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：项目建设

参数性质	序号	技术参数与性能指标
		# 第一部分 技术要求 ## 一、项目背景 2017年以来，国务院办公厅先后印发《政府网站发展指引》(国办发〔2017〕47号)、《政府网站集约化试点工作方案》(国办函〔2018〕71号)、《2022年政务公开工作要点》（国办发〔2022〕8号）等文件，要求各省（区、市）省要全面推进政府网站集约化建设工作，建设本地区政府网站集约化平台，打通信息壁垒、推进集约共享，提升政府网站管理和服务水平，努力建设整体联动、高效惠民的网上政府。 2021年8月24日，国务院办公厅公开办《关于推进政府网站、政务新媒体适老化与无障碍改造工作的通知》（国办公开办函〔2021〕28号），要求分步有序推进改造。各省级人民政府和国务院部门的政府门户网站原则上2021年底前完成改造，其他政府网站和政务新媒体2023年底前基本完成改造。 2022年6月，国务院印发《国务院关于加强数字政府建设的指导意见》（国发〔2022〕14号）明确要求，推进政务公开平台智能集约化发展，提升政务公开水平。一是优化政策信息数字化发布，二是发挥政务新媒体优势做好政策传播，三是紧贴群众需求畅通互动渠道。 二、项目目标 （1）完成网站集约整合。以100%省级部门网站集约化为目标，对剩余的36个省级部门网站进行迁移整合，与市级政府网站实现数据对接打通，实现省市政府网站集约化数据融通共享。 （2）提升网站信息无障碍水平。完成46个省级部门网站适老化与无障碍改造，围绕残疾人、老年人等特殊群体获取网站信息的需求，提升信息无障碍水平，便于广大人民群众更好享受信息化发展成果，进一步消除特殊群体面临的“数字鸿沟”。 （3）强化网站服务能力。深度融合政府网站数据，为公众提供统一的政务信息搜索、智能客服和问答服务门户入口；深入数据要素开发利用，更加注重大数据分析建设，推动全省政府网站的发展模式朝向服务个性化、决策智能化、推送主动化和响应敏捷化等方向转型；积极构建更加丰富的新媒体传播矩阵，用数字化手段构建多维立体的政民互动传播格局。 （4）提升安全防护保障。建设安全服务支撑系统，加强安全保障和自主可控技术能力：提供包括安全认证服务、信创适配等在内的统一安全防护措施；采用全栈自主可控的国产化基础软硬件技术，有效解决政府网站集约化条件下面临的身份真实性认证、操作行为防抵赖、维护过程可追溯、数据传输可加密等安全应用问题，确保省政府网站集约化平台运行安全稳定。设计应符合《陕西省电子政务网络安全管理办法》（陕办发[2016]53号）中关于电子政务系统和党政机关网站的身份认证相关要求，并全面支持IPv6协议。 三、项目建设内容

陕西省政府网站集约化省级平台（三期）项目建设内容包括：

1.集约化省级平台信创适配改造。基于信创云提供的国产芯片、国产操作系统、国产数据库、国产中间件等基础环境，完成集约化省级平台一、二期项目已建子系统的信创适配改造。

2.集约化省级平台升级及扩建。基于集约化省级平台一、二期项目的建设成果，完成智能搜索系统升级、统一问答知识库建设、政务新媒体矩阵建设、网页预归档系统建设。

3.省级部门网站改造。基于信创适配改造和升级扩建后的集约化省级平台，完成未集约整合的36个省级部门网站开发及无障碍改造（PC端网站开发、移动端网站适配、长者版适配、无障碍改造），完成一期10个试点省级部门网站适老化与无障碍改造（长者版开发、无障碍改造）。

4.网站数据迁移。完成36个省级部门网站数据迁移，将网站各类数据从原有网站系统迁移到信创适配改造和升级扩建后的集约化省级平台；将一期项目建设的11个网站（省政府门户网站和10个试点省级部门网站）从现有环境的集约化省级平台迁移到信创适配改造和升级扩建后的集约化省级平台。

5.为网页预归档系统的文件转换提供支撑，采购OFD版式支撑软件。

6.建设安全服务支撑系统。建设以国密算法为基础的政府网站集约化应用安全服务支撑系统，采用内控外防技术措施，实现网站管理人员、信息发布人员、运维人员和审核人员的身份真实性验证，为集约化省级平台提供电子存证与可追溯能力，利用SSL加密协议实现数据加密传输，提升集约化省级平台和全省47个（省政府门户网站及46个省级部门网站）省级部门网站的统一管控能力。

四、项目技术要求

4.1总体要求

4.1.1总体框架设计

采用面向服务的技术架构（SOA），结合微服务松耦合设计模式，各应用模块单独开发和维护，构建易于扩展和可伸缩的弹性系统。

4.1.2执行国家相关标准规范

平台设计严格执行国家相关标准规范，并遵从国际标准和规范。

4.1.3支持IPV6协议

按照《推进互联网协议第六版（IPv6）规模部署行动计划》要求，本次信创适配后的集约化省级平台及其承载的政府网站群均须支持IPv6协议。

4.1.4安全可靠环境部署

▲平台支持在安全可靠环境下部署，适配主流国产化数据库、操作系统及中间件。

4.1.5性能要求

▲1.在2000并发下，网站群性能指标需求如下：

（1）页面功能切换≤2秒；

（2）信息浏览≤2秒；

（3）一般查询端≤2秒；

（4）表单提交≤3秒；

（5）复杂报表端≤5秒；

（6）页面刷新时间≤2秒；

（7）满足系统自身运行性能需求，以及保证系统稳定运行保留的处理能力冗余。

2.在200并发下，集约化省级平台能指标需求如下：

（1）系统支持良好的大规模并发发布效率，200个并发下，系统操作及服务响应时间不超过3秒；

（2）200名编辑同时发布单篇文档的平均时间为3秒以内；

（3）满足系统运行性能需求，以及保证系统稳定运行保留的处理能力冗余；

（4）满足未来更多数据源单位的系统对接和数据共享。

4.2技术参数（功能）要求

4.2.1集约化省级平台信创适配改造

▲基于信创云提供的国产芯片、国产操作系统、国产数据库、国产中间件等基础环境，完成集约化省级平台一、二期项目已建子系统的信创适配改造，需要适配的业务系统如下：

序号	业务系统	业务子系统
1	省级网站集约化平台	集约化管理系统
2		内容管理系统
3		信息公开系统
4		互动交流系统
5		绩效考核系统
6		运维运营系统
7		无障碍系统
8		大数据分析系统
9		服务融合系统
10		通用工具系统
11		政策文件省级服务平台
12	统一信息资源库	统一信息资源库
13	平台自建应用支撑组件	基础组件
14		服务管理
15		流程管理
16		表单管理
17		通信队列组件

4.2.2集约化省级平台升级及扩建

本次项集约化省级平台的升级及扩建包括：智能搜索系统升级、统一问答知识库建设、政务新媒体矩阵建设、网页预归档系统建设。

1.▲智能搜索系统升级

依托一期建设的智能搜索系统功能进行底层架构升级和功能新建完善，全面提升跨地区、跨部门、跨站点的全省政府网站数据统一搜索服务能力。包括底层架构的重构改造和对前端应用功能的完善优化，实现全省政府网站数据的一站式检索服务。

（1）搜索架构升级

重构集约化省级平台智能搜索系统搜架构，具体包括:消息中间件配置,数据抽取配置,数据索引结构配置,数据同步配置,数据分词组件配置,租户管理,租户前端模版管理,物名/地名词条管理,拼音词条管理,纠错词词条管理,百姓体词条管理,同义词词条管理,敏感词词条管理,词条权重管理,实体库管理,内容维护管理,可视化统计分析。

（2）搜索功能升级

全省统一搜索、图片视频搜索、搜索框应用管理、搜索暗文、搜索排行管理、机构引导管理。

（3）搜索场景建设

主题搜索场景管理、领导人搜索场景管理、机构搜索场景管理、场景置顶管理。

2.▲统一问答知识库建设

依托政府网站集约化省级平台自有数据、政务服务网和12345平台等横向业务系统产生的数据资源，有效汇聚、整合并全面梳理我省政府网站的各类问答数据，形成问答知识沉淀与场景化服务能力，实现全省问答数据的融通，并在省政府门户网站集中展示，为公众提供浏览、查询等服务。

（1）问答知识库管理：问答数据采集、问答数据排重、问答数据标引。

（2）问答知识库服务：问答数据管理服务、在线审核管理服务、分类管理服务、问答反馈收集、问答知识检索。

（3）问答知识统计分析：间统计、分类统计、标签统计、热门问答分析。

3.▲政务新媒体矩阵建设

借鉴先进省份经验做法，依托先进的互联网采集手段，将省级各部门政务微信、政务微博等新媒体账号和发布内容统一汇聚，在省政府门户网站政务新媒体频道进行集中展示。实现数据同源、整体联动、同频共振，为政府网站集约化省级平台部门用户提供网站和政务新媒体内容融合发布服务。

（1）新媒体资源采集：按照省政务公开办公室提供名单，采集省级部门微信、微博等政务新媒体运营账号及文章数据，并导入统一信息资源库，同时，进行通过自动排重、自动摘要、自动过滤等功能模块完成对数据清洗。

（2）新媒体内容管理：文章管理、新媒体标签管理、文章内容标引标记。

（3）新媒体传播服务：支持按照不同类型的呈现设置，多样化的展示政务微信、微博数据。

4.▲网页预归档系统建设。

按照《陕西省机关网站网页归档管理暂行办法》（陕档局发[2023]31号）文件要求，建设省政府门户网站网页预归档系统，将省政府门户网站有价值的网页文件如网站首页、二级栏目首页、政策文件等信息进行电子档案归档，按要求将网页文件转换成ofd格式文件，并将网页信息生成、发布及归档过程中的元数据生成XML文件，并上传至省档案馆电子文件中心系统，提高电子文件的治理效能。

（1）预归档系统管理：支持预归档栏目管理、预归档策略配置、元数据管理、分类管理、立档单位信息管理除。

（2）归档内容管理：支持归档网页列表、归档状态、网页文件加工转换、预归档目录文件管理、质量效验、撤销归档、归档记录管理、数据导出、预归档查询检索、预归档信息预览。

（3）角色权限管理：支持角色权限配置、权限分级管理。

（4）省档案馆电子文件中心系统对接：预归档模块与省档案馆电子文件中心系统对接，实现预归档网站网页信息对接同步、和数据上传。

4.2.3省级部门网站改造设计

基于信创适配改造和升级扩建后的集约化省级平台，完成未集约整合的36个省级部门网站开发及无障碍改造（PC端网站开发、移动端网站适配、长者版适配、无障碍改造），完成一期10个试点省级部门网站适老化与无障碍改造（长者版开发、无障碍改造）。

▲未集约整合的36个省级网站开发及无障碍改造，包括PC端网站开发、移动端网站适配、长者版适配、无障碍改造四大项内容。本次PC端网站开发将同步考虑移动端网站和长者版的展示需求，移动端网站和长者版不需要单独开发功能，仅需于PC端网站进行适配。不同的省级部门网站需要结合各个省级部门的实际业务需求和数据现状分别进行单独改造。

▲一期10个试点省级部门网站适老化与无障碍改造，包括长者版开发、无障碍改造。

本次政府网站改版建设工作清单如下表所示：

序号	省级部门名称	PC端网站开发	移动端网站开发	长者版开发	无障碍改造
1	陕西省公安厅			√	√
2	陕西省民族宗教事务委员会			√	√
3	陕西省水利厅			√	√
4	陕西省卫生健康委员会			√	√
5	陕西省审计厅			√	√
6	陕西省林业局			√	√
7	陕西省统计局			√	√
8	陕西省文物局			√	√
9	陕西省政府研究室			√	√
10	陕西省中医药管理局			√	√
11	陕西省发展和改革委员会	√	√	√	√
12	陕西省教育厅	√	√	√	√
13	陕西省科学技术厅	√	√	√	√
14	陕西省工业和信息化厅	√	√	√	√
15	陕西省民政厅	√	√	√	√
16	陕西省司法厅	√	√	√	√
17	陕西省财政厅	√	√	√	√
18	陕西省人力资源和社会保障厅	√	√	√	√
19	陕西省自然资源厅	√	√	√	√
20	陕西省生态环境厅	√	√	√	√
21	陕西省住房和城乡建设厅	√	√	√	√
22	陕西省交通运输厅	√	√	√	√
23	陕西省农业农村厅	√	√	√	√
24	陕西省商务厅	√	√	√	√
25	陕西省文化和旅游厅	√	√	√	√
26	陕西省市场监督管理局	√	√	√	√
27	陕西省应急管理厅	√	√	√	√
28	陕西省国资委	√	√	√	√
29	陕西省退役军人事务厅	√	√	√	√
30	陕西省广播电视局	√	√	√	√
31	陕西省体育局	√	√	√	√
32	陕西省人民防空办公室	√	√	√	√
33	陕西省信访局	√	√	√	√
34	陕西省医疗保障局	√	√	√	√
35	陕西省乡村振兴局	√	√	√	√
36	陕西省地方金融监督管理局	√	√	√	√

37	陕西省地方志办公室	√	√	√	√
38	陕西省粮食和物资储备局	√	√	√	√
39	陕西省能源局	√	√	√	√
40	陕西省监狱管理局	√	√	√	√
41	陕西省药品监督管理局	√	√	√	√
42	陕西省知识产权局	√	√	√	√
43	陕西省供销合作总社	√	√	√	√
44	陕西省黄帝陵文化园区管理委员会	√	√	√	√
45	陕西省秦岭生态环境保护委员会办公室	√	√	√	√
46	陕西省机关事务中心	√	√	√	√

4.2.4 网站数据迁移

集约化省级平台完成信创适配改造和升级扩建后，需要将本次项目相关的47个网站的历史数据从原有系统迁移至集约化省级平台。本期项目所涉及的业务范围包括：

（1）▲本期集约的36个省级部门网站数据迁移。本期集约整合的36个省级部门网站数据迁移到信创适配改造和升级扩建后的集约化省级平台，并保证信息的有效、完整、准确性。迁移的数据类型包括但不限于：新闻类数据，信息公开类数据，领导信箱、在线访谈、意见征集、依申请公开等互动类型数据，图片、视频、附件等非结构化数据。36个省级部门网站清单如下：

序号	单位名称	网址
1	陕西省发展和改革委员会	http://sndrc.shaanxi.gov.cn/
2	陕西省教育厅	http://jyt.shaanxi.gov.cn/
3	陕西省科学技术厅	https://kjt.shaanxi.gov.cn/
4	陕西省工业和信息化厅	http://gxt.shaanxi.gov.cn/
5	陕西省民政厅	http://mzt.shaanxi.gov.cn/
6	陕西省司法厅	http://sft.shaanxi.gov.cn/
7	陕西省财政厅	http://czt.shaanxi.gov.cn/
8	陕西省人力资源和社会保障厅	http://rst.shaanxi.gov.cn/
9	陕西省自然资源厅	http://zrzyt.shaanxi.gov.cn/
10	陕西省生态环境厅	http://sthjt.shaanxi.gov.cn/
11	陕西省住房和城乡建设厅	https://js.shaanxi.gov.cn/
12	陕西省交通运输厅	https://jtyst.shaanxi.gov.cn/
13	陕西省农业农村厅	http://nynct.shaanxi.gov.cn/
14	陕西省商务厅	http://sxdofcom.shaanxi.gov.cn/
15	陕西省文化和旅游厅	http://whhlyt.shaanxi.gov.cn/
16	陕西省市场监督管理局	http://snamr.shaanxi.gov.cn/
17	陕西省应急管理厅	http://yjt.shaanxi.gov.cn/
18	陕西省国资委	http://sxgz.shaanxi.gov.cn/
19	陕西省退役军人事务厅	http://dva.shaanxi.gov.cn/

20	陕西省广播电视局	http://gdj.shaanxi.gov.cn/
21	陕西省体育局	http://tyj.shaanxi.gov.cn/
22	陕西省人民防空办公室	http://rfb.shaanxi.gov.cn/
23	陕西省信访局	http://xfj.shaanxi.gov.cn/
24	陕西省医疗保障局	http://ybj.shaanxi.gov.cn/
25	陕西省乡村振兴局	http://xczxj.shaanxi.gov.cn/
26	陕西省地方金融监督管理局	http://fsa.shaanxi.gov.cn/
27	陕西省地方志办公室	http://dfz.shaanxi.gov.cn/
28	陕西省粮食和物资储备局	http://lswz.shaanxi.gov.cn/
29	陕西省能源局	http://sxsnyj.shaanxi.gov.cn/
30	陕西省监狱管理局	http://jyglj.shaanxi.gov.cn/
31	陕西省药品监督管理局	http://mpa.shaanxi.gov.cn/
32	陕西省知识产权局	http://snipa.shaanxi.gov.cn/
33	陕西省供销合作总社	http://sxgxs.shaanxi.gov.cn/
34	陕西省黄帝陵文化园区管理委员会	https://huangdi.shaanxi.gov.cn
35	陕西省秦岭生态环境保护委员会办公室	http://qinling.shaanxi.gov.cn/
36	陕西省机关事务中心	http://jgswglj.shaanxi.gov.cn/
37	小计	

（2）▲一期项目建设的11个网站数据迁移。将一期建设的11个网站（省政府门户网站和10个试点省级部门网站）从现有环境的集约化省级平台迁移到信创适配改造和升级扩建后的集约化省级平台，并保证信息的有效、完整、准确性。迁移的数据类型包括但不限于：新闻类数据，信息公开类数据，领导信箱、在线访谈、意见征集、依申请公开等互动类型数据，图片、视频、附件等非结构化数据；网站前端静态页面、网页模板等网站框架性数据。11个网站清单如下：

序号	单位名称	网址
1	陕西省人民政府办公厅	http://www.shaanxi.gov.cn/
2	陕西省公安厅	http://gat.shaanxi.gov.cn/
3	陕西省民族宗教事务委员会	https://mzzj.shaanxi.gov.cn/
4	陕西省水利厅	http://slt.shaanxi.gov.cn/
5	陕西省卫生健康委员会	http://sxwjw.shaanxi.gov.cn/
6	陕西省审计厅	http://sjt.shaanxi.gov.cn/
7	陕西省林业局	http://lyj.shaanxi.gov.cn/
8	陕西省统计局	http://tjj.shaanxi.gov.cn/
9	陕西省文物局	http://wwj.shaanxi.gov.cn/
10	陕西省政府研究室	http://zys.shaanxi.gov.cn/
11	陕西省中医药管理局	http://atcm.shaanxi.gov.cn/

4.2.5 OFD版式转换系统

版式转换系统支持将多种格式的电子文档及网页的批量或实时在线转换成符合标准的OFD格式的电子文件，提供元数据处理、页面处理、权限处理、二维码处理、文件拆分合并、批量签章等二次加工功

	1	能。可有效满足网站内容转换为符合归档要求OFD版式文件生成与加工。 功能要求： ▲标准符合性：通过OFD标准符合性测试，提供信息处理产品标准符合性检测中心出具的检测报告。 基本功能：应支持将TXT、RTF、WPS、DPS、UOS、UOP、PDF、DOC/DOCX、XLS/XLSX、PPT/PPTX、HTML、XLSM、DWG、CEB/CEBX、JPG、TIF等多种格式文档转换为OFD格式；支持将OFD格式转换为OFD-A格式。 ▲转换配置：网页转OFD时，支持自定义参数配置，添加页码、页眉页脚等内容。支持长网页分页，支持多个网页合并生成OFD文件，网页内链接属性可保持活性。提供国家级第三方检测机构出具的测试报告。 文件加工：支持对OFD文件进行元数据处理、附件处理、水印处理、页面处理、页码处理，提供文档组合拆分、电子签章、数字签名等技术机制。 ▲字体嵌入：在文件转换过程中嵌入文档所用字体，各环境下永久保持原版原式呈现。提供国家级第三方检测机构出具的测试报告。 内容处理：可在文档指定区域添加掩膜，实现敏感内容遮盖。 ▲系统可靠性：支持集群式部署，保障系统高可靠性，支持7*24小时运行零报错，且保证转换生成的OFD文件不跑版。需提供国家级第三方检测机构出具的测试报告。 服务接口：系统以服务的方式部署在服务端，支持以JAVA API、HTTP等多种技术形态的功能调用。 性能指标：单服务器部署时流式文档转换速度应大于50页/秒。 4.2.6安全服务支撑系统 安全服务统一调度管理系统 安全服务统一调度管理系统按照集约化省级平台的实际安全保护需求，以集约化省级平台应用的安全性、易用性为原则，满足集约化平台的安全服务统一调度管理的要求。安全服务统一调度管理系统作为安全服务支撑系统的统一入口，提供身份认证、签名验签和电子存证等服务。安全服务统一调度管理系统主要由服务接入管理、认证服务调度管理、签名服务调度管理、日志数据集中管理、对外服务接口等组成。 功能要求： 提供服务资源接入管理：提供各类服务资源的注册接入、配置、管理功能； 提供认证服务调度管理：对业务应用系统的证书认证服务请求进行集中接收和调度分发； 提供签名服务调度管理：对业务应用系统的签名、验签服务请求进行集中接收和调度分发； 提供日志数据集中管理：对认证访问日志、电子签名日志、签名验证日志、电子存证日志、服务的配置管理日志、服务的调度分发日志等数据进行采集和管理，并可对日志数据进行条件查询，可按分类进行统计； 提供对外服务接口：对外提供标准服务接口，支持二次开发。服务接口主要包括身份认证接口、签名验签接口、日志数据接口。 资质要求：

▲提供中华人民共和国国家版权局签发的《计算机软件著作权登记证书》；
提供国家密码管理局商用密码检测中心颁发的类似产品《商用密码产品认证证书》；
提供不少于2个类似安全产品厂商的《产品兼容适配证明》。

证书应用服务系统

证书应用服务系统软件为集约化省级平台提供安全认证方式，保证网站管理人员、运维人员访问登录的身份真实性，防止用户身份假冒、伪造等现象，实现用户证书身份认证、认证过程审计和证书CRL列表、白名单查询功能，主要应用于证书登录方面。
功能要求：

提供数字证书身份认证功能；
提供认证过程审计功能；
内置CRL列表、白名单；
灵活支持单向或双向身份认证；
支持RSA、SM2算法；
针对应用系统资源进行细粒度的权限控制；
提供高强度的传输链路加密；
提供基于认证过程全方位监控、追踪和审计功能。

资质要求：

▲提供《软件产品证书》；
提供中华人民共和国国家版权局签发的《计算机软件著作权登记证书》。

日志签名验签服务软件

日志签名验签服务软件主要提供对日志数据进行电子签名以及签名的真实性和有效性验证功能，可应用于验证用户身份、检验交易凭证和防止抵赖等方面。
功能要求：

提供pkcs1/Pkcs7 attach/Pkcs7 detach/xml Sign等格式的数字签名验证功能；
保证关键密钥在任何时候不以明文形式出现在设备外，密钥备份文件也受到主密钥的保护；
支持多种操作系统，应用服务器与签名验证服务器之间采用TCP/IP协议进行通信；
支持连接密码及白名单，通过连接密码和白名单的支持，实现签名验证服务器对应用服务器的授权认证，进一步提高系统的安全性；
可根据应用需求灵活配置CA、CRL、OCSP级别验证证书，并可以配置外部地址或者从证书获取地址等方式验证证书。

资质要求：

▲提供国家密码管理局商用密码检测中心颁发的产品《商用密码产品认证证书》；
▲提供中华人民共和国公安部签发的产品《计算机信息系统安全专用产品销售许可证》；
提供中华人民共和国国家版权局签发的《计算机软件著作权登记证书》；
▲为保证系统安全，需要提供国家网络与信息系统安全产品质量检验检测中心颁发的《信息技术产品安全测试证书》；

▲具有中国质量认证中心颁发的《中国国家强制性产品认证证书》。

PKI安全中间件

PKI安全中间件向上为集约化平台提供开发接口，向下提供统一的密码算法接口和各种设备驱动接口，并完全支持国密算法体系，为集约化平台提供网站及后台管理所需的公钥基础设施各项安全服务。
功能要求：

▲基于各种厂商智能密码钥匙产品，提供统一、易用的应用开发接口，用于实现数字证书安全登录、数字签名、数据加密等安全功能；提供产品彩页证明。
支持符合CSP、PKCS11、国密接口的智能密码钥匙，智能密码钥匙只要符合其中一种接口规范，就可以接入PKI中间件；
▲支持SM2、RSA非对称算法；支持SM3、MD5、SHA1等摘要算法；支持SM4、DES、AES、SM1等对称算法，包括算法的软件实现和基于智能密码钥匙的硬件算法实现；提供产品彩页证明。
支持PKCS1签名格式和PKCS7签名消息格式的数字签名和验签；支持PKCS7加密消息格式的数据加解密；支持证书编码和解码、证书解析；
提供智能密码钥匙的列举、登录、登出、修改口令、初始化等设备管理功能；
提供设备中文件的创建、删除、读写等管理功能；
支持国产主流浏览器，支持IE、Firefox、Google Chrome等浏览器；
支持Windows和国产化的操作系统。

资质要求：

▲提供《软件产品证书》；

网站管理员USBKEY数字证书

采用合法的权威CA机构生产的USBKEY数字证书，用于标识网站管理人员（包括集约化省级平台维护人员、信息发布人员、审批人员和管理人员）在网络环境中的真实身份。
功能要求：

采用标准X.509 V3格式的数字证书；
支持国密算法：SM1,SM2,SM3,SM4,SSF33；支持SM2非对称算法加密、解密、签名、认证、密钥交换、数字信封等多种应用；
支持签名和加密双证书，支持国密SM2证书。

硬件要求：

USB Key为标准USB 1.1设备，支持USB2.0、USB3.0接口；
USB Key支持PC/SC驱动，支持智能卡登录，USB Key带LED状态指示灯，能够进行通讯状态指示和电源指示；
USB Key容量128K字节；
USB Key自身的安全要求：具备完善的PIN校验保护功能；
数据存储时间不小于10年，可擦写50万次以上；平均故障间隔时间（MTBF）≥4000小时；

操作系统支持Windows、Linux、MAC OS等；

浏览器支持IE、Firefox、Google Chrome等浏览器；

中间件支持MS CAPI、PKCS11、GM/T 0016-2012智能密码钥匙密码应用接口规范。

电子存证服务模块

电子存证服务模块提供对网站访问日志、操作日志进行存证和安全加固，确保网站维护日志的原始性、完整性和可追溯性，并形成完整证据链，满足网站后台日常管理操作行为可追溯、防抵赖的业务需求。

功能要求：

符合国家标准《电子数据存证技术规范 SF/T 0076-2020》，对接具有资质的国家电子数据鉴定机构，主要提供电子签名存证、文件上传存证、哈希值存证、网页存证、存证函服务及出证服务等功能；

存证管理：支持分页展示存证情况的记录信息；支持查询存证记录；支持导出与导入存证记录；

出证管理：支持分页展示出证申请的记录信息，包含审批结果；支持查询出证申请记录；支持审批出证申请；支持导出与导入出证记录；

统计报表：支持多种角度视图形式进行查询统计，包含用户接入情况统计、存证情况统计、出证情况统计等；

日志审计管理：支持分页展示系统管理员、系统用户操作日志的记录信息；支持分页展示系统接口调用日志的记录信息；支持查询相应操作日志记录；支持导出与导入相应日志记录；

接口服务：电子合同签约存证类接口、文件存证类接口、Hash存证类接口、网页存证类接口、存证函类接口、出证类接口、公证类接口；

系统管理：包含系统用户管理、角色管理、资源管理、参数配置管理、数据字典管理、许可证管理、系统备份与恢复等功能。

资质要求：

▲提供与国产应用服务器软件的《产品互认证明》；

提供中华人民共和国国家版权局签发的《计算机软件著作权登记证书》。

数据管理模块

数据管理模块提供对业务签名数据、登录数据、操作行为数据、运行数据、存证数据存储管理、数据保护管理、数据访问控制等功能。

功能要求：

存证数据存储管理：系统中的存证数据可进行分类存储管理，根据不同需求配置存证数据存储策略；

访问管理控制：系统可对访问权限进行配置和管理，实现在权限范围内对指定数据对象的访问；

数据保护：数据保护功能是通过将业务签名数据、登录数据、操作行为数据、运行数据等实时存证与保护，实现对各类待管理数据的原始记录，为数据管理提供可靠保障，使存证数据不可篡改、可留痕和易于追溯。

SSL安全认证网关

SSL安全认证网关为集约化省级平台网络应用提供基于数字证书的高强度身份认证服务、高强度数据链路加密服务及数字签名验证服务，确保数据在传送中不被改变，保证数据的完整性，实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证双方传递信息的安全性。

功能要求：

支持国家密码管理局批准的SM系列算法体系；支持国密算法的应用：支持ECC_SM2单、双向连接、支持ECDHE_SM2双向SSL协议，支持SM2、SM3、SM4等国密算法，安全访问、自主可控；

支持使用终端安全设备的身份认证方式，支持第三方认证方式的接口和扩展，具有良好的安全性和可扩展性；提供证书读取、证书解析、证书验证、数据加密、证书检查等功能；

支持终端注册，只有注册过并通过认证的可信终端才允许和安全网关之间建立安全链路，建立安全链路之后，可以通过安全策略自动中断终端和非可信网络之间的一切链路；

保证所有数据在网络传输过程中都是被加密的，防止通信数据被第三方监听；

支持分布式日志管理，支持标准SYSLOG协议。

硬件要求：

CPU：≥16核心32线程；

RAM：≥64G；

硬盘：固态硬盘≥500G；

网络接口：10G光口：≥2个，1G电口：≥3个。

性能要求：

L4 新建≥300000 CPS；

L4 并发≥600 万；

L4 吞吐≥18000Mbps；

SSL（RSA2048）新建≥55000 CPS；

SSL（RSA2048）并发≥360 万；

SSL（RSA2048）≥16000 Mbps；

SSL（SM2）新建≥12000 CPS；

SSL（SM2）并发≥300 万；

SSL（SM2）吞吐≥12000 Mbps。

资质要求：

▲提供国家密码管理局商用密码检测中心颁发的产品《商用密码产品认证证书》。

双算法自适应SSL证书

双算法自适应SSL证书用于标识集约化省级平台真实身份，并为访问者提供简单快速的识别方式，同时为网站的客户端与服务器端提供数据加密传输功能。双算法自适应SSL证书主要是解决政府网站在互联网中的身份标识问题，以及网站服务端与客户端之间进行数据交互的隐私保护问题。

功能要求：

算法满足：必须支持国密SM2签名算法、兼容RSA算法；国密算法证书必须使用国密SM2或更高的签名算法，满足ECC-SM4-SM3加密套件；国际算法证书必须使用SHA256或更高的哈希算法签名，并使用2048位以上RSA密钥或256位以上ECC算法；

浏览器要求：支持国密算法的浏览器，兼容主流浏览器；采用最高安全认证EV级别，浏览器显示单位名称；

证书验证：内置OCSP在线实时查询，支持CRL列表查询；提供基于客户端本地信任证书链的自动校验功能。

服务器端国密SSL支持模块，支持采用自适应双算法，优先采用国密算法加密，服务器软件自动识别浏览器，对国密浏览器返回国密SSL证书，对国际主流浏览器返回RSA SSL证书，自适应兼容主流浏览器。

资质要求：

▲提供不少于两个国产浏览器入根证明；

▲提供不少于两个商用密码根证书受信证明；

4.3其他要求

4.3.1互融互通要求

1.与省级政务数据共享交换平台、陕西省政务服务网、省级12345平台以及省数字档案室等外部系统进行对接，实现省级平台数据横向互联互通。

2.依托于省市两级政务数据共享交换平台，实现全省各地市政府网站集约化平台数据向集约化省级平台汇聚，实现省市政府网站数据纵向互联互通。

3.本次建设的平台需遵循接口开放原则，并预留有关已知的或可预知的接口，支持与在建以及未来规划建设的各类平台之间的无缝对接、互联互通。

五、项目实施及售后服务要求

（一）项目实施要求

供应商须根据本项目招标文件中工期要求列出详细的项目实施计划，合理划分项目实

施阶段，明确每个阶段应完成的工作及每个阶段完成后提交的产品及文档。供应商应为本项目建立一个完善和稳定的项目实施团队，项目团队应具有优秀的服务能力、项目管理能力、技术研发实力和行业实施经验等，供应商实施过程中出现资源、速度、质量协调控制不力、 采购方有权更换责任人。

（二）培训要求

根据项目要求提供平台使用培训。培训原则上采用统一培训的方式，培训地点在采购人指定地点。

1.培训对象包括系统使用人员及系统维护人员。

2.供应商应保证提供最有经验的培训讲师，培训包括技术培训和使用培训。培训教材应使用标准中文；为进行有效的技术交流，所有培训讲师必须具备熟练的中文会话和书写能力。

3.供应商应在响应文件中明确：

培训计划：应注明每次培训课程的时间、地点及课时。

培训大纲：应注明每次课程的内容和目的。

（三）售后服务要求

▲1.供应商需提供1年质保期的免费运维服务，质保期自项目验收合格之日起计算。具体售后服务内容如下：

		2.供应商提供免费软件系统支持维护服务，服务内容为系统设计总体框架不变下的系统调优、设计错误更改、软件 BUG 问题解决、功能微调等维护和修改工作。服务方式包括电话、互联网、E-MAIL、现场和定期巡检等方式。 3.服务期内，供应商应组建不少于5人的本地化服务团队，向用户提供 7×24 小时的故障技术支持服务，30分钟响应； 如在 60 分钟内无法远程解决用户提出的服务要求，必须在报修 2小时内派工程师到达现场。故障问题解决后 12 小时内，向使用单位提交问题处理报告，说明问题种类、问题原因、问题解决中使用的方法及造成的损失等情况。 4.提供重大节日和关键时期的重点保障服务，解决节日期间和关键时期的问题处理和技术支持等问题。 ▲5.提供投标生产厂商针对本项目服务要求承诺函及授权书，电子扫描件并加盖厂商公章。 包括但不限于： ①承诺本品牌产品无虚假宣传，对招标文件中列出的核心、重要指标，能完全符合； ②承诺提供原厂商服务。（应用适配、保障响应等） 第二部分 商务要求 ★一、建设期及地点： 1、本项目的建设工期6个月，试运行3个月，以双方签订合同之日算起。项目通过终验并正式上线后，进入质保期。 2、项目实施地点：陕西省政务大数据服务中心指定地点。 ★二、付款方式： 1、结算单位：采购人结算，在付款前，必须开具全额发票给采购人。 2、付款方式： 在合同签订生效后，甲方向乙方支付合同价款30%，初验合格后支付合同价款50%，终验后甲方向乙方支付合同价款20%. 3、支付方式：银行转账。乙方要如实开具发票，不得变更开票内容，开具发票出现税务争议时，乙方需承担税款、滞纳金、罚款等赔偿责任以及其他相关责任。 ★三、质保期 质保期：1年，自项目终验合格之日起计算。 四、验收要求 项目验收前，中标供应商应提交以下交付物：需求分析、实施方案、测试报告、试运行方案、系统维护手册、用户操作手册、应急方案、等保测评报告、密码应用评估报告、第三方软件测评报告。具体以项目采购人要求为准。 五、争议 以本项目签订合同为准。 六、其他 （一）合同份数 见正式合同。 （二）补充条款 具体内容以正式合同为准。

采购包2：

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：工程监理

参数性质	序号	技术参数与性能指标
		一、采购需求 1.1技术标准 监理服务须执行中华人民共和国相关国家标准规范，技术要求中所应用的标准规范应为现行最新版本。 监理单位应遵循科学、公正、诚信、守法的职业道德，以高度的责任心和丰富的专业技术经验，根据国家的有关法规、技术规范和标准以及业主与承建单位签订的合同，为项目建设提供专业的、规范的监理服务。 1.2监理目标 依照有关标准规范和业主单位的需求，对项目建设全过程开展全面的、专业的监督管理。通过“四控、三管、一协调”等全生命周期项目监督管理，保证项目建设及交付质量符合立项实施方案设计要求、合同要求和国家相关标准规范要求，使项目规范建设、规范验收，满足业主单位建设要求和用户单位使用需求，符合项目审计要求。 具体分解为如下目标： 1.质量控制目标：符合国家有关技术标准和规范，满足立项实施方案与合同要求。 2.进度控制目标：保证项目建设符合总体实施进度要求，各阶段任务在规定时间点前完成，按照合同要求时间点通过项目初步验收、最终验收、档案专项验收和竣工验收。 3.投资控制目标：以批复的立项实施方案、招标预算和合同文件为依据，以批复预算为投资控制目标，保证项目投资金额在相关法律、政策规范要求的范围内，保证项目投资的有效性。 4.变更控制目标：审核变更申请，评估并确定最优变更方案，跟踪、监督变更的执行情况，保证变更的合理性、必要性、合规性和科学性。 5.风险控制目标：确立风险控制指导原则，制定风险分析与防范措施，及时识别、分析风险，采取风险控制措施，保证项目建设交付按计划推进，使项目始终处于受控状态。 6.安全管理目标：通过建立信息安全管理制度，签订保密协议及承诺书，明确责任，结合网络安全等级保护及密码应用安全性评估要求，加强项目建设交付期的监督管理，杜绝系统安全和数据保密事故的发生。 7.合同管理目标：以合同规定的服务内容、工期、质量要求为依据，监督合同履约情况，确保合同执行的完整性和符合性。 8.文档管理目标：通过建立项目档案管理制度，制定文档归档清单和归档办法，加强文档过程审核，确保项目文档资料的及时性、完整性、规范性和准确性，项目文档分门别类，科学调用，妥善保管。 9.组织协调目标：通过建立会议汇报制度、协调联络机制、项目管理流程、审核反馈机制等措施，保证项目各相关方之间的良好沟通和信息对称，促使各方形成合力，共同推进项目建设交付，确保项目按期交付投用，保质、保量、保安全的完成项目任务。 1.3监理服务范围 根据项目立项实施方案、招标文件要求、投标文件承诺和合同书，承担项目全过程监理工作，具体包括合同签订阶段、开工准备阶段、实施阶段、试运行阶段、测评阶段和验收阶段的监理工作。 1.4监理服务内容 项目建设实施过程中的质量控制、进度控制、投资控制、变更控制，安全管理、合同管理、信息管理

	1	，参与项目相关方关系的沟通协调工作，配合业主单位完成项目建设交付和投用使用的目标。 （一）合同签订阶段 合同签订阶段指自中标结果确认开始，至业主单位与承建单位完成项目合同签订为止。此阶段监理主要的工作内容是： （1）结合立项实施方案、招标文件实质性内容，协助业主单位与成交服务商进行合同沟通、谈判； （2）审核合同文本及附件，出具监理报告； （3）协助业主单位与成交服务商完成合同签订。 （二）实施准备阶段 准备阶段指项目合同签订之日起，至项目基准（建设范围、进度计划、实施方案）经三方（或监理方）确认后，总监理工程师签发开工令为止。此阶段监理主要的工作内容是： （1）由监理现场负责人对所建立管理制度进行培训，提出管理要求； （2）与进场人员签订数据保密协议； （3）审核承建单位进场人员资格； （4）审查并实地复核实施方案，出具监理专题报告； （5）审核承建单位提交的项目进度（实施）计划等，出具监理专题报告； （6）监督设计交底的组织； （7）监督承建单位内部的技术交底和安全交底培训； （8）签发开工令。 （三）实施交付阶段 实施阶段指项目开工令签发之日起，至合同约定的服务条件全部具备并通过任务验收为止。此阶段监理主要的工作内容是： 1.质量控制 （1）软件开发计划的审核和确认； （2）对软件开发的需求分析、概要设计、详细设计、编码测试、应用测试等每个开发阶段进行把关； （3）对承建单位的开发质量记录进行审核； （4）对合同内容完成情况进行检查，组织系统功能和性能测试； （5）对系统部署情况、系统对接情况、应用安全情况、密码应用情况进行检查，督促问题整改； （6）审核确认承建单位的培训计划，检查培训教材、使用说明书、维护手册等资料内容，检查培训文档是否与实际培训内容相符合，协助业主单位方组织培训，监督承建单位实施其培训计划，并征求业主单位的反馈意见，对培训效果进行考核评估； （7）审核项目文档资料编制质量，提出审核意见，跟进整改情况。 2.进度控制 （1）根据已批准的项目实施计划，检查实际项目实施执行进度； （2）对承建单位提交的项目周报等内容进行进度真实性复核； （3）根据当前实施进度，判断或预测项目执行的时间风险，并出具监理建议； （4）定期以周报/月报形式向业主单位量化汇报项目实际的执行状态。 3.投资控制 （1）审核合同或备忘录中关于项目款项支付的条件； （2）审核承建单位提交的付款申请，参照合同支付条款进行实际工程量核算，确定支付的符合性，出具监理支付意见（支付证书）；

（3）对于项目款项变更、合同索赔进行造价评估。

4.变更控制

（1）审核承建单位提出的变更申请，就其变更动机的合理性出具监理专题报告，予以批准或否决；

（2）对初步批准的变更申请，组织三方审核变更方案，评估变更影响，并严格各方执行变更程序；

（3）监督变更方案的实施，并评估变更影响效果，出具监理专题报告。

5.安全管理

（1）协助建设单位审核安全管理方案和数据保密方案；

（2）定期/不定期对项目安全施工及数据保密管理方案执行情况进行检查；

（3）负责项目建设过程中所涉及的政府数据和资料的保护，保证不被非授权使用；

（4）负责项目实施过程中的安全管理，确保不出现安全事故。

6.文档管理

（1）批准承建单位提交项目文档管理计划，并根据计划及时敦促承建单位提交文档；

（2）审核承建单位提交的各类项目文档，并出具监理专题报告；

（3）负责对于项目过程产生的原始文档/文件进行收集，并定期整理；

（4）做好合同批复等各类往来文件的存档；

（5）做好项目协调会、技术专题会的会议纪要工作；

（6）管理实施期间的各类技术文档；

（7）编制监理周报、监理月报，根据项目需要签发监理意见书、监理通知书；

（8）审核交付验收文档，提出审核意见，督促承建单位按要求整改。

7.合同管理

（1）协助审核项目合同，按照要求就项目合同征求意见并根据意见进行修改完善；

（2）跟踪检查合同的执行情况，确保项目建设单位按时履约；

（3）对合同的工期的延误和延期进行审核确认；

（4）对合同变更、索赔等事宜进行审核确认；

（5）根据合同约定，审核项目承建单位的支付申请，签发付款凭证；

（6）对项目变更控制，明确界定项目变更的目标，防止变更范围的扩大化，加强变更风险以及变更效果的评估；

（7）评估项目是否具备服务启动条件。

8.沟通协调

（1）组织召开监理例会，并形成监理会议纪要；

（2）根据项目实际出现的建设问题，（协助业主单位）及时召开项目专题会议、项目例会，并形成监理会议纪要；

（3）对涉及多方的建设交互/协同问题，（协助业主单位）及时召开项目协调会，并形成监理会议纪要；

（4）协调推进系统定级备案；

（5）必要时，督促承建单位编制密码应用方案并审核，协调密评单位对密码应用方案进行审核。

（四）验收阶段

（1）协调业主单位和承建单位在验收计划、验收目标、验收范围、验收内容、验收方法和验收标准（初验和终验）等方面达成一致，填报项目备忘录（根据项目实际需要确定），并经三方签认；

（2）审核承建单位提交的验收申请（初验和终验），审核其中的验收计划、验收方案等；

（3）协助业主单位确定验收程序、验收标准和验收方案（初验和终验）；

		（4）核查项目建设完成情况、试运行情况和遗留问题整改情况，出具是否具备验收条件的监理意见； （5）依据项目档案管理规范，协助整理项目验收文档; （6）协助业主单位按照项目验收方案所规定的验收内容和方式组织初验、试运行和终验，对其结果进行确认，对验收过程中发现的问题提出监理意见，并督促承建单位进行整改； （7）敦促业主单位、承建单位按照事先约定，编制、签署并妥善保存验收阶段的各类文挡，敦促业主单位和承建单位及时整理并妥善保管整个项目的相关文挡； （8）编制项目监理总结报告，整理并向业主单位提交与项目有关的全部监理文挡； （9）协助业主单位组织初验和终验评审会； （10）协助业主单位和承建单位整理项目文档资料，为档案专项验收做好准备工作； （11）协助业主单位申请并通过档案专项验收； （12）协助业主单位对项目进行第三方审计，沟通审核第三方审计报告； （13）协助业主单位申请项目竣工验收，配合验收组织工作； （14）协助业主单位和承建单位完成项目和文档资料移交工作。 1.5 监理服务人员要求 投标人需为本项目派驻总监理工程师1名，总监理工程师代表1名，专业监理工程师不少于2名。 二、合同商务条款 1.服务地点：采购人指定地点。 2.服务期限：自监理服务合同签订之日起，至项目终验通过。 3.合同价款： 3.1合同总价包含监理服务费、税费等全部费用。 3.2本项目为固定总价合同，合同总价不受市场价格、工作量变化等其它因素的影响。 4.付款方式： 4.1合同生效后，采购人分三次支付本合同款项： 第一次：合同签订后，支付合同总价的40%作为首付款； 第二次：项目初验合格后，支付合同总价的40%； 第三次：项目终验合格后，支付合同总价的20%。 4.2供应商承诺在采购人办理支付手续前，为采购人出具等额的符合国家规定的发票。

采购包3：

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：等保测评

参数性质	序号	技术参数与性能指标
		★ | 1 | （一）、网络安全等级保护测评概述 等级保护测评是指经认定的专业第三方测评机构依据国家网络安全等级保护制度规定，按照有关管理规范和技术标准，对非涉及国家秘密网络安全等级保护状况进行检测评估的活动。网络安全等级保护是国家信息安全保障的基本制度、策略和方法。开展网络安全等级保护测评工作是保障信息化健康发展、平稳运行的一项重要工作。

★	2	（二）、测评要求 依据《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）、《信息安全技术网络安全等级保护测评要求》(GB/T 28448-2019)、《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）相关标准及行业管理规范，通过访谈、核查、测试、风险分析等多种方式对甲方指定的信息系统，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理10个方面进行网络安全等级保护测评服务。
★	3	（三）、等级保护测评流程 ① 协助备案，协助甲方对系统的备案资料整理并递交属地网安部门。 ② 系统调研：在系统相关人员的协助下，对信息系统进行调研和梳理，了解系统当前信息系统资产现状。 ③ 现场测评：根据《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）国家等级测评的相关标准及已编制的相关等级保护测评指导书对信息系统中的相关资产进行测评项的检查、记录检查结果。 ④ 分析整改：分析信息系统安全情况与等级保护基本要求的差距,提供差异化测评服务，并进行风险分析，可根据现场情况出具科学合理的整改建议及整改方案，配合甲方进行安全整改工作。 ⑤ 结论报告：根据前述工作内容，分析当前信息系统安全保护能力是否符合相应等级的安全要求，针对整改项进行再次测评,提供安全等级符合性测评服务，出具相关系统测评报告。
▲	4	、预期成果交付物及服务期限 各个系统《网络安全等级保护测评方案》、 各个系统《网络安全等级保护测评报告》、 各个系统《网络安全等级保护测评整改建议书》； 服务期限：45个日历日。

三级系统测评指标

层面	控制点	测评项
	物理位置选择	a) 机房场地应选择在具有防震、防风和防雨等能力的建筑内； b) 机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施。
	物理访问控制	a) 机房出入口应安排专人值守，控制、鉴别和记录进入的人员； b) 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围； c) 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域； d) 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

			安全物理环境	防盗器和防破坏	a) 应将主要设备放置在机房内； b) 应将设备或主要部件进行固定，并设置明显的不易除去的标记； c) 应将通信线缆铺设在隐蔽处，可铺设在地下或管道中； d) 应对介质分类标识，存储在介质库或档案室中； e) 应利用光、电等技术设置机房防盗报警系统； f) 应对机房设置监控报警系统。
				防雷击	a)应将各类机柜、设施和设备等通过接地系统安全接地； b)应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等。
				防火	a) 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火； b)机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料； c)应对机房划分区域进行管理，区域和区域之间设置隔离防火措施。
				防水和防潮	a)水管安装，不得穿过机房屋顶和活动地板下； b)应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透； c)应采取措施防止机房内水蒸气结露和地下积水的转移与渗透； d)应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。
				防静电	a)应采用防静电地板或地面并采用必要的接地防静电措施； b)应采取措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等。
				温湿度控制	应设置温湿度自动调节设施，使机房温湿度的变化在设备运行所允许的范围之内。
				电力供应	a) 应在机房供电线路上配置稳压器和过电压防护设备； b) 应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求； c) 应设置冗余或并行的电力电缆线路为计算机系统供电； d) 应建立备用供电系统。
				电磁防护	a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰； b) 电源线和通信线缆应隔离铺设，避免互相干扰； c) 应对关键设备和磁介质实施电磁屏蔽。
				网络架构	a) 应保证网络设备的业务处理能力满足业务高峰期需要； b) 应保证网络各个部分的带宽满足业务高峰期需要； c) 应划分不同的网络区域，并按照方便管理和控制的原则为各网络区域分配地址； d) 应避免将重要网络区域部署在边界处，重要网络区域与其他网络区域之间应采取可靠的技术隔离手段； e) 应提供通信线路、关键网络设备和关键计算设备的硬件冗余，保证系统的可用性。
				通信传输	a) 应采用校验技术或密码技术保证通信过程中数据的完整性； b) 应采用密码技术保证通信过程中数据的保密性。
				可信验证	可基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

			安全通信网络	边界防护	a) 应保证跨越边界的访问和数据流通过边界设备提供的受控接口进行通信； b) 应能够对非授权设备私自联到内部网络的行为进行检查或限制； c) 应能够对内部用户非授权联到外部网络的行为进行检查或限制； d) 应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
				访问控制	a) 应在网络边界或区域之间根据访问控制策略设置访问控制规则，默认情况下除允许通信外受控接口拒绝所有通信； b) 应删除多余或无效的访问控制规则，优化访问控制列表，并保证访问控制规则数量最小化； c) 应对源地址、目的地址、源端口、目的端口和协议等进行检查，以允许/拒绝数据包进出； d) 应能根据会话状态信息为进出数据流提供明确的允许/拒绝访问的能力； e) 应对进出网络的数据流实现基于应用协议和应用内容的访问控制。
				入侵防范	a) 应在关键网络节点处检测、防止或限制从外部发起的网络攻击行为； b) 应在关键网络节点处检测、防止或限制从内部发起的网络攻击行为； c) 应采取技术措施对网络行为进行分析，实现对网络攻击特别是新型网络攻击行为的分析； d) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目标、攻击时间，在发生严重入侵事件时应提供报警。
				恶意代码防范	a) 应在关键网络节点处对恶意代码进行检测和清除，并维护恶意代码防护机制的升级和更新； b) 应在关键网络节点处对垃圾邮件进行检测和防护，并维护垃圾邮件防护机制的升级和更新。
				安全审计	a) 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户； b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； d) 应能够根据记录数据进行分析，并生成审计报表； e) 应保护审计进程，避免受到未预期的中断； f) 应保护审计记录，避免受到未预期的删除、修改或覆盖等。
				可信验证	可基于可信根对边界设备的系统引导程序、系统程序、重要配置参数和边界防护应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警， 并将验证结果形成审计记录送至安全管理中心。
				身份鉴别	a) 应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； b) 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； c) 当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听； d) 应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别， 且其中一种鉴别技术至少应使用密码技术来实现。

			安全计算环境	访问控制	a) 应对登录的用户分配账户和权限； b) 应重命名或删除默认账户，修改默认账户的默认口令； c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在； d) 应授予管理用户所需的最小权限，实现管理用户的权限分离； e) 应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则； f) 访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级； g) 应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。
				安全审计	a) 应启用安全审计功能，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； b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等； d) 应对审计进程进行保护，防止未经授权的中断。
				入侵防范	a) 应遵循最小安装的原则，仅安装需要的组件和应用程序； b) 应关闭不需要的系统服务、默认共享和高危端口； c) 应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； d) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； e) 应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞； f) 应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时提供报警。
				恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
				可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证， 并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证 结果形成审计记录送至安全管理中心。
				数据完整性	a) 应采用校验技术或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个人信息等； b) 应采用校验技术或密码技术保证重要数据在存储过程中的完整性，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个人信息等。
				数据保密性	a) 应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等； b) 应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
				数据备份恢复	a) 应提供重要数据的本地数据备份与恢复功能； b) 应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地； c) 应提供重要数据处理系统的热冗余，保证系统的高可用性。

				剩余信息保护	a) 应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； b) 应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。
				个人信息保护	a) 应仅采集和保存业务必需的用户个人信息； b) 应禁止未授权访问和非法使用用户个人信息。
			安全管理中心	系统管理	a) 应对系统管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行系统管理操作，并对这些操作进行审计； b) 应通过系统管理员对系统的资源和运行进行配置、控制和管理，包括用户身份、系统资源配置、系统加载和启动、系统运行的异常处理、数据和设备的备份与恢复等。
				审计管理	a) 应对审计管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全审计操作，并对这些操作进行审计； b) 应通过审计管理员对审计记录应进行分析，并根据分析结果进行处理，包括根据安全审计策略对审计记录进行存储、管理和查询等。
				安全管理	a) 应对安全管理员进行身份鉴别，只允许其通过特定的命令或操作界面进行安全管理操作，并对这些操作进行审计； b) 应通过安全管理员对系统中的安全策略进行配置，包括安全参数的设置，主体、客体进行统一安全标记，对主体进行授权，配置可信验证策略等。
				集中管控	a) 应划分出特定的管理区域，对分布在网络中的安全设备或安全组件进行管控； b) 应能够建立一条安全的信息传输路径，对网络中的安全设备或安全组件进行管理； c) 应对网络链路、安全设备、网络设备和服务器等的运行状况进行集中监测； d) 应对分散在各个设备上的审计数据进行收集汇总和集中分析，并保证审计记录的留存时间符合法律法规要求； e) 应对安全策略、恶意代码、补丁升级等安全相关事项进行集中管理； f) 应能对网络中发生的各类安全事件进行识别、报警和分析。
	1			安全策略	应制定网络安全工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。
				管理制度	a) 应对安全管理活动中的各类管理内容建立安全管理制度； b) 应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； c) 应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的安全管理制度体系。
				制定和发布	a) 应指定或授权专门的部门或人员负责安全管理制度的制定； b) 安全管理制度应通过正式、有效的方式发布，并进行版本控制。
				评审和修订	应定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

		安全管理机构	岗位设置	a) 应成立指导和管理网络安全工作的委员会或领导小组，其最高领导由单位主管领导担任或授权； b) 应设立网络安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责； c) 应设立系统管理员、审计管理员和安全管理员等岗位，并定义部门及各个工作岗位的职责。
			人员配备	a) 应配备一定数量的系统管理员、审计管理员和安全管理员等； b) 应配备专职安全管理员，不可兼任。
			授权和审批	a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度； c) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。
			沟通和合作	a) 应加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题； b) 应加强与网络安全职能部门、各类供应商、业界专家及安全组织的合作与沟通； c) 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息。
			审核和检查	a) 应定期进行常规安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； b) 应定期进行全面安全检查，检查内容包括现有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； c) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报。
		安全管理人员	人员录用	a) 应指定或授权专门的部门或人员负责人员录用； b) 应对被录用人员的身份、安全背景、专业资格或资质等进行审查，对其所具有的技术技能进行考核； c) 应与被录用人员签署保密协议，与关键岗位人员签署岗位责任协议。
			人员离岗	a) 应及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备； b) 应办理严格的调离手续，并承诺调离后的保密义务后方可离开。
			安全意识教育和培训	a) 应对各类人员进行安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施； b) 应针对不同岗位制定不同的培训计划，对安全基础知识、岗位操作规程等进行培训； c) 应定期对不同岗位的人员进行技能考核。

				外部人员访问管理	a) 应在外部人员物理访问受控区域前先提出书面申请，批准后由专人全程陪同，并登记备案； b) 应在外部人员接入受控网络访问系统前先提出书面申请，批准后由专人开设账户、分配权限， 并登记备案； c) 外部人员离场后应及时清除其所有的访问权限； d) 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得复制和泄露任何敏感信息。
			安全建设管理	定级和备案	a) 应以书面的形式说明保护对象的安全保护等级及确定等级的方法和理由； b) 应组织相关部门和有关安全技术专家对定级结果的合理性和正确性进行论证和审定； c) 应保证定级结果经过相关部门的批准； d) 应将备案材料报主管部门和相应公安机关备案。
				安全方案设计	a) 应根据安全保护等级选择基本安全措施，依据风险分析的结果补充和调整安全措施； b) 应根据保护对象的安全保护等级及与其他级别保护对象的关系进行安全整体规划和安全方案设计，设计内容应包含密码技术相关内容，并形成配套文件； c) 应组织相关部门和有关安全专家对安全整体规划及其配套文件的合理性和正确性进行论证和审定，经过批准后才能正式实施。
				产品采购和使用	a) 应确保网络安全产品采购和使用符合国家的有关规定； b) 应确保密码产品与服务的采购和使用符合国家密码管理主管部门的要求； c) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。
				自行软件开发	a) 应将开发环境与实际运行环境物理分开，测试数据和测试结果受到控制；b) 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则； c) 应制定代码编写安全规范，要求开发人员参照规范编写代码； d) 应具备软件设计的相关文档和使用指南，并对文档使用进行控制； e) 应保证在软件开发过程中对安全性进行测试，在软件安装前对可能存在的恶意代码进行检测； f) 应对程序资源库的修改、更新、发布进行授权和批准，并严格进行版本控制； g) 应保证开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。
				外包软件开发	a) 应在软件交付前检测其中可能存在的恶意代码； b) 应保证开发单位提供软件设计文档和使用指南； c) 应保证开发单位提供软件源代码，并审查软件中可能存在的后门和隐蔽信道。
				工程实施	a) 应指定或授权专门的部门或人员负责工程实施过程的管理； b) 应制定安全工程实施方案控制工程实施过程； c) 应通过第三方工程监理控制项目的实施过程。
				测试验收	a) 应制订测试验收方案，并依据测试验收方案实施测试验收，形成测试验收报告； b) 应进行上线前的安全性测试，并出具安全测试报告，安全测试报告应包含密码应用安全性测试相关内容。

		系统交付	a) 应制定交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点； b) 应对负责运行维护的技术人员进行相应的技能培训； c) 应提供建设过程文档和运行维护文档。
		等级测评	a) 应定期进行等级测评，发现不符合相应等级保护标准要求的及时整改； b) 应在发生重大变更或级别发生变化时进行等级测评； c) 应确保测评机构的选择符合国家有关规定。
		服务供应商选择	a) 应确保服务供应商的选择符合国家的有关规定； b) 应与选定的服务供应商签订相关协议，明确整个服务供应链各方需履行的网络安全相关义务； c) 应定期监督、评审和审核服务供应商提供的服务，并对其变更服务内容加以控制。
		环境管理	a) 应指定专门的部门或人员负责机房安全，对机房出入进行管理，定期对机房供配电、空调、温湿度控制、消防等设施进行维护管理； b) 应建立机房安全管理制度，对有关物理访问、物品带进出和环境安全等方面的管理作出规定； c) 应不在重要区域接待来访人员，不随意放置含有敏感信息的纸档文件和移动介质等。
		资产管理	a) 应编制并保存与保护对象相关的资产清单，包括资产责任部门、重要程度和所处位置等内容； b) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施； c) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。
		介质管理	a) 应将介质存放在安全的环境中，对各类介质进行控制和保护，实行存储环境专人管理，并根据存档介质的目录清单定期盘点； b) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，并对介质的归档和查询等进行登记记录。
		设备维护管理	a) 应对各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理； b) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、维修和服务的审批、维修过程的监督控制等； c) 信息处理设备应经过审批才能带离机房或办公地点，含有存储介质的设备带出工作环境时其中重要数据应加密； d) 含有存储介质的设备在报废或重用前，应进行完全清除或被安全覆盖，保证该设备上的敏感数据和授权软件无法被恢复重用。
		漏洞和风险管理	a) 应采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补或评估可能的影响后进行修补； b) 应定期开展安全测评，形成安全测评报告，采取措施应对发现的安全问题。

			安全运维管理	网络和系统安全管理	a) 应划分不同的管理员角色进行网络和系统的运维管理，明确各个角色的责任和权限； b) 应指定专门的部门或人员进行账户管理，对申请账户、建立账户、删除账户等进行控制； c) 应建立网络和系统安全管理制度，对安全策略、账户管理、配置管理、日志管理、日常操作、升级与打补丁、口令更新周期等方面作出规定； d) 应制定重要设备的配置和操作手册，依据手册对设备进行安全配置和优化配置等； e) 应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容； f) 应指定专门的部门或人员对日志、监测和报警数据等进行分析、统计，及时发现可疑行为； g) 应严格控制变更性运维，经过审批后才可改变连接、安装系统组件或调整配置参数，操作过程中应保留不可更改的审计日志，操作结束后应同步更新配置信息库； h) 应严格控制运维工具的使用，经过审批后才可接入进行操作，操作过程中应保留不可更改的审计日志，操作结束后应删除工具中的敏感数据； i) 应严格控制远程运维的开通，经过审批后才可开通远程运维接口或通道，操作过程中应保留不可更改的审计日志，操作结束后立即关闭接口或通道； j) 应保证所有与外部的连接均得到授权和批准，应定期检查违反规定无线上网及其他违反网络安全策略的行为。
				恶意代码防范管理	a) 应提高所有用户的防恶意代码意识，对外来计算机或存储设备接入系统前进行恶意代码检查等； b) 应定期验证防范恶意代码攻击的技术措施的有效性。
				配置管理	a) 应记录和保存基本配置信息，包括网络拓扑结构、各个设备安装的软件组件、软件组件的版本和补丁信息、各个设备或软件组件的配置参数等； b) 应将基本配置信息改变纳入变更范畴，实施对配置信息改变的控制，并及时更新基本配置信息库。
				密码管理	a) 应遵循密码相关国家标准和行业标准； b) 应使用国家密码管理主管部门认证核准的密码技术和产品。
				变更管理	a) 应明确变更需求，变更前根据变更需求制定变更方案，变更方案经过评审、审批后方可实施； b) 应建立变更的申报和审批控制程序，依据程序控制所有的变更，记录变更实施过程； c) 应建立中止变更并从失败变更中恢复的程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。
				备份与恢复管理	a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等； b) 应规定备份信息的备份方式、备份频度、存储介质、保存期等； c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略、备份程序和恢复程序等。

安全事件处置	a) 应及时向安全管理部门报告所发现的安全弱点和可疑事件； b) 应制定安全事件报告和处置管理制度，明确不同安全事件的报告、处置和响应流程，规定安全事件的现场处理、事件报告和后期恢复的管理职责等；c) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程， 总结经验教训； d) 对造成系统中断和造成信息泄漏的重大安全事件应采用不同的处理程序和报告程序。
应急预案管理	a) 应规定统一的应急预案框架，包括启动预案的条件、应急组织构成、应急资源保障、事后教育和培训等内容； b) 应制定重要事件的应急预案，包括应急处理流程、系统恢复流程等内容； c) 应定期对系统相关的人员进行应急预案培训，并进行应急预案的演练； d) 应定期对原有的应急预案重新评估，修订完善。
外包运维管理	a) 应确保外包运维服务商的选择符合国家的有关规定； b) 应与选定的外包运维服务商签订相关的协议，明确约定外包运维的范围、工作内容； c) 应保证选择的外包运维服务商在技术和管理方面均应具有按照等级保护要求开展安全运维工作的能力，并将能力要求在签订的协议中明确； d) 应在与外包运维服务商签订的协议中明确所有相关的安全要求，如可能涉及对敏感信息的访问、处理、存储要求，对 IT 基础设施中断服务的应急保障要求等。

采购包4：

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：安全测评

参数性质	序号	技术参数与性能指标
		服务内容与要求 **一、项目背景** 面对国家安全的新形势，我国已在多部法律法规中明确规定了密码应用的要求，包括《密码法》、《网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例（征求意见稿）》、《网络安全等级保护条例（征求意见稿）》等，形成了以《密码法》为主导的密码管理法律法规体系。为提升信息系统安全水平，提高信息系统密码应用保障能力，推动国产密码应用工作的进一步落实，加强密码技术在信息系统中合规、 正确和有效的应用,确保各项信息化系统的安全稳定运行，现需根据相关标准对目标系统从密码技术应用、密钥管理、安全管理等方面验证是否满足国家关于信息系统密码应用安全性的要求。通过商用密码应用安全性评估服务，深入查找密码应用的薄弱环节和安全隐患，分析面临的风险，为信息资产安全和业务持续稳定运行提供保障，为提升信息系统安全奠定基础。

二、测评目的及范围

依据《信息系统密码应用基本要求》，针对目标系统从技术要求、密钥管理、安全管理三个角度出发，围绕信息系统的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全以及密钥管理、安全管理开展密码测评工作，以期发现信息系统与其相应安全等级要求之间的差距以及存在的安全隐患，为密码应用测评标准提供工作建议，保障信息系统密码合规、正确、有效地应用。

此次测评范围为：XXXX（此次需测评的系统名称）

供应商需提供整改建议咨询服务。

三、测评依据

1、法律法规：

《电子签名法》

《电子认证服务管理办法》

《信息安全等级保护商用密码管理办法》

2、行业标准：

新国标GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》

GM/Y 5001-2017《密码标准应用指南》

GM/Z 0001-2013《密码术语》

GM/T 0028-2014《密码模块安全技术要求》

GM/T 0039-2015《密码模块安全检测要求》

GM/T 0036《采用非接触卡的门禁系统密码应用指南》

GM/T 0060-2018《签名验签服务器检测规范》

GM/T 0024-2014《SSL VPN技术规范》

GM/T 0025-2014《SSL VPN 网关产品规范》

GM/T 0015-2012《基于SM2密码算法的数字证书格式规范》

《商用密码应用安全性评估管理办法》

《商用密码应用安全性测评机构管理办法》

《商用密码应用安全性评估测评过程指南（试行）》

《商用密码应用安全性评估测评作业指导书（试行）》

被测机构送审文档：

《支付机构国产密码应用试点实施方案》

《支付机构国产密码应用试点应用解决方案》

《国密试点项目技术方案概要设计》

《国密试点详细设计说明书》

《国产密码算法库接口使用说明文档》

3、术语和定义

下列术语和定义适用于本文件

（1）机密性 confidentiality

保证信息不被泄露给非授权的个人、进程等实体的性质。

（2）完整性 data integerity

数据没有遭受以非授权方式所作的篡改或破坏的性质。

（3）真实性 authenticity

确保主体或资源的身份正是所声称的特性。真实性适用于用户、进程、系统和信息之类的实体。

4、国密算法

国密算法是由国家密码局发布的一系列商用密码算法标准。

5、数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验签，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

四、测评原则

1、客观公正原则

测评人员保证在最小主观判断情形下，按照双方认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

2、经济性和可重用性原则

测评工作采信可重用已有测评结果中相同的检测项目，包括商用密码安全产品测评结果，信息系统密码测评结果和等级保护测评结果。所有重用结果都以结果适用于待测系统为前提，并能够客观反映目前系统的安全状态。

3、可重复性和可再现性原则

依照同样的要求，使用同样的测评方法，在同样的环境下，不同的测评机构对每个测评实施过程的重复执行应得到同样的结果。可再现性和可重复性的区别在于，前者关注不同测评者测评结果的一致性，后者则与同一测评者测评结果的一致性有关。

4、结果完善性原则

在正确理解《信息系统密码应用基本要求》各个要求项内容的基础之上，检测所产生的结果应客观反映信息系统的运行状态。测评过程和结果应服从正确的测评方法，以确保其满足要求。

五、密码应用安全性评估测评实施

1、测评目标和对象

通过对待测系统在商用密码技术应用、密钥管理及安全管理方面的分析，对系统商用密码应用的合规性、正确性、有效性作出判断，确定了测评目标和测评对象。

表1测评对象列表

序号	测评层面	测评对象
1	通用测评要求	密码管理员、密码算法、密码技术、密码产品、密码服务技术文档
2	物理和环境安全	物理安全负责人、系统管理员、机房监控系统、门禁系统、技术文档
3	网络和通信安全	交换机、堡垒机、应用系统、网络安全运维人员、技术文档
4	设备和计算安全	交换机、堡垒机、系统管理员、数据库管理员、业务服务器、数据库服务器、证书服务器、密钥管理服务器、技术文档
5	应用和数据安全	应用系统管理员、操作系统、存储各类密钥的管理系统、技术文档
6	安全制度	安全管理制度

2、测评方法

（1）测评方式

本次密码测评的主要方式有：访谈、文档审查、配置审查、工具测试、实地察看。

访谈

检验人员与被测系统有关人员（个人/群体）进行交流、讨论等活动，获取相关证据，了解有关信息。在访谈范围上，不同等级信息系统在测评时有不同的要求，一般应基本覆盖所有的安全相关人员类型，在数量上可以抽样。

文档审查

检查《信息系统密码应用基本要求》和《信息系统密码测评要求》中规定的必须具有的制度、策略、操作规程等文档是否齐备。

检查是否有完整的制度执行情况记录和人员管理情况记录，如机房出入登记记录、电子记录、高等级系统的关键设备的使用登记记录等。

对上述文档进行审核与分析，检查他们的完整性和这些文件之间的内部一致性。

配置审查

根据测评结果记录表格内容，利用上机验证的方式检查应用系统、主机系统、数据库系统、密码设备以及网络设备的配置是否正确，是否与文档、相关设备和部件保持一致，对文档审核的内容进行核实。

如果系统在输入无效命令时不能完成其功能，将要对其进行错误测试。

工具测试

根据测评指导书，利用技术工具对系统进行测试，包括网络协议分析、密码算法和密码协议的识别和验证等。

实地察看

根据被测系统的实际情况，检验人员到系统运行现场通过实地的观察人员行为、技术设施和物理环境状况判断人员的安全意识、业务操作、管理程序和系统物理环境等方面的安全情况，测评其是否达到了相应等级的密码安全要求。

（2）测评工具

对目标业务系统进行验证测试，涉及到网络密码协议分析、密码算法检测等多种测评方式，测评工具类型列表见表2所示。

表2 测评工具类型列表

序号	工具类型	测评对象
1	网络协议分析工具	实现对被测系统所在主机从应用安全\密码安全等方面进行评测分析□通过协议分析工具，对客户端与服务器之间的通信协议包进行抓取，并从应用安全、密码安全等方面进行评测分析。
2	数字证书合规性验证工具	对数字证书格式、数字证书签名值验证等方面进行合规性检测，分析证书使用是否合规，密码功能是否正确等。

针对被测系统的网络边界和抽查设备、主机和业务应用系统的情况，需要在被测系统及其互联网络中设置测试工具接入点。

（3）风险分析及防范措施

测评阶段可能面临的风险以及风险规避措施如表3所示：

表3 风险分析列表

风险概述	风险分析	风险规避
有效性风险	在商用密码应用安全性测评过程中首先要进行的是信息收集工作，在信息收集的过程中，经常会存在信息收集不完整、信息描述不准确等问题，而不准确的信息将会对测评方案编制工作中测评指标及测评对象的选择带来偏差。 在现场测评中，不同工程师对标准要求的理解也会影响到测评工作的有效性和准确性。 在报告编制过程中测评师对测评结果的分析是否合理，对于测评结论的有效性也有较大影响。	信息收集过程中尽量确保信息收集完整、信息描述准确，测评机构应与被测评单位及时沟通。 测评过程中，测评实施人员应及时与被测评方就测评中发现的问题及时沟通，避免因对标准理解的偏差导致的必须要问题出现。 报告编制过程中应指派至少两名及以上测评师负责测评结果的分析，确保对测评结果的分析正确、合理。

公正性风险	在测评过程中，测评工程师、测评机构通常会受到市场竞争压力、测评机构自身业务发展压力、被测评机构合同及财务压力等多方面的影响，从而导致测评结论的公正性问题。	加强测评人员测评素质培训，对测评机构的测评实施过程记性监督管理。 测评实施过程中，测评方应保证在符合国家密码主管部门要求及最小主观判断情形下，按照与被测单位共同认可的密评方案，基于明确定义的测评方式和解释，实施测评活动。
保密性风险	商用密码应用安全性测评工作，要求测评机构深入了解被测评系统的管理、技术及业务方面的信息。而这些信息大部分涉及到企业或机构的商业、工作秘密。如果测评工作中，测评机构泄漏了检测单位的系统状态信息，如网络拓扑、IP地址、业务流程、安全机制、安全隐患和有关文档信息，将会对检测单位的信息系统带来极大的安全问题。 在测评过程中，资料收集、现场测评记录、编制报告等活动都会使用到被测评单位系统相关信息，在信息的使用和交换过程中多存在着信息泄漏的风险。	加强测评人员保密意识培训，测评人员与被测评单位签署安全保密协议，保密协议建议由被测单位提供。 被测评单位完善信息保密控制措施，根据“业务需要”和“最小权限”原则提供材料和系统使用权限。 在测评过程中，被测系统的常规性资料以人员面对面形式进行递交，敏感性材料按照被测单位的相关要求，可采取现场查阅或访谈的方式进行；传递介质以光盘为主。
测评过程风险	验证测试可能影响被测信息系统正常运行：在现场测评时，需对设备和系统进行一定的验证测试工作，部分测试内容需上机查看信息，可能对被测信息系统的运行造成不可预期的影响。 工具测试可能影响被测信息系统正常运行：在现场测评时，根据实际需要可能会使用一些测评工具进行测试。测评工具使用时可能会产生冗余数据写入，同时可能会对系统的负载造成一定的影响，进而对被测信息系统中的服务器和网络通信造成一定影响甚至损害。 可能导致被测信息系统敏感信息泄漏：测评过程中，可能泄露被测信息系统的敏感信息，如加密机制、业务流程、安全机制和有关文档信息等。 其他可能面临的风险：在测评过程中，也可能出现影响被测信息系统可用性、机密性和完整性的风险。	签署委托测评协议书：在测评工作正式开始之前，测评方和被测单位需要以委托协议的方式，明确测评工作的目标、范围、人员组成、计划安排、执行步骤和要求以及双方的责任和义务等，使得测评双方对测评过程中的基本问题达成共识。 签署保密协议：测评相关方应签署合乎法律规范的保密协议，规定测评相关方在保密方面的权利、责任与义务。 签署现场测评授权书：现场测评之前，测评方应与被测单位签署现场测评授权书，要求测评相关方对系统及数据进行备份，采取适当的方法进行风险规避，并针对可能出现的事件制定应急处理方案。 现场测评要求：需进行验证测试和工具测试时，应避开被测信息系统业务高峰期，在系统资源处于空闲状态时进行测试，或配置与被测信息系统一致的模拟/仿真环境，在模拟/仿真环境下开展测评工作；需进行上机验证测试时，密评人员应提出需要验证的内容，由被测单位的技术人员进行实际操作。整个现场测评过程，由被测单位和测评方相关人员进行全程监督。 测评工作完成后，密评人员应交回在测评过程中获取的所有特权，归还测评过程中借阅的相关资料文档，并将测评现场环境恢复至测评前状态。

3、测评指标

依据信息系统确定的业务信息安全保护等级和系统服务安全保护等级，选择《基本要求》中对应级别的安全要求作为密码测评的基本指标，以表格形式在表中列出。

此次测试从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理、安全管理六个方面考虑罗列出本次测评指标范围,如表4所示。

测评范围内的测评指标：

表4　测评范围内测评指标列表

序号	层面	测评指标
1	物理和环境安全	身份鉴别
2		电子门禁记录数据完整性
3		视频记录数完整性
4	网络和通信安全	身份鉴别
5		网络边界访问控制信息的完整性
6		通信数据完整性
7		通信数据机密性
8		安全接入认证
9	设备和计算安全	身份鉴别
10		远程管理通道安全
11		系统资源访问控制信息完整性
12		重要信息资源安全标记完整性
13		日志记录完整性
14		重要可执行程序完整性、重要可执行程序来源真实性
15	应用和数据安全	身份鉴别
16		访问控制完整性
17		数据传输机密性
18		数据存储机密性
19		数据传输完整性
20		数据存储完整性
21		日志完整性
22		重要信息资源安全标记完整性
23		不可否认性
24	安全管理	制度安全
25		人员安全
26		实施安全
27		应急安全

4、通用测评要求

1

测评对象：密码管理员、密码算法、密码技术、密码产品、密码服务技术文档

（1）密码算法和密码技术合规性

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。（第一级到第五级）

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。（第一级到第五级）

（2）密钥管理

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。（第一级到第五级）

采用的密码产品，达到 GB/T 37092 一级及以上安全要求。（第二级）

采用的密码产品，达到 GB/T 37092 二级及以上安全要求。（第三级）

采用的密码产品，达到 GB/T 37092 三级及以上安全要求。（第四级）

采用的密码服务，符合法律法规的相关要求，需依法接受检测认证的，应经商用密码认证机构认证合格。（第一级到第四级）

5、测评内容和对象

（1）物理和环境安全

测评对象：机房物理环境、物理安全负责人、电子门禁系统、视频监控系统、系统管理员、技术文档

测评判定：对机房进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表5　物理和环境安全测评要求列表

测评项	测评指标	测评方法
身份鉴别	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。（第一级到第四级）	遵循物理和环境安全测评要求，对服务端设备所在机房环境进行测评（以核实新增记录的真实性、完整性为主）。
电子门禁记录数据完整性	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。（第一级到第四级）	
视频记录数完整性	采用密码技术保证视频监控音像记录数据的存储完整性。（第三级到第四级）	

（2）网络和通信安全

测评对象：交换机、堡垒机、应用系统、网络安全运维人员、技术文档

测评判定：对网络设备和通信进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表6　网络和通信安全测评要求列表

测评项	测评指标	测评方法
身份鉴别	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。（第一级到第三级） 采用密码技术对通信实体进行双向身份鉴别，保证通信实体身份的真实性。（第四级）	

		接入点JA：在前置服务器前的外部接入交换机处接入，主要目的是捕获通信数据，分析数据交互双方是否加密、通信密码协议是否合规，分析密码服务是否合规、正确、有效。
通信数据完整性	采用密码技术保证通信过程中数据的完整性。（第一级到第四级）	
通信数据机密性	采用密码技术保证通信过程中重要数据的机密性。（第一级到第四级）	
网络边界访问控制信息的完整性	采用密码技术保证网络边界访问控制信息的完整性。（第一级到第四级）	
安全接入认证	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，确保接入设备身份的真实性。（第三级到第四级）	

（3）设备和计算安全

测评对象：交换机、堡垒机、系统管理员、数据库管理员、业务服务器、数据库服务器、证书服务器、密钥管理服务器、技术文档

测评判定：对服务器和存储设备进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表7　设备和计算安全测评要求列表

测评项	测评指标	测评方法
身份鉴别	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。（第一级到第四级）	尝试正常登录和异常登录（包括错误的口令、不插入智能密码钥匙或插入未授权的智能密码钥匙等情况）情况下，是否按照预期结果完成身份鉴别。
远程管理身份鉴别信息机密性	远程管理设备时，采用密码技术建立安全的信息传输通道。（第三级到第四级）	在管理区JA交换机接入通信协议分析工具，查看用于设备管理涉及的管理员口令等鉴别数据和敏感数据在传输中是否进行了机密性保护。
访问控制信息完整性	采用密码技术保证系统资源访问控制信息的完整性。（第一级到第四级）	在JB交换机接入通信协议分析工具捕获通信数据，分析业务服务器（内置密码模块）是否被有效调用。尝试修改访问控制信息和日志记录（或对应的MAC），查看完整性保护机制的有效性。
敏感标记完整性	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。（第三级到第四级）	核实“不适用”的论证依据。

重要可执行程序完整性、重要可执行程序来源真实性	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。（第三级到第四级）	1.尝试修改访问业务服务器上重要程序和文件，查看完整性保护机制的有效性。 2.获取重要程序及其对应数字签名和数字证书（根据实际情况确定）。 3.不插入智能密码钥匙或插入未授权的智能密码钥匙（或其他鉴别设备、口令等），查看完整性保护机制的有效性。
日志记录完整性	采用密码技术保证日志记录的完整性。（第一级到第四级）	在JB交换机接入通信协议分析工具捕获通信数据，分析业务服务器（内置密码模块）是否被有效调用。尝试修改访问控制信息和日志记录（或对应的MAC），查看完整性保护机制的有效性。

（4）应用和数据安全

测评对象：应用系统管理员、数据库系统、待测系统业务应用、存储各类密钥的密钥管理平台、设计文档；

测评判定：对待测系统的应用和数据安全进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表8　应用和数据安全测评要求列表

测评项	测评指标	测评方法
身份鉴别	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。（第一级到第四级）	1）查看设计文档中身份鉴别采用的密码技术及实现机制； 2）访谈应用管理员，了解应用系统在对用户实施身份鉴别过程中是否使用了密码技术来实现用户身份信息的鉴别，具体采用了何种密码技术和安全设备。 3）核查专用密码产品，如密码算法模块、证书服务管理模块等是否具有国家密码管理部门批准的商用密码产品型号证书。 4）核查待测系统用户身份鉴别信息使用密码技术的正确性和有效性；在接入点JA使用网络协议分析工具，抓取报文，分析身份鉴别过程是否正确实现。
访问控制	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。（第一级到第四级）	1) 核查是否使用密码技术对访问控制策略进行完整性保护（如使用支持SM2/SM3/SM4算法的密码机/密码算法模块执行密码运算，对数据库表访问控制信息、重要资源敏感标记进行保护）；
重要信息资源安全标记完整性	采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。（第三级到第四级）	1）核实“不适用”的论证依据; 2）检查重要信息资源安全标记的保护措施。

数据传输机密性	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。（第一级到第四级）	1) 在接入点JA使用网络协议分析工具和密码算法合规性验证工具，捕获通信数据，分析系统是否使用SM4算法保证待测系统与XXXX之间交易数据传输机密性。 2) 查看系统所使用的密码算法、国密算法模块是否经过了国家密码管理部门核准；并截取相关关键数据，作为证据材料。
数据存储机密性	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。（第一级到第四级）	1) 在接入点JB接入网络协议分析工具，捕获业务服务器发往数据库服务器的通信数据，分析数据存储是否进行机密性保护； 2）在接入点JB（业务服务器和密钥管理平台之间）接入网络协议分析工具，捕获通信数据，分析密钥管理平台提供的加密功能是否被有效调用； 3) 查看系统所使用的密码算法、密码算法模块是否经过了国家密码管理部门核准；并截取相关关键数据，作为证据材料。
数据传输完整性	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。（第一级到第四级）	1) 通过JA工具接入点接入网络协议分析工具和数字证书合规性验证工具，捕获通信数据，分析待测系统业务服务器与XXXX之间的通讯数据是否使用国密算法数字证书进行签名和完整性保护。 2) 查看系统所使用国家密码管理局认可的密码算法、数字证书是否经过了国家密码管理部门核准；并截取相关关键数据，作为证据材料。
数据存储完整性	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。（第一级到第四级）	1) 在接入点JB接入数据包捕获工具，捕获业务服务器发往数据库服务器的通信数据，分析数据存储是否进行完整性保护。
不可否认性	在可能涉及法律责任认定的应用中，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。（第三级到第四级）	核实应用是否存在不可否认性的需求； 检测不可否认性的实现方式和密码算法（SM2算法）

（5）安全管理

测评对象：安全管理制度

测评指标：对安全管理制度进行现场测评。符合程度根据被测信息系统实际保护状况判定为符合、部分符合、不符合。

表9　安全管理测评要求列表

测评项	测评指标
人员安全	应了解并遵守密码相关法律法规。
	建立密码应用岗位责任制度
	建立上岗人员培训制度

	定期进行安全岗位人员考核
	建立关键岗位人员保密制度和调离制度
制度安全	具备密码应用安全管理制度
	密钥管理规则
	建立操作规程
	定期修订安全管理制度
	明确管理制度发布流程
	制度执行过程记录留存
建设运行安全	制定密码应用方案
	制定密钥安全管理策略
	制定实施方案
	投入运行前进行密码应用安全性评估
	定期开展密码应用安全性评估及攻防对抗演习
应急安全	应急策略
	事件处置
	向有关主管部门上报处置情况

6、测评实施流程

密码应用安全性测评实施流程图

（1）准备阶段

本阶段是开展密码测评工作的前提和基础，主要任务是掌握被测系统的详细情况，准备测试工具，为编制测评方案做好准备。

主要任务有：项目启动、信息收集与分析、工具和表单准备。

（2）方案编制阶段

本阶段是开展密码测评工作的关键活动，为现场测评提供最基本的文档和指导方案。

主要任务有：测评对象确定、测评指标确定、测评工具接入点确定、测评内容确定、测评方案编制。

（3）现场测评阶段

本阶段是开展密码测评工作的核心活动，按照测评方案的总体要求，严格执行测评实施手册，分步实施所有测评项目，包括单元测评和整体测评两个方面。

主要任务有：测评实施准备、现场测评和结果记录、结果确认和资料归还。

（4）分析与报告编制阶段

本阶段是给出密码测评结果的活动，对被测系统国产密码整体安全保护能力做出综合评价的活动。

主要任务有：单项测评结果判定、单元测评结果判定、整体测评、风险分析、密码测评结论形成、密码测评报告编制。

7、测评实施计划

（1）项目组构成

工作实施组

工作实施组负责具体项目的实施与测评工作，为被测方密码测评项目提供足够证据。工作实施组由招标主体、测评机构组成工作实施组具体负责测评工作推进实施并向主管部门汇报沟通，测评机构成立测评实施小组，负责目标系统的商用密码应用安全性测评工作。

测评实施小组的主要工作包括：

审阅已提交的测评申请文档资料

制定密码测评技术方案

制定密码测评项目工作计划

现场安全技术性测试

撰写现场安全评估初步结果声明文档

撰写综合密码测评报告

项目协调小组

项目协调组由被评估方委派相关人员组成，能够在必要时有效调动其他部门人员。测评机构与招标主体分别成立项目协调小组协助测评实施小组做好测评工作。

项目协调小组的主要工作包括：

被评估方为评估实施小组提供现场办公场所，安排会议地点。

被评估方应确保评估方能及时与本次安全评估有关的人员交流和接触。

被评估方应提供必要的测评及核查条件，如测试环境、管理文档、技术资料、会议地点等等。

（2）项目实施计划

表10　项目实施计划表

阶段	任务	
测评准备阶段	实施方案制定	内部项目启动会议
		根据系统规模成立项目组、编制项目计划书
		与被测方沟通，填写信息采集表
		实施方案编写
	测评对象确定	被测系统整体结构、边界、网络区域、重要节点、测评对象等。
	测评指标确定	选择相应等级的安全要求作为测评指标。
	测评工具接入点确定	结合网络拓扑图，选择测试路径。
	测试内容确定	确定单元测评
	测评方案编制	测评内容、测评实施计划
现场测评阶段	现场测评准备	召开现场首次会议。授权书、确认资源、必要的测评程序更新。
	现场测评和结果记录	人员访谈、文档审查、上机验证、工具测试
	结果确认和资料归还	召开现场结束会议，确认现场问题。
非现场综合	结果判断、整体测评、风险分析	
报告出具阶段	综合评估及报告生成	

六、预期成果交付物

密码测评工作结束后，根据测评内容记录各系统的密码应用现状，出具各系统的《信息系统密码测评报告》。测评报告中以密码应用基本要求为基准，逐项比对各被测系统密码应用的符合性、规范性和正确性，对与标准存在差异的检查项。

序号	交付物名称	介质形式
1	《商用密码应用安全性评估报告》	电子和纸质
2	《整改建议书》	电子和纸质

同时，测评工作也可对现有密码应用测评标准测评内容的准确性进行验证，根据各信息系统密码应用现状和行业应用需求，总结共性问题，指出密码应用改造的难点、疑点和下一步工作计划。

七、售后服务

（一）服务内容

投标人需向招标人提供包括安全培训、配合检查、安全咨询等相关服务。具体服务内容如下：

1、安全培训：在项目实施过程中或在项目实施结束后，通过安全培训使有关人员加深对密码安全工作的掌握程度，并对行业内的最佳实践案例进行分享，从而达到将密码安全工作与信息系统、安全设备的安全运维工作相结合的状态。

2、根据需要组织开展信息安全服务培训，通过大量的当前典型安全事件导入，从感性认知层面对目前的信息安全威胁给予直观、形象的描述，加深对当前信息安全威胁的认识。

3、配合检查服务：投标人免费协助招标人响应密码管理局、单位内部以及第三方机构针对商用密码应用安全性评估工作的检查工作。服务内容包括协助招标人进行系统资料准备、完善各类资料文档，配合检查过程中的答疑及技术支持及其他现场检查的响应。

4、安全咨询服务：投标人为招标人免费提供一年技术咨询服务，包括新建信息系统密码安全建设方案咨询服务以及其他相关安全咨询服务，技术服务工程师在接到招标人服务请求后应立即响应，帮助客户解决信息安全相关技术问题，全面配合招标人做好业务系统安全保障工作。

（二）备案工作

对系统进行密评备案工作，取得商用密码应用安全性评估报告后，按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案，并协助招标人获得相应密评备案证明。

（三）培训工作

供应商应提供相关的技术、管理等人员安全方面培训，培训方式包括现场培训和集中培训。供应商须提供培训方案，最终的培训方案以项目启动后商定的详细培训方案为准。培训内容应包括测评、整改指导等，并提供全套培训教材和培训计划表。

（四）合同履行期限及地点

1、合同履行期限：自甲方通知入场评测之日起30个日历日内出具《商用密码应用安全性评估报告》和《整改建议书》。

2、服务地点：采购人指定地点。

八、违约责任

（一）按《中华人民共和国民法典》中的相关条款执行。

（二）未按合同要求提供服务或服务质量不能满足服务方案与措施要求，采购单位有权终止（或解除）合同，并对供应商违约行为进行追究。

采购包5：

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：第三方审计

参数性质	序号	技术参数与性能指标
	1	一、项目概况 陕西省政府网站集约化省级平台（三期）项目主要内设内容为集约化省级平台在信创环境适配改造、集约化省级平台的升级扩建、省级部门网站改造、网站数据迁移、OFD版式支撑软件、安全服务支撑系统建设，本次为采购该项目的财务决算专项审计。 二、商务要求 1、服务期限：接受采购人提报完整的审核资料后30天内完成审计任务。 2、质量标准：达到国家现行法律法规及行业要求合格标准。 3、付款方式： 审计进场后一周内先行支付30%，出具成果文件后一次性支付70%。 与本合同项目相关的所有费用，不因任何因素调整合同总价； 如有特殊情况，付款方式与采购人协商解决。 支付方式：银行转账 结算方式：乙方持发票、中标通知书、合同与甲方结算；甲方支付价款前，乙方应向甲方提供正式等额、合法合规并符合甲方要求的增值税普通发票，否则，甲方有权拒绝付款并不承担任何逾期付款的违约责任。 三、审计目标 通过审计，全面了解项目建设的实际情况。审查项目建设资金筹措、到位、管理和使用情况；核实项目竣工决算的真实、合法、有效性；揭示项目在基本建设程序、建设管理和建设资金使用等方面存在的问题，进一步强化审计监督在“健全制度，强化监督，促进管理，提高效能”等方面的作用。

采购包6：

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：第三方软件测评

参数性质	序号	技术参数与性能指标
		一、项目概况 陕西省政府网站集约化省级平台（三期）项目建设内容包括： 1.集约化省级平台信创适配改造。基于信创云提供的国产芯片、国产操作系统、国产数据库、国产中间件等基础环境，完成集约化省级平台一、二期项目已建子系统的信创适配改造。 2.集约化省级平台升级及扩建。基于集约化省级平台一、二期项目的建设成果，完成智能搜索系统升级、统一问答知识库建设、政务新媒体矩阵建设、网页预归档系统建设。 3.省级部门网站改造。基于信创适配改造和升级扩建后的集约化省级平台，完成未集约整合的 36 个省级部门网站开发及无障碍改造（PC 端网站开发、移动端网站适配、长者版适配、无障碍改造），完成一期 10 个试点省级部门网站适老化与无障碍改造（长者版开发、无障碍改造）。 4.网站数据迁移。完成 36 个省级部门网站数据迁移，将网站各类数据从原有网站系统迁移到信创适配改造和升级扩建后的集约化省级平台；将一期项目建设的 11 个网站（省政府门户网站和 10 个试点省级部门网站）从现有环境的集约化省级平台迁移到信创适配改造和升级扩建后的集约化省级平台。 5.为网页预归档系统的文件转换提供支撑，采购 OFD 版式支撑软件。 6.建设安全服务支撑系统。建设以国密算法为基础的政府网站集约化应用安全服务支撑系统，采用内控外防技术措

施，实现网站管理人员、信息发布人员、运维人员和审核人员的身份真实性验证，为集约化省级平台提供电子存证与可追溯能力，利用 SSL 加密协议实现数据加密传输，提升集约化省级平台和全省 47个（省政府门户网站及 46 个省级部门网站）省级部门网站的统一管控能力。。

二、商务要求

1.服务地点：采购人指定地点；

2.服务期限：具备测试条件开始至测试完成并出具测试报告止；

3.质量要求：合格、符合国家相关标准要求；

4.团队要求：在项目实施周期内，项目组成员应专职于本合同内的项目工作，未经采购人同意不得随意更换项目负责人及参加项目的其他人员。（供应商需提供“不更换项目人员承诺书”格式自拟）

三、技术要求

1、测试依据

本次测评需要依据的文件：

1.GB/T 25000.51-2016《系统与软件工程系统与软件质量要求和评价（SQuaRE）第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则》；

2.项目相关软件开发设计文档；

3.采购人出具的相关行业标准及其他具体意见和要求；

4.经由采购人确认的项目蓝图、项目实施单，项目造价过程中审定的功能点清单；

5.开发方提供的其他相关技术文档。

2、测试流程

供应商应严格按照流程进行测试，包括测试计划制定，测试需求分析，测试设计，测试环境准备，测试执行，回归测试和测试总结。

3、总体技术要求

3.1评测内容要求

为了保证系统项目质量，供应商应从应用系统的功能、性能效率、可靠性等多个方面开展测试，对委托测试的系统进行全面充分的检验，重点测试各系统中定制化开发的模块、功能。

（1）功能测试需求：功能性测试依据测试需求中的技术要求，并结合用户对系统建设的整体功能方向，对系统内涉及到的所有功能逻辑、功能项进行全覆盖测试，包括陕西省政府网站集约化省级平台（三期）项目建设包括的软件系统进行测试，发现潜在的缺陷和问题，使软件在部署之前能够达到预期的质量标准，安全可靠运行，减少实际使用过程中软件故障和崩溃的风险，提高软件的可靠性。

（2）性能测试需求：核实系统在所指定的业务功能在正常的预期工作量、预期峰值工作量下的处理时间及资源利用率能够满足实际业务需求，充分考虑省政府门户网站及省级部门网站长期运行后数据量大量增长的实际情况，确保前台公众访问和后台运维人员操作的响应性能，性能需求主要参考WEB 应用性能指标展开分析。

1.网站群用户数及并发数需求

根据对《2022 年度陕西省政府门户网站和省级部门网站年度公开报表》的调研统计，当前陕西省政府门户网站平均每日访问量约为 70000，省级部门网站日访问量从几千到几万不等。通过本期项目建设，完成剩余 36 个省级部门集约整合，集约化省级平台将支撑47个网站（省政府门户网站及46个省级部门网站），预计日均总访问量为 400000 人次。最大用户数按照日均访问量的 20% 计算：最大在线用户数=400000*20%=80000。最大并发用户数按照日均访问量的 5‰计算：最大并发用户数=400000*5‰=2000。

2.网站群前端性能指标

在 2000 并发下，网站群性能指标需求如下：

（1）页面功能切换≤2 秒；

	1	（2）信息浏览≤2 秒； （3）一般查询端≤2 秒； （4）表单提交≤3 秒； （5）复杂报表端≤5 秒； （6）页面刷新时间≤2 秒； （7）满足系统自身运行性能需求，以及保证系统稳定运行保留的处理能力冗余。 3.平台用户数及并发数需求 陕西省政府网站集约化省级平台共需支撑不少于 47 个网站，每个网站后台使用人员按照不少于 10 人预估，后台用户约 500 人。同时平台能够注册和创建的用户数不受限制，可以根据实际需要进行用户账号新建。集约化平台后台最大在线用户数为按照总用户数的 60%计算，后台最大在线用户数为 300 人。最大并发用户数按照总用户数的 40%计算，最大并发用户数为 200 人。 4.平台性能指标 在 200 并发下，集约化省级平台能指标需求如下： （1）系统支持良好的大规模并发发布效率，200 个并发下，系统操作及服务响应时间不超过 3 秒； （2）200 名编辑同时发布单篇文档的平均时间为 3 秒以内； （3）满足系统运行性能需求，以及保证系统稳定运行保留的处理能力冗余； （4）满足未来更多数据源单位的系统对接和数据共享。 5.前台性能指标 根据对《2022 年度陕西省政府门户网站和省级部门网站年度公开报表》的调研统计，当前陕西省政府门户网站平均每日访问量约为 70000，省级部门网站日访问量从几千到几万不等，因此陕西省 46 个省级部门网站及省政府门户网站每日总访问人数总计可达 400000 人左右。 在 2000 并发下，前台性能指标需求如下： （1）页面功能切换≤2 秒； （2）信息浏览≤2 秒； （3）一般查询端≤2 秒； （4）表单提交≤3 秒； （5）复杂报表端≤5 秒； （6）页面刷新时间≤2 秒； （7）满足系统自身运行性能需求，以及保证系统稳定运行保留的处理能力冗余。 （3）系统安全性测试需求：核实所测试业务系统的安全性是否达到各系统安全性要求，从软件运行过程中是否拥有有效的用户登录、远程访问等信息验证机制及权限管理机制，发现软件在运行过程中，信息及数据的泄漏、重要数据的丢失、非法入侵、非法操作，定位软件安全漏洞和缺陷。 （4）可移植性测试需求：系统、产品或组件能够从一种硬件、软件.或者其他运行(或使用)环境迁移到另一种环境的有效性和效率的程度。主要从集约化省级平台在满足国家信创环境，使用国产操作系统、国产数据库和国产中间件等基础软硬件运营环境，确保集约化省级平台在信创环境下正常运行适应性 （5）可靠性测试需求：系统应满足用户的各项应用要求，稳定、可靠、实用，界面友好，操作方便，兼容性体验良好，检索简单快捷。系统有效运行时间大于 99.9%。系统需采用分布式集群部署，其中任意一台发生软硬件故障，不影响其他服务器，即服务不会中断。 （5）用户文档集测试：软件验收所要求提供的文档按照规定要求实现。 3.2评测结果要求 供应商根据项目建设方案、谈判采购文件、委托书、合同、技术文档等其他有效文件为参考，编制需求规格说明书

		，设计测试实施方案，并取得采购人认可。 可测试的功能点100%作为测试需求；测试需求100%被测试用例覆盖；测试用例100%被实施。 对项目需求规格说明书中明确的所有软件指标（性能、性能、信息安全性、兼容性等）进行测试、核对，测试要满足规格说明书中的各项指标。对项目软件设计说明书中明确要提交的文档进行测试，测试要满足说明书中的各项要求。 3.3评测单位责任 评测单位对所评测的功能点及最终出具的评测报告负有全部责任。 4、评测范围 根据项目建设方案、谈判采购文件、委托书、合同、技术文档等其他有效文件为参考，覆盖系统建设涉及所有模块和关键功能节点。 5、测评成果 项目现场测评工作实施完成后，根据相关要求，最终出具加盖检测机构印章的《软件测评报告》。 6、交付计划 供应商项目组负责制定《项目测试计划》并按进度完成各阶段工作任务，按时提交阶段成果。 1.供应商提供的测试相关文件内容必须正确、完整，能充分满足系统测试要求。 2.对供应商所提资料的要求： （1）供应商所提供的文件如有修改，供应商在新版中明确标示并相应提供文字说明。 （2）供应商所提交的技术资料内容至少应包括本测试报告、问题报告。 （3）供应商应在规定的时间内提供资料。 7、技术资料 （1）供应商提供的资料应使用国家法定单位制即国际单位制，语言为中文。 （2）资料的组织结构清晰、逻辑性强。资料内容要正确、准确、一致、清晰完整，满足使用要求。 （3）供应商资料的提交及时充分，满足项目上线进度要求。 （4）对于其他没有列入合同技术资料清单，确是工程所必需的文件和资料，一经发现，供应商也应及时免费提供。 四、付款方式 （1）合同签订后七日内，甲方向乙方支付合同总价的60%， （2）乙方完成全部测试并出具全部测试报告后七日内，甲方向乙方支付合同总价的40%。 五、其他要求 对于测试验收中发现的问题应及时与采购人沟通，能现场整改的应要求施工方随进度整改；不能现场整改的要向采购人提交说明材料，并协助采购人确定整改期限。整改完成后需要进行复测复验的，不再收取任何费用。

3.2.3人员配置要求

采购包1：

服务期内，供应商应组建不少于5人的本地化服务团队，向用户提供 7×24 小时的故障技术支持服务，30分钟响应； 如在 60 分钟内无法远程解决用户提出的服务要求，必须在报修 2小时内派工程师到达现场。故障问题解决后 12 小时内，向使用单位提交问题处理报告，说明问题种类、问题原因、问题解决中使用的方法及造成的损失等情况

采购包2：

投标人需为本项目派驻总监理工程师1名，总监理工程师代表1名，专业监理工程师不少于2名。

采购包3：

满足采购人需求