书应当使用商密数字证书。数字证书的颁发机构应具有国家密码管理局颁发的《电子认证服务使用密码许可证》，在国家密码管理局“电子政务电子认证服务机构目录”中。

设计依据

商用密码相关政策依据

《中华人民共和国密码法》
《中华人民共和国网络安全法》
《商用密码管理条例(修订草案征求意见稿)》
《商用密码应用安全性评估量化评估规则》
《信息系统密码应用高风险判定指引》
GB/T 39786-2021 《信息安全技术 信息系统密码应用基本要求》
GM/T 0115-2021 《信息系统密码应用测评要求》
GM/T 0116-2021 《信息系统密码应用测评过程指南》
《内蒙古自治区商用密码事中事后监管方案》
《电子认证服务密码管理办法》

密码产品与密码技术相关标准规范

GM/T 0002-2012 《SM4分组密码算法》
GM/T 0003-2012 《SM2椭圆曲线公钥密码算法》

GM/T 0004-2012 《SM3密码杂凑算法》

GM/T 0006-2012 《密码应用标识规范》

GM/T 0009-2012 《SM2密码算法使用规范》

GM/T 0015-2012 《基于SM2密码算法的数字证书格式规范》

GM/T 0017-2012 《智能密码钥匙密码应用接口数据格式规范》

GM/T 0018-2012 《密码设备应用接口规范》

GM/T 0019-2012 《通用密码服务接口规范》

GM/T 0022-2014 《IPSec VPN技术规范》

GM/T 0023-2014 《IPSec VPN网关产品规范》

GM/T 0024-2014 《SSL VPN技术规范》

GM/T 0025-2014 《SSL VPN网关产品规范》

GM/T 0027-2014 《智能密码钥匙技术规范》

GM/T 0028-2014 《密码模块安全技术要求》

GM/T 0104-2021 《云服务器密码机技术规范》

GM/T 0030-2014 《服务器密码机技术规范》

GM/T 0029-2014 《签名验签服务器技术规范》

GM/T 0034-2014 《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》

GM/T 0035-2014 《射频识别系统密码应用技术要求》

GM/T 0036-2014 《采用非接触卡的门禁系统密码应用技术指南》

GB/T 37092-2018 《信息安全技术密码模块安全要求》

技术方案

密码应用技术框架

为满足GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的网络和通信安全第三级信息系统商用密码应用指标要求，采用密码技术的机密性功能来实现鉴别信息的防窃听需满足要求中网络和通信安全的身份鉴别、访问控制信息完整性、通信数据完整性、通信数据机密性和集中管理通道安全的相关要求。

本方案依托于《中华人民共和国密码法》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等，对现有信息系统进行符合商用密码应用安全性评估改造设计。通过对现有信息系统中增加、部署独立的、可替换的商用密码产品，采用网络或应用升级改动较小的方式，完成信息系统密码应用改造，满足业务系统对密码的适应性建设需求。依托对密码建设的框架优化。

密码资源层：作为基本的基础能力支撑和技术理论支撑，提供基础性的密码算法资源，底层提供序列、分组、公钥、杂凑、随机数生成等基础的密码算法，为密码支撑层提供基本的算法软件、算法IP核、算法芯片等封装后的密码算法能力。

密码支撑层：作为密码改造核心支撑层，集成包括密码芯片、密码模块、密码整机和密码系统类等相关产品类组成，集成密码资源层的各类算法实现，以密码设备、系统、软件模块的形式出现，方便在业务现场进行部署实施和集成，分别在密码支撑层设备包括，

物理和环境支撑：国密视频监控，国密电子门禁；

网络和通信：IPSEC/SSL VPN综合安全网关；

设备和计算：IPSEC/SSL VPN综合安全网关，云服务器密码机，密码服务平台；

应用和数据：云服务器密码机，密码服务平台；

用户端：数字证书、智能密码钥匙；

主要产品能力如下：

云服务器密码机：支持国密SM2、SM3、SM4等算法，可提供虚拟密码机提供服务，实现数据加解密、完整性校验等功能。

密码服务平台：对密码资源进行统一纳管，向用户提供集中的密码运算、设备管理、密钥管理等密码服务。

数据加解密服务：提供基于SM4等国密算法的加解密运算能力，保障应用数据的机密性。

杂凑运算服务：提供基于SM3等密码算法的杂凑运算能力，保障应用数据的完整性。

签名验签服务：支持SM2/RSA密码算法，能够提供签名验签的能力实现对登入用户进行身份鉴别，保障用户的身份真实性。

协同签名服务：依托于密钥分割、协作签名的专利技术，实现在无硬件介质的情况下实现对移动端用户的身份真实性鉴别。

IPSec/SSL VPN 综合安全网关：支持SM1、SM2、SM3、SM4算法，可保障用户在密评网络与通信层面的安全，主要对于网络传输信息进行机密性、完整性的保护，实现安全传输。

国密电子门禁系统：可提供国密算法进行密钥分散，实现门禁卡的“一卡一密”，使用国密算法实现对门禁数据的完整性保护。

国密视频监控系统：支持国密算法，采用HMAC-SM3技术，实现实时视频流和视频录像的完整性保护。

密码服务层：是密码支撑层的服务抽象，通过接口（密码设备安全服务的API接口）对外提供各类多样的密码服务能力，主要从对称密码服务和公钥密码服务作为能力提供。为上层提供基于数据在保密性、完整性、身份鉴别、抗抵赖等基本功能。

业务应用层：作为密码改造的核心，主要采用上述密码支撑层和密码服务层实现对密码合规性改造的能力，实现业务信息系统的合规。

物理和环境安全

设计原理

身份鉴别

西安市全民健康信息平台部署在西安市电子政务云上，西安市电子政务云机房部署符合《GM/T 0036-2014 采用非接触卡的门禁系统密码应用技术指南》的国密门禁系统，采用对称密钥分散和对称加解密技术，实现一卡一密，确保人员身份的真实性。

电子门禁与视频监控记录数据存储完整性

西安市全民健康信息平台机房部署符合《GM/T 0036-2014 采用非接触卡的门禁系统密码应用技术指南》的国密门禁系统，采用HMAC-SM3或SM2数字签名技术，对门禁系统人员进出记录做完整性保护，防止进出记录被篡改。部署视频监控系统，支持视频录像的完整性保护，防止录像文件被篡改。视频监控系统包含支持密码模块的IPC网络摄像机、NVR网络录像机、视频客户端。采用HMAC-SM3技术，实现实时视频流和视频录像的完整性保护。

密码服务流程

国密门禁

门禁控制系统是以国密CPU卡技术、密码应用技术、计算机技术为核心，加上可靠的门、通道控制设备，从而实现进出门方便、安全、实时的现代化管理；该系统可实现人员出入权限及信息监督管理功能。

本方案采用国家密码管理局指定的SM1分组加密算法进行密钥分散，实现一卡一密；采用国家密码管理局指定的SM4分组加密算法进行门禁卡与门禁读卡器之间的身份鉴别。

门禁卡采用SM4分组密码算法，卡内存放发行信息及卡片密钥。

在门禁读卡器中，射频接口模块负责读卡器与门禁卡间的射频通信；MCU负责读卡器内部的数据交换，与后台管理系统及门禁执行机构的数据通信。SM4/SM1安全存取模块负责读卡器中的安全密码运算，鉴别门禁卡的合法性，存放系统根密钥。

门禁读卡器上传鉴别结果给后台管理系统，后台管理系统进行实时或非实时门禁权限及审计管理，门禁执行机构具体执行完成门禁操作。

视频监控系统

视频监控系统包含支持密码模块的IPC网络摄像机、NVR网络录像机、视频客户端。采用SM3算法的HMAC，实现视频流和视频录像的完整性保护。

视频监控系统为闭环网络，通过L2层交换机实现前后端的互联互通，不允许任何外部网络或设备接入。本系统中所有密码产品包括：多个前端安全IPC网络摄像机（内置密码模块），1台32路安全NVR网络录像机（配置智能密码钥匙），1台视频安全客户端（内置PCI-E密码卡）。

提供的密码服务主要包括：实时视频流和视频录像的完整性保护。

安全摄像机内置国密算法芯片，支持SM3、SM4国密算法，支持密钥生成、更新、使用、存储、注销等功能。支持1080P高清视频流的HMAC保护和视频加密传输，实现视频传输过程的机密性和完整性保护。

安全NVR支持32路高清视频接入。配专用智能密码钥匙，存储视频加密密钥，支持加密视频的解密预览。

视频客户端内置密码卡，支持实时视频和视频录像的浏览，支持视频完整性验证，支持投屏。

工作流程

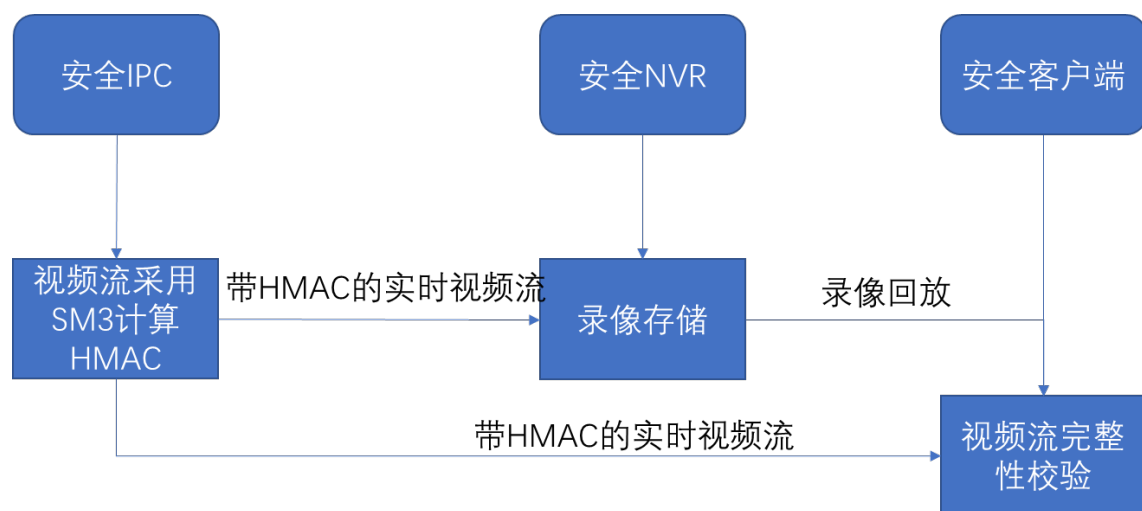


图 53 视频监控系统工作流程

流程说明：

- 1) 设备部署前，由安全客户端生成统一的HMAC密钥，离线导入到各安全IPC集成的TF密码卡中。
- 2) 安全IPC上线后，采用SM3+HMAC技术，对实时视频流做完整性保护。
- 3) 带HMAC的视频流存储到安全NVR中。
- 4) 实时视频流和视频录像通过安全客户端进行调用，调用预览过程，对视频流进行完整性验证，确保视频数据的完整性。

部署方式

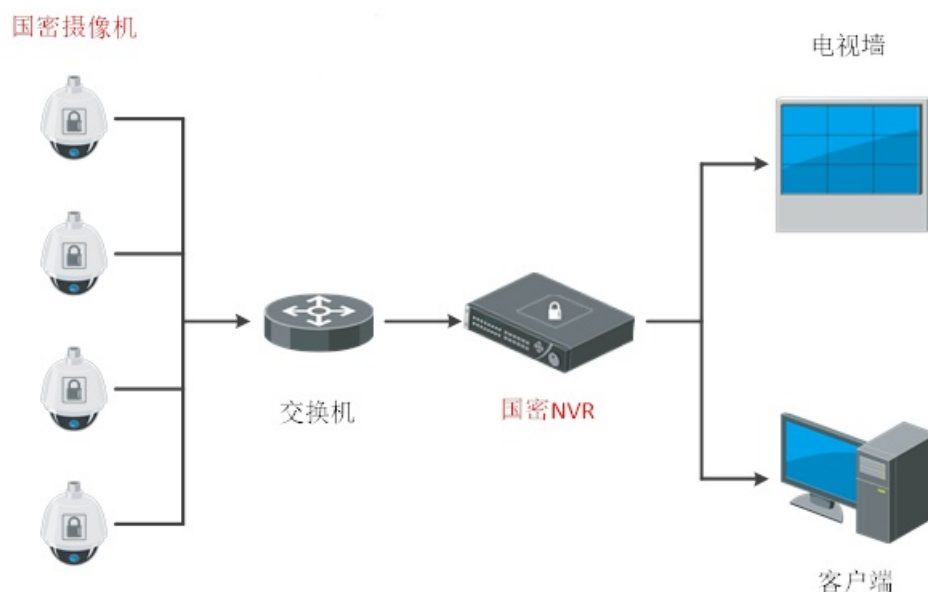


图 54 视频监控系统网络拓扑图

安全摄像机、安全NVR、安全客户端之间通过L2交换机组网。

安全摄像机：内置安全TF卡，支持SM2、SM3、SM4算法，支持HMAC计算。

安全NVR：配智能密码钥匙，支持SM2、SM3、SM4算法，支持视频录像的完整性保护。

安全客户端：内置密码卡，支持SM2、SM3、SM4算法，实现视频流实时监控和录像回放，支持视频录像回放的完整性验证，支持投屏。

网络和通信安全

设计原理

身份鉴别

部署符合GM/T 0022-2014《IPSec VPN 技术规范》、GM/T 0024-2014《SSL VPN 技术规范》等的IPSEC/SSL VPN综合安全网关，PC端用户通过部署的网关客户端采用用户口令+智能密码钥匙的方式接入，智能密码钥匙中存放CA颁发给个人用户的数字证书，保障接入系统中设备、终端的身份的真实性。

对于移动端用户，通过部署IPSEC/SSL VPN综合安全网关、协同签名SDK及相关组件实现在网络层通信双方的身份鉴别。

通信数据完整性

采用符合GM/T 0022-2014《IPSec VPN 技术规范》、GM/T 0024-2014《SSL VPN 技术规范》等的IPSEC/SSL VPN综合安全网关，通信过程中，采用国密SSL协议实现登录客户端与服务端之间的密钥协商，采用ECC（SM2）_SM4_SM3的SSL算法套件，实现通信数据的完整性保护。

通信过程中重要数据机密性

采用部署符合GM/T 0022-2014《IPSec VPN 技术规范》、GM/T 0024-2014《SSL VPN 技术规范》等的IPSEC/SSL VPN综合安全网关，通信过程中，采用国密SSL协议实现登录客户端与服务端之间的密钥协商，采用ECC（SM2）_SM4_SM3的SSL算法套件，保障网络层数据安全，保证通信过程中敏感信息数据字段或整个报文的机密性。

网络边界访问控制信息的完整性

通过符合GM/T 0022-2014《IPSec VPN 技术规范》、GM/T 0024-2014《SSL VPN 技术规范》等的IPSEC/SSL VPN综合安全网关设备内置的密码硬件模块，调用SM3算法对网络边界和系统资源访问控制信息的完整性保护，由设备自身完成。

安全接入认证

系统不涉及外部网络接入的设备，本项不适用。

密码服务流程

身份认证流程

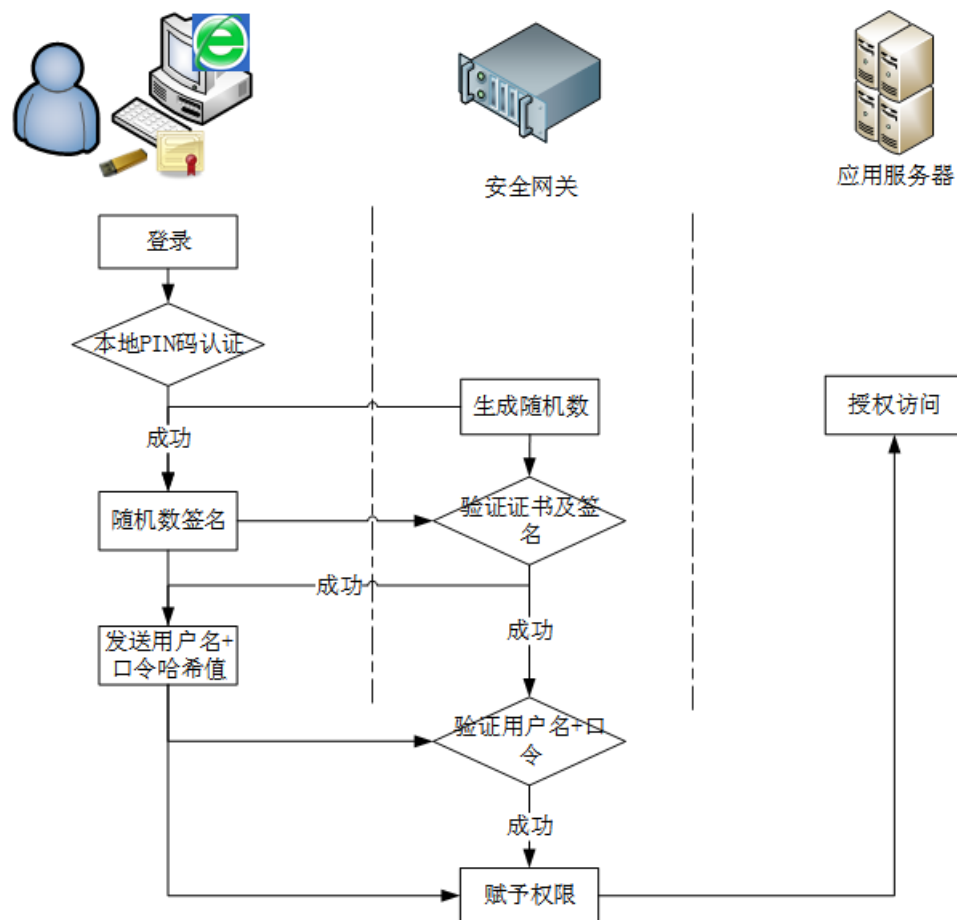


图 55 身份认证服务流程

用户在登录页面选择数字证书登录，插入USBKEY介质后，由系统后台进行身份验证并返回验证结果，验证成功后可登录到系统。具体登录流程如下：

- 1) 用户通过本地认证客户端发起访问请求，VPN综合安全网关产生随机数并发送至客户端。
- 2) 客户端插入USBKEY，首先进行本地PIN码认证。PIN码认证通过后，开启USBKEY权限。
- 3) 发送随机数签名值。
- 4) 服务端验证签名证书有效性，并验证签名值正确性。同时建立国密SSL通道。
- 5) 客户端在访问页面输入用户名、口令，启动USBKEY，对登录口令进行哈希运算。
- 6) 客户端将用户名、口令哈希值通过国密SSL通道发送至服务端。
- 7) 服务端验证用户名和口令。
- 8) 比对一致，则登录成功，分配适用于该用户的资源访问权限。
- 9) 以上任何一步鉴别失败，则返回登录失败相关提示信息。

安全传输通道建立流程

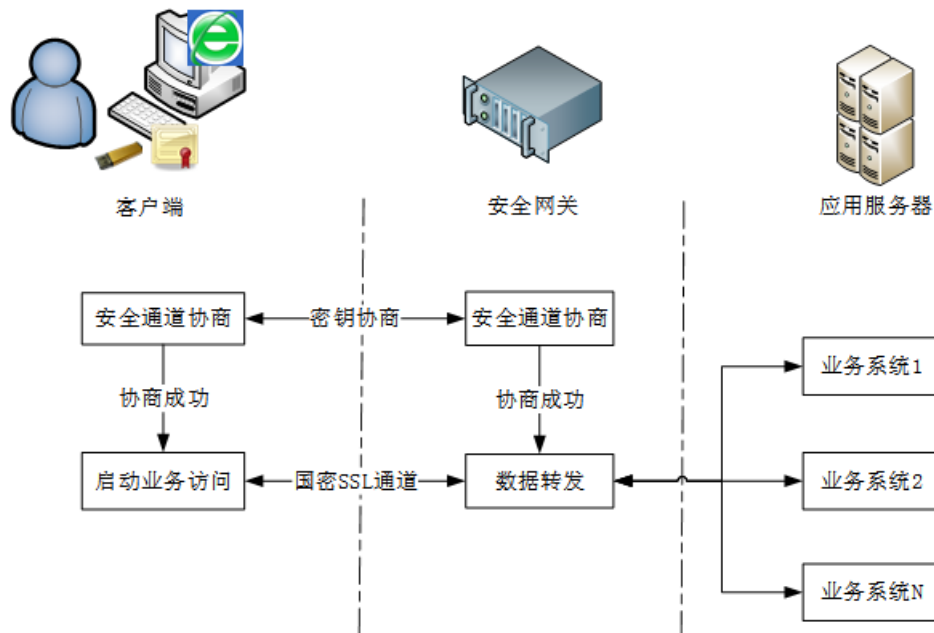


图 56安全传输通道建立流程

客户端用户访问业务流程如下：

- 1) 客户端输入认证客户端账号、密码，插入USBKEY通过数字证书认证，登录IPSEC/SSL VPN综合安全网关；
- 2) 客户端和IPSEC/SSL VPN综合安全网关协商VPN安全通道。
- 3) 提交应用业务登录请求。
- 4) 平台客户端和IPSEC/SSL VPN综合安全网关间通过SSL 安全通道进行数据传输，保障互联网数据传输的安全性。
- 5) IPSEC/SSL VPN综合安全网关和应用服务器间通过普通通道进行数据传输。

设备和计算安全

设计原理

身份鉴别

通过符合GM/T 0022-2014 《IPSec VPN 技术规范》、GM/T 0024-2014 《SSL VPN 技术规范》等的IPSEC/SSL VPN综合安全网关结合堡垒机提供设备和计算层面的身份鉴别，结合智能密码钥匙（内置身份证书，采用国产密码算法），并且与各个账户对应。

远程管理通道安全

将系统中所有设备纳入到堡垒机中进行统一运维管理，运维管理员通过依托于符合GM/T 0022-2014 《IPSec VPN 技术规范》、GM/T 0024-2014 《SSL VPN 技术规范》等的IPSEC/SSL VPN综合安全网关代理堡垒机登录界面实现符合规定的SSL协议，对运维管理员用户进行身份鉴别和远程管理身份鉴别信息传输机防止非授权人员登录、管理员远程登录身份鉴别信息被非授权窃取。因此，设备远程管理鉴别信息的传递均发生在基于国密算法的安全通道上，保障了机密性和完整性，从而保证了鉴别信息的防窃听。

访问控制信息完整性

在本系统中对资源访问控制信息采用堡垒机完成，但无法对其访问控制列表、访问控制信息进行完整性保护；针对系统中具有合格的商用密码产品认证证书的密码设备，设备自身已实现系统资源访问控制信息的完整性。

重要信息资源安全标记完整性

系统不涉及信息资源安全标记，此项为不适用。

日志记录完整性

系统通过日志审计系统收集服务器、交换机、安全设备的日志，通过日志审计调用密码服务平台的杂凑运算服务进行性保护。针对系统中具有合格的商用密码产品认证证书的密码设备，设备自身已实现日志记录完整性。

重要可执行程序完整性、重要可执行程序来源真实性

针对目前机房中网络及安全设备和操作系统等无法基于现有的密码技术对其重要可执行程序 and 重要资源安全标记的完整性要求，重要可执行程序均从官方渠道获取，且在安装前对程序进行验证，保证其没有受到篡改。在一定程度上降低重要可执行程序完整性、重要可执行程序来源真实性保护的安全风险。针对系统中具有合格的商用密码产品认证证书的密码设备，设备自身已实现重要可执行程序完整性、重要可执行程序来源真实性。

密码服务流程

身份认证流程

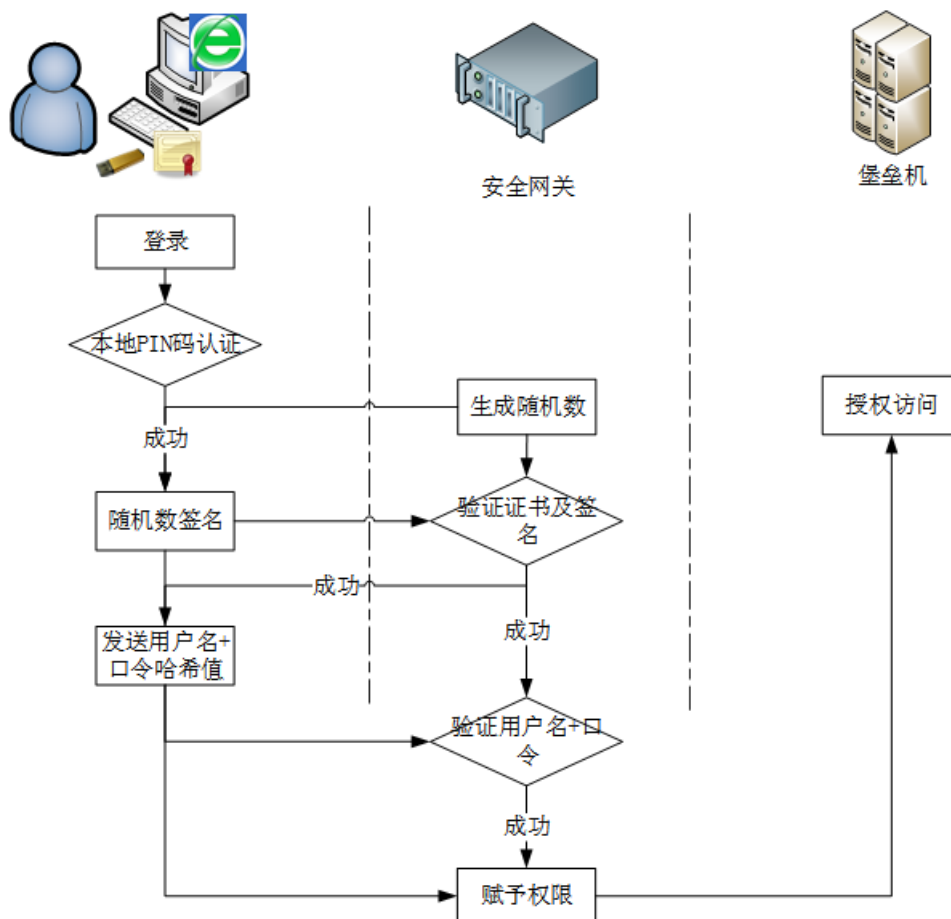


图 57 身份认证服务流程

- 1) 运维人员插入智能密码钥匙(USBKEY)，首先进行本地PIN码认证。PIN码认证通过后，开启智能密码钥匙(USBKEY)权限。
- 2) 运维人员通过本地认证客户端发起访问请求，网关产生随机数并发送至客户端
- 3) 客户端发送随机数签名值及签名证书
- 4) 服务端验证签名证书有效性，并验证签名值正确性。同时建立国密SSL通道。
- 5) 运维人员在访问页面输入用户名、口令登录堡垒机。以上任何一步鉴别失败，则返回登录失败相关提示信息。

安全传输通道建立流程

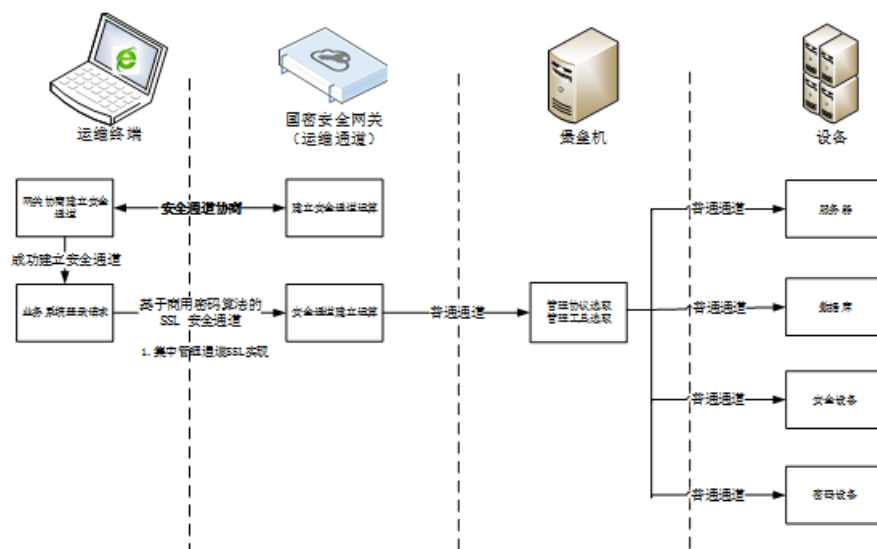


图 58安全传输通道建立流程

客户端用户访问业务流程如下：

- 1) 客户端输入认证客户端账号、口令，插入USBKEY通过数字证书认证，登录VPN综合安全网关；
- 2) 客户端和VPN综合安全网关协商VPN安全通道。
- 3) 提交应用业务登录请求。
- 4) 平台客户端和VPN综合安全网关之间通过SSL安全通道进行数据传输，保障互联网数据传输的安全性。
- 5) VPN综合安全网关和堡垒机间通过普通通道进行数据传输。

应用和数据安全

设计原理

身份鉴别

对于PC端用户，则使用符合密码服务平台的签名验签服务进行身份鉴别。用户使用智能密码钥匙登入业务系统，业务系统调用签名验签服务的接口采用SM2算法签名验签实现身份鉴别，保障系统用户的身份真实性。

对于移动端登录用户，则使用密码服务平台的协同签名服务对移动端用户进行身份鉴别。通过客户端扫码等方式进行协同签名，实现对登录用户身份真实性的鉴别。

访问控制信息完整性

应用系统通过调用密码服务平台的杂凑运算服务完整性接口对用户访问权限配置文件进行HMAC-SM3完整性保护，防止访问控制信息被恶意非授权篡改。

重要信息资源安全标记完整性

系统中暂未涉及重要信息资源安全标记。

重要数据传输机密性和完整性

系统部署符合GM/T 0022-2014《IPSec VPN技术规范》、GM/T 0024-2014《SSL VPN技术规范》等的IPSEC/SSL VPN综合安全网关代理当前业务系统的网页，用户通过PC端网关客户端与业务系统通过合规的SSL安全通信链路建立安全传输通道，通过国密算法对传输数据进行保密性和完整性保护。

重要数据存储机密性和完整性

针对业务的用户账号及口令数据及其他关键数据调用密码服务平台的数据加解密服务，采用SM4对称加密算法对关键数据提供加密运算，实现数据的加密存储。针对业务中系统登录日志、操作日志等数据需要进行完整性保护的数据，通过调用密码服务平台的杂凑运算服务使用HMAC-SM3生成摘要值，实现数据存存储的完整性保护。

不可否认性

根据规划情况，本系统不涉及法律责任认定，因此无需采用密码技术提供数据原发证据和数据接收证据。

密码服务流程

数字签名流程

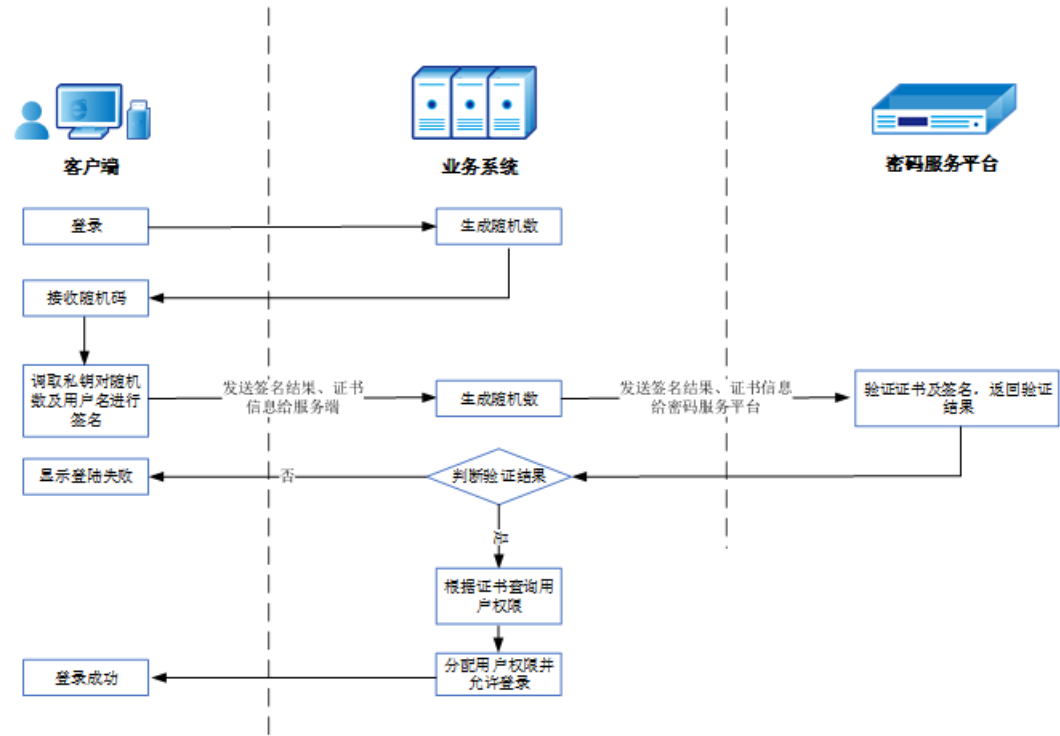


图 59数字签名流程

对关键业务数据制作数字签名流程如下：

- 1）调用密码服务平台接口，将待签名数据和认证授权码送往密码服务平台。
- 2）密码服务平台验证认证授权码，确认应用系统身份是否具备访问数字签名服务的权限。
- 3）授权验证通过后，密码服务平台根据应用系统的要求，对待签名数据做数字签名，并将签名后的结果数据返回给应用系统。
- 4）应用系统将签名结果与业务数据共同存入数据库。

签名验证流程

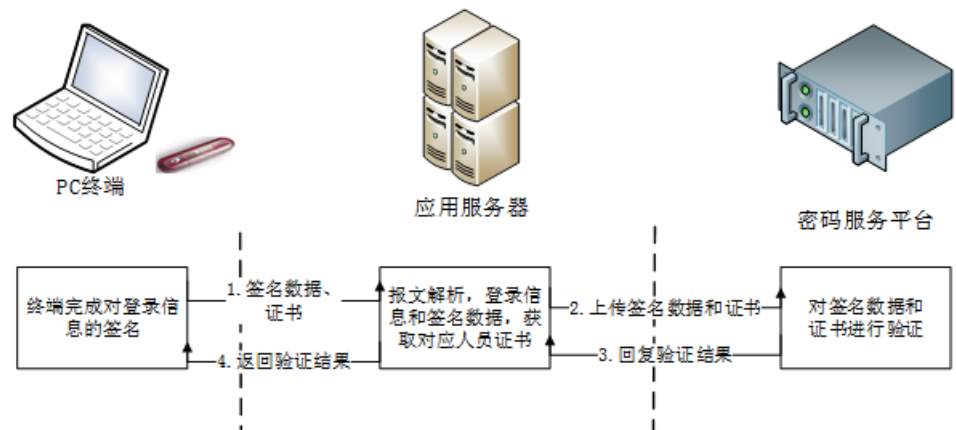


图 510 签名验证流程

签名数据验证流程如下：

- 1) 用户登录应用系统，进行业务操作。
- 2) 应用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) 应用系统判断客户端是否插入数字证书，如果没有则提示用户插入数字证书。
- 4) 客户端调用签名控件对关键数据做数字签名。
- 5) 应用系统接收客户端签名数据，并发送到密码服务平台进行验证。
- 6) 密码服务平台确认应用系统访问权限后，对签名数据进行验证，并将验证结果返回给应用系统。
- 7) 应用系统根据返回的验证结果，确认客户端签名是否有效。如果有效，将签名数据存入数据库；如果签名无效，则将错误信息返回给客户端，要求重新制作数字签名。

数据加密流程

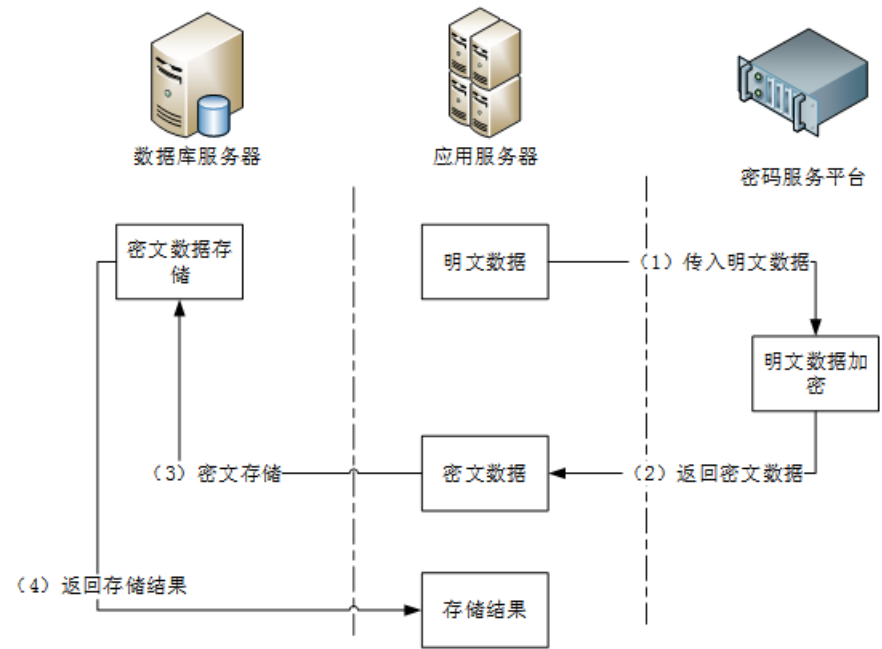


图 511 数据加密流程

具体业务流程如下：

- 1) 应用系统将收到的明文数据上传到密码服务平台。
- 2) 密码服务平台根据应用标识和分配的加密密钥将明文数据使用对称加密算法加密后返回给应用系统。
- 3) 应用系统将加密后的数据存储到数据库。
- 4) 数据库返回存储结果给应用系统。

数据解密流程

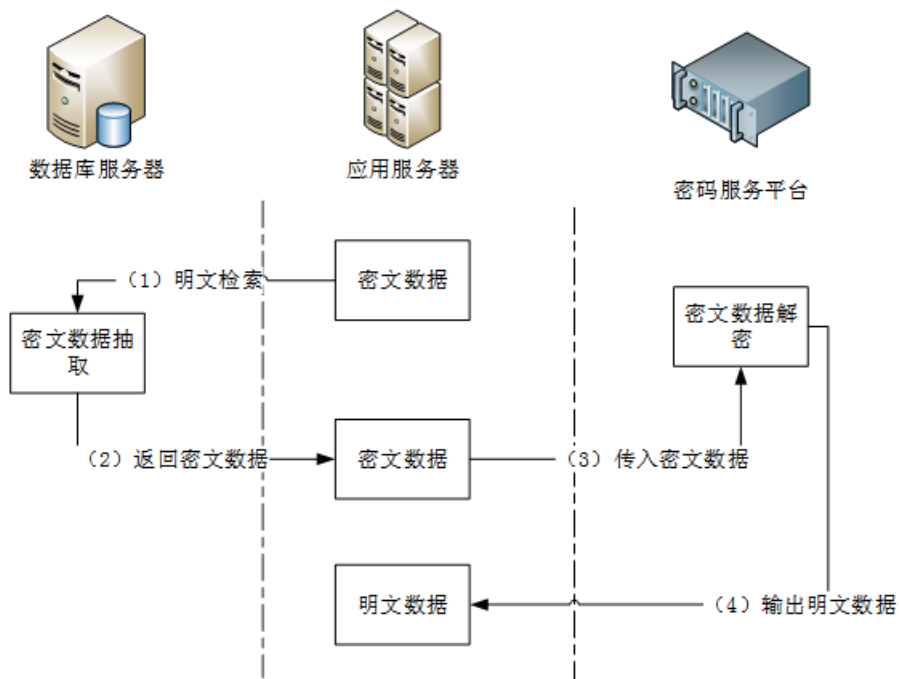


图 512 数据解密流程

具体业务流程如下：

- 1) 应用系统通过明文索引检索数据库保存的密文信息。
- 2) 应用系统将密文传递至密码服务平台。
- 3) 密码服务平台根据应用标识和分配的加密密钥将明文数据使用对称算法进行解密，并将解密后的明文数据回传至应用系统。
- 4) 应用系统将检索的明文信息通过国密SSL通道，安全传递至客户端。

密钥管理设计

密钥设计背景

密钥管理是设计安全的密码系统所必须考虑的重要问题，数据加密、验证和签名等需要管理大量的密钥，这些密钥经加密后以密文形式发送给合法用户。本办法参考国内组织有关密钥管理的知识、经验和相关标准编写。

密钥结构体系

密钥根据实际使用情况划分成三层，分别是管理密钥、用户密钥/设备密钥/密钥加密密钥、会话密钥，以下是三级密钥体制示意图。

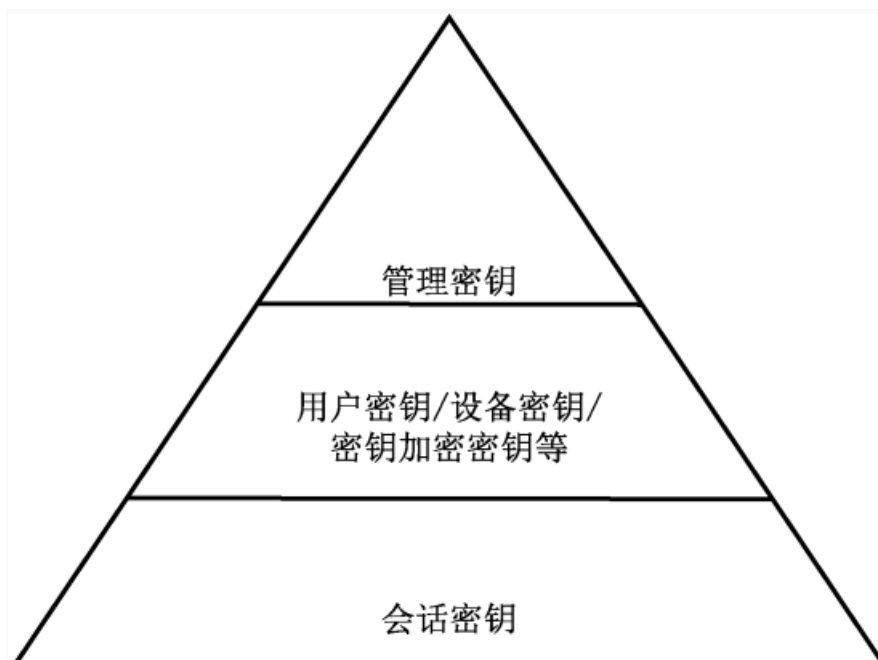


图 513 三级密钥体制示意图

管理密钥：用于保护服务器密码机中其他密钥和敏感信息的安全，包括对其他密钥的管理、备份、恢复等。不同服务器密码机的管理密钥互不相同，管理密钥必须安全存储。

用户密钥：包括签名密钥对和加密密钥对，用于实现用户签名、验证、身份鉴别以及会话密钥的保护和协商等，代表用户或应用者的身份。

设备密钥：是云服务器密码机的身份密钥，包括签名密钥对和加密密钥对，用于设备管理，代表云服务器密码机的身份。

密钥加密密钥：是定期更换的对称密钥，用于在与分配密钥情况下，对于会话密钥的保护。云服务器密码机可以支持密钥加密密钥。

会话密钥：用于数据加解密。

密钥生命周期的安全管理

密钥管理对于保证密钥全生存周期的安全性是至关重要的，可以保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，可以保证公钥不被非授权的修改和替换。信息系统的应用与数据层面的密钥体系由业务系统根据密码应用需求在密码应用解决方案中明确。密钥管理包括密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节。

- 1）密钥产生：密钥可以以随机产生、协商产生等不同的方式来产生，密钥产生所使用的随机数发生器或密钥协商算法是否为经国家密码管理部门核准的。
- 2）密钥分发：密钥分发过程保证密钥的机密性、完整性以及分发者、接收者身份的真实性等。
- 3）密钥存储：严禁密钥以明文形式存储在密码产品外部，密钥（除公钥）存储过程保证不被非授权的访问或篡改，并采取严格的安全防护措施。针对公钥，需采用安全防护措施，保证其不被非授权的篡改。
- 4）密钥使用：所有密钥都有明确的用途且各类密钥是否均被正确地使用、管理。
- 5）密钥更新：密钥根据相应的更新策略进行更新。结合应用处置方案，在不同场景，如密钥使用超过期限、密钥泄露、密钥存在泄露风险等，制定相应的密钥更新策略。
- 6）密钥归档：密钥归档过程保证密钥的安全性和正确性，并生成审计信息。
- 7）密钥撤销：公钥证书具备撤销机制。

8) 密钥备份：密钥备份过程保证密钥的机密性和完整性，并生成审计信息。

9) 密钥恢复：密钥具备恢复机制，并生成审计信息。

10) 密钥销毁：密钥具备销毁机制，销毁过程具备不可逆性。

密钥管理规定与监督检查

对密钥维护人员岗位设置、工作职责和审批手续做出严格的制度规定，并定期进行专项检查。

组建密钥安全管理工作组

1) 组织形式

密钥工作组由本单位部门领导任组长，由涉及密钥生命周期全过程的相关部门共同参加。

2) 工作职责

按照规定结合单位实际状况，制定严格而有效的实施细则，落实岗位责任制；

制订其他有关的安全专项管理制度，对涉及到密钥的生成、传输、保管各个环节的设备提出相应的安全管理要求，如出入登记制度、机房管理制度、岗位操作制度、密钥存储介质管理制度等。

负责密钥生命周期，包括生成、分发与传输、注入与启用、保管、删除与销毁、泄漏与重置等各环节全方位、全过程的规范操作与安全管理。

根据密钥特性，妥善保管密钥组件、密码函、IC密码卡、软件、源代码、涉及密钥安全管理的各种文档。

定期检查密钥安全管理状况，按规定填报有关表格、报告。

密钥安全管理工作人员

1) 基本规定

根据本办法，配备专职人员，专门负责密钥生命周期各环节的具体操作。

专人负责：所有的审批和操作指定专人负责，各专管人员均有自己的业务主管权限，未经有权人批准，不得擅自互换或代替。

密钥管理员每两年须轮换一次，如密钥管理员自行辞职，按重要岗位离职进行审核，同时经六个月的脱密期后，才让其离开。

基本素质要求

具有一定的计算机系统知识基础、接受能力和基本操作技能；

了解数据传输加密体系与加密设备的基本操作；

具有较强的工作责任心，工作坚持原则。

系统管理与设备维护人员要求

熟悉密钥分层管理的原理与基本流程；

熟练掌握交换系统主机、前置机、密钥操作PC机（如有）、终端设备密钥的操作实务；

熟悉加密设备的使用和维护。

2) 岗位设置

按照本办法设置如下一些基本岗位：密钥监督员、设备管理员、设备操作员、密钥生成员（注入、接收工作）、档案管理员、密钥销毁员等。

密钥监督员

1

负责监督本单位密钥安全管理的各项工作，即在整个密钥生命期内监督生成、保管、注入、分发及销毁等操作的正确性；

制止不正确操作，杜绝违规操作或超越权限操作的行为；

严格考察本单位重要岗位的工作状况，对不适合密钥维护工作或发现有不良行为的人员，提出调整要求；

协助完成定期或不定期的专项辅导检查工作。

设备管理员

设备管理员维护加密机等机密设备保持良好的运行状态。

负责对其他密钥维护人员讲解有关生成、装载等操作原理、操作步骤、操作要点和注意事项，指导密钥维护人员将密钥建置在各个相关设备的安全模组内，并在审批表格上记录相关操作情况。

凡手续不完备的需求，加密机管理员有权拒绝。

设备管理员一般可以由机房系统管理员兼任，履行机房安全管理工作的一般性要求。

协助完成定期或不定期的专项辅导检查工作。

设备操作员

负责加密设备的界面操作，协助完成生成、装载等操作过程。

审查有关审批表格的要求是否合理，操作结束在审批表签名认可。凡手续不完备的申请，操作员有权拒绝。

协助完成定期或不定期的专项辅导检查工作。

密钥生成（保管）员

密钥生成（保管）员同时履行注入、保管等工作职责。

按照信息择分、随机性、不可测等原则生成密钥组件；

分别保管主密钥组件；

接收密钥资料（组件），验证接收到的新密钥资料是否受损；

键入和改变密钥资料；

在监督下销毁密钥组件备份介质；

协助完成定期或不定期的专项辅导检查工作。

档案管理员

负责收集、归档所有的审批和登记表格等密钥档案，按不同的操作特征和类型分类，保存在档案室、磁带备份室等安全区域；

对档案建立较高的保密级别，未经书面授权，不允许借阅、复制及传播。

维护经管理人员授权后使用密钥的记录；

协助完成定期或不定期的专项辅导检查工作。

密钥销毁员

在监督下，完成密钥组件备份介质、文档等密钥资料的销毁。

审批制度

对密钥的任何操作必须履行相关审批手续，执行表格登记制度，未经履行审批手续的操作过程一律视为违章操作，应严格禁止。

应急措施

根据本单位的具体情况制定应急措施以防范以外因素导致的业务无法正常运营，应急措施包括申请审

批手续、启动与恢复流程、记录操作日志等内容。

监督

按照严格要求做好自查，并配合做好相关监督与调查工作。

密码应用部署

产品选型原则

- (1) 开放性
- 产品接口开放、产品总体架构可扩展性强。产品应提供多类别接口，满足服务提供时所面临的多种使用方式。
- (2) 扩展性
- 系统投入运营后，将面临业务流量不断增长的压力。产品应满足处理能力及资源的横向扩展和纵向扩展的需要，能在逐渐增加资源的情况下不断增长相应的处理能力。产品的扩展应尽量减少对现有系统运行的影响，保证系统的稳定运行。
- (3) 安全性
- 产品应有效地防止非法用户的入侵，确保系统安全。产品应提供严格的安全检查和日志管理，以提高系统运作的安全性。
- (4) 灵活性、方便性
- 产品要满足最大程度的灵活性，包括对业务扩展的灵活性。在各功能的实现上，应当体现模块化的思想。
- (5) 技术的成熟性
- 本项目应使用业界成熟、可靠和实用的技术，以满足产品的可用性、可靠性和实用性。
- (6) 先进性
- 本工程采用先进的技术和设备，能够满足和适应系统快速变化和发展的要求。
- (7) 可管理性
- 为保证产品的可管理性，就必须降低产品的复杂性。整个产品应便于操作、维护，应保证系统切换操作的简单化。
- 本次密码应用部署主要在物理机房和系统资源侧部署了相关密码设备保障系统的信息安全。在物理机房部署国密电子门禁、国密视频监控各一套，保障信息系统物理和环境的安全。
- 另外部署云服务器密码机4台、IPSEC/SSL VPN综合安全网关4台配合密码服务平台保障应用系统的用户真实性、数据安全等内容。
- 同时根据实际用户需求，配置对应用户数量的数字证书、智能密码钥匙、移动端协同签名组件等。

产品清单

序号	产品名称	类型	单位	数量
1	密码服务平台	软件	套	2

2	签名验签服务模块（支持杂凑算法）	软件	套	1
3	数据库加密服务模块	软件	套	1
4	协同签名服务模块	软件	套	1
5	IPSec/SSL VPN 综合安全服务模块	软件	套	4
6	云服务器密码机	设备	台	4

安全与合规性分析

针对第 3 章中安全需求的满足情况进行分析，重点对政策法规、标准规范的符合程度进行自我评价。包含《密码应用合规性对照表》，对每一项符合性进行自评价（符合或不适用）对于自查中不适用的项目，逐一说明其原因（比如环境约束、业务条件约束、经济社会稳定性等），并指出所对应的风险点采用了何种替代性风险控制措施来达到等效控制。

密码应用合规性对照表

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）
物理和环境安全	身份鉴别	在本系统所在机房部署符合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，并对门禁进出记录及视频记录数据进行完整性保护。	符合	
	电子门禁记录数据完整性	机房部署国密门禁系统，采用HMAC-SM3或SM2数字签名技术，对门禁系统人员进出记录做完整性保护，防止进出记录被篡改。	符合	

		视频记录数据完整性	部署视频监控系统，支持视频录像的完整性保护，防止录像文件被篡改。视频监控系统包含支持密码模块的IPC网络摄像机、NVR网络录像机、视频客户端。采用HMAC-SM3技术，实现实时视频流和视频录像的完整性保护。	符合	
		密码模块实现	在电子门禁和视频监控系统中实现密码算法、密码技术、密钥管理，且该产品符合GM/T0028《密码模块安全技术要求》第二级要求。	符合	
	网络和通信安全	身份鉴别	PC端系统用户接入内网时通过IPSEC/SSL VPN综合安全网关配合智能密钥匙，保障接入系统中终端的身份鉴别。 对于移动端用户，通过部署IPSEC/SSL VPN综合安全网关、协同签名SDK及相关组件实现在网络层通信双方的身份鉴别。	符合	无
		通信数据完整性	部署IPSEC/SSL VPN综合安全网关，采用国密SSL协议实现登录客户端与服务端之间的密钥协商，采用ECC（SM2）_SM4_SM3的SSL算法套件，实现通信数据的完整性保护。	符合	无
		通信数据机密性	部署IPSEC/SSL VPN综合安全网关，采用国密SSL协议实现登录客户端与服务端之间的密钥协商，采用ECC（SM2）_SM4_SM3的SSL算法套件，实现通信数据的机密性保护。	符合	无

访问控制信息完整性	采用部署的IPSEC/SSL VPN综合安全网关客户端对访问控制信息进行完整性保护。	符合	无
安全接入认证 (四级)	无	不适用	系统不涉及外部网络接入的设备。
密码模块实现	在IPSEC/SSL VPN综合安全网关等产品中实现密码算法、密码技术、密钥管理，且该产品符合GM/T0028《密码模块安全技术要求》第二级要求。	符合	无
身份鉴别	通过对PC端部署IPSEC/SSL VPN综合安全网关客户端并向系统管理员配发USBKey，对登录堡垒机用户进行身份鉴别和远程管理身份鉴别信息传输机密性保护	符合	无
远程管理身份鉴别信息机密性	IPSEC/SSL VPN综合安全网关代理堡垒机登录界面实现符合规定的SSL协议，对运维管理员用户进行身份鉴别和远程管理身份鉴别信息传输机防止非授权人员登录、管理员远程登录身份鉴别信息被非授权窃取。	符合	无
访问控制信息完整性	本系统中对资源访问控制需要通过智能密码钥匙结合IPSEC/SSL VPN综合安全网关登录堡垒机完成，或基于用户名口令和VPN登录平台进行维护，但无法对其访问控制信息进行完整性保护。针对系统中具有合格的商用密码产品认证证书的密码设备，设备自身已实现系统资源访问控制信息的完整性。	部分符合	
重要信息标记的完整性	——	不适用	本系统不涉及重要信息的敏感性标记。

			设备和 计算安 全	日志记录完整性	系统通过日志审计系统收集服务器、交换机、安全设备的日志，通过日志审计调用密码服务平台的杂凑运算服务HMAC-SM3进行性保护。针对系统中具有合格的商用密码产品认证证书的密码设备，设备自身已实现日志记录完整性。	符合	
				重要可执行程序完整性 重要可执行程序真实性	针对目前机房中网络及安全设备和操作系统等无法基于现有的密码技术对其重要可执行程序 and 重要资源安全标记的完整性要求，重要可执行程序均从官方渠道获取，且在安装前对程序进行验证，保证其没有受到篡改。在一定程度上降低重要可执行程序完整性、重要可执行程序来源真实性保护的安全风险。针对系统中具有合格的商用密码产品认证证书的密码设备，设备自身已实现重要可执行程序完整性、重要可执行程序来源真实性。	部分符合	
				密码模块实现	在IPSEC/SSL VPN综合安全网关、云服务器密码机、密码服务平台中实现密码算法、密码技术、密钥管理，且该产品符合GM/T0028《密码模块安全技术要求》第二级要求。	符合	无

应应用 和数据 安全	身份鉴别	PC端系统用户通过智能密码 钥匙进行身份鉴别，业务系 统调用密码服务平台的签名 验签服务对用户身份真实性 进行鉴别。 对于移动端登录用户，则使 用密码服务平台的协同签名 服务对移动端用户进行身份 鉴别。通过客户端扫码等方 式进行协同签名，实现对登 录用户身份真实性的鉴别。	符合	
	访问控制信 息完整性	业务系统通过调用密码服务 平台的杂凑运算服务对ACL 做完整性保护。	符合	无
	重要信息资 源安全标记 的完整性	——	不适用	本系统不涉及 重要信息资源 安全标记完整 性。
	数据传输机 密性	业务系统进行数据传输采用V PN综合网关的SM2-SM3-SM 4算法加密套件的SSL协议保 障数据传输的机密性。	部分符合	无
	数据存储机 密性	业务系统通过密码服务平台 的数据加解密服务的SM4算 法对数据进行加密保障数据 存储的机密性。	符合	无
	数据传输完 整性	业务系统进行数据传输采用V PN综合网关的SM2-SM3-SM 4算法加密套件的SSL协议保 障数据传输的完整性。	部分符合	无
	数据存储完 整性	业务系统通过调用密码服务 平台的杂凑运算服务的HMA C-SM3对数据进行加密保障 数据存储的完整性。	符合	无
	不可否认性	本系统暂不涉及	--	无

密码模块实现	云服务器密码机、密码服务平台、智能密码钥匙等产品中实现密码算法、密码技术、密钥管理，且该产品符合GM/T0028《密码模块安全技术要求》第二级要求。	符合	无
--------	--	----	---

安全管理方案

包含系统采取的密码安全相关制度、人员、建设、应急等方面的管理措施。

制度

《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》、《商用密码管理条例（修订草案征求意见稿）》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》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。

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。

信息系统规划阶段，依据相关标准，制定密码应用方案，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。

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。

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。

第二章 密码运行要求

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。

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。

第三章 密码人员管理要求

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。

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智能，明确管理责任，做到责任到部门责任到人。

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。

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。

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。

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。

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。

第四章 密码使用责任要求

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。

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。

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。

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。

第五章 密码设备维护规定

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。

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。

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。

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。

《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。

（1）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。

（2）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。

（3）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。

（4）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。

（5）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露和替换；密钥泄露时，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。

（6）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。

（7）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。

（8）密钥销毁

本单位已具有在紧急情况下销毁密钥的措施。

人员

《商用密码人员管理制度》

依据本单位《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。

总章

密码人员应了解并遵守密码相关法律法规。

在岗密码人员应能够正确、合理使用密码产品。

密码人员岗位与职责

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。

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智能，明确管理责任，做到责任到部门责任到人。

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。

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。

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。

密码人员培训规范

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。

培训参加。定期参与省密码管理局开展的密码培训会议。建立本单位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。

人员档案管理。建立针对密码管理人员建立员工培训档案，接收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。

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。

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”。

密码人员考核与奖惩

依托本单位人员绩效考核管理制度，制定密码人员考核管理办法。

针对测评机构、省密码管理局、国家密码管理局的定期检查、抽查效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。

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。

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。

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

组织架构和人员管理

密码安全管理小组

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

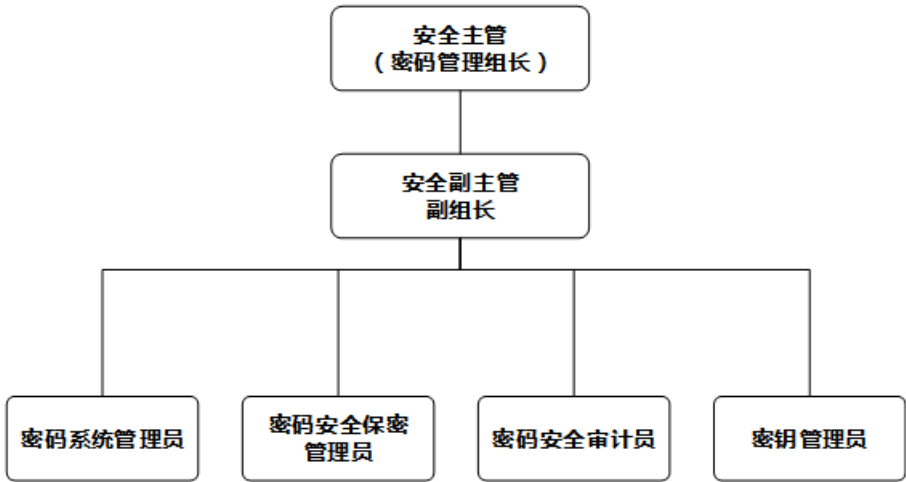


图 61密码安全管理小组

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：

（1）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。

（2）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。

（3）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。

（4）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。

《密码安全操作规范》

第一章 密码设备安全操作规范

认真执行岗位责任制和相关规章制度

严格遵守安全操作规程，保证密码设备的安全运行。

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。

密码设备操作人员必须经过培训，并留存培训记录。

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。

密码设备操作应严格遵守相关规章制度和操作规范。

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。

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。

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。

严谨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。

严谨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。

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。

厂家人员操作，应用相关技术人员全程陪同监督。

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

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；

系统维护密码应至少由两人共同设置、保管和适用，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。

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露应立即修改，并详细记录用户名、修改时间、修改人等。

禁止非工作人员操作网关系主机，不使用网关时，应注意锁屏。

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）。超级管理员应制定专人管理，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。

所有密码不得外泄。

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

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；

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。

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；

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；

避免在公共场所或他人计算机上使用数字证书；

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陆不明网络站点，下载、安装不明软件或运行不明程序。

实施

完成本方案编制后，委托密评机构对本方案进行评估，评估通过后，将本系统密码应用改造方案向密码管理部门备案，并同步对本系统进行密码应用改造，选用通过检测认证合格的云服务器密码机、国密安全网关、智能密码钥匙、数字证书等商用密码产品，合规、正确、有效的建设密码保障系统。依据评估通过的密码应用方案改造完成后，委托密评机构对本系统进行密评，密评通过后上线运行，上线运行后，每年对本系统进行一次密码应用安全性评估，并根据评估意见进行整改。当本系统在运行过程中发现重大密码应用安全隐患时，将停止系统运行，制定整改方案，按照整改方案对系统进行整改和密码应用安全性评估，评估通过后重新上线运行。

应急

密码安全事件分级

根据网络系统的重要程度、系统损失和社会影响，将密码安全事件划分为三个级别：特别重大安全事

件（一级）、重大安全事件（二级）、较大安全事件（三级）和一般安全事件（四级）。

（一）特别重大密码安全事件（一级）

特别重大安全事件是指能够导致灾难性破坏或影响的网络与密码安全事件，对社会稳定和国家安全产生灾难性危害，包括以下情况：

- 1、全部用户及密码相关业务瘫痪，无法使用；
- 2、密码业务模块不能正常工作，密钥及核心安全配置失效；
- 3、密码加密功能失效，涉密信息广泛传播；
- 4、密码相关终端与应用服务中断运行24小时以上。

（二）重大密码安全事件（二级）

重大安全事件是指能够导致严重影响或破坏的网络与密码安全事件，对社会稳定和单位利益产生严重危害，包括以下情况：

- 1、大范围用户与密码相关业务受到影响；
- 2、大部分密码业务模块不能正常工作；
- 3、密码相关功能模块存在高危安全漏洞；
- 4、密码相关终端与应用服务中断运行24小时以上。

（三）较大密码安全事件（三级）

较大密码安全事件是指能够导致较严重影响或破坏的网络与密码安全事件，对社会稳定和单位利益产生一定危害，包括以下情况：

- 1、部分用户及密码相关业务受到影响。
- 2、部分密码业务模块不能工作；
- 3、密码相关终端与应用服务中断运行2小时以上，12小时以下。

（四）一般密码安全事件（四级）

一般密码安全事件是指影响较低的网络与密码安全事件，对社会稳定和单位利益产生危害较小或影响轻微，包括以下情况：

- 1、个别用户与密码相关用户受到影响；
- 2、单个密码业务模块异常；
- 3、密码相关终端与应用服务中断运行2小时以下。

应急处置组织机构

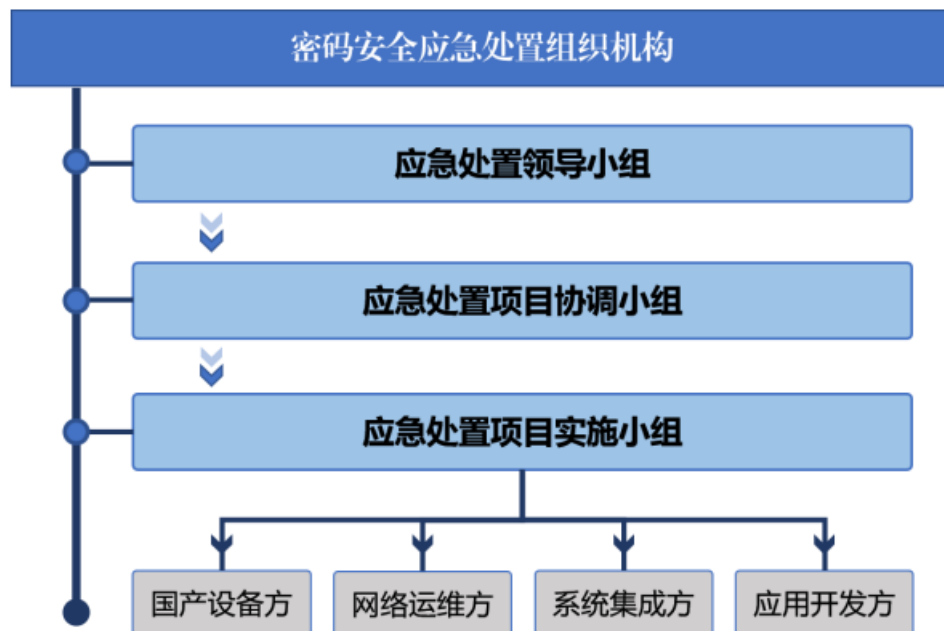


图 62 密码安全处置机构结构图

应急处置领导小组由项目建设方相关领导及主要负责人组成，对密码安全事件应急处置机制进行统筹和规划，具有如下职责：

- （一）指导系统密码安全事件的防范与应急处置工作；
- （二）推动系统密码安全事件应急响应机制的建立和落地执行。

应急处置领导项目协调小组由单位部门领导及主要负责人组成，对密码安全应急处置项目实施进行指导和工作协调，具有如下职责：

- （一）评审和更新密码安全事件管理规范；
- （二）协调和监督密码安全事件处置、纠正和预防措施的执行；
- （三）组织调查密码安全事件，配合有关部门进行网络与密码安全案件的调查与取证；
- （四）向密码安全处置领导小组报告并提出处理意见。

应急处置领导项目实施小组由相关技术服务方负责与实施人员组成，应对对密码安全应急处置项目实施工作，具有如下职责：

- （一）国产硬件设备提供方负责对所提供硬件设备进行技术支持与应急技术服务实施工作；
- （二）网络运维支撑服务方负责对系统所在网络的服务器物理环境、网络通信线路和网络边界的安全防护与应急处置技术支持、实施工作；
- （三）系统集成服务方负责对系统整体架构、部署运行与功能响应等进行技术支持，协调相关技术服务方落实应急响应实施工作。
- （四）应用系统开发方负责对相关系统的实际应急响应工作进行技术支持与实施工作。

应急响应机制

使用单位或者人员发现网络与密码安全突发事件后，应及时报告应急处置小组。应急协调小组及时组织应急实施小组查找故障原因，在半小时内依据故障情形和修复时间进行初步判断，确定故障级别，若是较大（三级含）及以上的突发事件应报告应急处置领导小组。

突发事件发生后，根据突发事件严重程度，由领导向上级主管单位与所属密码管理局进行报告，并指定特定小组或者人员及时向公众发布故障信息。

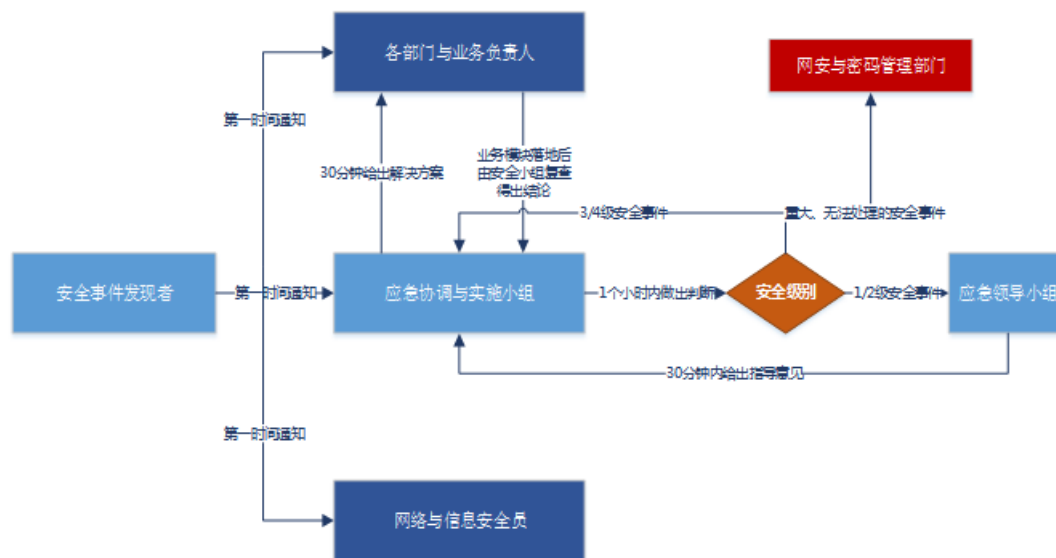


图 63 密码安全应急处置流程

（一）当网络与密码安全事件发生时，根据事件类型及影响大小，按照规定汇报角色和处理流程。

- 1、内部人员发现疑似网络与密码安全事件或收到外部报告的信息安全事件时，发现人应同时告知本通报部门网络与信息安全专员、应急协调与实施小组并告知各相关部门与业务负责人；
- 2、各部门网络与信息安全专员在发生网络与密码安全事件时，应立即向网络与密码安全应急小组报告。

（二）信息安全事件汇报内容应尽量涵盖事件发生的事实、可能影响的范围、损失评估、需要的支持、采取的应对措施等。

（三）网络与密码协调小组在收到报告后，应对事件进行判断和分析：

- 1、判定为非网络与密码安全事件时，将结果回复发现人。
- 2、判定为网络与密码安全事件时，则进一步分析事件影响，并按相关制度流程进行处理：

（1）当发生一般安全事件时，由网络与密码协调与实施小组处理，并采取相关的纠正及预防措施，以防止类似事件发生。

（2）当发生较大或重大安全事件时，应上报应急处置领导小组，并由应急协调与实施小组根据领导小组的决策对事件进行处理。

（3）处理过程中如发现造成的影响大于原先判定事件，应重新执行事件分析。

（四）处理网络与密码安全事件时，若需内部资源，则由应急处置协调小组沟通协调工作；如需要外部资源协助，则由应急处置领导小组进行协调。当重大安全事件发生需对外说明时，由单位的统一外宣窗口统一对外说明情况与处置方式，同时报送上级主管部门及密码管理部门。

（五）建立相应机制，监视并记录安全事件，并对其类型、数量和造成损失的代价进行统计。

（六）当一个安全事件涉及民事或刑事诉讼，需要进行司法取证时，应注意：

- 1、设备封存过程需当事人、调查者及司法鉴定部门同时在场，封存处必须有各方签字；
- 2、数据的保存和证据的挖掘过程均需司法鉴定部门在场，以确保数据的完整性和可靠性；
- 3、司法鉴定机构需对获取证据的过程出具司法鉴定报告。

（七）重大安全事件和无法处理的安全事件上报公安部门与密码管理部门。

（八）针对信息安全事件的处理时间：

响应时间	安全事件等级	故障处理时间
1小时	四级	2-8个小时
1小时	三级	2-6个小时

30分钟	二级	1-2小时
30分钟	一级	1-2小时

应急处置流程

网络与密码安全事件应急处置涉及事件程序评估制定，并即时开展应急实施行为，尽快将受影响的系统服务恢复正常。有关程序大致可分为五个阶段：确认、升级处理、遏制、杜绝和恢复。认识各阶段具体工作有利于在发生安全事件时迅速做出响应。

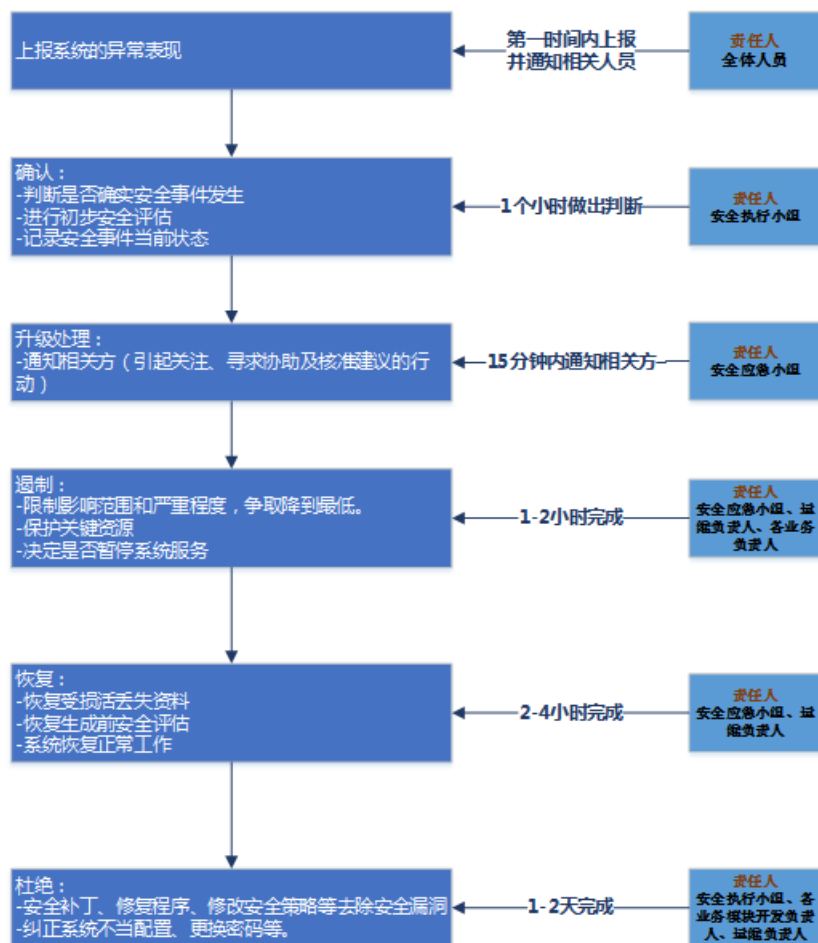


图 64 安全事件应急响应流程

应急公告流程

按照造成应用系统密码应用的中断运行时间，将突发事件级别划分为一般（三级）、较大（二级）、重大（一级）。

发生安全事件后：

应急小组应第一时间采取有效措施进行先期处置，将损害和影响降到最小范围，并判断突发事件级别，若是较大（二级）及以上级别，需要马上口头报告上级主管部门。

报告内容包括：

- （1）时间地点；
- （2）简要经过；
- （3）事件类型与分级；
- （4）影响范围；

- (5) 危害程度；
- (6) 初步原因分析；
- (7) 已采取的应急措施。

上级主管部门向各应急响应小组（例如损失评估小组、网络恢复小组、数据备份恢复小组等）下达指令的流程，损失评估组做好损失的评估工作，网络恢复组做好快速恢复网络的工作，数据备份恢复组做好数据备份工作，各应急处理人员的通信畅通性，并设置紧急联系人。涉及人为主观破坏事件应同时报告当地公安机关。

事中情况报告和处置：

- （一）事中情况报告应在安全事件发生后2小时内以书面报告的形式进行报送。
- （二）事中情况报告应急小组编写，由应用领导组审核后，报送上级主管部门，

事件处置完成后：

- （一）事后整改报告应在安全事件处置完毕后5个工作日内以书面报告的形式进行报送；
- （二）事中情况报告应急小组编写，由应急领导组审核后，报送上级主管部门和密码管理局。

损失评估

损失评估应有专门的损失评估小组负责。安全事件发生后，损失评估小组应最先被指令到达现场，执行损失评估。

损失评估组人员在应急协调组和应急实施组的陪同下进入机房，并对设备进行检查和评估，并记录损失情况形成报告，损失报告应包含具体的事件经过，事件发生原因分析，物理财产损失、业务损失、公信力损失，风险改进计划等多方面，用于应急预案的激活条件。

及时跟进行动包括评估事件所造成的破坏、系统改良以防止再度发生事件、安全政策和程序更新及为日后的检控进行个案调查。

预案激活条件

根据不同的安全事件分类级别，采取相应措施进行密码应用应急处理。事件处理过程中，必要时应急实施组根据事件情况及时调整事件级别，由应急损失评估组评估事件损失。

一般（三级）：应急实施组组织开展系统应急处理工作，
较大（二级）及以上：应急实施组向应急协调组报告事件级别和事件情况，由应急协调组向应急领导组报告事件级别和事件情况，并激活相应的事件应急预案。

密码服务平台技术参数

产品名 称	技术指 标	规格要求
	▲适配证明	支持和云管系统的无缝集成，支持华为云通过云管系统对密码服务资源进行开通与管理。（提供与云管集成的证明材料）

功能性要求	▲支持产生平台使用情况的可视化大屏，例如支持展示不同类型和厂商的密码资源数量、密码服务数量和租户及租户业务应用数量，支持展示租户及密码服务开通情况的历史曲线、各类密码服务访问量情况的历史曲线，支持监控平台组件、密码机和密码服务的状态，并对异常情况告警。 (需提供相关证明材料)
	支持对云服务器密码机进行上架、配置、查看、下架等管理，可对云服务器密码机进行停机、重启等控制管理，支持虚拟密码机创建及创建率查看。
	▲支持接入多厂商的异构云密码机设备及管理。支持管理异构云密码机认证凭证、查看认证状态等操作。(需提供相关证明材料)
	支持虚拟密码机管理功能。支持虚拟密码机新增、更新、关机、重启等管理操作，支持对虚拟密码机进行网络设置，支持对虚拟密码机可用状态进行在线测试，支持查看虚拟密码机访问趋势。
	支持普通密码设备纳管，包括服务器密码机设备、密码卡的接入管理。
	支持密码机组的管理。支持创建、删除、编辑密码机组，支持从密码机组中加入或移除密码机。
	支持虚拟密码机密钥管理。支持以密码机组进行密钥管理，可以创建对称、非对称密钥对，支持导入及导出密钥信息，支持查看密钥机柄的密钥访问情况。具备密码机组内密码机密钥同步配置功能，
	▲支持按虚拟密码服务节点、物理密码设备产品进行密码资源分类纳管。支持对组内的物理设备进行增减，支持对组中API接口信息管理及单点登录配置。(需提供相关证明材料)
	支持同时管理多厂商密码设备作为平台密码资源。
	支持对密码资源进行资源区管理，实现密码资源隔离管理。
	支持密码服务的管理，可以对服务进行创建、修改、删除、查看等生命周期管理，支持服务上架、启用、停用、下架的控制管理。

功能性要求	支持将密码资源池化成密码服务，支持按虚拟密码机组、密码机设备组、密码产品设备组进行资源组封装。
	▲支持通过在密码服务关联中管理节点组和服务节点组的方式，可对密码资源进行增加资源、减少资源等动态调整。（需提供相关证明材料）
	▲支持对密码服务的开通管理，支持租户自助申请开通密码服务，包括在申请单中指定要申请的服务规格和申请使用的周期等信息，并支持安全保密管理员进行审批，系统管理员进行申请单的实施和开通；服务开通后，支持租户对服务进行延期申请和提前释放操作。（需提供相关证明材料）
	支持对密码服务的授权管理，包括可指定租户、指定业务应用访问特定的密码服务。
	支持查看密码服务访问情况，包括按密码服务分类查看，支持按租户、业务应用筛选查看，支持根据时间段筛选查看。
功能性要求	支持国密算法和国际标准算法并行。
	支持国密SM1、SM2、SM3、SM4等算法。
	支持通过统一SDK、restful http接口两种方式提供密码服务。
	支持统一密码服务访问入口，支持密码服务熔断、限流、降级等流量控制。
	支持通过纳管和调度密码产品设备，为业务应用提供多种密码服务。
性能要求	支持通过虚拟化技术结合硬件密码机资源，为业务应用提供多种虚拟密码服务。
	▲支持按场景创建不同模式的密码服务，至少支持共享服务、专享服务、平台公共服务三种服务类型。（需提供相关证明材料）
	最大可支持租户数：≥1000个；最大可接入应用数量：≥5000个；
	最大可纳管设备数量：≥1000台（套）；最大密码服务节点数量：≥2000个；

				密码服务平台	<p>▲提供国家密码管理局的信创适配证明盖章件，可以适配统信UOSV20和龙芯3A5000、鲲鹏920；银河麒麟V10和飞腾FT-2000、兆芯ZX-E K X-U6780A；</p> <p>▲ 支持RSA、SM2、ECC、CFCASM2多种格式的站点证书，支持密钥不落地方式上传站点证书；（需提供相关证明材料）</p> <p>支持客户端代理服务。支持为两个不同的网络应用提供代理级的加密通道，应用和网关基于http或者国际SSL协议通信，两台网关之间通过GM SSL链路加密通信。保证公网传输安全性的同时，不改变内网原有通信协议；</p> <p>IPSEC性能要求：加密吞吐≥4Gbps；每秒新建隧道≥99；并发隧道数≥10000；</p> <p>SSL性能要求：加密吞吐率≥10Gbps；并发连接数≥12W；RSA每秒新建连接≥ 6K；SM2每秒新建连接≥16K；HTTP TPS（每秒交易数）≥5W</p>
				IPSec/SSL VPN综合安全网关模块	<p>▲当系统出现故障时（比如：License即将过期），首页会弹窗提示管理员，并提供详情查看调整引导。告警事件可提供建议处置措施，方便运维人员进行维护管理。（需提供相关证明材料）</p> <p>支持单一代理服务可以配置多个后端服务节点，并且支持HTTP Session、客户端IP地址、权重轮询、最快响应和哈希分配等负载均衡调度算法；</p> <p>支持友好错误页面，使终端用户得到明确友好的错误提示。同时支持根据状态码进行自定义和外部URL跳转至第三方错误页面。</p> <p>支持图表数据实时查看隧道各阶段的建立情况,包括对端地址、对端身份信息、算法、本端保护网络、对端保护网络、流入/流出速率、建立时间等信息。</p> <p>支持为两个不同的网络应用提供代理级的加密通道，应用和网关基于http或者国际SSL协议通信，两台网关之间通过GM SSL链路加密通信。保证公网传输安全性的同时，不改变内网原有通信协议不变。</p>

协同签名 服务模块	<p>▲支持在同一个服务实例中，配置RSA和SM2两张站点证书，并同时启用，根据客户端的算法能力进行自动适应（提供相关证明材料）；</p> <p>支持快速检索海量（超过100万条目数）的证书黑名单；</p> <p>支持密钥分割技术，保证私钥安全，需具有安全的两方协作SM2签名方法的能力；</p> <p>协同签名客户端具有国家密码管理局颁发的商用密码产品型号证书《协同linux客户端密码模块》、《协同windows客户端密码模块》、《协同Android客户端密码模块》、《协同IOS客户端密码模块》资质，能兼容linux、windows、Android和IOS计算环境，符合GM/T 0028-2014《密码模块安全技术要求》和GM/T 0039-2015《密码模块安全检测要求》安全等级第二级相关要求</p>
数据库加 密服务模 块	<p>数据库加密系统：系统支持Mysql、Oracle、Sql Server、postgresql、达梦、人大金仓、oceanbase、阿里rds、华为高斯等多种数据库，支持国密算法；</p> <p>▲支持应用系统免改造加密，支持字段级别的数据内容加密，支持图形化自定义能力，提供历史数据管理；提供灵活的加密状态和非加密状态的双向转换（提供相关证明材料）；</p> <p>提供图形化的数据加密配置，可以对指定数据表列的全部数据进行一次加密，加密初始化时使用与字段加密配置一样的加密算法和密钥；</p> <p>▲数据库中的敏感数据以密文方式存储，通过数据库客户端工具查看时，敏感数据以密文方式显示，防止敏感数据泄露（提供相关证明材料）；</p>

签名验签 服务模块	支持 SM2、SM3、SM4等密码算法，具有签名验签、身份认证等功能提供数据签名与签名验证功能；提供证书存储功能，实现对客户端证书的存储，管理员可以通过页面进行证书导入和查找，业务系统可以通过接口获取已存储的证； ▲产品基于HTTP消息方式提供使用SM2算法的数字签名和验签服务，支持注册应用实体并为其产生签名密钥对和证书请求，支持导入应用实体的签名证书、加密证书和加密密钥对，提供证书存储、更新和验证功能，对证书和密钥等数据提供备份恢复功能（提供相关证明材料）；
--------------	---

根据项目内容要求，需提供4台云服务器密码机作为辅助服务设备。具体参数如下：

密码服 务功能	虚拟密码机：在物理实体机上，提供多台虚拟密码机（VSM），每台虚拟密码机均可对主机提供应用层数据加/解密、消息来源正确性验证、密钥管理等功能
	随机数生成：采用由国家密码管理局批准使用的物理噪声源发生器芯片生成随机数。
	密钥生成：支持生成 SM2 密钥对和RSA 密钥对
	密钥存储：VSM 内可存储对称密钥、SM2 密钥对和 RSA 密钥对，并且私钥部分受系统保护密钥的加密保护。
	数据加密和解密：支持对称算法的 ECB/CBC/CTR/GCM 等模式的数据加密和解密运算
	消息鉴别码的产生和验证：支持基于对称算法的 MAC 产生及验证
	数据摘要的产生和验证：支持基于杂凑算法的摘要运算
	数字签名和验证：支持利用内部存储的私钥或外部导入私钥对请求数据进行数字签名或验证
	签名验证格式：支持 PKCS#1、PKCS#7、XML 等格式的数据签名、签名验证功能，支持文件签名验证功能
	密钥备份及恢复：支持基于主密钥保护下的密钥的备份和恢复功能
	设备管理:提供云密码机、虚拟密码机集中安全管理。
	支持虚拟密码机的增删、启停、配置、分配、分组等操作。

		云密码机	密钥管理功能	支持云密码机、虚拟密码机的状态监控。
				支持开放设备管理协议和服务接入标准，满足对第三方密码设备的兼容。
				密钥管理:将各密码设备的密钥的产生、存储、更新、销毁等生命周期的各个环节进行集中安全管理。
				建立密钥与设备（组）、密钥与业务的关系。
				日志审计:管理系统具备完善的日志审计功能，针对人员操作提供带签名的日志记录，方便审计管理。
				审计管理员独立于其他人员权限，负责所有人员及设备的日志信息的审计工作。
			密码服务接口	密码服务接口:提供符合《GM0018密码设备应用接口规范》的标准化接口，接口支持C、Java等主流编程语言。
				接口调用:支持多进程、多线程调用密码服务接口。
			设备管理	权限管理:管理用户采用三权分立的模式，保障设备的安全访问，划分为系统管理员、安全管理员、审计管理员、系统操作员四种类型。管理员和操作人员身份通过USBKEY进行双因子认证。
				系统监控:支持对设备CPU/内存资源的使用率、当前并发连接数量、服务进程状态等进行实时监控。
				业务连续性:支持断链修复功能，支持多虚拟密码机并行及负载均衡。
				日志审计:支持审计管理员对密码机的管理操作行为进行审计。
				管理系统:提供云密码机管理系统。
			安全性设计	物理安全:采用防拆、防撬结构设计，在暴力拆解下密钥将自动销毁
				白名单:提供IP包过滤，只有授权的用户才可以访问密码机
			性能指标	SM2签名≥10000tps;SM2验签≥4500tps;SM2密钥对生成≥3000对/秒;SM3运算≥300Mbps;SM4_CBC加密≥500Mbps;SM4_CBC解密≥500Mbps;SM1_CBC加密≥500Mbps;SM1_CBC解密≥400Mbps;随机数生成≥500Mbps
3.2.3人员配置要求		配置要求	标准机架2U双电、信创硬件平台、内存≥64G、存储≥512G、千兆电口≥6、万兆光口≥2	
采购包1:				

3.2.4设施设备要求

采购包1:

根据项目内容配备，具体要求详见服务内容。

3.2.5其他要求

采购包1:

1.项目密码改造完成后需取得专业测评机构出具的测评报告，并在密码管理局完成备案。2.保密要求：对工作中了解到的甲方的技术、机密等进行严格保密，不得向他人泄漏。本合同的解除或终止不免除乙方应承担的保密义务。

3.3商务要求

3.3.1服务期限

采购包1:

自合同签订之日起至验收合格通过为止。

3.3.2服务地点

采购包1:

西安市卫生统计信息中心

3.3.3考核（验收）标准和方法

采购包1:

1.项目建设完毕后，由采购方、使用单位组织项目相关人员按照国家行业规范标准和文献资料进行验收。2.采购人应按照政府采购合同约定的技术、服务、安全标准组织对供应商每一项技术、服务、安全标准的履约情况进行验收，并出具验收书。

3.3.4支付方式

采购包1:

分期付款

3.3.5支付约定

采购包1：付款条件说明：合同签订后30天内，甲方向乙方支付合同总价款30%作为预付款，乙方需提供相关收款依据，达到付款条件起 15 日内，支付合同总金额的 30.00%。

采购包1：付款条件说明：合同签订后，总体项目建设完成第一阶段，密码应用改造工作验收合格后，甲方向乙方支付合同总价款40%，乙方需提供相关收款依据，达到付款条件起 15 日内，支付合同总金额的 40.00%。

采购包1：付款条件说明：总体项目建设完成第二阶段，密码应用改造工作验收合格后，甲方向乙方支付合同总价款20%，乙方需提供相关收款依据，达到付款条件起 15 日内，支付合同总金额的 20.00%。

采购包1：付款条件说明：总体项目建设完成后按照相关要求试运行结束后进行总体验收，总体验收合格一年后，甲方向乙方支付合同总价款10%，乙方需提供相关收款依据，达到付款条件起 15 日内，支付合同总金额的 10.00%。

3.3.6违约责任及争议解决的方法

采购包1:

1.按《中华人民共和国民法典》中的相关条款执行。2.未按合同要求提供服务或服务质量不能满足技术要求，采购人有权终止合同，并对供方违约行为进行追究，同时按《中华人民共和国政府采购法》的有关规定进行处罚。

3.4其他要求

1.本项目采购标的对应的中小企业划分标准所属行业为软件和信息技术服务业。2.成交人在领取成交通知书时提供一正两副纸质竞争性磋商响应文件。装订：纸质竞争性磋商响应文件采用书籍（胶装）方式装订成册，与电子竞争性磋商响应文件一致的签字、盖章的完整版本。

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磋商文件的规定，对响应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。	6.资格证明文件 响应函
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。	6.资格证明文件
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。	6.资格证明文件 响应函

4.2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			

4.3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	提供投标人合法注册的法人或其他组织的营业执照/事业单位法人证书/非企业专业服务机构执业许可证/民办非企业单位登记证书	提供投标人合法注册的法人或其他组织的营业执照/事业单位法人证书/非企业专业服务机构执业许可证/民办非企业单位登记证书；	6.资格证明文件
2	财务状况报告	财务状况报告：提供具有财务审计资质单位出具的2022年或2023年度财务报告（成立时间至开标时间不足一年的可提供成立后任意时段的资产负债表）或开标前六个月内其基本账户银行出具的资信证明或政府采购信用担保机构认可的担保函；	6.资格证明文件

3	税收缴纳证明	税收缴纳证明：提供截止至开标时间前六个月内任意一个月的缴纳凭据；（增值税、企业所得税至少提供一种，依法免税的供应商应提供相关文件证明）；	6.资格证明文件
4	社会保障资金缴纳证明	社会保障资金缴纳证明：提供截止至开标时间前六个月内任意一个月的社保缴纳凭据或社保机构开具的社会保险参保缴纳情况证明；（依法不需要缴纳社会保障资金的供应商应提供相关证明）；	6.资格证明文件
5	提供具有履行本合同所必需的设备和专业技术能力的说明及承诺	提供具有履行本合同所必需的设备和专业技术能力的说明及承诺（提供书面说明及承诺，加盖供应商公章）；	6.资格证明文件
6	提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明	提供参加政府采购活动前三年内在经营活动中没有重大违法记录的书面声明（提供书面声明，加盖供应商公章）；	6.资格证明文件
7	法定代表人授权委托书	法定代表人授权委托书（附法定代表人身份证复印件及被授权人身份证复印件）；法定代表人直接参加磋商只须提供法定代表人资格证明书（附法定代表人身份证复印件）；采购文件凡是法定代表人之处，非法人单位的负责人均参照执行（式样见响应文件格式）；	5.法定代表人授权委托书（格式） 6.资格证明文件
8	信用信息查询	不得为“信用中国”网站(http://www.creditchina.gov.cn)列入“失信被执行人（页面跳转至“中国执行信息公开网” http://zxgk.court.gov.cn/shixin/ ）、重大税收违法失信主体、政府采购严重违法失信行为记录名单”的供应商；不得为中国政府采购网(http://www.ccgp.gov.cn)“政府采购严重违法失信行为记录名单”中的供应商。（根据财库【2019】38号文规定，此项在磋商截止日当天在“信用中国”网站和中国政府采购网站进行查询，截图留档；如网站无供应商信息的，供应商须提供相关证明资料或书面声明）；	6.资格证明文件
9	控股关系	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。（根据财库【2019】38号文规定，此项在磋商截止日当天在“国家企业信用信息公示系统”进行查询，截图留档；如网站无供应商信息的，供应商须提供相关证明资料或书面声明）。	6.资格证明文件

第五章 磋商过程中可实质性变动的内容

磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第八章“拟签订采购合同文本”，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

在磋商过程中，磋商小组根据项目实际需要制定磋商内容，在获得采购人代表确认的前提下，可以根据磋商情况实质性变动相关内容。磋商小组对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应及时通知所有参加磋商的供应商。

第六章 磋商办法

6.1 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》《政府采购竞争性磋商采购方式管理暂行办法》《陕西省政府采购评审专家管理实施办法》等法律法规，结合本采购项目特点制定本竞争性磋商评审方法。

二、评审工作由代理机构组织，具体评审事务由依法组建的磋商小组负责。

三、评审工作应遵循客观、公正、审慎的原则，并以相同的磋商程序 and 标准对待所有的供应商。

四、本项目采取电子评审，通过项目电子化交易系统完成评审工作。磋商小组成员、采购人、代理机构和供应商应当按照本磋商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审活动。

五、评审过程中的书面材料往来均通过项目电子化交易系统传递，评审委员会成员使用互认的证书及签章进行签名后生效，供应商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，评审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、评审过程应当独立、保密，任何单位和个人不得非法干预评审活动。供应商非法干预评审活动的，其响应文件将作无效处理；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审活动的，将依法追究其责任。

6.2 磋商小组

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。

一、磋商小组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、推荐磋商小组组长。采购人代表可以使用采购人代表专用签章确认评审意见。

二、磋商小组成员获取解密后的响应文件，开展评审活动。出现应当回避的情形时，磋商小组成员应当主动回避；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响应文件，按规定重新组建磋商小组，解封响应文件后，开展评审活动。

三、磋商小组按照磋商文件规定的磋商程序、评分方法和标准进行评审，并独立履行下列职责：

- （一）熟悉和理解磋商文件；
- （二）审查供应商响应文件等是否满足磋商文件要求，并作出评价；
- （三）根据需要要求采购组织单位对磋商文件作出解释；根据需要要求供应商对响应文件有关事项作出澄清、说明或者更正；
- （四）推荐成交候选供应商，或者受采购人委托确定成交供应商；
- （五）起草资格审查报告、评审报告并进行签署；
- （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。

6.3 评审程序

6.3.1 熟悉和理解磋商文件和停止评审

一、磋商小组正式评审前，应当对磋商文件进行熟悉和理解，内容主要包括磋商文件中供应商资格条件要求、采购项目技术、服务和商务要求、磋商办法和标准、政府采购政策要求以及政府采购合同主要条款等。

二、本磋商文件有下列情形之一的，磋商小组应当停止评审：

- （一）磋商文件的规定存在歧义、重大缺陷的；

- (二) 磋商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，但是磋商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，但是磋商文件未依法体现促进中小企业发展相关规定的；
- (五) 磋商文件将供应商的资格条件列为评分因素的；
- (六) 磋商文件载明的成交原则不合法的；
- (七) 磋商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审情形的，磋商小组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，磋商小组不得以任何方式和理由停止评审。

出现上述应当停止评审情形的，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。采购组织单位认为磋商小组不应当停止评审的，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。

6.3.2符合性审查

一、磋商小组依据本磋商文件的实质性要求，对符合资格的响应文件进行审查，以确定其是否满足本磋商文件的实质性要求。本项目的符合性审查事项必须以本磋商文件的明确规定的实质性要求为依据。

二、在符合性审查过程中，如果出现磋商小组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磋商文件规定。

三、磋商小组对所有响应文件进行审查后，确定参加磋商的供应商名单。

符合性审查标准见下表：

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.在磋商过程中，磋商小组认为供应商的报价明显低于其他实质性响应的供应商报价，有可能影响产品质量或者不能诚信履约的，磋商小组应当要求其在评审现场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，逐项就供应商提供的货物、工程和服务的主营业务成本（应根据供应商企业类型予以区别）、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.供应商提交的相关证明材料，应当加盖供应商（法定名称）电子印章，在磋商小组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。供应商不能证明其报价合理性的，磋商小组应当将其响应文件作为无效处理。</p>	标的清单 报价表

2	格式编制	除明确允许供应商可以自行编写的外，响应文件文件必须按照竞争性磋商文件给定的格式和要求编制	响应文件封面 5.法定代表人授权委托书（格式） 4.商务条款响应偏离表（格式） 3.服务条款响应偏离表（格式） 6.资格证明文件 18.《供应商参与政府采购活动的承诺函》（格式） 17.《拒绝政府采购领域商业贿赂承诺书》（格式）
3	签字盖章	磋商响应文件必须按照磋商文件的要求盖章签字	响应文件封面 5.法定代表人授权委托书（格式） 4.商务条款响应偏离表（格式） 3.服务条款响应偏离表（格式） 6.资格证明文件 18.《供应商参与政府采购活动的承诺函》（格式） 17.《拒绝政府采购领域商业贿赂承诺书》（格式）
4	磋商报价不得超过采购预算	磋商报价不得超过采购预算	响应文件封面 标的清单 响应函
5	磋商有效期	磋商有效期符合磋商文件的要求	响应文件封面 5.法定代表人授权委托书（格式） 响应函
6	磋商文件商务要求及服务要求	对磋商文件商务要求作出明确且实质性响应，对磋商文件技术要求作出明确响应，对不得偏离的要求作了实质性响应	响应文件封面 4.商务条款响应偏离表（格式） 3.服务条款响应偏离表（格式）

7	无法律、法规和磋商文件规定的其他无效响应情形	无法律、法规和磋商文件规定的其他无效响应情形	响应文件封面 4.商务条款响应偏离表（格式） 3.服务条款响应偏离表（格式） 18.《供应商参与政府采购活动的承诺函》（格式） 响应函 16.供应商认为有必要说明的事宜（若有） 17.《拒绝政府采购领域商业贿赂承诺书》（格式）
8	无采购人不能接受的附加条件	无采购人不能接受的附加条件	响应文件封面 4.商务条款响应偏离表（格式） 3.服务条款响应偏离表（格式） 16.供应商认为有必要说明的事宜（若有）

6.3.3磋商

一、磋商小组按照磋商文件的规定与邀请参加磋商的供应商分别进行磋商，磋商顺序由磋商小组确定。

二、磋商小组所有成员集中与单一供应商对技术、服务、合同条款等内容分别进行一轮或多轮的磋商。在磋商中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

三、磋商小组可以根据磋商文件和磋商情况实质性变动第三章“磋商项目技术、服务、商务及其他要求”、第八章“拟签订采购合同文本”，但不得变动磋商文件中的其他内容。实质性变动的内容，须经采购人代表确认。

四、对磋商文件作出的实质性变动是磋商文件的有效组成部分，磋商小组应通过项目电子化交易系统，将变动情况同时通知所有参加磋商的供应商。磋商过程中，磋商小组可以根据磋商情况调整磋商轮次。

五、磋商过程中，磋商文件变动的，供应商应当按照磋商文件的变动情况和磋商小组的要求就磋商文件变动部分，以“供应商响应表”形式在线提交磋商小组。“供应商响应表”作为响应文件的组成部分，响应文件应加盖供应商（法定名称）电子印章，否则无效。

六、经最终磋商后，响应文件仍有下列情况之一的，应按照无效响应处理：

- （一）响应文件仍不能实质响应磋商文件可实质性变动的实质性要求的；
- （二）响应文件中仍有磋商文件规定的其他无效响应情形的。

七、磋商小组对供应商在磋商、评审过程中的书面交换材料，未按要求加盖电子印章或签字的，视同未提交书面交换材料。

八、磋商小组在最终磋商后，对所有响应文件的有效性、完整性和响应程度进行审查后，确定最后报价的供应商名单。

九、磋商过程中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。

十、磋商过程中，磋商小组发现或者知晓供应商存在违法行为的，应当磋商报告中予以记录，并向本级财政部门报告，依法应将该供应商响应文件作无效处理的，应当作无效处理。

6.3.4最后报价

一、方案评审

采购包1：磋商/谈判/协商文件不能详细列明采购标的的技术、服务要求，需由供应商提供最终设计方案或解决方案的，磋商/谈判/协商结束后，磋商/谈判/协商小组应当按照少数服从多数的原则投票推荐3家实质性响应的供应商的设计方案或解决方案，进入最后报价环节；不足3家的，终止本次采购活动。

二、磋商小组开启报价后，供应商应随时关注项目电子化交易系统信息提醒，登录项目电子化交易系统，通过“等候大厅”进行报价并签章后提交。

三、供应商在未提高响应文件中承诺的标准情况下，其最后报价不得高于对该项目之前的报价，否则，磋商小组将对其响应文件作无效处理，并通过电子化交易系统告知供应商，说明理由。

四、供应商最后报价属于明显低价不正当竞争的，磋商小组应按照“供应商须知前附表”第8项规定处理。

五、供应商未在响应文件提交截止时间内提交报价或未按要求进行报价的，视为无效响应，由供应商自行承担不利后果。

六、供应商未按磋商小组要求在规定时间内提交最后报价的，视为其退出磋商。

七、最后报价一旦提交后，供应商不得以任何理由撤回。

八、最后报价为有效报价应符合下列条件：

- （一）供应商所提供的最后报价是在规定的时间内提交。
- （二）供应商的最后报价应加盖供应商（法定名称）电子印章。
- （三）供应商的最后报价应符合磋商文件的要求。
- （四）最后报价唯一，且不高于最高限价。

九、最后报价出现下列情况的，不需要供应商澄清，按以下原则处理：

- （一）报价中的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；
- （二）单价金额小数点或者百分比有明显错位的，应以总价为准，并修改单价；
- （三）总价金额与按单价汇总金额不一致的，以单价汇总金额计算结果为准；

同时出现两种以上不一致的，按照前款规定的顺序修正。修正后的最后报价经加盖供应商（法定名称）电子印章后产生约束力，供应商不确认的，其最后报价无效。

6.3.5解释、澄清有关问题

一、评审过程中，磋商小组认为磋商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磋商文件的原义或者影响公平、公正，解释事项如果涉及供应商权益的以有利于供应商的原则进行解释。

二、对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，磋商小组应当要求供应商作出必要的澄清、说明或者更正，并给予供应商必要的反馈时间。供应商应当按磋商小组的要求进行澄清、说明或者更正。供应商的澄清、说明或者更正不得超出响应文件的范围或者改变响应文件的实质性内容。澄清不影响响应文件的效力，有效的澄清、说明或者更正材料是响应文件的组成部分。

三、供应商的澄清、说明或者更正需进行电子签章，应当不超出响应文件的范围、不实质性改变响应文件的内容、不影响供应商的公平竞争、不导致响应文件从不响应磋商文件变为响应磋商文件的条件。下列内容不得澄清：

- （一）供应商响应文件中不响应磋商文件规定的技术参数指标和商务应答；
- （二）供应商响应文件中未提供的证明其是否符合磋商文件资格、符合性规定要求的相关材料。
- （三）供应商响应文件中的材料因印刷、影印等不清晰而难以辨认的。

四、响应文件报价出现前后不一致的情形，按照本章前述规定予以处理，不需要供应商澄清。

五、代理机构宣布评审结束之前，供应商应通过项目电子化交易系统随时关注评审消息提示，及时响应磋商小组发出的澄清、说明或更正要求。供应商未能及时响应的，自行承担不利后果。

六、磋商小组应当积极履行澄清、说明或者更正的职责，不得滥用权力。

6.3.6比较与评价

磋商小组应当按照磋商文件规定的评标细则及标准，对符合性检查合格的响应文件进行商务和技术评估，综合比较和评价。

6.3.7复核

评审结束后，磋商小组应当进行复核，特别要对拟推荐为成交候选供应商的、报价最低的、响应文件被认定为无效的的重点复核。

评审结果汇总完成后，磋商小组拟出具磋商报告前，代理机构应当组织2名以上的工作人员，在采购现场监督人员的监督之下，依据有关的法律制度和磋商文件对评审结果进行复核，出具复核报告。代理机构复核过程中，磋商小组成员不得离开评审现场。

除资格检查认定错误、分值汇总计算错误、分项评分超出评分标准范围、客观评分不一致、经磋商小组一致认定评分畸高、畸低的情形外，采购人或者代理机构不得以任何理由组织重新评审。采购人、代理机构发现磋商小组未按照磋商文件规定的评审标准进行评审的，应当重新开展采购活动，并同时书面报告本级财政部门。

6.3.8推荐成交候选供应商

磋商小组应当根据综合评分情况，按照评审得分由高到低顺序推荐如下成交候选供应商，并编写磋商报告。

采购包1： 3家； 评审得分相同的，按照最后报价由低到高的顺序推荐。评审得分且最后报价相同的，按照技术指标优劣顺序推荐。评审得分且最后报价且技术指标得分均相同的，成交候选供应商并列。

6.3.9编写磋商报告

磋商小组推荐成交候选供应商后，应向代理机构出具磋商报告。磋商报告应当包括以下主要内容：

- （一）邀请供应商参加采购活动的具体方式和相关情况；
- （二）响应文件开启日期和地点；
- （三）获取磋商文件的供应商名单和磋商小组成员名单；
- （四）评审情况记录和说明，包括对供应商响应文件审查情况、磋商情况、报价情况等；
- （五）提出的成交候选供应商的排序名单及理由。

磋商报告应当由磋商小组全体人员签字或加盖电子签章认可。磋商小组成员对磋商报告有异议的，磋商小组按照少数服从多数的原则推荐成交候选供应商，采购程序继续进行。对磋商报告有异议的磋商小组成员，应当在报告上签署不同意见并说明理由，由磋商小组记录相关情况。磋商小组成员拒绝在磋商报告上签字或加盖电子签章又不书面说明其不同意见和理由的，视为同意磋商报告。

6.3.10评审争议处理规则

在磋商过程中，对于符合性审查、对响应文件作无效响应处理的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，但不得违背磋商文件规定。持不同意见的磋商小组成员应当在磋商报告中签署不同意见及理由，否则视为同意评审报告。持不同意见的磋商小组成员认为认定过程和结果不符合法律法规或者磋商文件规定的，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。

6.4评审办法及标准

一、磋商小组只对通过资格审查的响应文件，根据磋商文件的要求采用相同的评审程序、评分办法及标准进行评价和比较。

二、磋商小组成员应依据磋商文件规定的评分标准和方法独立对每个有效响应的文件进行评价、打分，然后汇总每个供应商每项评分因素的得分。

6.4.1评分办法

本次评审采用综合评分法，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。

6.4.2评分标准

采购包1：

评审因素		评审标准			
分值构成		详细评审 90.0000 分 报价得分 10.0000 分			
评审因素分类	评审项	详细描述	分值	客观/主观	关联格式
	技术要求	完全符合、满足竞争性磋商文件技术要求的，计 20 分；参数中“▲”号技术号技术指标每有一条负偏离扣 2 分，非“▲”号技术号技术指标每有一条负偏离扣 0.5 分，基本分扣完为止	20.0000	客观	3.服务条款响应偏离表（格式）
	业绩	以合同形式提供供应商自 2021 年 1 月 1 日以来签订的类似项目业绩，每个业绩 1 分，计满 3 分为止。未提供的不计分	3.0000	客观	10.业绩
	项目理解	供应商对系统现状有较深理解，明确服务要求和目标，且分析思路清晰，理解准确。①对系统业务现状有较深理解，分析思路清晰明确，对服务要求和目标理解准确的，计 6 分；②针对以上要求，阐述不详实，分析简单的，计 4 分；③针对以上要求，理解与用户需求有偏差的，计 2 分；④未提供本项内容的均不计分。	6.0000	主观	1.项目理解

项目部署方案	<p>供应商需结合本项目的特点，提供详细的项目部署方案，包括但不限于云平台密码应用现状分析、基于现状的密码建设方案、网络等资源规划内容及应用系统对接调测内容等。</p> <p>①方案内容详细完整，专业化程度高且完全满足采购需求的，计10分； ②针对以上方案要求，有方案阐述不详实、用户实际需求匹配度不高、内容不完整等情况之一的，计9分； ③针对以上方案要求，有方案阐述但与用户实际需求有偏差的，计8分； ④针对以上方案要求，有1项欠缺的或只用简单话语概括的，计6分； ⑤针对以上方案要求，有2项欠缺的，计4分； ⑥针对以上方案要求，有3项欠缺的计2分； ⑦未提供本项内容的均不计分。</p>	10.0000	主观	2.项目部署方案
应用对接方案	<p>供应商结合项目实际情况提供具体可行的应用对接方案，内容包括：数据加密、改造说明、应用服务选择及资源申请等。</p> <p>①方案内容详细完整，专业化程度高且完全满足采购需求的，计10分； ②针对以上方案要求，有方案阐述不详实、用户实际需求匹配度不高、内容不完整等情况之一的，计9分； ③针对以上方案要求，有方案阐述但与用户实际需求有偏差的，计8分； ④针对以上方案要求，有1项欠缺的或只用简单话语概括的，计6分； ⑤针对以上方案要求，有2项欠缺的，计4分； ⑥针对以上方案要求，有3项欠缺的计2分； ⑦未提供本项内容的均不计分。</p>	10.0000	主观	3.应用对接方案

详细评审	项目建设保障方案	<p>供应商根据项目情况制定科学适用的项目建设保障方案，包括但不限于项目组织能力、质量管控措施、进度保障措施、人员配备等。①项目建设保障方案内容详细具体且能确保项目快速响应使用方需求的，计10分；②针对以上方案要求，有方案阐述不详实、用户实际需求匹配度不高、内容不完整等情况之一的，计9分；③针对以上方案要求，有方案阐述但与用户实际需求有偏差的，计8分；④针对以上方案要求，有1项欠缺的或只用简单话语概括的，计6分；⑤针对以上方案要求，有2项欠缺的计4分；⑥针对以上方案要求，有3项欠缺的计2分；⑦未提供本项内容的均不计分。</p>	10.0000	主观	4.项目建设保障方案
	售后服务方案	<p>供应商需提供切合本项目的售后服务方案，包括但不限于售后技术支持、故障处理的流程、响应时间、管理体制、服务措施、技术支撑人员等。①售后服务方案详细完善，响应迅速，措施具体可行的，计8分；②针对以上方案要求，有方案阐述不详实、措施不完整等情况之一的，计7分；③针对以上方案要求，响应时间较慢，有方案阐述但与用户实际需求有偏差的，计6分；④针对以上方案要求，有1项欠缺的或只用简单话语概括的，计5分；⑤针对以上方案要求，有2项欠缺的计4分；⑥针对以上方案要求，有3项欠缺的计2分；⑦未提供本项内容或有4项以上欠缺的均不计分。</p>	8.0000	主观	5.售后服务方案

	风险管理	<p>供应商提供针对本项目制定相应的风险管理方案。①能够根据需求分析预判在服务过程中可能出现的安全风险，风险点考虑全面，相应的应急处置方案详细，针对性强，可实施性高，预期能够保证有效的应急处置效果的，计6分；②针对以上方案要求，有方案阐述不详实、用户实际需求匹配度不高、措施不完整、体系不完善等情况之一的，计4分；③针对以上方案要求,有1项欠缺的计2分；④未提供本项内容的均不计分。</p>	6.0000	主观	6.风险管理
	保密措施	<p>供应商针对项目安全保密职责提供具体的保密措施。①保密措施内容详细完整，能够提供廉洁承诺，且保密措施利于项目实施的，计6分；②针对以上方案要求，有方案阐述不详实、用户实际需求匹配度不高、措施不完整、体系不完善等情况之一的，计4分；③有廉洁承诺无具体的保密措施的，计2分；④未提供本项内容的均不计分。</p>	6.0000	主观	7.保密措施
	合理化建议	<p>供应商提供针对本项目的合理化建议。①合理化建议合理科学、可实施性强的，计5分；②针对以上要求，内容阐述简单的，计3分；③针对以上要求，内容与项目需求有偏差的计1分；④未提供本项内容的均不计分。</p>	5.0000	主观	8.合理化建议
	培训服务方案	<p>供应商具有完善的培训服务方案，包括培训计划,培训内容、培训流程等内容。①方案内容全面详细、切实可行的，计6分；②针对以上要求，内容阐述简单的，计4分；③针对以上要求，内容欠缺或仅有框架的，计2分；④未提供本项内容的均不计分。</p>	6.0000	主观	9.培训服务方案

价格分	价格分	磋商报价采用低价优先法计算，即满足磋商文件要求且最后磋商报价最低的报价为评审基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：磋商报价得分=（评标基准价/磋商报价（最终报价）） $\times 10$ 。（注：计算分数时四舍五入取小数点后两位）	10.0000	客观	报价表 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	10.0000 %	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 $\times (1-C1)$ ；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 标的清单 报价表 监狱企业的证明文件

6.5 终止采购活动

出现下列情形之一的，采购人或者代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动：

- （一）因情况变化，不再符合规定的竞争性磋商采购方式适用情形的；
- （二）出现影响采购公正的违法、违规行为的；
- （三）除《政府采购竞争性磋商采购方式管理暂行办法》第二十一条第三款规定的情形外，在采购过程中符合要求的供应

商或者报价未超过采购预算的供应商不足3家的（财政部另有规定的除外）；

（四）法律法规规定的其他情形。

6.6确定成交供应商

一、评审结束后，代理机构在评审结束之日起2个工作日内将磋商报告及有关资料送交采购人。

二、采购人在收到磋商报告后5个工作日内，在磋商报告确定的成交候选供应商名单中按顺序确定成交供应商。成交候选供应商并列的，由采购人采取随机抽取的方式确定成交供应商。

三、采购人逾期未确定成交供应商且不提出异议的，视为确定磋商报告提出的排序第一的供应商为成交供应商。

四、根据采购人确定的成交供应商，代理机构在陕西省政府采购网上发布成交结果公告，同时向成交供应商发出成交通知书。

6.7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。

6.8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，不得修改或细化磋商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，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。

第七章 响应文件格式

采购包1:

分册名称: 投标响应文件分册

详见附件: 响应文件封面

详见附件: 响应函

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: 报价表

详见附件: 标的清单

详见附件: 3.服务条款响应偏离表(格式)

详见附件: 4.商务条款响应偏离表(格式)

详见附件: 5.法定代表人授权委托书(格式)

详见附件: 6.资格证明文件

详见附件: 1.项目理解

详见附件: 2.项目部署方案

详见附件: 3.应用对接方案

详见附件: 4.项目建设保障方案

详见附件: 5.售后服务方案

详见附件: 6.风险管理

详见附件: 7.保密措施

详见附件: 8.合理化建议

详见附件: 9.培训服务方案

详见附件: 10.业绩

详见附件: 16.供应商认为有必要说明的事宜(若有)

详见附件: 17.《拒绝政府采购领域商业贿赂承诺书》(格式)

详见附件: 18.《供应商参与政府采购活动的承诺函》(格式)

第八章 拟签订采购合同文本

详见附件：合同.docx

