**检察全流程可信子系统采购需求**

# 项目概况

2017年6月，最高检印发了《检察大数据行动指南（2017－2020年）》，提出要顺应信息化发展趋势，贯彻落实国家大数据战略，深化刑事案件的改革创新举措，积极探索完善轻微刑事案件和解工作机制等新时代检察院的重点工作。

2019年10月，中共中央政治局就区块链技术发展现状和趋势进行第十八次集体学习时强调“区块链技术的集成应用在新的技术革新和产业变革中起着重要作用，要把区块链作为核心技术和自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展”，本次会议将区块链技术上升为国家战略。

2021年1月，中国中央印发《法治中国建设规划（2020－2025年）》，规划提出要全面建设“智慧法治”，推进法治中国建设的数据化、网络化、智能化，优化整合法治领域各类信息、数据、网络平台，推进全国法治信息化工程建设。

2021年4月，最高人民检察院制定下发《“十四五”时期检察工作发展规划》，对未来五年检察工作进行谋篇布局。**《发展规划》要求，推进智慧检务工程建设，加强大数据、人工智能、区块链等新技术应用。**全面应用统一业务应用系统2.0，持续优化流程办案、辅助办案、数据应用和知识服务功能。加快推进智慧检务创新平台、视频云平台、融媒体平台等建设，提升检察工作智能化水平。

**2021年12月由最高人民检察院、最高人民法院、司法部以及上海、江苏、江西三地法检司单位共同参与的科技部司法区块链关键技术及典型应用示范研究课题正式启动，为区块链技术在检察领域横、纵向的创新应用奠定了前沿的技术基础。**

2022年6月全国检察机关数字检察工作会议召开，最高人民检察院张军检察长，在会上提出要加快数字检察建设，以“数字革命”驱动新时代法律监督提质增效，推进“数字赋能监督，监督促进治理”的法律监督模式变革。

2023年4月，最高人民检察院印发《关于加强新时代检察机关网络法治工作的意见》，提出要注重发挥新技术对检察履职赋能作用。积极推动网络司法规则制定，探索具有中国特色的网络检察工作模式和路径，不断推进网络时代检察理论创新、实践创新和制度创新。

2024年1月，国家区块链创新应用试点总结交流会召开，会议强调，要加强跟踪研判，准确把握区块链技术应用发展新趋势新挑战，要把握工作重点，坚持创新驱动、系统谋划、需求导向、协同联动、规范发展，**扎实推进区块链创新发展再上新台阶**。会议通报了国家区块链创新应用试点终期评估情况，发布了《中国区块链创新应用发展报告（2023）》，**其中上海市人民检察院作为“区块链+检察”应用领域优秀试点单位，向大会做了“区块链赋能数字检察 打造上海检察全流程全息在线办案体系”的专题汇报。**

区块链技术，作为数字经济、数字社会的底座，其自带的分布式账本、共识算法、数据防篡改、零知识证明、智能合约可信计算等核心技术能力，可以为法治工作提供最重要的“可信数据”及“可信计算”技术保障。通过区块链+检察特色领域试点应用，在数字检察体系内，市检察院构建了一种新的数据信任与安全保障体系，在推进数据共享与跨部门协同、优化司法服务流程与提升司法公信等方面可以发挥巨大的作用，对于推进法治国家、法治政府、法治社会一体建设，具有十分重要的推动作用。

# 建设目标

贯彻落实党中央，市委，市政府对区块链领域创新发展工作的决策部署和最高人民检察院关于加强区块链应用意见的要求，上海检察院积极运用区块链技术大力推进数字检察的建设。

平台依托于最高检区块链，借助区块链可信计算的特点，为区块链可信应用提供上链存证、固证、核验、智能合约等基础服务。

构建跨链协同平台，实现异构/同构区块链间业务互通。

通过构建电子文书全生命周期可信管理系统，实现电子文书管理的全面数字化转型。

建设电子档案全流程可信应用模块，加强电子档案形成全过程流转中安全可信和链上可视化监管，促进全流程网上办案规范化。

# 项目建设内容

本项目通过区块链+检察特色领域试点应用，在数字检察体系内，市检察院构建了一种新的数据信任与安全保障体系，在推进数据共享与跨部门协同、优化司法服务流程与提升司法公信等方面可以发挥巨大的作用，具体建设内容如下：

1. **检务可信应用管理**

在检察工作网和互联网分别建设检务可信应用管理平台，包含区块链业务系统管理、区块链应用管理、统一接口管理、智能合约管理、运行监测管理、应用数据管理等模块。

1. **跨链协同平台**

建设跨链协同平台，包含接入管理、跨链协同事务管理、跨链协同业务流程管理、跨链网关、跨域网关、运行预警管理、工单管理、消息中心、平台管理、协同管理信息同步等模块。

1. **电子文书全流程可信应用**

建设电子文书全流程可信应用，包含电子文书可信存证、电子文书可信协同、电子文书可信流转、电子文书核验及溯源助手等模块。

1. **电子档案全流程可信应用**

建设电子档案全流程可信应用，包含电子档案可信收集、电子档案可信检测、电子档案可信利用等模块。

## （一）、检务可信应用管理

### 1、区块链业务系统管理

区块链应用场景繁多，需灵活支持不同的业务条线，涉及对接的业务系统复杂、繁多，为强化管理，应构建统一的区块链业务系统管理模块，实现对涉链系统的统一管理。

#### （1）注册及接入

对申请接入可信应用管理的申请者进行身份管理，申请者以业务系统为身份进行注册管理，注册时需明确技术支持单位，并留下联系方式。注册字段包括接入系统名称、密码、技术支持单位、联系方式、网络类型、接入说明。

#### （2）审批与授权

检察院管理员可对申请接入可信应用管理的业务系统进行审批与授权。通过待申请列表查看注册申请，查看接入系统名称、技术支持单位、接入说明来决定是否允许该系统接入可信应用管理。

#### （3）禁用与冻结

通过接入系统列表管理已接入的系统，可以查看接入系统名称、技术支持单位、接入说明、接入时间、有权接口等信息，也可以控制禁用与冻结该系统的接入权限。

#### （4）接入凭证

经检察院审批通过后，业务系统可使用系统名称和密码登陆分平台。登陆后可查看个人信息以及申请接口。个人信息中除展示系统名称、支持单位等注册信息外，还会展示acesskey信息，acesskey是系统在调用接口时的凭证，调用接口时需提供。

### 2、区块链应用管理

构建统一的区块链应用管理模块，对所有接入的区块链的应用进行统一登记，并以应用为管理域，进行应用内数据、智能合约、跨链协同的统一管理。

#### （1）区块链应用创建

支持接入的业务系统自行建立区块链应用，并基于区块链应用实现存验证、智能合约等区块链能力的调用。

#### （2）应用信息管理

对区块链应用信息进行维护，包括应用名称、建设日期、描述、创建业务系统、涉及业务系统、对接区块链、应用分类、业务分类、建设主体、使用主体、用户对象、行业领域等。

#### （3）区块链应用冻结

将已失效的区块链应用进行冻结，冻结后无法使用。

#### （4）统一接口管理

在区块链应用内可查看当前应用全量的接口、智能合约信息和源码信息，支持对接口信息的新增、查询、冻结等操作。

### 3、统一接口管理

应支持统一的对外服务接口管理，结合业务需求产生的数据存验证接口、定制的合约调用、跨链协同调用等接口均应纳入统一管理范围。支持接口权限控制、异常使用监测与自动熔断机制。

#### （1）接口配置

由系统管理员根据检察院业务部门的要求对接口进行预先创建，供获得授权的接入系统选择调用。

#### （2）接口参数配置

接口参数包括入参、返回值，入参字段需设置字段名称、是否必填、最大长度、是否为索引字段、是否需单独验证等。验证接口会随存证接口配置完成一并完成，可使用索引字段对存证字段进行整体或独立验证。

1）主数据结构配置

针对结构化类数据存证，可配置每个字段的字段名、类型、是否必填、是否引用等

涉及到子数据的字段，可在子数据结构配置中设置每个字数据的字段名、类型、是否必填、是否引用等

2）hash存证

针对只上传hash的文件或数据，系统支持hash类数据存证非结构数据存证。针对需要上传文件本体的场景，系统支持非结构化数据配置

#### （3）接口生成

根据已配置好的接口参数，系统可自动生成相应的接口，包含存证、核验、查询等。

#### （4）接口文档获取

业务人员可选择相应的接口，并输入相应的url即可获取完整的接口文档。

#### （5）接口列表概览

系统支持展示全量接口信息，展示内容包含接口名称、地址、描述、所属目录、所属应用等信息。

#### （6）接口详情

点击接口信息即可查看当前接口全量信息，包含接口基本信息、入参信息、返回信息等。

#### （7）接口查询

支持按照多维度接口查询，包含名称、所属目录、状态、调用系统等。

#### （8）接口申请

接入可信应用管理的业务系统，可申请接口服务；点击“新增申请”，查看可使用接口清单，接口清单支持根据接口类型、业务方向进行快捷筛选。

### 4、智能合约管理

面向区块链应用，应支持统一的智能合约管理功能。包括合约登记、审批、发布、合约凭证管理、业务系统绑定与认证、用户授权、调用、反馈等行为记录审计等功能。

#### （1）智能合约编辑器

合约编辑器是开发者开发智能合约的窗口，提供了编辑工作空间、代码编写、代码提示等功能。开发者可在工作空间中管理、添加、移动、删除文件夹或代码文件。其中文件管理支持新建打开本地文件、链接本体主机获取文件。合约代码编写完成后，可进行编译。

#### （2）智能合约编译器

合约编译器可对已经编写完成的智能合约进行编译，支持自动编译、隐藏警告、包含每日构造版本等编译过程可选设置，可对编译的脚本直接执行。支持根据URL添加自定义编译器。

#### （3）智能合约调试器

智能合约调试器，可对预发布的智能合约进行调试，其中Solidity合约支持使用生成的源进行调试，调试过程日志可在IDE下方窗口输出。调试时可选择监听所有链上事务，能够按交易哈希或地址进行检索。

#### （4）智能合约源码管理

应支持智能合约源代码登记、审计、核验等功能，应当记录合约信息、源码版本号、合约编程语言、合约技术类型等信息，由于合约发布后不可删除，只能更新或冻结，为确保编译后的合约与源码一致，应提供合约源码核验服务，可对当前登记的合约字节码与源码一致性进行核验，确保源码编译后的字节码与登记的一致。

#### （5）智能合约登记

智能合约的登记，应支持合约基本信息、合约初始管理状态信息、合约调用初始权限信息、合约管理权限信息的录入保存。

#### （6）智能合约审批

支持自定义的审批控制，支持相关管理员对登记的区块链智能合约进行审批，只有审批通过的智能合约才能发布。

#### （7）智能合约发布

支持自定义的发布控制，支持相关管理员对审批通过的区块链智能合约进行发布操作，发布的智能合约将固化在区块链中，根据预设的权限进行调用控制。

#### （8）合约列表概览

系统支持展示全量合约信息，展示内容包含合约名称、地址、登记编号、梨树区块链、所属应用等信息

点击合约信息即可查看当前合约全量信息，包含基本信息、合约状态、合约接口信息等。

支持按照多维度合约查询，包含名称、地址、梨树区块链、状态、合约技术等。

#### （9）合约禁用

针对已失效的合约，系统支持禁用功能，禁用后，当前合约失效

#### （10）智能合约部署和发布中心

对于测试确认无误的智能合约，支持统一部署发布，部署发布时，需指明发布环境、发布账户并设置与该合约相关合约的地址信息。应记录当前已部署的合约列表。

### 5、运行检测管理

#### （1）应用运行管理

为管理员展示应用运行情况，包括应用名称、对接系统、服务状态、响应时间等信息。

#### （2）异常数据检测

在办案过程中各个节点办理记录的结构化数据存证、验证过程一旦发现调用异常的，对异常数据提供预警提示功能，提醒业务人员。

#### （3）异常数据分析

提供异常数据的分析功能，包含存证异常、数据验证不通过、合约调用异常情况分析。

#### （4）风险预警管理

提供区块链服务异常预警监测功能，并对异常情况进行预警。预警内容包含节点磁盘水位预警和接口调用异常监控。

#### （5）日志审计

提供日志数据的全生命周期管理，统一汇聚日志数据，基于异常日志实时告警帮助运维人员快速发现问题、分析问题。

### 6、应用数据管理

#### （1）区块链应用数据概括统计

1）区块链应用分类统计

将存验证应用数量、调用数量，合约应用数量、合约调用数量，根据网络环境、业务分类等维度进行统计。可通过变更统计时间查看不同时间段的数量。点击业务分类的统计数据跳转至业务应用列表。

2）业务应用列表

展示全部应用的基本信息及数据，包括应用名称、调用次数等。提供统计时间、业务分类、接口类型、调用系统等筛选条件。变更筛选条件后，应用的统计数据也会改变。点击应用卡片可进入应用详情页。

3）应用详情

应用详情页可查看当前应用的基本信息，包括应用基本信息、接口目录、智能合约目录等。并可查看调用记录明细

调用记录列表展示每一条调用记录，包括调用人、调用时间、存证内容/验证结果/合约判断结果、交易哈希。

点击调用记录列表中的信息可跳转至案件记录明细，展示每个调用记录的详细入参信息。

4）接口调用分析

存验证接口管理列表中提供接口调用分析功能。统计全部接口数量的增长情况，各业务类型分布情况。还统计接口调用数量的增长情况，及各业务类型分布情况。

5）合约调用分析

提供合约调用分析功能，包含合约数量的增长情况，各业务类型分布情况、合约调用数量的增长情况、各业务类型分布情况等。

#### （2）电子档案全流程可信应用分析

1）电子档案存证分析

提供电子档案全流程各业务环节的存证分析，包括数据统计、存证列表、详情。数据统计包括存证态势分析、操作行为分布分析。存证列表展示操作人、存证时间、文件名称、文件哈希等核心信息。详情展示具体业务信息。

2）电子档案异常分析

提供电子档案全流程各业务环节异常数据分析，包括异常状态发生时间点、异常状态、异常业务流程点等

3）电子档案智能合约应用分析

提供电子档案全流程各业务环节的合约调用分析，包括合约调用统计、调用列表、详情。包括合约态势分析、调用结果分布。列表展示操作人、调用时间、调用结果等核心信息。详情展示具体合约信息。

## （二）、跨链协同平台

### 1、接入管理

接入管理负责跨链协同参与要素，如区块链、跨链网关、业务系统、组织机构等信息登记、身份真实性验证，以及正确开展跨链协同所必需的能力评估测试认证信息管理。

#### （1）区块链接入管理

包含区块链登记认证、区块链接口完备度评测、区块链调度合约功能评测、区块链接入审批、已登记区块链列表概览、已登记区块链查询、已登记区块链详情查看、已登记区块链信息修改等

#### （2）跨链网关接入管理

包含新建跨链网关登记认证、跨链网关接口完备度评测、跨链网关接入审批、已登记跨链网关列表概览、已登记跨链网关查询、已登记跨链网关详情查看、已登记跨链网关信息修改等

### 2、跨链协同事务管理

跨链协同事务管理负责跨链协同事务的创建、运行监控、质效分析、开通许可授权等管理工作。

#### （1）跨链协同事务维护

包含跨链协同事务创建、跨链协同事务应答、跨链协同事务列表概览、跨链协同事务查询、跨链协同事务详情查看、跨链协同事务运行状态控制等。

#### （2）跨链协同事务实例管理

包含跨链协同事务实例列表概览、跨链协同事务实例查询、跨链协同事务实例详情查看。

#### （3）跨链协同事务质效分析

包含跨链协同事务数量统计分析、跨链协同事务链路性能分析、跨链协同事务发起网关参与情况统计、跨链协同事务接收网关参与情况统计、跨链协同事务途径网关参与情况统计

#### （4）跨链协同事务运行监控

包含跨链协同事务运行链路状态分析、协同事务区块链运行趋势分析、协同事务跨链网关运行趋势分析等。

### 3、跨链网关

建设检察区块链协同服务平台跨链网关，具备实现异构跨链过程中的交易捕获、信息传输以及身份验证等能力，提供跨部门同构、异构区块链平台的跨链交互底层能力支撑，实现对跨链可信协同过程中的跨链数字身份认证、跨链任务监听、数据跨链发送、数据跨链接收、跨链合约调用、跨链协同回执等服务，满足本期项目建设过程中对电子换押场景的支持。

跨链网关通过接口适配，支持对接各种区块链底层平台，跨链网关在协同平台上完成登记及认证，获取跨链授权凭证，实现与外单位（如法院）的区块链跨链协同。

### 4、跨域网关

建设检察区块链协同服务平台跨域网关，主要用于支撑检察区块链在3个网域之间的数据流转应用，跨域网关对跨域数据进行封装，并通过不同网域间安全边界进行数据跨域安全传输，实现网域间区块链跨链协同，满足不同网域可信协同过程中跨域数字身份认证、跨域任务监听、数据跨域发送、数据跨域接收、跨域合约调用、跨域协同回执等服务。

### 5、运行预警管理

运行预警管理模块负责创建和管理协同管理平台中的各类预警规则，支持对预警规则进行设置、预警监查、通知订阅、提供预警信息。

#### （1）预警设置

预警设置为协同管理平台运营人员提供交互界面，对各种可监控预警的点依据自身的预警策略设置预警阈值。

#### （2）预警监查

平台对参与协同的各类要素进行监测，并根据预设规则进行预警提示。

#### （3）通知订阅

通知订阅模块负责将预警通知信息向设定的预警通知通道中进行发送，如短信、邮件、管理平台界面等。

#### （4）预警信息

提供预警通知查阅功能，便于协同管理平台运营人员了解预警的具体信息。

### 6、工单管理

工单管理负责为协同管理平台运营人员提供工单管理功能，如工单发起、工单应答。

#### （1）工单创建

工单创建是在出现需要运维人员干预的异常事项时，运营人员可通过此界面创建运维工单，与其他协同单位一同排查修复异常。

#### （2）工单级别定义

运维人员在创建工单时，可以根据实际异常情况，维工单定义不同的优先级别，主要包括：“紧急、重要、一般、次要”四个级别。

#### （3）工单应答

协同管理平台在收到运维工单后，通过多种通知手段告知工单指定的应答方，以便其及时进行后续的运维处理工作。工单应答负责展示特定运维人员需要处理的运维申请，并通过运维工单中的信息清晰了解运维工作相关的详细信息，并及时将运维处理结果反馈给运维申请人员。

#### （4）工单列表概览

协同平台呈现当前已经接收的所有工单信息列表，包括工单编号、工单类型、优先级、标题、状态、状态变更时间、受理方组织名称等信息。

平台支持对工单进行查询检索，可通过工单编号、工单类型、工单状态、优先级等内容进行查询。

平台可查看协同工单具体信息内容，以辅助运维人员进行分析排查，内容包括所含附件内容。

### 7、消息中心

消息中心模块负责管理协同管理平台支持的事件通知手段，以及协同管理平台中所有通知信息。支持查看系统通知、工单处理通知、接入处理通知、监控预警通知、通知查询、通知详情查看等

### 8、平台管理

平台管理模块负责管理协同管理平台自身的相关配置信息和平台管理员账户管理。包括平台信息维护、平台管理员信息维护。

### 9、协同管理信息同步

协同管理信息同步管理负责在不同的协同集成管理平台间建立信息交换通道，将跨链协同管理信息准确、安全、可靠的传递给特定的区块链协同集成管理平台，最终实现区块链协同集成管理业务联动。为此需保证各个协同平台之间有高效稳定的数据同步。

#### （1）协同管理平台信息同步

协同管理平台是一套分布式协同平台，单个分平台部署后或信息更新后，需将本平台的基本情况与其他分平台进行同步，确保各个协同平台保持信息一致。

#### （2）区块链信息同步

平台通过底层接口将当前本协同管理平台认证接入的区块链信息同步给跨链协同的另一方协同管理平台以及其他协同平台，并获取其他协同平台登记认证的区块链信息，从而减少接入登记信息的重复登记和认证。

#### （3）跨链网关信息同步

平台通过底层接口将当前本协同管理平台认证接入的跨链网关信息同步给跨链协同的另一方协同管理平台以及其他协同平台，并获取其他协同平台登记认证的跨链网关信息，从而减少接入登记信息的重复登记和认证。

#### （4）业务系统信息同步

平台通过底层接口将当前本协同管理平台认证接入的业务系统信息同步给跨链协同的另一方协同管理平台以及其他协同平台，并获取其他协同平台登记认证的业务系统信息，从而减少接入登记信息的重复登记和认证。

### 10、跨链协同应用

打通与数据局区块链平台，实现可信业务交互，提供跨链可信数据共享、跨部门智能合约调用等服务。

#### （1）检察院案件信息协同

将人民检察院依法要求，需要向社会发布的案件信息，通过跨链模式推送到数据局区块链平台中，借助数据局存证中心向社会公众展示。

#### （2）公益诉讼协同

获取在数据局存证的公益诉讼线索信息和证据信息跨链到检察办案系统中，并支持进行跨链核验，确保原始数据的真实性。为检察官提起公益诉讼提供数据支撑。

#### （3）法律援助协同

基于区块链实现法律援助办案数据、电子材料的源头上链存证以及和司法行政机关的协作信息存证。利用可信验证全程可信监管，保障案件在办理过程安全可信和防篡改，保障办案材料效力。加强法律援助案件办理过程中人民检察院、司法行政机关的可信协作配合。

## （三）、电子文书全流程可信应用

通过构建电子文书全生命周期可信管理系统，实现电子文书管理的全面数字化转型。该系统包括电子文书及信息存证、电子文书溯源助手等内容。

### 1、电子文书可信存证

针对文书本体存证、结构化存证进行统一管理，便于快速检索至任意一条存证记录。

#### （1）电子文书本体存证

将检察院生成的电子文书进行固化和存证，通过智能合约上链保存，从而保证文书的原始性和真实性。这一过程不仅能增强文书的可信度，也为后续的法律程序提供了坚实的数据基础。

#### （2）电子文书结构化数据存证

对电子文书内的结构化数据进行固化和存证，为后期智能合约调用提供数据支撑

对电子文书进行的处理操作信息进行存证，按时间顺序逐一记录上链存证。包括但不限于内容编辑、格式转换、重新排版等操作。

### 2、电子文书可信协同

与大数据中心存证中心进行对接，将送达类电子文书进行存证

### 3、电子文书可信流转

记录电子文书在检察院内部流转的全过程，包括流转过程中的操作信息，如文书接收时间、操作人员身份、操作类型等。通过自动记录并上链保存这些信息，确保文书流转的透明性和可追溯性，为文书的管理和审计提供有力支持。

#### （1）电子文书内部流转过程信息存证

对电子文书在检察院内部的各个流程节点进行全面记录和追溯，自动记录电子文书在各个流程节点的操作信息，包括文书接收时间、操作人员身份、操作类型（如审批、修改、传递）、操作时间等。

### 4、电子文书核验及溯源助手

为电子文书全生命周期提供详细记录和跟踪，完整记录文书的生命周期各个环节和具体操作，同时提供流转轨迹、一致性、关联性、完整性证明。这不仅可以提升文书管理的透明度和准确性，还可以帮助工作人员全面掌握每个电子文书的历史和状态，从而提高工作效率和决策质量。

#### （1）电子文书全生命周期溯源证明智能合约

对每个电子文书从生成到归档的全过程进行详细记录和跟踪，对文书在不同阶段的处理、流转、处理、归档等操作进行全面汇总，并在用户界面以综合仪表盘和交互式图表形式展示文书的生命周期各个环节和具体操作，帮助工作人员全面掌握每个电子文书的历史和状态，提升文书管理的透明度和准确性。

#### （2）电子文书一致性核验智能合约

在文书的全生命周期各个环节，对电子文书进行一致性的核验。

基于电子文书副本数字指纹，系统基于存证数据自动生成电子文书副本与原件血缘关系证明。

## （四）、电子档案全流程可信应用

整个应用平台共建设3个子系统，其中包含数字档案可信收集系统、数字档案可信检测系统及数字档案可信利用系统。

### 1、电子档案室可信收集系统

为解决电子档案形成和收集环节，如何保证形成者、形成活动、形成时间能够可信追溯的痛点，数字档案可信收集系统主要包含针对文书类、照片类、录音类、录像类等八类电子文件提供文件哈希存证、文件元数据存证及文件关键操作行为存证服务及管理等功能。

#### （1）文件哈希存证

通过哈希算法对文件进行散列处理，将结果作为文件的唯一标识进行上链存证，便于以后进行验证和追溯。

#### （2）文件可信管理

针对文件哈希存证、元数据存证、关键操作行为存证进行统一管理，便于快速检索至任意一条存证记录。

### 2、电子档案可信检测系统

为解决整理和归档环节，如何有效进行真实性、完整性、可用性、安全性检测的痛点，数字档案可信检测系统通过区块链智能合约，可以实现真实性、完整性检测，准确快速检查档案真实性、是否被篡改、是否完整，有效保证档案工作符合程序规范，要素合规要求。具体包含文件真实审查合约、来源真实审查合约、文件真实审查报告、来源真实审查报告及可信检测管理功能。

#### （1）文件真实性核验合约

可以判断该电子文件是否存证，有效防止文件归档错误，提升归档准确性；

#### （2）来源真实审查合约

可以通过链上合约获取该文件的所有操作行为，有效溯源电子文件的形成者、形成活动及形成时间。

通过审查合约的执行，可生成来源真实性审查报告，详细说明文件来源检查的结果和过程。

#### （3）可信检测管理

针对文件真实性、完整性等合约运行进行统一管理，便于快速检索至任意一条合约运行记录。

### 3、电子档案可信利用系统

为确保电子档案充分利用同时兼顾好电子档案安全的问题，数字档案可信利用系统运用档案副本防伪双层水印技术、文件碎密安全存储等技实现档案利用可信安全管理，对档案借阅流转全过程进行追踪、留痕。可以满足档案借阅、跨部门流转、律师网上阅卷等各类场景下，档案副本的追踪、溯源、核验等核心需求。具体包含防伪双层水印、副本上链存证、碎密可信存储、超期删除合约等功能。

#### （1） 防伪双层水印

应用双层水印技术为电子文档添加独特的标识，以防止文件被篡改或伪造。

#### （2）副本上链存证

将电子档案副本的元信息上链，形成不能篡改的存证记录，从而实现档案的追踪与溯源。

#### （3）碎片化加密存储

采用碎片化加密存储技术，将电子档案切分为多个碎片进行加密存储，有效防止未授权访问和数据泄露。

#### （4）超期删除合约

通过智能合约设置借阅档案副本的生命周期，超期后自动删除，防止借阅档案副本长期露在风险之中。

#### （5） 文件追踪管理

系统能够对档案的借阅、流转、阅读等操作进行实时监控和记录，确保档案利用的合规性。

# 电子政务云资源需求

根据批复内容和实际情况，描述拟申请的云资源量。

参考如下：

根据项目前期资源现状，本次建设根据估算拟向电子政务云申请40台服务器资源CPU184核 、内存432G、存储14.7TB，其中虚拟机40台，物理机0台。

# 其他工作要求

## 售后服务要求

项目验收通过后，提供1年的免费质量保证服务，承诺为系统提供终身技术支持服务。服务对象为全市检察机关与项目相关的单位、部门和用户。为确保系统的正常运行，及时解决发生的各类问题，需结合项目实际，制定有效的运维保障方案和安全应急措施。并按约定，提供以下方式服务：

1.重大活动伴随服务

用户若有跟系统相关的重大活动，项目组需提供活动所需专人进行事前调试和始终伴随服务，以确保系统的正常运行，最终实现用户活动的顺利完成。

2.巡检服务

每月进行一次巡检服务，由专业的技术支持人员上门通过专业的方式对系统运行状况进行全面检查测试，及时发现和排除隐患，确保数据备份的可靠性，保证系统可持续正常运行。并向市院信息中心提交巡检报告。

3.远程支持服务

热线电话服务

提供项目组技术人员的7\*24小时服务热线；针对检察院提出的问题，通过电话解答咨询、指导应用和故障排除。对于无法解决的问题，及时受理登记，安排运维任务。

电子邮件服务

提供项目组负责人邮箱地址，若遇到疑难的问题，用户可将问题通过E-mail的方式发给项目组相关负责人，项目组每天至少接收一次邮件，并在2个工作日内及时予以回复。

其它

将各项运维服务纳入上海检察机关统一运维平台，实现问题统一受理、解决、反馈和汇总，所有运维工作均应在运维管理平台中全程详细记录，并不断丰富应用系统常见问题知识库。

## 应急响应要求

供应商对系统故障应能够实时响应，若系统发生故障，接到通知后30分钟之内响应，专业工程师2小时内到达现场。特殊故障与客户沟通协商后，按照协商的方式制定解决方案并进行处理。

具体故障级别及对应的应急响应要求如下：

一级故障：在1小时内确诊，总故障解决时间不超过4小时。

二级故障：在2小时内确诊，并在4小时内由专家到达现场确诊并解决，总故障解决时间不超过8小时；

三、四级故障：在4小时内确诊故障，总故障解决时间不超过16小时。

## 培训要求

对系统使用单位提供业务操作培训，应提供详细培训方案。

(1)在12个月的质量保证期内，提供2次与项目相关的必要培训。

(2)供应商需要开展分层次的人员培训工作，每次培训后应对参加培训人员进行测试，评估培训成果。培训应具有培训教材、培训环境和高水平的培训讲师。

(3)供应商应提供一般用户的基础操作培训和部门信息管理员的日常应用维护的培训，确保用户对象能够掌握对应的操作技能。

## 进度要求

供应商应根据建设内容，分阶段制定合理的时间进度，并且应根据采购人要求进行调整和细化。

2025年10月底前，完成项目整体内容的建设。

## 企业综合能力要求

供应商具有ISO9001质量管理体系认证证书、ISO20000信息技术服务管理体系认证证书、拥有ISO27001信息安全管理体系认证证书的优先考虑。

## 项目团队及驻场人员要求

1）供应商须具有稳定的在职技术保障力量，能够提供及时的技术支援或服务，应针对本项目提供不少于13人的项目服务团队（包括项目经理、产品负责人、技术负责人、研发等），供应商的相关服务人员需具备相应的服务能力，需提供相关证明。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量** | **人员要求** | **驻场要求** |
| 项目负责人 | 负责项目质量和进度控制 | 1人 | 信息系统项目管理师证书，具有与本项目类似的工作业绩 | 不做要求 |
| 产品经理 | 负责项目需求评估与产品设计 | 1人 |  | 不做要求 |
| 研发经理 | 负责项目具体开发与实施的管理 | 1人 |  | 不做要求 |
| 技术工程师 | 负责项目具体开发与实施 | 10人 |  | 不做要求 |

2）供应商应针对本项目提供不少于3人的质保期间支撑团队（其中技术经理1人，产品经理1人，技术工程师不少于1人）；供应商的相关服务人员需具备相应的服务能力，需提供相关证明（最近一个季度依法缴纳社保费的证明）。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **角色** | **主要职责** | **人员数量** | **人员要求** | **驻场要求** |
| 项目经理 | 负责项目质量和进度控制 | 1人 | 信息系统项目管理师证书 | 不做要求 |
| 产品经理 | 负责项目需求评估与产品设计 | 1人 |  | 不做要求 |
| 技术工程师 | 负责项目运行维护 | 1人 |  | 不做要求 |

## 等级保护要求

本项目等级保护要求： 三级等保。

## 商业密码应用需求

本项目完成后需通过第三方密码应用测评。

# 附录

1、《政务网络安全监测平台总体技术要求》



2、《上海市电子政务外网建设和运行管理指南（试行）》



3、其他标准