**技术需求书**

# 项目概述

为了适应当前的安全形势，进一步提高机关网安全保密能力，我院将在安全可靠环境下对机关网密码安全平台系统进行升级改造。新建系统必须能够在安全可靠环境下运行，并且与当前密码安全平台系统保持相同的体系结构、应用方法和管理模式，能够有效接入机关网，满足机关网稳定运行、运维管理和使用习惯等各方面的要求。

密码安全平台为业务应用提供密码服务和信任服务保障，由密码管理系统、数字证书认证系统、信任服务设施、电子文件集中加密存储系统组成。

机关网中配备有密码设备，密码设备需由密码管理系统进行统一密钥管理、在线集中管控，以确保密码设备安全使用。

建设数字证书认证系统，采用数字证书作为实体身份验证凭证，保障机关网中用户、应用、设备等身份可信，为用户、应用、设备等颁发证书，并提供证书全生命周期管理、证书查询验证服务。

建设机关网信任服务设施，实现机关网中用户、组织机构、应用、网络等资源统一管理，实现应用访问、网络接入统一授权，实现用户统一认证、应用单点登录，实现设备时间统一、提供时间戳服务，实现电子公文签章、验章，确保公文完整性、真实性及抗抵赖性。

机关网中各类业务应用系统将产生大量电子文件，为确保电子文件安全，需建设电子文件集中加密存储系统，对电子文件进行集中加密存储。

# 建设内容

本项目建设密码管理系统、数字证书认证系统、信任服务设施和电子文件集中加密存储系统。本项目只采购软件系统，硬件设备在其他项目中统一采购。

1. **密码管理系统**

建设密码管理系统，对密钥进行全生命周期管理，对密码设备进行在线管理，提升机关网信息安全保障所需的密码管理支撑能力。

1. **数字证书认证系统**

建设数字证书认证系统，为机关网中的用户、应用、设备等各种实体签发公钥证书，作为实体在机关网中的唯一可信身份标识，并对公钥证书及其密钥进行全生命周期的管理，从而建立实体间信任的基础，使得机关网中基于证书的身份认证机制得以有效实现。

1. **信任服务设施**

建设信任服务设施，对机关网中的资源信息进行统一管理，对应用访问和网络接入进行统一授权，对用户进行统一身份认证，提供统一时间同步和时间戳服务，提供电子公文签章验章服务，实现机关网网络环境可信、可管。

1. **电子文件集中加密存储系统**

建设电子文件集中加密存储系统，对存储在后台的文件进行加密，实现可控的数据安全共享，确保只有用户本人或其授权用户才能访问数据，为用户提供安全可靠的网络集中存储环境。

表1招标货物清单

|  |  |  |  |
| --- | --- | --- | --- |
| **产品名称** | **形态** | **数量** | **单位** |
| 密码管理系统 | 软件 | 1 | 套 |
| 数字证书认证系统 | 软件 | 1 | 套 |
| 信任服务设施 | 软件 | 1 | 套 |
| 电子文件集中加密存储系统 | 软件 | 1 | 套 |

# 产品技术要求

## 密码管理系统

密码管理系统为机关网中配用的密码设备提供密钥管理及密码设备在线管理服务。密码管理系统对密钥进行全生命周期管理，包括对称密钥、非对称密钥的生成、存储、分发、更换、销毁等；密码管理系统对密码设备进行在线管理，包括对机关网中密码设备基本信息的录入管理、在线监管密码设备的运行状态、对密码设备进行远程管控等。

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 密钥管理   （1）支持密钥产生  （2）支持密钥分发  （3）支持密钥管控   1. 密码设备管理   （1）支持密码设备信息管理  （2）支持密码设备状态监管  （3）支持密码设备远程管控 |
| 性能指标 | 1. 管理的密码设备证书：>1万张 2. 存储的对称密钥：>100万条 3. 管理的密码设备：>1000台 4. 支持的密码设备并发连接数：>100个 5. 安全审计的信息记录：>1万条 |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

## 数字证书认证系统

数字证书认证系统由证书签发管理子系统、证书密钥管理子系统、证书注册子系统、证书发布子系统组成。

证书签发管理子系统实现机构证书、管理证书、管理员证书、应用证书的签发、撤销、更新、延期、冻结、解冻等业务功能，并进行系统的维护管理和安全管理。

证书密钥管理子系统实现应用证书密钥的生成、导入、存储、分发、撤销、更新、恢复等业务功能，并进行系统的维护管理和安全管理。

证书注册子系统实现证书的申请、审核、制作、发放等业务功能，并进行系统的维护管理和安全管理。

证书发布子系统提供LDAP服务和证书状态查询服务，并进行系统的维护管理和安全管理。

### 证书签发管理子系统

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 证书签发   （1）接收证书注册系统提交的证书申请，根据申请向证书密钥管理系统在线申请密钥，并根据申请信息签发证书；  （2）支持签发下级证书管理中心机构证书；  （3）支持签发应用证书，包括个人应用证书、设备应用证书等。   1. 证书撤销。支持撤销证书，并通知证书密钥管理系统撤销对应的证书密钥。 2. 证书更新。支持机构证书更新，支持应用证书更新。 3. 证书延期。支持证书延期，更新证书的有效期。 4. CRL签发。支持根据CRL签发策略定期签发CRL。 5. 证书和CRL发布。根据证书签发、撤销、更新、冻结及解冻情况向证书发布系统发布证书和证书状态信息。 |
| 性能指标 | 1. 证书签发能力：≥2000个双证书/小时 2. 证书管理能力：≥10万张证书 |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

### 证书密钥管理子系统

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 密钥生成，支持生成非对称密钥。 2. 密钥导入，支持非对称密钥的离线或在线获取。 3. 密钥存储，密钥在其整个生命周期中都以密文形式存储在密钥数据库中，并进行完整性保护。 4. 密钥分发，采用证书业务处理协议将密钥分发给证书签发管理系统，密钥分发过程中密钥不能以明文形式出现。 5. 密钥撤销，根据证书签发管理系统的请求撤销证书当前使用的密钥。 6. 密钥更新，根据证书签发管理系统的请求分配新的密钥对，同时撤销旧的密钥。 7. 密钥恢复，支持非对称密钥的在线恢复和密钥离线恢复。 |
| 性能指标 | 1. 密钥管理能力： ≥10万对ECC密钥对 2. 密钥分发能力：≥2000对/小时 |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

### 证书注册子系统

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 业务请求受理。包括用户证书申请受理、用户证书更新受理、用户证书暂停受理和用户证书暂停恢复受理； 2. 业务请求审核。提供即人工审核与自动审核功能； 3. 证书下载制证。将证书签发系统签发的用户数字证书下载到本地，并将数字证书安全写入证书介质，完成制证操作； 4. 系统人员管理。提供对注册审核系统的管理员、操作员信息进行查询、修改、增加、注销、设置权限等； 5. 日志审计。提供对本系统管理人员、操作人员的操作日志及系统日志的查询与统计。 |
| 性能指标 | 1. 证书注册能力：支持≥10万张证书申请 |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

### 证书发布子系统

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 提供本地查询与下载服务，应用系统可以调用目录服务提供的接口对数据进行查询及下载； 2. 提供目录服务信息配置、账户管理配置、对象类及属性配置管理等多种系统配置管理功能； 3. 业务处理。提供证书状态查询业务的集中处理功能，将应用系统提交的证书状态查询请求进行统一处理； 4. 证书状态查询。系统收到证书状态查询业务请求后可对证书的有效期、信任链以及是否被撤销等方面进行检查，最后将结果返回给应用系统； 5. 系统配置。提供目录服务地址、端口、连接用户名和口令等相关信息进行配置管理； 6. 提供管理员操作日志以及系统服务运行日志的管理功能。 |
| 性能指标 | 1．证书/CRL查询下载响应时间：≤1s  2. 证书/CRL查询、下载并发服务能力:支持≥40并发  3. 证书状态查询服务响应时间:≤1s   1. 证书状态查询服务并发服务能力:支持≥40并发 |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

## 信任服务设施

基于数字证书认证系统建设信任服务设施，包括资源信息管理服务系统、授权管理服务系统、身份认证应用服务系统、可信时间服务系统、电子印章系统，为构建用户、应用、网络等实体可信、行为可信、资源共享安全可信的网络信任体系，提供信任服务支撑。

### 资源信息管理服务系统

资源信息管理服务系统主要对机关网中的组织架构、用户、应用、网络资源信息进行统一管理，为信任服务设施其他系统和业务应用提供资源信息共享服务，支撑机关网资源有序管理、高效利用、安全共享。

系统管理的资源信息包括用户资源信息、应用资源信息、有关网络资源信息和组织架构资源信息4类；系统由资源信息管理、资源信息注册同步服务、资源信息目录服务和资源信息库等子系统组成。

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 按需制定注册策略，定义拟接入的资源信息； 2. 按需制定同步策略，定义资源信息同步内容（资源信息和属性信息）和同步对象（业务应用、资源信息管理服务系统和其他信任服务系统）； 3. 按需制定资源信息目录发布策略，定义资源信息发布内容和发布范围； 4. 用户、应用、有关网络和组织架构等资源信息可由管理人员通过手工方式直接录入，也可以由业务应用通过资源信息服务实现在线注册，系统依照“资源信息注册策略”接收资源信息并由管理人员审核确认； 5. 提供资源信息的更新维护功能； 6. 根据资源信息同步策略，将资源信息共享给本地业务应用、信任服务设施相关系统，以及其他部门资源信息管理服务系统使用； 7. 向业务应用提供资源信息在线查询下载服务； 8. 对系统自身运行状态、资源信息同步和共享情况等进行实时监控管理，出现异常及时向管理人员报警； 9. 提供资源信息统计和按需报送功能。 |
| 性能指标 | 1. 系统可管理资源信息数量达100万条目； 2. 并发用户数不低于200个； 3. 查询平均响应时间小于1秒。 |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

### 授权管理服务系统

授权管理服务系统是对用户的网络接入与应用资源访问进行授权的管理系统，也是基于权限信息为网络通行和业务应用的访问提供在线鉴权的服务系统，为本部门业务受控访问、跨地区跨部门业务协同和资源共享提供支撑。

授权管理服务系统支持基于身份、属性或角色的授权策略，支持直接授权和委托授权工作模式，对用户的网络接入和应用访问进行权限管理，为网关和业务应用提供在线鉴权服务。授权管理服务系统由授权管理子系统、鉴权服务子系统、本地权限信息库三部分组成。

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 对用户的网络接入权限进行管理与配置，并通过资源信息管理服务系统将网络接入权限信息同步至网关，支撑网关进行本地鉴权； 2. 对用户访问应用的权限进行管理和配置，并通过资源信息管理服务系统将应用访问权限信息同步至对应网关，支撑网关进行本地鉴权； 3. 针对机关网用户跨部门访问业务应用的权限需要，提供直接授权和委托授权两种工作模式； 4. 支持基于身份、属性、角色的授权； 5. 基于本地权限信息库中存储的授权结果数据，在线为网关或业务应用提供鉴权服务； 6. 对系统自身运行状态进行监管，出现异常时及时报警； 7. 提供本级授权管理信息统计和按需报送功能。 |
| 性能指标 | 1. 资源条目最大支持：300万 2. 并发鉴权数：不低于200 3. 鉴权平均响应时间：小于0.5S |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

### 身份认证应用服务系统

身份认证应用服务系统通过为用户、应用、设备等实体提供基于数字证书的身份识别和访问控制服务，实现机关网身份的互信互认，网络访问和信息共享的安全可控。

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 基于数字证书认证系统的证书验证服务查询用户、应用和设备证书合法、有效性，使用密码运算验证实体是否为数字证书的合法持有者，保障实体身份的真实性和有效性，为单点登录、权限鉴别、访问控制、安全审计提供支撑。 2. 为通过身份认证的实体颁发身份票据，并以API接口形式为业务应用提供身份票据验证服务，为业务应用系统的用户认证和单点登录提供支撑。 3. 用户通过身份认证后获得身份票据，访问业务应用时只需要进行身份票据验证，不必重复证书验证，实现用户一次登录即可访问多个业务应用。 |
| 性能指标 | 1. 单次身份认证时间：不超过1秒； 2. 单次票据验证时间：不超过0.5秒； 3. 并发连接数：不低于1000。 |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

### 可信时间服务系统

可信时间服务系统为信任服务设施、网络和业务应用提供标准时间同步、时间戳服务，为机关网业务开展和行为追溯提供可信时间服务支撑。

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 普通时间同步服务：面向网络设备、安全设备、应用服务器及终端，提供基于通用时间同步协议（NTP）的时间校准及同步服务； 2. 安全时间同步服务：面向特殊应用需求，提供基于安全时间同步协议（NTP-S）的时间校准及同步服务。信任服务设施内部采用安全时间同步协议； 3. 时间戳申请及颁发：系统接收时间戳加盖申请并验证请求消息合法性，验证通过后以标准格式生成时间戳数据发给申请者，完成时间戳颁发； 4. 提供时间戳验证功能；为应用系统提供时间戳验证组件，应用系统通过调用组件的方式验证时间戳有效性； 5. 提供时间戳的存储、归档、备份、检索等管理功能； 6. 监管可信时间服务系统的运行状态、时间同步状态及时间戳服务子系统的时间戳服务情况统计等内容，出现异常及时报警。 |
| 性能要求 | 1. 支持3000个终端； 2. 支持50个并发； 3. 时间同步服务能力(NTP)：500次/S 4. 安全时间同步服务能力（NTP-S）:80次/S 5. 单次同步平均响应时间小于1S 6. 时间戳签发：70次/s 7. 时间戳验证：120次/s |
| 兼容性要求 | 1. 系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台 2. 系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等 3. 系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等 |

### 电子印章系统

电子印章系统为机关网提供电子印章的签章、验章服务，有效保障电子文件的真实性、完整性和签章行为的不可否认性，是实现电子公文流转、部门协同办公的重要信任支撑。电子印章系统提供电子印章全生命周期管理服务，包括电子印章注册申请、电子印章签发、电子印章撤销、印章状态发布等。

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 基本要求 | 1.应选用入围党政机关电子公文系统安全可靠产品目录的电子印章系统。 |
| 功能指标 | 1.具备电子印章信息注册及信息变更的申请和审批功能。  2.具备电子印章载体制作功能，电子印章数据应能存储在电子印章载体和集中存储在系统中。  3.具备电子印章签发服务和管理功能，根据相关申请及审核结果制作电子印章，采用商用密码算法制作电子印章。  4.具备电子印章在线查询、下载功能。  5.具备电子印章状态数据管理功能，提供电子印章在线验证功能。  6.具备电子印章签章功能。提供版式文件的电子印章签章功能，使用电子印章签章时需验证电子印章的合规性和有效性。  7.具备电子签章验证功能。提供电子签章验证功能，使用电子签章验证时需验证电子签章数据的合规性和有效性。  8.能识别合法的电子印章载体并从中获取必要信息，能合法调用载体中密码服务功能。  9.电子印章系统应采用签名/验签技术确保系统通信数据的真实性。 |
| 性能指标 | 1.电子印章系统服务端平均响应时间≤5秒  2.电子印章系统服务端并发数≥30次/秒  3.对大小为300KB的电子公文进行签章时，签章时间应≤5秒  4.对大小为300KB的电子公文进行验章时，验章时间应≤5秒 |
| 兼容性要求 | 1.系统应支持安全可靠的基础计算环境，包括龙芯、飞腾等国产CPU平台  2.系统应兼容安全可靠的操作系统，包含中标麒麟、银河麒麟等  3.系统应兼容安全可靠的数据库系统，包含南大通用、达梦、人大金仓等  4.系统应兼容数科、福昕等版式软件 |

## 电子文件集中加密存储系统

电子文件集中加密存储系统对机关网用户集中存放的数据进行实时加密，并以密文形式保存在存储介质中，确保数据存储安全；对存储在后台的文件采用多层加密模式，实现可控的数据安全共享，确保只有用户本人或其授权用户才能访问数据，任何其他用户包括管理员在内均不具备读取权限；系统应采用细粒度访问控制策略，保证共享用户只具备共享者授予其的访问权限，为用户提供安全可靠的网络集中存储环境。系统应对用户应用透明，具备良好的扩展性和兼用性，能够处理各种格式的文件。

|  |  |
| --- | --- |
| **指标项** | **技术指标要求** |
| 功能指标 | 1. 集中安全存储   用户数据集中存放在安全存储服务器中，系统为每个用户划分两个存储区域用于数据的存储和共享，并以一文一密、三层加密的方式对存储在服务器上的数据进行加密处理，确保数据的离线安全。基于密钥的访问控制技术，确保用户数据的在线安全，个人数据只能自己访问，任何包括管理员在内的其他用户都无法访问。   1. 加密共享   系统针对用户进行文件共享，通过采用加密处理机制来实现用户数据的加密共享，支持目录、文件级的加密共享以及细粒度的授权设置。用户在共享数据时，不需要对文件进行解密传输，且任何非授权用户都无法访问他人共享数据。   1. 网络访问控制   采用基于白名单的网络访问控制，对登录系统的用户终端进行网络管控，防止数据通过网络途径外泄。  若用户需要访问办公必须的可信网络及服务器，可将其网络地址添加至白名单中，系统便可允许用户访问可信网络。   1. 安全审计   系统可记录用户以及管理员操作记录，确保系统用户以及管理员的行为可追踪、可审计。 |
| 性能指标 | 1. 系统身份认证响应时间小于8秒； 2. 1TB数据恢复时间在4小时内完成； 3. 存储1G文件时间不大于5分钟； 4. 打开集中管控环境内文件时间不大于5秒 5. 常规情况下24x365稳定运行，稳定运行率达到99.9%。 |

# 实施要求

本项目要求：合同签订后12个月内完成密码管理系统、数字证书认证系统、信任服务设施、电子文件集中加密存储系统的建设工作。

投标人应制定合理的工程实施方案，按照招标人要求，完成对各系统的初验、试运行、终验等工作，确保各系统顺利正式运行。

投标人需进行产品适配工作，所提供密码管理系统、数字证书认证系统、信任服务设施、电子文件集中加密存储系统需要适配安全可靠的计算环境，包括服务器端和客户端，服务器端适配内容包括安装主流国产CPU的服务器、国产服务器操作系统、国产数据库、国产中间件；客户端适配内容包括安装主流国产CPU的终端，国产桌面操作系统，IE、安卓、firefox等主流浏览器等。

投标人需进行业务应用系统对接工作，信任服务设施需与现有业务应用系统进行对接，实现资源信息统一管理，实现操作系统、业务应用系统的统一单点登录，实现电子印章的签章、验章，实现时间可靠统一。

投标人须成立合理的组织机构，安装调试需要有专业的实施人员进行现场设备及软件系统的实施工作。投标人须提供项目建设详细人员计划，包括人员姓名、简历、资质和在本项目中的职责分工。

投标人应配备经验丰富的项目经理承担本项目工作。投标人应明确项目经理在本项目中的岗位职责、任职资格及管理权限，以确保工程顺利实施。

# 培训要求

投标人应根据招标货物内容提供相应培训，保证用户培训后能够独立使用系统，并确保系统稳定、合理运行。

投标人应明确课程内容、课程教材、培训时间、课时等内容。培训方式包括集中培训、现场培训。

根据本项目产品的实际情况，提供免费培训服务：

1、提供现场培训——确保一线人员能简单使用部署的系统。

2、提供集中培训——对用户一线人员进行深层次的培训，使用户能对系统出现的简单故障进行排除。

# 技术支持和售后服务要求

项目终验后，投标人应提供至少3年免费的本项目实施范围内系统的质保服务。质保期内，提供7X24小时免费电话技术支持，在接到保修电话后，30分钟内响应，1个小时到达现场，8个小时内解决问题。

质保期内免费服务内容应包括：远程技术服务、现场技术服务、软件系统升级等，提供7\*24小时服务，并提供书面承诺函。